Міжнародна науково-практична конференція

“Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку”

14 березня 2024 року, м. Харків

Міжнародна науково-практична конференція “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” / Збірник тез доповідей (м. Харків, 14 березня 2024 р.). – Харків. – 2024. – 400 с.

Організатори конференції: Національна академія Національної гвардії України (м. Харків); Харківський національний університет радіоелектроніки (м. Харків).

Адреса організаційного комітету: 61001, м. Харків, майдан Захисників України, 3, Національна академія Національної гвардії України, науково-організаційний відділ.
Телефон: +38097-69-81-250. **Електронна адреса**: nanguki@ukr.net.
Тези доповідей опубліковано в авторській редакції, мовою оригіналу: **http://kinf.nangu.edu.ua**

Ministry of Internal Affairs of Ukraine
National Academy of the National Guard of Ukraine

Ministry of Education and Science of Ukraine
Kharkiv National University of Radio electronics

International scientific and practical conference

“Application of information technologies in the preparation and operation of law enforcement forces”

March 14, 2024

Kharkiv

International scientific and practical conference "Application of information technologies in the preparation and operation of law enforcement forces" / Collection of theses of reports (Kharkiv, March 14, 2024). – Kharkiv. – 2024. – 400 p.

Conference organizers: National Academy of the National Guard of Ukraine (Kharkiv), Kharkiv National University of Radio Electronics (Kharkiv).

Organizing committee address: 61001, Kharkiv, Maidan Defenders of Ukraine, 3, National Academy of the National Guard of Ukraine, scientific and organizational department.
Phone: +38097-69-81-250 (Iokhov O. Yu.). **Email:** nanguki@ukr.net.
Theses of reports are published in the author's edition, in the original language: **http://kinf.nangu.edu.ua**

УДК 004.49:007.51

Адаменко А.А., Порохончук О.М., Попов М.О.

АНАЛІЗ ТА ПРОГНОЗУВАННЯ ТЕНДЕНЦІЙ РОЗВИТКУ КІБЕРОЗБРОЄННЯ

Розвиток інформаційних та кібертехнологій, а також зростаюча глобальна інформатизація призвели до того, що інформаційна та кіберсфери стали сферами, в яких та через які здійснюються різноманітні деструктивні впливи на усі сфери діяльності суспільства. Кіберпростір доповнив існуючі: сухопутний, морський, повітряний, космічний простір та став новою і першою штучно утвореною сферою конфліктів і можливих бойових дій, що спонукало введення та стрімкий розвиток нового виду озброєння – кіберозброєння [1].

Підтвердженням зростаючої ролі кіберозброєння стали численні факти його застосування російською федерацією, як в початковій, так і в активній фазі військової агресії проти України [2]. Висока ефективність та всеохоплююча проникаюча здатність кіберозброєння обґрунтовують актуальність вирішення проблеми щодо протидії його застосуванню противником, його ефективного застосування силовими структурами України в інтересах захисту національної безпеки України, з одного боку, та недостатності відповідного кіберозброєння та методології його застосування в силових структурах України, з іншого.

Ґрунтуючись на аналізі доступних наукових видань [3], присвячених проблематиці кібербезпеки, можна виділити основні тенденції розвитку перспективного кіберозброєння та способів його застосування.

1) Штучний інтелект, машинне навчання, роботизовані системи, квантові обчислення. Використання штучного інтелекту та машинного навчання може підвищити ефективність атак та робити їх більш складними для виявлення. Атаки можуть використовувати алгоритми машинного навчання (нейронних мереж тощо) для адаптації до заходів забезпечення безпеки. Використання штучного інтелекту для аналізу великих обсягів даних і виявлення кіберзагроз може значно покращити здатність виявлення і реагування на кібератаки. Успіхи штучного інтелекту активно втілюються в роботизовані системи як бойового, так і забезпечуючого характеру, які в свою чергу можуть розглядатися як потенційні об’єкти кібервпливів противника. Розвиток квантових обчислень може потенційно створити нові криптографічні методи та засоби для якісної захисту інформації, а також нові можливості для кібернетичних атак.

2) Кіберозброєння для ураження кіберфізичних систем. Зростає кількість підключених до комп’ютерних мереж об'єктів, від медичних пристроїв та автомобілів, до атомних електростанцій та супутникових систем. Зокрема, об’єктами кібервпливу стають бойові системи противника (озброєння та військова техніка, системи розвідки та навігації, системи управління зброєю та військами тощо), особливу вразливість та небезпеку складають бойові системи, що будуються за мережецентричними принципами чи є роботизованими. Кіберозброєння може бути використане для атак на такі системи, що може призвести до значних фізичних наслідків та людських втрат.

3) Гібридні (комбіновані) засоби кібердій. Сумісне використання радіоелектронних, апаратних, програмних та інших засобів різного базування (наземного, повітряного, морського чи космічного) та призначення (зокрема, безпілотних), для проведення кібератак на інформаційно-кібернетичні об’єкти противника.

4) Співпраця з іншими видами озброєння та військами. Кіберозброєння може використовуватися в гібридних спецопераціях разом з іншими видами озброєння (фізичного чи нефізичного ураження) та військами на різних стадіях їх застосування з метою ураження (виведення з ладу, нейтралізації тощо) фізичних об’єктів чи особового складу

противника.

5) Кіберпідрозділи, навчання і підготовка кадрів. Забезпечення наявності висококваліфікованих кадрів у сфері розробки (виробництва), супроводження та застосування кіберозброєння. Створення спеціальних "кіберпідрозділів" в силових структурах для здійснення кібероперацій та кіберзахисту. Підвищення загальної обізнаності та освіти особового складу в області кібербезпеки.

6) Серійне виробництво спеціалізованих інструментів для кібероперацій. Серійне створення засобів, спеціально призначених для багаторазового виконання військових кібероперацій (кібератак), їх тестування та вдосконалення на віртуальних та реальних середовищах.

7) Розробка планів і тактик кібероперацій. Розробка планів та тактик для використання кіберозброєння в рамках військових операцій.

8) Моніторинг та прогнозування кібервразливостей, створення нових засобів та методів кібердій. Розробка засобів та середовищ для моніторингу та прогнозування кіберзагроз, що можуть виникнути у власних кіберсистемах, та пошук вразливості кіберсистем противника. Відповідно до цього здійснюється розробка нових засобів та методів проведення кібердій відповідного характеру (кіберрозвідка, кібервплив чи кіберзахист).

9) Прогностичне проєктування кібервразливостей противника. Розробка та реалізація засобів, методів, організаційних та технічних заходів щодо завчасного створення передумов для здійснення кібератак на кіберсистеми противника в майбутньому.

10) Зростання ролі соціальної інженерії в кіберпросторі. Розвиток арсеналу соціальної інженерії як ефективного способу маніпулювання людьми – найбільш вразливою частиною будь-якої кіберсистеми, з метою отримання конфіденційної інформації, зокрема, необхідної для проведення майбутніх кібератак. Збільшення кількості носіїв (сайтів, програм, соціальних мереж тощо) елементів арсеналу соціальної інженерії в кіберпросторі.

11) Кіберозброєння високої точності (атаки APT - Advanced Persistent Threats). Використання високотехнологічних засобів, методів та ресурсів кібердій, направлених на досягнення конкретних цілей з визначенням конкретних об'єктів впливу в кібернетичних системах та їх елементах.

12) Циклічність кібервпливів. Кібервпливи на певні кібернетичні системи противника можуть мати циклічний характер з метою унеможливити на тривалий термін їх штатне функціонування. Для цього можуть застосовуватися, у тому числі, гібридні засоби кібервпливів у різних варіаціях їх застосування на різних стадіях підготовки та здійснення кібератак.

13) Управління кіберзнаннями. Управління кіберзнаннями – це здійснення збору, обробки, накопичення, проектування та обмін знаннями щодо об'єктів кібердій (зокрема, їх кібервразливості), засобів та методів кібердій, а також суб'єктів кібердій. Створення науково-технічної бази кіберзнань, науково-дослідних та виробничих установ щодо планування, дослідження, розробки та супроводження кіберозброєння.

Наведений перелік не є вичерпним, оскільки кіберпростір на сучасному етапі являє собою таку сферу людського суспільства, що динамічно розвивається, становиться більш складнішою та породжує нові виклики для її кібербезпеки та нові напрямки щодо розвитку відповідного кіберозброєння для її порушення чи захисту.

Разом з тим, слід визначити, що кіберозброєння не може в повному обсязі замінити звичайне "кінетичне" озброєння і має певні недоліки й ризики щодо його застосування [4].

На відміну від звичайного озброєння, наслідки застосування кіберозброєння (як засобу кібервпливу) цілком непрогнозовані.

Причиною тому є, по-перше, взаємопов'язаність об'єктів кіберпростору. Якщо застосувати кіберозброєння на один об'єкт кібервпливу, то має місце ризик, що результати його активної дії будуть розповсюджені за його межами (навіть, на інші об'єкти, організації, держави, що не беруть участі у конфлікті).

По-друге, об’єкт кібервпливу (його система кіберзахисту) з часом змінюється. Протягом терміну від моменту кіберрозвідки до моменту застосування відповідного кіберозброєння, об’єкт кібервпливу може застосувати певні міри щодо свого кіберзахисту. Крім того, повторне застосування одного й того ж зразка кіберозброєння щодо того ж самого об’єкту або об’єкту того ж самого типу не гарантує отримання саме того результату, на який очікується. Слід розуміти, що противник постійно адаптується до кібератак. Кіберозброєння для здійснення дій кіберрозвідки та кіберзахисту також не може гарантувати стійкий результат їх застосування.

Неможливість гарантувати результат застосування кіберозброєння стає наслідком третьої причини – великий ризик планування та проведення складних гібридних військових операціях, де проводяться одночасні дії на землі, в повітрі та в кіберпросторі, ефективність яких залежить від результатів дій кожної складової.

Тому, на нашу думку, в перспективі застосування кіберозброєння для Збройних Сил України та інших силових структур України має містити забезпечувальний характер для виконання покладених завдань, що будуть виконуватися, в основному, із використанням звичайного озброєння.

Список використаних джерел

1. Указ Президента України №447/2021 “Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України””.

2. Про основні засади забезпечення кібербезпеки України: Закон України (зі змінами) від 17.08.2022 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 19.02.2024).

3. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.

4. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. 09 Jul. 2016 - Press Release (2016) 100 Issued on 09 Jul. 2016. Last updated: 01 Jul. 2022 16:42. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en (дата звернення 19.02.2024).

УДК 004.01

Алфімова Л.Д., Душкін В.Д.

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ GOOGLE FORMS ДЛЯ ОРГАНІЗАЦІЇ САМОКОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧАМИ ОСВІТИ

Однією з основних вимог до випускників вищих навчальних закладів є сформованість здатності до опановування нових напрямів професійної діяльності, використовуючи здобуті знання та самостійного навчання. Формуванню цієї здатності сприяє самостійне опрацювання певних розділів або окремих питань. При самостійному опануванні учбового матеріалу у здобувачів освіти виникає необхідність проведення самооцінки отриманих знань. Тому створення засобів для здійснення формувального та прогностичного оцінювання є важливим елементом успішності засвоєння знань.

Інтерактивні тестові завдання – не ідеальний спосіб перевірки знань, але цей спосіб дозволяє здійснити швидку автоматичну перевірку правильності відповідей без участі викладача. До того ж він дозволяє проходити тестування у обраному здобувачем освіти темпі в асинхронному до проведення занять режимі, дозволяє у разі необхідності бага-

торазово проходити певні тести. Саме тому інтерактивні тестові завдання все більше використовуються в учбовому процесі закладів вищої освіти [1-5] .

Одним із найдоступніших видів програмного забезпечення, який широко використовується в світі для створення тестових завдань є Google Forms. Користуватися ним можна на безоплатній основі будь кому, хто має обліковий запис у Gmail . Google Forms використовують самостійно чи як складник платформи Google Classroom дає можливості створювати різні типи завдань,

За допомогою Google Forms створюють різні типи завдань, зокрема такі, що передбачають множинний вибір (Multiple choice): вибір однієї правильної відповіді з кількох; вибір декількох правильних відповідей (Checkboxes), які потрібно відзначити галочкою; вибір зі списку (Choose from a list): вибір однієї правильної відповіді з поданого переліку та інші типи.

Досвід викладання фундаментальних дисциплін довів ефективність використання тестових завдань створених за допомогою Google Forms в якості елемента он-лайн курсів створеної на платформі Google Classroom [6-9]. Частина тестів, яку розробили і використовують викладачі кафедри фундаментальних дисциплін, дають можливість їх анонімного багаторазового проходження. Ці тести призначені в першу чергу для перевірки розуміння базових питань та відпрацювання правильності виконання окремих кроків загальних алгоритмів розв'язання задач. Можливість анонімного проходження тесту позбавляє від психологічного тиску, пов'язаного із побоюванням зробити помилку у присутності викладача. Завдяки можливості читати коментарі до тестових завдань після проходження тесту а також можливості знайти правильні відповіді на наведені питання в учбовій літературі перед повторним проходженням тесту сприяють не лише успішному проходженню тестів, але й загальному покращенню знань з відповідного розділу курсу.

Незважаючи на анонімність проходження тестів окремим здобувачем освіти, Google Forms надає викладачам доступ до відомостей успішності проходження усіма здобувачами освіти у цілому. Ці автоматично створені данні містять список запитань, на які часто даються неправильні відповіді; діаграми, що показують відсоток правильних відповідей; надає інформацію про середню та медіанну успішності проходження тестів та кількість балів. Ця інформація дає змогу викладачам оцінити успішність засвоєння окремих питань модуля і дає змогу акцентувати увагу на ці питання здобувачам освіти під час підготовки до підсумкового контролю. Проведені за результатами вивчення дисциплін опитування здобувачів освіти показали, що більшість добре встигаючих курсантів оцінюють їх позитивно та вважають гарним тренуванням перед здачею модульного контролю.

Список використаних джерел

1. Гурняк І. Використання Google Forms і Microsoft Forms в процесі навчання. Фізико-математична освіта. 2018. Випуск 2(16). С. 40–45

2. Кухаренко В. М., Рибалко О. В., Сиротенко Н. Г. Дистанційне навчання: умови застосування. Дистанційний курс : навч. посіб. / за ред. Кухаренка В. М. Харків : НТУ «ХПІ». 2001. 282 с.

3. Мороховець Г. Ю. Тестування як форма контролю та діагностики знань здобувачів вищої освіти. Полтава, 2018. 15 с.

4. Богачков Ю. М., Букач А. В., Ухань П. С. Комплексне застосування Google Classroom для створення варіативних дистанційних курсів. Інформаційні технології і засоби навчання. 2020. Т. 76, № 2. С. 290–303. DOI: https://doi.org/10.33407/itlt.v76i2.3338 (дата звернення: 08.02.2024).

5. Алфімова Л.Д. Мельник В.М. Професійно орієнтоване навчання вищої математики при підготовці майбутніх офіцерів Національної академії Національної гвардії Укра-

їни./ Молодь і ринок , Дрогобицький державний педагогічний університет імені Івана Франка. - 9 (176). -2019. –с. 133-137

6. Душкін В.Д., Мельник В.М., Сидоренко І.І. Використання MS EXCEL при самостійному опрацюванні питань з лінійної алгебри / Тези міжнародної науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку " 14-15 березня 2018 року, м. Харків, с. 41

7. Алфімова Л. Д., Душкін В. Д., Мельник В. М. Використання вебсервісу Google Classroom при вивченні теми ―Лінійна алгебра / Тези міжнародної науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку " Міжнародна науково-практична конференція 15 березня 2021 року, м. Харків, с. 24-25

8. Душкін В. Д., Зуб О. В., Мельник В. М. Використання сервісу Google Forms для проведення опитування здобувачів освіти . алгебри / Тези міжнародної науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку " Міжнародна науково-практична конференція 15 березня 2022 року, м. Харків, с. 35-36

9. Алфімова Л. Д., Душкін В. Д. Застосування вебсервісу Google Classroom при організації формувального та прогностичного оцінювання / Тези міжнародної науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку " Міжнародна науково-практична конференція 15 березня 2023 року, м. Харків, с. 36-37

Арасланов М.Р., Малишев О.А., Пасічник В.О., Сингаївський А.О., Гончарова М.М.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ СИСТЕМ СЕЛЕКЦІЇ РУХОМИХ ЦІЛЕЙ В ОГЛЯДОВИХ АНАЛОГОВИХ РАДІОЛОКАЦІЙНИХ СТАНЦІЯХ ЧЕРЕЗ ВИКОРИСТАННЯ COTS-ТЕХНОЛОГІЙ

Під час російсько-української війни для ураження воєнних і цивільних об'єктів противник застосовує засоби повітряного нападу різних класів, одним з яких є ударні дрони-камікадзе типу "Shahed-136/131". Особливістю цих засобів є, з одного боку, складність виявлення, а з іншого (за умов їх наближення та візуального спостереження) – можливість вогневого знищення штатною стрілецькою зброєю підрозділів, як Збройних Сил України (ЗСУ), так і сил охорони правопорядку. Ефективність такого знищення підвищується за умов якомога раннього виявлення ударних дронів та своєчасного оповіщення про них усіх силових структур.

Серед різних способів виявлення дронів-камікадзе (візуального, акустичного, радіолокаційного, радіотехнічного) основним залишається спосіб із застосуванням засобів радіолокації. Це обумовлено можливістю виявлення цілей на великих дальностях, високою точністю визначення їхніх координат, незалежністю від погодних умов, тощо.

В той же час радіолокаційне спостереження за повітряною обстановкою має певні особливості, які знижують його ефективність, якщо не вжити спеціальних додаткових заходів. Одним з таких факторів є ускладнення (а зазвичай неможливість) виявлення повітряних об'єктів (ПО) на фоні відбитків зондувального сигналу радіолокаційних станцій (РЛС) від підстеляючої поверхні та місцевих предметів. Такі відбитки є фактично пасивними завадами (ПЗ) під час роботи РЛС.

Для боротьби з ПЗ в радіолокації застосовуються системи селекції рухомих цілей (СРЦ). Сутність їх роботи полягає у виявленні відмінностей сигналів, відбитих від рухомих та нерухомих об'єктів. Застосування таких систем в засобах радіолокації, зокрема, в оглядових РЛС, довело їх досить високу ефективність. Тому системи СРЦ вико-

ристовувались та продовжують використовуватись в РЛС різних поколінь: як в РЛС "старого" парку (на базі аналогової апаратури), так і в новітніх цифрових станціях.

В той же час відмінності елементних баз РЛС зазначених класів даються взнаки на методах захисту від ПЗ, які можливо реалізувати в цих станціях. Так в аналогових РЛС виправдане використання способу черезперіодного віднімання (ЧПВ) ехосигналів, а в новітніх РЛС – фільтрової обробки.

Останній спосіб є логічною складовою загальної цифрової обробки сигналів, і практично не може бути реалізований на ламповій елементній базі.

Пристрої ЧПВ історично використовувались в аналогових РЛС і входили до складу окремого когерентно-імпульсного тракту, який вмикався оператором лише в області дії ПЗ. При коректному настроюванні таких пристроїв (за умов використання приладів з невеликим часом напрацювання) подавлення ПЗ було досить ефективним. Але з огляду на природній процес погіршення характеристик електронно-вакуумних приладів якість роботи ЧПВ значно погіршувалась.

На сьогодні внаслідок вичерпання запасів необхідних комплектуючих на складах та припинення взагалі їх виробництва гостро стає питання щодо відновлення спроможності РЛС "старого" парку здійснювати захист від пасивних завад. З огляду на те, що таких РЛС на озброєнні підрозділів радіотехнічних військ (РТВ) Повітряних Сил та підрозділів протиповітряної оборони (ППО) Сухопутних військ ЗСУ ще значна кількість, зазначене питання залишається актуальним.

Можливим шляхом відновлення систем СРЦ в оглядових РЛС "старого парку" є переведення елементної бази цих систем з аналогової на сучасну цифрову. Це дозволить при працездатних інших системах РЛС відновити (і навіть покращити) процес виявлення ПО на фоні ПЗ.

Для здійснення такої неглибокої модернізації РЛС пропонується спеціалізований модуль, виконаний з використанням COTS-технологій (commercial-off-the-shelf – “готові до застосування модулі комерційного призначення”). Зазначені технології дозволяють використовувати стандартні модулі, що розроблені на сучасній елементній базі, для виготовлення нової апаратури та модернізації старої [1].

Такий підхід дозволить в стислі терміни з мінімальними витратами модернізувати РЛС “старого парку”, що покращить їх технічні та експлуатаційні параметри, розширить функціональні можливості, підвищить надійність роботи, зменшить витрати споживаної електроенергії. Крім того, така модернізація не вимагає спеціального обладнання або заводського устаткування, тобто може бути проведена силами військових ремонтних органів.

Отже, COTS-технології можуть бути використані і для модернізації систем СРЦ в оглядових аналогових РЛС, зокрема, метрового діапазону хвиль [2].

Для переведення пристрою ЧПВ на цифрову елементну базу запропонована структурна схема модернізованої системи СРЦ. Вона містить: набір буферних каскадів; два аналогово-цифрових перетворювача (АЦП), мікропроцесор, оперативний запам’ятовуючий пристрій (ОЗП) та цифро-аналоговий перетворювач (ЦАП). Буферні каскади узгоджують амплітудний діапазон відповідних каскадів РЛС з амплітудним діапазоном АЦП і ЦАП. АЦП забезпечують перетворення аналогових сигналів у цифровий вигляд. Процесор та ОЗП виконують власне функцію черезперіодного відніманя та, додатково, накопичення ехосигналів для підвищення відношення сигнал/шум на виході пристрою й придушення несинхронних імпульсних завад. ЦАП забезпечує перетворення обробленого ехосигнала в аналоговий вигляд.

Для забезпечення роботи пристрою на нього з РЛС надходять імпульси початку дистанції (імпульси запуску). Розмір зони, в межах якої необхідно здійснювати процедуру ЧПВ, встановлюється за допомогою спеціальних перемикачів та контролюється по цифровому індикатору. В пристрої додатково передбачений вхід для стробу від РЛС, який

визначає зону дії дипольних завад. На сигнальні входи пристрою подаються ехосигнали з когерентного та амплітудного каналів РЛС.

Після придушення пасивних завад оброблені та накопичені ехосигнали через ЦАП надходять до вихідного підсилювача і далі до штатної апаратури РЛС.

Мікропроцесор разом з ОЗП забезпечують реалізацію алгоритму ЧПВ за правилом

$$Ui = |U_{i0} - 2U_{i1} + U_{i2}|,$$

де U_{i0} – і-а дискрета поточного періоду зондування;

U_{i1} – і-а дискрета попереднього періоду зондування;

U_{i2} – і-а дискрета затриманого на два періоди зондування.

Обчислені значення надходять на пороговий пристрій і далі на накопичувач.

Апаратурно реалізувати пристрій СРЦ пропонується на уніфікованих платах Arduino Due. Стандартний модуль Arduino Due вибраний з міркувань, що він розроблений на базі мікроконтролеру Atmel SAM3X8E, який містить АЦП та ЦАП.

Для розробки програмного забезпечення такого модуля була використана апаратно-програмна платформа Arduino 1.7.8 з бібліотеками, які є на офіційному сайті Arduino.

Додатково для відображення рівня порогу відсічки шумів та інших параметрів пристрою пропонується використати індикатор LCD 5110 зі складу стандартних модулів Arduino.

Для апробації запропонованого варіанту модернізації системи СРЦ був виготовлений відповідний пристрій, який являє собою невеликий за розмірами блок, що замінює собою цілу шафу лампової апаратури штатної системи РЛС. Пристрій виконаний в малогабаритному корпусі (160мм х 140мм х 60 мм) і складається з двох однакових П-образних кришок стягнутих між собою чотирма гвинтами.

Принципова схема плати узгодження та схема розведення й монтажу елементів розроблена в системі проектування PCAD. Безпосередньо плата виготовлена друкарським способом. З апаратурою РЛС пристрій з'єднується за допомогою п'яти коаксіальних кабелів.

Вироблений пристрій СРЦ був апробований у військових умовах шляхом безпосереднього застосування в РЛС типу 5Н84А на протязі двох років. Апробація підтвердила не лише можливість виконання розробленим пристроєм очікуваних процедур ЧПВ, але й показала ефективність використання COTS-технологій для відновлення працездатності та модернізації вузлів та блоків РЛС "старого" парку, що знаходяться на озброєнні підрозділів РТВ Повітряних Сил та ППО Сухопутних військ ЗСУ.

Таким чином, запропонований спеціалізований модуль, виконаний з використанням COTS-технологій, дозволяє за рахунок неглибокої модернізації апаратури відновити працездатність систем СРЦ в оглядових аналогових РЛС метрового діапазону хвиль, зокрема, в станціях типу 5Н84А та П-18. Це дозволить більш ефективно виявляти засоби повітряного нападу різних класів, зокрема, дрони-камікадзе типу "Shahed-136/131", та оперативно надавати отриману інформацію як до підрозділів ЗСУ, так і сил охорони правопорядку для безпосереднього вогневого знищення таких засобів.

Список використаних джерел

1. Арасланов М. Р., Климченко В. Й., Малишев О. А., Куц В. С., Бєлоус М. В., Черток О. А. Використання COTS-технологій для відновлення працездатності й модернізації вузлів та блоків аналогових радіолокаційних станцій радіотехнічних військ. *Системи озброєння і військова техніка*. 2023. № 2(74). С. 6–16. https://doi.org/10.30748/soivt.2023.74.01.

2. Арасланов М. Р., Климченко В. Й., Малишев О. А., Сидоров В.В., Тах'ян К.А. Підвищення можливостей виявлення БПЛА аналоговими РЛС метрового діапазону хвиль через модернізацію системи СРЦ. *Новітні технології – для захисту повітряного простору*: зб. тез доп. XIX міжнар. наук. конф. Харківського національного університету Повітряних Сил ім. І. Кожедуба. Харків: ХНУПС ім. І. Кожедуба, 2023. С. 226-227.

УДК 355.433

Бабенко О.І., Сізон Д.О., Пилипенко В.М.

ВИБІР МЕТОДІВ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У ВІЙСЬКОВІЙ СФЕРІ

Методи підтримки прийняття рішень у військовій сфері використовуються, як правило, коли має місце невизначеність — відсутня повна інформація про ситуацію, задум противника, задіяні сили та засоби та існує ризик прийняття помилкового рішення. Існує імовірність коли прийняття рішень здійснюється в найкоротші терміни за умов неповної інформації про противника. У цьому випадку при коректній постановці завдання та адекватного ставлення до ситуації, яка виникла, рішення приймається з мінімальним ризиком.

Вибір рішення з багатьох допустимих рішень складає основу регулярної процедури. Тому необхідно виділити особливості методів та теорії підтримки прийняття рішень, в яких використовуються такі варіанти невизначеності.

1. Відсутня інформація про повну сукупність характеристик та оцінок варіантів, а відомий лише дискретний ряд оцінок у просторі "варіанти - умови", що означає прийняття рішень, якщо задана дискретна (зазвичай кінцева) безліч оцінок варіантів за різних умов. Для ухвалення рішень у цій ситуації використовується "метод системних матриць", сутність якого полягає у застосуванні різних алгоритмів обробки цих матриць, що складаються з оцінок варіантів.

2. Задано ймовірнісні чи статистичні характеристики (оцінки) явища, процесу, сукупності, і потрібно мінімізувати ймовірність неправильного рішення. У цій ситуації використовуються методи мінімізації ризику, причому моделі ризику будуються з урахуванням можливих моделей випадкових подій і від невизначених факторів.

3. Задано "графові переваги" між варіантами, що вимагає перетворення графа з метою лінійного впорядкування, коли вибір рішення тривіальний. Для прийняття рішень у цій ситуації використовуються методи комбінаторної апроксимації.

4. Невизначеність задана у вигляді чисел і множин, потрібно створення адекватного обчислення нечітких чисел та множини для перетворення завдання прийняття рішень до задачі лінійного впорядкування. До завдань з нечіткими змінними відносяться задачі з лінгвістичними змінними, для яких запроваджені нечіткі числа.

5. Невизначеність задана імовірнісно чи статистично, а процес прийняття рішень використовує перевірку вероятностно-статистических гіпотез.

Основні методи теорії підтримки прийняття рішень базуються на тому чи іншому принципі обробки оцінок, узгодженому з критерієм вибору варіанта. Обґрунтування вибору варіанта дозволяє за умов наявності ризику прийняти правильне рішення і визначає принцип вибору.

Приклади такого обґрунтування часто мають якісний характер. Наприклад, метод системних (вирішальних) матриць, класичні та комбіновані критерії прийняття рішень; експертні оцінки мінімаксного методу, методів Байєса – Лапласа та Севіджа.

Ці критерії визначають оптимістичні, песимістичні стратегії, стратегії нейтралітету чи врівноваженого типу. Вивчення методів отримання оцінок (на основі методів системного аналізу) та методів обробки оцінок дозволяє сформувати необхідні методи підтримки прийняття рішень.

УДК 621.396

Балабуха О.С., Ковтунов А.Л., Кітов В.С., Курилко А.О., Галузінський А.Г., Сокова Т.В.

ПРОПОЗИЦІЇ ЩОДО ПОБУДОВИ АВТОМАТИЗОВАНОГО РОБОЧОГО МІСЦЯ У СКЛАДІ АВТОМАТИЗОВАНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ МОБІЛЬНОГО КОМПЛЕКСУ ОЗБРОЄННЯ

В доповіді розглядаються питання щодо побудови автоматизованого робочого місця у складі автоматизованої системи підтримки прийняття рішення мобільного комплексу озброєння, розроблена класифікація та перелік команд (наказів) бойового управління, підтверджень про їх отримання та доповідей про їх виконання, які необхідні для підготовки та застосування за призначенням мобільного комплексу озброєння.

Відбиття широкомасштабної збройної агресії з боку російської федерації потребує наявності на оснащенні Збройних Сил (ЗС) України сучасних мобільних комплексів озброєння. На даний час у ЗС України на озброєнні знаходиться озброєння (зокрема зенітні ракетні комплекси та ракетні комплекси Сухопутних військ (СВ)) які створювалась ще за радянських часів, терміни його технічної придатності неодноразово подовжувались, проводиться часткова модернізація та капітальний ремонт але ці заходи істотно не можуть вплинути на характеристики озброєння які в повній мірі вже не відповідають сучасним вимогам, особливо часовим показникам. Вищезазначене вказує на необхідність, як глибокої модернізації існуючих систем озброєння, так і на розробку нових сучасних високотехнологічних систем.

У зв'язку із закінченням строків технічної придатності та невідповідності тактико-технічних характеристик існуючих систем (комплексів, зразків) озброєння сучасним вимогам технічний стан його є критичним. ЗС України потребують оснащення найсучаснішим високотехнологічним озброєнням, інтегрованим у єдину систему управління військами.

Сучасні тенденції ведення збройної боротьби свідчать про пріоритетність розвідувально-ударних операцій, підвищення ролі саме мобільних комплексів озброєння (МКО) у здійсненні вогневого ураження противника. Наявність відповідної зброї у збройних силах держав з оборонною воєнною доктриною є надійним фактором стримування можливої агресії та запобігання посиленню загрози національній безпеці.

Основною тенденцією проектування, створення і модернізації мобільних систем (комплексів) озброєння є підвищення точності ураження цілей та удосконалення транспортних агрегатів.

При цьому, одним з найважливіших елементів МКО є автоматизована система підтримки прийняття рішення (АСППР) з відповідним інформаційним, математичним, програмним та лінгвістичним забезпеченням, технічні характеристики якої дозволять в як найповнішій мірі реалізувати потенційні бойові можливості МКО та максимально скоротити час виконання функціонального циклу МКО, що з урахуванням параметрів рухомості транспортних агрегатів дозволить забезпечити необхідний рівень живучості елементів МКО. Відповідно розгляд питань, пов'язаних з розробкою інформаційного забезпечення АСППР та алгоритмів прийняття рішень вибору варіантів застосування (переміщення) елементів МКО для забезпечення потрібного показника живучості на різних етапах функціонального циклу застосування за призначенням (з урахуванням параметрів рухомості транспортних агрегатів), є актуальною задачею.

Розглянуто питання щодо розробки та обґрунтування складу інформації бойового управління АСППР з урахуванням можливостей засобів розвідки, яка використовується для підготовки і застосування МКО за призначенням. Розроблена класифікація та пере-

лік наказів (команд) бойового управління, підтверджень про їх отримання та доповідей про їх виконання, які необхідні для підготовки і застосування МКО за призначенням. Наведено перелік команд (наказів) бойового управління військами (підрозділами озброєними мобільними комплексами озброєння). Показано процедуру формування в автоматизованому вигляді формалізованого бойового наказу як результату послідовного формування та видачі з ланки управління наказів (команд) бойового управління на підготовку і застосування МКО за призначенням, управління військами (підрозділами).

Проведено аналіз критеріїв оптимізації руху агрегатів мобільного комплексу озброєння, пропонується створення уніфікованого автоматизованого робочого місця (АРМ) у складі АСППР командира бойової машини (БМ) МКО родів військ СВ та Повітряних Сил (ПС), як основного елементу перспективного пункту управління (ПУ) та бойових засобів при управлінні бойовими діями підрозділів СВ та ПС. Такий ПУ може використовуватися для управління бойовими діями мобільних підрозділів: зенітних ракетних, ракетних та артилерійських підрозділів, підрозділів забезпечення бойових дій СВ та ПС.

Таким чином, пов’язані в єдину систему в складі перспективного ПУ уніфіковані АРМ у складі АСППР повинні забезпечувати автоматизоване вирішення наступних завдань: приведення підлеглих підрозділів у різні ступені бойової готовності; збір, обробка та відображення інформації про обстановку, яка надходить від приданих засобів розвідки, мережі оповіщення та бойових засобів підлеглих підрозділів; прийом та відображення даних про місцезнаходження та стан бойових засобів підлеглих підрозділів; інформаційна підготовка та вироблення оптимального варіанту розв'язання задачі цілерозподілу; видача цілевказівки підлеглим підрозділам та контроль за виконанням поставлених завдань; топогеодезична підготовка керування вогнем БМ (підрозділу); проведення тактичних (оперативно-тактичних) розрахунків; документування процесу бойової роботи; імітація бойової обстановки для тренувань розрахунку перспективного ПУ та бойових засобів МКО.

Список використаних джерел

1. Греков В. П., Акуленко І. М., Балабуха О. С. Оцінювання ефективності бойового застосування засобів ураження з врахуванням впливу технічних характеристик систем розвідки та управління. Збірник наукових праць Об’єднаного науково-дослідного інституту. 2005. Вип. 2 (2). С. 79 - 84.

2. Федченко В. В., Греков В. П., Балабуха О. С. Оцінювання ефективності ракетних ударів з урахуванням надійності озброєння та протидії противника. Моделювання та інформаційні технології. 2005. Вип. 2 (2). С. 41 - 46.

3. Герасимов С. В. Дергачов К. Ю., Балабуха О. С. Логістична модель застосування мобільного комплексу озброєнь. Матеріали наукового семінару ″Моделювання в військово-наукових дослідженнях″. 2006. Вип. 3 (4). С. 10 - 13.

4. Герасимов С. В. Дергачов К. Ю., Балабуха О. С. Структура программного обеспечения диспетчерской системы слежения за подвижными объектами. Матеріали І міжнародної науково-практичної конференції ″Європейська наука XXI століття: Стратегія і перспективи розвитку″. 2006. Т. 23. С. 6 - 8.

5. П’янков А. А., Піскачов О. І., Балабуха О. С. Підвищення рухомості самохідної пускової установки як перспективний шлях зменшення імовірності її ураження. Збірник наукових праць Об’єднаного науково-дослідного інституту. 2007. Вип. 1 (6). С. 54 - 59.

Балюк Р.В., Мілько А.М., Хижняк І.А.

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ПРОТИДІЇ БПЛА НА ПОЗИЦІЇ ОКРЕМОГО РАДІОЛОКАЦІЙНОГО ВЗВОДА ЗА ДОСВІДОМ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Досвід ведення російсько-української війни показав, що в умовах ведення швидкоплинних бойових дій та різкої зміни обстановки застосування безпілотних літальних апаратів (БПЛА) є одним з основних засобів отримання розвідувальної інформації в масштабі реального часу для подальшої можливості здійснити вогневий вплив противником на особовий склад та об'єкти інтересу. На сьогоднішній день жодна держава не спроможна у повному обсязі протистояти спланованим діям БПЛА. Виходячи з цього боротьба з БПЛА є одним із пріоритетних завдань протидії системам розвідки, управління і бойового застосування противника.

На сьогодні противником в російсько-українській війні активно використовується дві версії ударного БПЛА, так званих "баражуючих боєприпасів" – "Ланцет - 1" та "Ланцет - 3" (далі – УБпЛА типу "Ланцет"). Обидві версії мають однаковий планер з подвійними Х-подібними крилами і схожими внутрішніми системами.

Основною ж відмінністю є розміри та корисне навантаження БПЛА. Максимальна злітна вага "Ланцет - 3" сягає 12 кг, "Ланцет - 1" – 5 кг, з бойовими частинами 3 кг та 1 кг відповідно. Комплекси можуть літати автономно, відповідно до польотного завдання по завчасно закладеному маршруту, з можливістю його корегування, самостійно знаходити задану ціль та уражати її. Ефективна дальність польоту УБпЛА типу "Ланцет" становить від 40 до 60 кілометрів. Політ виконується на висоті від 60 до 3000 метрів в діапазоні швидкостей від 80 до 110 км/год. Тривалість польоту УБпЛА "Ланцет" від 30 до 40 хвилин відповідно. Під час пікірування можуть розвивати швидкість до 300 км/год.

Для ефективної протидії УБпЛА типу "Ланцет" на позиції окремого радіолокаційного взводу (орлв) можна розглянути наступні пропозиції:

1. Радіоелектронна боротьба. Використання систем радіоелектронної боротьби для перехоплення та приглушення сигналів управління УБпЛА, що може призвести до втрати їх контролю та втрати ефективності в бою.
2. Протиповітряна оборона. Розгортання зенітно-ракетних комплексів та протиповітряних ракетних систем для знищення ворожих УБпЛА на підході до позицій орлв.
3. Активні системи захисту. Використання активних систем захисту, таких як системи лазерного впливу або системи перехоплення та руйнування атак противника, для захисту позицій орлв від ударів УБпЛА.
4. Активне виявлення та знищення. Розгортання систем активного виявлення та знищення, таких як зенітно-ракетні комплекси або протиповітряні ракетні системи, для нейтралізації розвідувальних БПЛА.
5. Фізичні перешкоди. Розгортання фізичних перешкод, таких як сітки, бар'єри або екранувальні споруди, для ускладнення проникнення БПЛА на позиції орлв.
6. Заходи безпеки. Встановлення фізичних заходів безпеки, таких як укриття та екранування, для захисту від атак з повітря.
7. Розвідка та розведення. Систематична розвідка та розведення для вчасного виявлення та ідентифікації ворожих БПЛА, що дозволить прийняти необхідні заходи для їх знищення чи відвернення атаки.

Отже, перелічені підходи можуть бути інтегровані в комплексну стратегію захисту позицій окремого радіолокаційного взводу від атак УБпЛА.

Басараб О.К., Радіон Н.В.

АКУСТИЧНА ПЕЛЕНГАЦІЯ БЕСПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ МЕТОДОМ ПОРІВНЯНЯ СИГНАЛІВ

Як показав досвід ведення бойових дій, сучасна війна – це війна безпілотних авіаційних комплексів (далі – БпАК), дронів тощо. Ведення ними розвідки, нанесення вогневого ураження як броньованій техніці так і живий силі противника, транспортування засобів ведення війни, навіть, допомога у виході з оточення своїх бійців стало тими бойовими завданнями, що виконуються за допомогою електронних «пташок». Військові формування України інтенсивно застосовують в бойовій діяльності широкий спектр різноманітних БпАК, отже собівартість комплектуючих одного комплекту найпростішого дрону може бути меншою за 300$, а збір не набагато складніший за конструктори Lego. Нажаль, противник використовує не в меншому обсязі власні дрони та інші БпАК. Так, за даними певних джерел, в період з серпня 2023 року по січень 2024 року загальна кількість зафіксованих уражень ударними FPV (first person view) -дронами (далі – FPV) українською стороною – 3886 випадків, тоді коли з російської – 2889 [1]. Як бачимо, загальна кількість уражень поки що на користь Сил Оборони України, проте, спостерігається тенденція збільшення інтенсивності застосування FPV ворогом. Отже, один з основних пріоритетів в протиборстві з агресором є протидія БпАК, FPV тощо, розробка та застосування сучасних засобів виявлення та ефективного їх знищення [2].

Умовно, боротьбу з БпАК можна розділити на 2 кроки – виявлення та протидія. Проте, в даному дослідженні нас більше цікавить процес виявлення, оскільки «хто попереджений, той озброєний» (лат. Praemonitus, praemunitus — «попереджений, озброєний»).

Виявлення БпАК може здійснюватися різними методами, вибір яких залежить від багатьох факторів, насамперед: тип, матеріал виготовлення та габарити цілі; параметри руху цілі – висота, швидкість; особливості місцевості – рельєф, рослинність, забудова тощо. З основних методів виявлення можна виділити радіоелектронне виявлення за допомогою радіолокаційних станцій та акустичне виявлення. Радіолокаційне виявлення є більш вартісним способом у порівнянні з акустичним, та більш небезпечним, якщо йдеться про активну радіолокацію. Водночас, радіолокаційне виявлення більш вибагливе до умов застосування – відносно потужне електроживлення, більше часу на розгортання тощо. А в умовах застосування мобільних протидронних груп, що озброєні, як правило, стрілковою зброєю, це неприпустимі, критичні вимоги. Разом з тим, швидкість руху більшості БпАК вимагає від мобільних груп швидкого реагування та автоматизації наведення вогневих засобів. Особливих складнощів це набуває в умовах обмеженої видимості, в ночі тощо. Отже, на наш погляд, в даному аспекті, перспективним напрямком розвитку «протидронної» боротьби є вимірювання кутових координат БпАК, тобто, пеленгація, «на звук».

Для звукової пеленгації БпАК пропонується метод порівняння сигналів, схожий до аналогічного методу в радіолокації [3]. Метод включає побудову комплексу виявлення БпАК та автоматичного наведення мобільного протидронного вогневого засобу на основі двох напрямних мікрофонів, які розміщені на певній відстані один від одного, мікроконтролера для аналізу та крокового двигуна з приводом, що обертає платформу з встановленим комплексом. Звук двигуна БпАК буде уловлюватися обома мікрофонами, оцифровуватися за допомогою аналогово-цифрових перетворювачів та на основі перетворення будуть побудовані осцилограми прийнятих сигналів. При цьому, будемо використовувати напрямну властивість мікрофону, тобто, чим точніше направлений на ціль мікрофон, тим вище значення амплітуди осцилограми прийнятого сигналу. Проте, найбільш точним вимірювання буде в момент рівності сигналів, отриманих з обох мікрофонів, тому використання двох мікрофонів є критичним для запропонованого методу.

На основі обрахунку мікроконтролер буде видавати управляючі сигнали на кроковий двигун, який, в свою чергу, буде направляти платформу з мобільним антидронним комплексом, вогневим засобом тощо, на джерело звуку.

Таким чином, пропонується метод пеленгації БпАК з використанням звукового каналу, що утворений звуком двигуна літального засобу. Зазначений варіант дешевий у виконанні та має перевагу при виявленні БпАК на низьких та наднизьких висотах, в умовах обмеженої видимості тощо.

Список використаних джерел

1. Update on FPV drone warfare (27-01-2024). Tochnyi.info. URL: https://tochnyi.info/2024/01/update-on-fpv-drone-warfare-27-01-2024-2/ (дата звернення 04.03.2024)

2. The Commander-in-Chief of Ukraine's Armed Forces on How to Win the War. The Economist. URL: https://Www.Economist.Com/By-Invitation/2023/11/01/The-Commander-In-Chief-Of-Ukraines-Armed-Forces-On-How-To-Win-The-War (дата звернення 04.03.2024)

3. Основи побудови радіолокаційних засобів розвідкиповітряного простору : конспект лекцій / К. С. Васюта та ін. Харків : ХУПС,2013. – 212 с.

УДК 519.876.5:658.512

Безкоровайний В.В., Безугла Г.Є., Чоломбитько Д.В.

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ПРОЦЕСІВ РОЗПОДІЛУ ТА ВИКОНАННЯ ПАКЕТІВ РЕМОНТНИХ РОБІТ

Запропонована та програмно реалізована аналітико-імітаційна модель процесу розподілу та виконання пакетів ремонтних робіт. У ній розроблено адаптивний алгоритм багатокритеріального розподілу робіт за показниками витрат, часу виконання та якості. Це дозволяє на практиці враховувати стохастичний характер потоків пакетів та часу їх виконання, поточний стан виконавців, можливу необхідність їх доопрацювання і зміну пріоритетів робіт.

В умовах пандемії, військового стану, ведення бойових дій швидко і суттєво змінилися вимоги до систем ремонту та обслуговування техніки. Це потребує відповідних змін у структурі, параметрах, топології та технології функціонування систем ремонту техніки (СРТ) [1]. Більшість задач оптимізації СРТ мають комбінаторний характер, розв'язуються за множиною функціональних і вартісних показників в умовах неповної визначеності цілей і даних [2–3]. Запити з ремонту техніки являють собою пакети робіт, які можуть виконуватися послідовно, паралельно або з урахуванням інших зв'язків між ними. Однією з найважливіших задач, що виникає у процесах реінжинірингу та керуванні подібними об'єктами є задача динамічного розподілу пакетів робіт між їх елементами (бригадами, виконавцями, обладнанням тощо) [4–5]. Недетермінованість потоку пакетів та часу виконання окремих робіт, неповна визначеність алгоритмів призначення робіт та необхідність врахування множини функціональних і вартісних показників актуалізує задачі моделювання процесів розподілу та виконання пакетів робіт при системній оптимізації СРТ.

Задачі розподілу пакетів робіт розглядаються як специфічні задачі про призначення n робіт n виконавцям. У багатьох випадках пакети робіт можна розбивати на множини незалежних ланцюжків чи окремих робіт. СРТ пропонується розглядати як трифазну багатоканальну систему масового обслуговування (СМО). Канал першої фази виконує

розподіл робіт, n каналів другої фази виконують окремі роботи чи ланцюжки робіт, а канал третьої фази об'єднує роботи, виконані на другій фазі. Необхідно циклічно виконувати найкращий розподіл робіт серед каналів другої фази за показниками витрат фінансових (матеріальних) ресурсів $k_1(x)$, витрат часу $k_2(x)$ та якості виконання робіт $k_3(x)$ (де $x \in X$ – варіант розподілу робіт з множини допустимих) [4–5]:

$$k_1(x) = c_\Delta + \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}x_{ij} \to \min_{x\in X}, \tag{1}$$

$$k_2(x) = \tau_\Delta + \max_i\left\{\tau_{ij}x_{ij}\right\} \to \min_{x\in X}, \tag{2}$$

$$k_3(x) = \min_{1\le i,j\le n}\left\{q_{ij}x_{ij}\right\} \to \max_{x\in X}, \tag{3}$$

де c_Δ, τ_Δ – сумарні витрати ресурсів і часу на першій і третій фазі; $c_{ij} = (c_{ij}^o + c_{ij}')$, $\tau_{ij} = (\tau_{ij}^0 + \tau_{ij}')$, q_{ij}, $i, j = \overline{1,n}$ – загальні витрати ресурсів, часу та якість виконання i-ї роботи j-м виконавцем; c_{ij}^o, τ_{ij}^o – номінальні витрати ресурсів і часу на виконання i-ї роботи j-м виконавцем; c_{ij}', τ_{ij}' – витрати ресурсів і часу на перехід до виконання поточної роботи; $x = [x_{ij}]$, $i, j = \overline{1,n}$ – матриця призначення ($x_{ij} = 1$, якщо i-та робота призначена j-му виконавцю; $x_{ij} = 0$ – в іншому випадку).

Для загальної оцінки варіантів розподілу робіт $x \in X$ одночасно за показниками (1) – (3) запропоновано використати їх адитивну згортку:

$$P(x) = \sum_{l=1}^{3}\lambda_l\xi_l(x) \to \max_{x\in X},\ \xi_l(x) = \{[k_l(x) - k_l^-] / [k_l^+ - k_l^-]\}^{\alpha_l},\ l = \overline{1,3}, \tag{4}$$

де $P(x)$ – функція оцінки загальної якості розподілу робіт $x \in X$; λ_l – вагові коефіцієнти локальних критеріїв, $\lambda_l \ge 0$, $l = \overline{1,3}$, $\sum_{l=1}^{3}\lambda_l = 1$; $\xi_l(s)$ – функція корисності локального критерію $k_l(x)$; k_l^+, k_l^- – найкраще та найгірше значення критерію $k_l(x)$; α_l – параметри, що визначають вид функції корисності (лінійна, випукла чи увігнута).

Для циклічного розв'язання задач розподілу запропоновано використовувати модифікований угорський алгоритм. Для визначення стану каналів на момент надходження чергового пакету, оцінок загального часу розподілу та виконання пакетів робіт пропонується використати метод аналітико-імітаційного статистичного моделювання. Моделювальний алгоритм побудовано за принципом послідовного проведення заявок.

При виборі мови програмування враховувалась необхідність гнучкої взаємодії засобів опису варіантів побудови СРТ і оцінювання їх функціональних характеристик. Це обумовило вибір мови загального призначення Java.

Для отримання результатів з похибкою ε, що не перевищує задане значення ε^*, вирішено завдання тактичного планування комп'ютерних експериментів:

– обрано початкові умови моделювання, що наближені до усталеного режиму роботи СРТ;

– визначено необхідну для цього кількість експериментів;

– для зменшення дисперсії отримуваних оцінок запропоновано відкидати статистику початкового етапу моделювання;

– визначено умови автоматичного припинення експериментів по досягненні результатів заданої точності.

Отримані результати дозволяють підвищити ефективність технологій структурно-технологічної та технологічної оптимізації систем ремонту техніки в процесах їх проєктування, реінжинірингу чи керування ними. Практичне використання запропонованої

моделі сприятиме підвищенню продуктивності систем ремонту за рахунок скорочення часу виконання пакетів робіт.

Список використаних джерел

1. Морозов О. О. Методика розв'язання задачі синтезу топологічної та функціональної структур систем ремонту озброєння і військової техніки // Науковий вісник Київського інституту національної гвардії України, 2023. №1. 2023. С. 6–10.

2. Beskorovainyi V., Imanhulova Z. Technology of large-scale objects system optimization // ECONTECHMOD. 2017. Vol. 06. No. P. 3–8.

3. Beskorovainyi V. Combined method of ranking options in project decision support systems // Innovative Technologies and Scientific Solutions for Industries, 2020. No. 4 (14). P. 13–20.

4. Bezkorovainyi V., Bezuhla H., Cholombytko D. Mathematical models of the cyclic work package distribution task. Innovative integrated computer systems in strategic project management: Collective monograph. Riga: ISMA, 2022. P. 7–15.

5. Bezkorovainyi V., Bezuhla H. Simulation modelling of the process of distribution and execution of work packages. Information systems in project and program management: Collective monograph. Riga: ISMA, 2023. P. 16–28.

УДК 004.9: 519.81

Безкоровайний В.В., Драз О.М.

МАТЕМАТИЧНА МОДЕЛЬ БАГАТОКРИТЕРІАЛЬНОЇ ЗАДАЧІ РЕІНЖИНІРИНГУ ТОПОЛОГІЧНОЇ СТРУКТУРИ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Розширення множини користувачів, їх функціональних задач, підвищення вимог до оперативності та надійності, поява більш досконалих технологій на певному етапі призводять до необхідності реінжинірингу існуючих корпоративних комп'ютерних мереж. Процес реінжинірингу передбачає вирішення множини завдань оптимізації їх структури, топології, параметрів елементів та каналів передачі інформації [1–2].

Найбільшу обчислювальну складність мають задачі оптимізації варіантів побудови топологічних структур мереж. Вони розв'язуються за множиною функціональних та вартісних показників з урахуванням структурних і топологічних обмежень існуючих мереж та мають специфічні відмінності від традиційних задач проєктування [3].

Об'єктом дослідження є трирівнева централізована мережа. Для неї задані: множина елементів (центр, вузли, комп'ютери) мережі $I = \{ i \}$, $i = \overline{1,n}$; варіант топологічної структури існуючої мережі $s' \in S*$ (де $S*$ – множина допустимих варіантів), що задається місцями розташування елементів (для центру $i = 1$), а також зв'язками між елементами $[s'_{ij}]$, $i, j = \overline{1,n}$ (де $s'_{ij} = 1$, якщо між елементами i та j існує безпосередній зв'язок і $s'_{ij} = 0$ – в іншому випадку); витрати на створення чи модернізацію вузлів $[c_i]$, $[d_i]$, $i = \overline{1,n}$ і зв'язків між елементами $[c_{ij}]$, $[d_{ij}]$, $i = \overline{1,n}$. Необхідно визначити найкращий за показниками оперативності (часу доступу до інформації), надійності, живучості та витрат варіант реінжинірингу топологічної структури $s^o \in S*$.

Множина допустимих варіантів побудови мережі визначається умовами:

$$S^* = \{s\} = \begin{cases} [s_{ij}],\ s_{ij} \in \{0,1\},\ \ i, j = \overline{1,n},\ s_{11} = 1; \sum_{i=j}^{n} s_{ij} \geq 1\ \forall j = \overline{1,n}; \\ \sum_{j=1}^{n}\sum_{i=j}^{n} s_{ij} = n + \sum_{i=1}^{n} s_{ii},\ s_{ii} = 1 \rightarrow s_{i1} = 1\ \forall i = \overline{1,n}; \\ s_{ii} \wedge s_{ij} = 1 \rightarrow ij = \arg \min\limits_{1 \leq i, j \leq n} c_{ij}\ \forall i, j = \overline{1,n}. \end{cases} \quad (1)$$

Варіант реінжинірингу задається кількістю вузлів у ній u, місцями їх розміщення та схемою зв'язків між елементами, вузлами та центром $[s_{ij}],\ i, j = \overline{1,n}$. При цьому: вузли мережі розміщуються у безпосередній близькості від комп'ютерів користувачів; вони підключаються до вузлів за показником мінімуму витрат; обсяги запитів $\alpha = [\alpha_i],\ \alpha_i \approx const$ і відповідей $\beta = [\beta_i],\ \beta_i \approx const$, $i = \overline{1,n}$ мають приблизно однакові обсяги.

Як критерій оперативності пропонується використати час відповіді на запит:

$$k_1(s) = \left\{ \tau^C + \frac{\overline{\alpha}}{\gamma_1} + \tau^E + \frac{\overline{\beta}}{\gamma_2} + \left(\frac{\overline{\alpha}}{\gamma_1} + \frac{\overline{\alpha}}{h_1} + \frac{\overline{\beta}}{h_2} + \frac{\overline{\beta}}{\gamma_2} \right) \sum_{j=1}^{n}\sum_{l=j}^{n} s_{jl} s_{jj} \right\} \rightarrow \min\limits_{s \in S^*}, \quad (2)$$

де τ^C, τ^E – час на видачу запиту та отримання інформації користувачем; $\overline{\alpha}$, $\overline{\beta}$ – обсяги інформації в запиті та відповіді на запит; γ_1, γ_2 – пропускні здатності каналів зв'язку «центр-вузол» і «вузол-комп'ютер»; h_1, h_2 – швидкості обробки запиту та відповіді у вузлах мережі.

Як показник надійності мережі використовуємо коефіцієнт її готовності:

$$k_2(s) = \delta^C \times \ \delta^{U\ \ u} \times \ \delta^{E\ \ n} \times \ \delta^{CU\ \ u} \times \ \delta^{UE\ \ n} \rightarrow \max\limits_{s \in S^*}, \quad (3)$$

де δ^C, δ^U, δ^E, δ^{CU}, δ^{UE} – коефіцієнти готовності центру, вузла, комп'ютера, каналів зв'язку «центр-вузол» та «вузол- комп'ютер»; n, $u = \sum\limits_{i=1}^{n} s_{ii}$, – кількості комп'ютерів та вузлів у мережі.

Для оцінки живучості використовуємо значення частини комп'ютерів пов'язаних з центром у мережі при одиночних пошкодженнях її компонентів. Незалежно від виду структури мережі при пошкодженні центру – $k_3(s) \equiv 0$, а при пошкодженні одного комп'ютера або зв'язку «вузол-комп'ютер» $k_3(s) \equiv (n-1)/n$ [3]. З урахуванням цього критерій живучості:

$$k_3(s) = \left\{ \min\limits_{1 \leq j \leq n} \left[\left(n - \sum_{j=2}^{n}\sum_{i=j}^{n} s_{ji} s_{ii} \right) / n \right] \right\} \rightarrow \max\limits_{s \in S^*}. \quad (4)$$

Цільова функція наведених витрат на реінжиніринг матиме такий вигляд:

$$k_4(s', s) = \sum_{i=1}^{n} [c_i(1 - s'_{ii})\, s_{ii} + d_i s'_{ii} s_{ii}] + \sum_{j=1}^{n}\sum_{i=j}^{n} [c_{ij}(1 - s'_{ij})\, s_{ij} + d_{ij} s'_{ij} s_{ij}] \rightarrow \min\limits_{s \in S^*}. \quad (5)$$

Отримані результати можуть бути використані для підтримки прийняття рішень у технологіях реінжинірингу корпоративних комп'ютерних мереж. Напрямком подальших досліджень у цій галузі можуть бути врахування у моделях невизначеності вхідних даних, функціональних та вартісних характеристик обладнання мереж [6].

Список використаних джерел

1. Chaidir J., Haerofiatna H. Network Infrastructure Development in Serang District // International Journal of Management Technology, 2023. Vol. 10. No. 1. P. 11–19.
2. Optimization and mathematical modeling of communication networks / V. M. Bezruk, V. V. Semenets, D. V. Chebotarova, N. M. Kaliuzhniy [etc.]. Kharkiv: PC «Technology Center», 2019. 192 p.
3. Beskorovainyi V. V., Petryshyn L. B., Honcharenko V. O. Mathematical models of a multi-criteria problem of reengineering topological structures of ecological monitoring networks // Applied Aspects of Information Technology. 2022. Vol. 5 No. 1. P. 11–24.
4. Beskorovainyi V., Russkin V. Directed search of variants in technologies for reengineering of corporate computer networks // Intelligent information systems for decision support in project and program management: Collective monograph edited by I. Linde. European University Press. Riga : ISMA, 2021. P. 15-24.
5. Beskorovainyi V., Kolesnyk L., Russkin V. Decision making support under conditions of incomplete consistency of expert advantages // Innovative integrated computer systems in strategic project management": Collective monograph edited by I. Linde. European University Press. Riga: ISMA, 2022. P. 16-26.
6. Beskorovainyi V., Kolesnyk L. Interval model of multi-criterion task of reengineering physical structures of distributed databases // Intelligent information systems for decision support in project and program management: Collective monograph edited by I. Linde. European University Press. Riga: ISMA, 2021. P. 7-14.

УДК 004.02

Безугла Г.Є., Артеменко А.Д.

ІНФОРМАЦІЙНА СИСТЕМА АНАЛІЗУ ТА КОНТРОЛЮ ЧАСУ ВИРОБНИЧОГО ЦИКЛУ НА ПІДПРИЄМСТВІ

В роботі розглянута задача інтеграції інформаційної системи у виробничий процес з метою забезпечення планування робочого часу та ресурсів для ефективного виконання замовлень на виробничому підприємстві

Відповідно до вимог сучасності необхідно підвищувати гнучкість управління виробничим процесом для його модифікації відповідно до різних типів замовлень та вимог замовника, забезпечувати контроль якості та більш швидку доставку готових виробів. Інформаційна система контролю та планування виробничого процесу – є необхідним інструментарієм для виробничих підприємств дрібносерійного виробництва, що забезпечить виявлення вузьких місць для кожного типу замовлень, визначення часу роботи кожної виробничої дільниці, планування термінів виконання замовлення відповідно до поточного навантаження виконавців, виконання динамічного корегування виробничого плану.

В дрібносерійному виробничому підприємстві потрібно виконати замовлення не пізніше ніж за визначений в замовленні термін, отже мінімізація часу виробничого циклу не є головним критерієм ефективності. Для оптимізації виробничого процесу потрібно проводити аналіз часу простою обладнання, враховувати резерви часу на контроль якості кожного етапу виробництва, витрат часу відповідно до режиму роботи підприємства, наявності міжопераційних витрат часу на знаходження деталей у незавершеному виробництві, що обумовлено необхідністю переналадки або звільнення необхідного обладнання для роботи. Послідовний тип руху деталей є найбільш простим для планування. В цьому випадку деталі передаються на кожну наступну операцію всією партією

після обробки її на попередній. Тривалість операційного циклу обробки деталей визначається за формулою:

$$\mathrm{T_п} = n \sum_{1}^{m} \frac{t_\mathrm{н}}{\mathrm{C}},$$

де m - число операцій в технологічному процесі; n - кількість деталей у партії; C - число робочих місць на операції; $t_\mathrm{н}$ - штучно-калькуляційна норма час на операцію. Використання паралельного типу виробничого циклу дозволить більш ефективно використовувати виробниче устаткування, але для синхронної роботи підприємства необхідно чітко визначити момент часу початку виконання наступного замовлення. Застосування інформаційної системи контролю часу виробничого циклу дасть можливість визначити реальні часові інтервали шляхом відмітки про виконання кожного етапу та передачі на наступну дільницю виробництва. Після завершення кожного етапу виробництва проводиться обов'язкова перевірка на виявлення можливих дефектів або браку, а також присвоюється унікальний статус кожному замовленню. Передбачається використання інформаційній картки з позначенням часу його початку та закінчення кожного етапу виробничого циклу, та відповідного статусу. Кожен із цих статусів надає інформаційній системі детальний огляд стану замовлення, що сприяє ефективному та оперативному управлінню. Аналіз тривалості виробничого циклу декількох схожих замовлень дозволить точніше визначити вузькі місця та реальний час його виконання на всіх етапах виробництва. Це дозволяє оптимізувати виробничі процеси та розподіляти ресурси з урахуванням конкретних потреб та термінів виконання. Інтеграція інформаційної системи у виробничий процес надає переваги в контексті оптимізації виробництва, дозволяє визначити прогнозований час виробництва, забезпечити більш точне планування робочого часу та ресурсів для ефективного виконання замовлень на виробничому підприємстві.

UDC 681.3

Bekirov A., Krasnorutskyi A., Kazmirov I.

ANALYZING THE FUNCTIONALITY OF STATISTICAL STEGANOGRAPHIC EMBEDDING ALGORITHMS

A large number of publications related to the development of new methods or the enhancement of existing characteristics of steganographic transformations is accompanied by the creation of effective detection methods for covert embeddings within containers. Considering that steganographic modification alters the statistical characteristics of elements in original containers, a significant number of steganographic analysis methods are based on the calculation and evaluation of metrics that characterize the degree of inter-element affinity within a container [1–4].

The complexity of applying steganographic analysis methods is linked to the absence of prior information about the embedding method, the length of the payload message, and the embedding regions (in the case of pre-selection of working areas). For the most prevalent steganographic analysis methods, the assessment result regarding the presence of embedding typically represents a probability value, for instance: "the probability of the presence of embedding is 56%" [3]. Therefore, solving the embedding detection problem involves the integrated use of several different principle-based methods of steganographic analysis [5-6].

The most well-known method of steganographic embedding in images is the least significant bit substitution method, whose operational principle relies on replacing the least significant bit of the binary representation of container elements. Alongside its simplicity and

high steganographic capacity, this method is vulnerable to statistical steganographic analysis algorithms, namely the "chi-square" method and the RS-method [7].

Further development of steganographic methods aimed at enhancing embedding resilience to steganographic analysis involves the selection of elements for embedding. For example, the pseudo-random interval method entails embedding bits not in every container element but through intervals determined based on a pseudo-random law. In this case, the rule for generating pseudo-random sequences serves as additional key information that must be known at both the transmitting and receiving ends. Analysis of the algorithm's resilience to embedding detection based on the "chi-square" method demonstrates a significant decrease in the probability of identifying the presence of additional information. However, the pseudo-random interval method is vulnerable to steganographic analysis using the RS-method [8-9].

A further development of the least significant bit method is the pseudo-random distribution of the embedded message. The essence of the method lies in embedding bits distributed based on a pseudo-random rule. The composition of the original information message at the receiving end is based on a key rule. The method is resilient to attacks aimed at extracting the embedded message but does not affect changes in the static characteristics of the container [10–12].

To ensure the resilience of methods for modifying spatial representation elements to statistical steganographic analysis, it is proposed to develop an algorithm for selecting container elements for covert embedding based on the least significant bit method.

Considering the operational peculiarities of steganographic embedding methods, the development of the algorithm for searching working elements must meet a set of requirements, characterizing the algorithm from the perspective of reducing container distortions while simultaneously ensuring the specified steganographic capacity of the embedding method.

Based on an analysis of the operating features of statistical steganographic analysis methods for modification algorithms of least significant bits, a direction is proposed to enhance steganographic resilience, involving the application of an algorithm for searching embedding elements.

A set of requirements corresponding to the functioning features of steganographic embedding methods has been formulated. Notable characteristics of the embedding element search algorithm include:

– varying search results under identical operational conditions for different containers;

– application of the search algorithm with different key rules for the same container resulting in different embedding element positions;

– algorithm resilience to detecting embedded element positions on the receiving end against container distortions arising from embedding;

– adaptive adjustment of key rule coefficients based on the length of the information sequence;

– consideration of the semantic component of the container and the human visual system in determining embedding element positions [13].

References

1. Задирака В.К. Статистичний аналіз систем с цифровими водяними знаками / В.К. Задирака, Н.В. Кошкіна, Л.Л. Никитенко // Штучний інтелект. – 2008. – № 3. – С. 315-324.

2. Al-Shatnawi A.M. A new method in image steganography with improved image quality / A.M. Al-Shatnawi // Applied Mathematical Science. – 2012. – № 6(79). – P. 3907-3915.

3. Avinash K.G. A high capacity secured image steganography method with five pixel pair differencing and LSB substitution / K.G. Avinash, S.J. Madhuri // Graphics and Signal Processing. – 2015. – № 5. – P. 66-74.

4. Юдін О.К. Захист інформації в мережах передачі даних: підручник / О.К. Юдін, Г.Ф. Конахович, О.Г. Корченко. – К.: ТОВ НВП "ІНТЕРСЕРВІС", 2009. – 714 с.

5. Danik Yu. Synergistic effects of information and cybernetic interaction in civil aviation / Yu. Danik, R. Hryschuk, S. Gnatyuk // Aviation. – 2016. – № 3(20). – P. 137-144.

6. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатов. – К.: Юниор, 2003. – 501с.

7. Ravi Shankar Reddy M. A novel method for steganography in spatial domain / M. Ravi Shankar Reddy, Sri J. Swami Naik // International Journal of Advanced Research in Computer Science and Software Engineering. – 2013. – № 3(10). – P. 1117-1122.

8. Бекіров А.Е. Технологія селекції областей аерофотознімку з різною насиченістю для стеганографічного перетворення / А.Е. Бекіров, В.Ж. Ященок, О.М. Крейдун // Сучасні інформаційні технології у сфері безпеки та оборони. – 2019. – № 1(34). – С. 55-60. https://doi.org/1.33099/2311-7249/2019-34-1-115-120.

9. Fufang L. Text steganography based on ci-poetry generation using Markov chain model / Li Fufang, Yubo Luo, Yongfeng Huang, Chinchen Chang // KSII Transactions on Information and Systems. – 2016. – № 10(9). – P. 4568-4584.

10. Jassim F.A. Five modulus method for Image compression / F.A. Jasim // Signal and Image Processing. – 2012. – № 5(3). – P. 26-34.

11. Бекіров А.Е. Стеганографічний метод на основі безпосереднього та непрямого вбудовування даних для областей зображення з різною насиченістю / А.Е. Бекіров, В.Ж. Ященок, О.М. Крейдун // Сучасні інформаційні технології у сфері безпеки та оборони. – 2020. – № 1(37). – С. 115-120. https://doi.org/10.33099/2311-7249/2020-37-1-55-60.

12. Cox I.J. Digital watermarking and steganography / I.J. Cox, J.A. Bloom, T. Fridrick. – Burlington: Morgan Kaufman Publishers. – 591 p.

13. Бекіров А. Е. Формулювання вимог до алгоритму пошуку елементів просторового представлення контейнеру для стеганографічного вбудовування //Системи озброєння і військова техніка. – 2021. – №. 2 (66). – С. 32-36. https://doi.org/10.30748/soivt.2021.66.04.

УДК 355.5:004

Бідник І.І.

АКТУАЛЬНІ ПИТАННЯ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-ЦИФРОВИХ ТЕХНОЛОГІЙ ПРИ ПІДГОТОВЦІ МАЙБУТНІХ САПЕРІВ

Проблема розвитку пізнавальної активності курсантів під час навчання, вимагає пошуку нових підходів до подальшого вдосконалення змісту, форм, методів і способів підготовки, спрямованих на формування фахових компетентностей майбутніх офіцерів.

Швидкий розвиток інформаційно-комунікаційних технологій призвів до виникнення нових понять, таких як: цифровізація, цифрова трансформація, діджиталізація, цифрові технології тощо. Інформаційні технології усе ширше впроваджуються в систему підготовки фахівців-саперів. Переваги їх застосування в педагогічній діяльності є безперечними. Вони дозволяють курсантам підвищити наочність та мобільність процесу отримання навчального матеріалу, одержувати потрібну інформацію миттєво з різних джерел, навчатися на робочому місці в зручному для них темпі та під час самопідготовки. Крім того, використання ІТ дає можливість оперативного оновлення інформації та практично миттєвого зворотнього зв'язку, забезпечуючи інтерактивність здобуття знань.

Інформаційно-цифрові технології активно використовуються при проведенні навчальних та практичних занять з курсантами. Для подачі навчального матеріалу можуть бути використані сучасні технології візуалізаці. Основними напрямами використання цифрових технологій у підготовці саперів є:

- впровадження елементів дистанційного навчання з використанням сервісів відео- та текстової комунікації (Meet, Zoom, Skype, Viber тощо), засобів для організації дистанційного навчання та спільного опрацювання документів (наприклад, Google Клас і Google Документи), зберігання матеріалів у «хмарних» сховищах (наприклад, Google Диск);
- використання навчального відео з сервісів YouTube;
- використання «розумних» інструментів смартфонів (лінійка, рівень, компас, секундомір, лупа тощо) для проведення досліджень і вимірювань, під час виконання навчальних та практичних занять.

Для підвищення якості навчання, підготовки військових фахівців використовуються інформаційні ресурси мережі Internet та інформаційних платформ типу Moodle, iSpring Online, Dokeos, Forma LMS, Zoom, Google Classroom в якості елементу системи дистанційного навчання.

Основною перевагою використання комп'ютерних технологій є те, що методичні матеріали, котрі надаються через мережу Інтернет, мають можливість регулярного оновлення та доповнення, вони дозволяють їх використовувати в будь-який час, організовувати онлайн трансляції для аудиторії в різних місцях.

Слід зазначити, що особливість підготовки військових фахівців-саперів, є надбання і закріплення навичок, отриманих під час теоретичної підготовки і доведення до автоматизму моторики виконання більшості основних завдань, які необхідні для здатності в будь-яких умовах, у встановлені терміни успішно виконувати завдання під час ведення бойових дій.

Комп'ютерні засоби навчання дозволяють вирішити такі завдання: забезпечити для кожного курсанта обсяг роботи з матеріалом, що вивчається, і послідовність, що полягає в чергуванні вивчення теорії, розбору прикладів, відпрацювання початкових професійних навичок, рішення типових компетентнісно-орієнтованих завдань; забезпечити можливість самоконтролю якості набутих знань та умінь; скоротити час, необхідний для вивчення матеріалу

Таким чином, реалізація цього напряму навчання створить для військових фахівців міцну основу їхнього безперервного професійного зростання та самоосвіти. Тому можна стверджувати, що інформаційно-цифрові технології сприяють кращому засвоєнню знань завдяки тим властивостям, якими вони володіють: мультимедійність, інтерактивність, адаптивність, диференційованість тощо.

Окрім того, за допомогою інформаційно-цифрових технологій викладач має змогу більш ширше застосовувати метод проектів, навчальних ігор (наприклад засобами комп'ютерних та ігрових симуляторів), дослідницький метод тощо. Важливим також є той факт, що за допомогою інформаційно-цифрових технологій у викладача є можливість організувати освітній процес індивідуально для кожного курсанта.

Включення мультимедійних освітніх матеріалів за рахунок використання сучасних інформаційних технологій у навчальний процес дозволяє: представити навчальні матеріали не тільки у друкованому вигляді, а й з використанням відеоряду, у графічному, звуковому вигляді, що дає багатьом курсантам реальну можливість засвоїти матеріал на більш високому рівні; автоматизувати систему самоконтролю; автоматизувати процес засвоєння, закріплення та застосування навчального матеріалу з урахуванням інтерактивності багатьох електронних навчальних посібників; здійснити індивідуалізацію навчання; оперувати великим обсягом інформації; навчати їх знаходити і використовувати різні види інформації, що є одним з найважливіших умінь у сучасному світі.

Бойчук Б.М., Опалинський В.Б.

НЕПОМІТНА БИТВА У КІБЕРПРОСТОРІ

З повномасштабним вторгненням росії в Україну, почалася друга, менш помітна битва - у кіберпросторі. З 24 лютого 2023 року урядовою командою реагування на комп'ютерні надзвичайні події CERT-UA було зафіксовано та опрацьовано понад 7000 кіберінцидентів. Така кількість кіберінцидентів вивела Україну на друге місце серед найбільш атакованих країн світу після США.

В основному найчастіше кібератаки стосувалися фінансового сектору, комерційних організацій та сектору телекомунікацій і розробки програмного забезпечення.

Основною задачею кібершахраїв було отримати доступ до організацій-жертв завдяки таргетованому фішингу, за рахунок втручання у їхню систему, та розповсюдження шкідливого програмного забезпечення, щоб налагодити шпигування, збір даних, використовуючи для цього вразливості сервісів.

На сьогоднішній день об'єктами атак є державні структури, IT-компанії, мобільні оператори, інтернет-провайдери, обленерго, водоканали, логістичні й страхові компанії, телебачення, медіа, веб-сторінки ЗМІ, підприємства малого бізнесу, навчальні заклади та навіть готелі, інші організації, структури і галузі. Експерти зазначають що високоактивними є кібератаки, спрямовані на викрадення коштів.

Ще одна особливість кібервійни - повторні напади на одні й ті ж відомства.

Прикладом такої особливості можуть бути атаки на системи «Київстару» які стали, мабуть, найбільш успішною операцією росіян проти України. Водночас це зайвий раз продемонструвало, що, окрім конвенційних операцій на полі бою, триває війна в кіберпросторі, яка почалася ще 2014 року. Деякі її прояви змогли зачепити багатьох українців, наприклад кібератаки на українські енергетичні компанії чи вірус Petya.A.

Трохи більше як за місяць до початку повномасштабного вторгнення, 14 січня 2022 року, кілька десятків українських державних ресурсів постраждали від потужної кібератаки. Цей січневий напад до атаки на системи «Київстару» був одним з найбільш помітних за останні два роки. Натомість відсутність видимих результатів кібернападів чи інформації про них не означає, що їх не було.

В ході проведення аналізу можливостей та засобів впливу на наші об'єкти в кіберпросторі дослідниками з кібербезпеки компанії ESET було виявлено ряд програм, які здатні на програмному рівні наносити шкоду роботі державним організаціям та службам України.

Одним з таких наборів шкідливих інструментів є Spacecolon, який використовується для поширення програм-вимагачів Scarab у всьому світі. Ймовірно, загроза проникає в організації через компрометацію уразливих вебсерверів або через підбір облікових даних до віддаленого робочого столу (RDP).

Ймовірно, кіберзлочинці намагаються скомпрометувати веб сервери організацій-жертв з уразливістю ZeroLogon або з обліковими даними RDP, які можна зламати методом підбору паролів. Крім того, Spacecolon може забезпечити доступ за допомогою бекдора для зловмисників. Останні не докладають багато зусиль, щоб приховати своє шкідливе програмне забезпечення, і залишають багато слідів в інфікованих системах.

Набір інструментів Spacecolon складається з трьох основних компонентів Delphi – ScHackTool, ScInstaller і ScService, які дозволяють встановлювати віддалений доступ, розгортати додаткові інструменти та навіть запускати атаки програм-вимагачів.

ScHackTool, діючи як координатор, керує розгортанням ScInstaller і ScService.

Єдиною метою ScInstaller є встановлення ScService, який функціонує як бекдор, дозволяючи програмі-агресору виконувати команди, завантажувати корисні дані та отримувати інформацію про систему.

Окрім цих основних компонентів, оператори Spacecolon значною мірою покладаються на ряд сторонніх інструментів, як законних, так і зловмисних, які доступні на вимогу.

Після компрометації уразливого вебсервера кіберзлочинці розгортають ScHackTool. Цей основний компонент дозволяє хакерам управляти атакою, завантажуючи та запускаючи додаткові інструменти на пристрої. Якщо ціль вважається цікавою, зловмисники можуть розгорнути інші інструменти, які забезпечують подальший віддалений доступ.

Останньою розгортається версія програми-вимагача Scarab. Цей варіант може внутрішньо розгортати ClipBanker, шкідливе програмне забезпечення для відстеження та зміни вмісту буфера обміну, який може бути адресою гаманця криптовалюти, на адресу зловмисників.

Оскільки програмне забезпечення-вимагач робить кібербезпеку більш важливою, ніж будь-коли, більшість компаній прийняли принцип «поглибленого захисту». Це передбачає впровадження брандмауерів, захисту кінцевих точок, безпеки додатків і API, захисту даних, захисту від фішингу, безпеки Інтернету речей (IoT) і, можливо, навіть блокування комутаторів.

Організаціям та установам будь яких галузей варто усвідомити, що у них є два шляхи. Перший - чекати, поки відбудеться атака, і вже потім намагатися врятувати свої системи. Другий – завчасно шукати недоліки, серед іншого - і за допомогою фахівців державних установ, запроваджувати ефективну систему захисту та знижувати ймовірність успішної атаки до прийнятного рівня.

Кіберпростір не має кордонів, тому незалежно від регіону ви можете зазнати атаки з боку хакерів. І це спільна проблема, яка стосується і держави, і бізнесу, і громадських організацій, і ЗМІ та всіх інших. Тому неабияк важливо забезпечити ефективне співробітництво і разом працювати над посиленням стійкості, як впроваджуючи передові практики, так і активно доносячи інформацію про можливість застосування різних інструментів та підходів.

УДК 623.746.519

Бордунова К.І., Іванов Б.В.

ПРОБЛЕМНІ АСПЕКТИ ЗАСТОСУВАННЯ БПЛА СИЛАМИ БЕЗПЕКИ ПІД ЧАС ВИКОНАННЯ СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ

До проблемних аспектів застосування безпілотних літальних апаратів (БПЛА) силами безпеки під час виконання службово-бойових завдань можна віднести:

– збір, зберігання і обробка інформації, отриманої за допомогою БПЛА, потребує високого рівня захисту даних від несанкціонованого доступу;

– високі вимоги до надійності БПЛА. Відмови в роботі БПЛА можуть виникати під час їх експлуатації, що може вплинути на успішність виконання завдань;

– наявність відповідної підготовки та навичок особового складу для ефективного застосування БПЛА;

– відсутність чіткої юридичної бази для застосування БПЛА у відповідності до міжнародного та національного законодавства, зокрема щодо ведення бойових дій та збору інформації;

– недостатній рівень стандартизації та вдосконалення технічних засобів комунікації та обміну даними.

До окремого класу проблем БПЛА можна віднести навмисний вплив засобів радіоелектронної протидії на БПЛА. На сьогоднішній день відомі основні методи впливу за-

собів радіоелектронної протидії на БПЛА, умовно їх можна поділити на декілька категорій, що включають:

– методи впливу на сигнали управління БПЛА. Перехоплення радіосигналів, які використовуються для керування БПЛА (спуфінг). Це може призвести до втрати контролю над апаратом або зміни його маршруту;

– методи перешкоджання радіоканалу керування БПЛА. Засоби радіоелектронної протидії створюють інтерференцію на радіоканалі, що використовується для зв'язку з БПЛА. Це може призвести до втрати зв'язку або до нестабільної роботи БПЛА;

– методи інтелектуального змішування сигналів, щоб утруднити розпізнавання та виявлення радіосигналів, що відносяться до БПЛА.

– джаммінг GPS-сигналів. Системи радіоелектронної протидії створюють перешкоджання GPS-сигналам, які використовуються для навігації БПЛА. Це може спричинити втрату точності місцезнаходження та навігації;

– зміна параметрів радіосигналів, що використовуються для управління БПЛА, наприклад, зміна частоти або потужності сигналу;

– використання різних типів антенних систем для забезпечення ефективної роботи в різних умовах і для забезпечення максимальної зони покриття.

Ці методи впливу засобів радіоелектронної протидії на БПЛА використовуються для забезпечення контролю над радіоелектронним середовищем та зниження ефективності використання БПЛА.

Захист БПЛА від радіоперешкод включає в себе кілька стратегій та технологій:

– частотна розгортка. БПЛА може використовувати алгоритми частотної розгортки, що дозволяє змінювати частоту передачі сигналів з певною періодичністю. Це ускладнює процес перехоплення або перешкоджання радіосигналів;

– шифрування сигналів. Використання шифрування даних та комунікаційних сигналів дозволяє захистити інформацію що передається від несанкціонованого доступу або перехоплення;

– використання антенних систем. БПЛА може мати раціонально побудовані антенні системи, які забезпечують високу направленість та ефективність прийому та передачі сигналів, що допомагає у зменшенні впливу радіоперешкод;

– алгоритми самовиправлення. БПЛА може мати вбудовані алгоритми самовиправлення, які дозволяють автоматично виявляти та коригувати помилки або перешкоди у радіоканалі (коди з виправленням помилок);

– використання альтернативних комунікаційних каналів. Деякі БПЛА можуть мати можливість використовувати альтернативні комунікаційні канали, такі як оптичні або супутникові, що зменшує вразливість до радіоперешкод;

– фізичний захист. Крім захисту комунікаційних сигналів, важливо також забезпечити фізичний захист самого БПЛА від несанкціонованого доступу та пошкоджень.

Ці стратегії та технології дозволяють забезпечити ефективний захист БПЛА від радіоперешкод та зберегти його функціональність під час виконання службово-бойових завдань.

УДК 004.056.53

Ботвінчук В.І., Данилов А.Д.

ЗАХИСТ ВІД АТАК МЕТОДОМ ВИКРАДЕННЯ СЕСІЙ

Атака викрадення сесій є однією з найбільш поширених загроз веб-безпеці. Під час такої атаки зловмисник може отримати доступ до сесійних ключів, що дозволить йому

використовувати сесію або виконувати дії від імені користувача без його дозволу. Атаки можуть призвести до крадіжок особистої інформації, фінансових втрат, зниження довіри до компанії або бренду, і втрати користувачів. Такі атаки можуть також вплинути на репутацію організації і призвести до втрати довіри від зацікавлених сторін.

Викрадення сеансу − це тип атаки, коли зловмисник отримує контроль над дійсним сеансом користувача у веб-програмі. Зловмисник може використовувати це, щоб отримати доступ до конфіденційної інформації, виконати несанкціоновані дії або припустити особу жертви. Викрадення сеансу можна здійснити за допомогою різних методів, зокрема перехоплення мережевого трафіку, викрадення файлів cookie сеансу або використання вразливостей у веб-додатку чи базовому стеку програмного забезпечення. Зловмисник перехоплює ідентифікатор сеансу та використовує його, щоб видати себе за жертву та виконувати дії від її імені, змінювати налаштування облікового запису або викрадення конфіденційної інформації. Викрадення сеансу може статися через уразливості веб-додатків або через незахищені мережеві з'єднання. Важливо впровадити заходи безпеки, щоб запобігти атакам захоплення сеансів:

1 використання HTTPS: За допомогою протоколу HTTPS (Hypertext Transfer Protocol Secure), всі дані, що передаються між браузером і сервером, шифруються. Це забезпечує, що навіть якщо зловмисник використовує методи вимірювання засідок (man-in-the-middle), він не зможе переглядати або змінювати дані, що передаються;

2 використання безпечних куків (secure cookies): Застосування безпечних куків дозволяє браузеру вимагати, щоб куки, які відправляються до сервера, були шифровані за допомогою протоколу HTTPS. Це унеможливлює зловмисникам читати або змінювати ці куки, якщо вони були викрадені;

3 використання двофакторної автентифікації: Двофакторна автентифікація вимагає від користувача не тільки пароля, але й додаткового підтвердження, такого як одноразовий код, який надсилається на мобільний телефон або інший вторинний канал. Це дозволяє ускладнити атакам викрадення сесій, оскільки зловмисники будуть мати потребу в крадіжці не тільки пароля, але й доступу до додаткового підтвердження;

4 моніторинг активності користувача: Великі організації часто використовують системи моніторингу активності користувачів для виявлення незвичних паттернів поведінки, що можуть вказувати на атаки викрадення сесій або інші види атак;

5 захист від уразливостей: Важливо регулярно оновлювати програмне забезпечення, використовувати відомі уразливості та встановлювати заходи безпеки, які мінімізують ризики викрадення сесій.

Ці методи можуть допомогти у підвищенні безпеки веб-додатків та захисті від атак методом викрадення сесій. Важливо також зазначити, що безпека веб-додатків є постійною боротьбою, і важливо використовувати комбінацію різних методів захисту та постійно вдосконалювати інфраструктуру захисту.

Бурцева В.В., Григорчук Р.В., Рарог Р.М.

ПЕРСПЕКТИВИ РОЗВИТКУ ПІДСИСТЕМИ ЦІЛОДОБОВОГО СЕРВІСУ НАДАННЯ ТОЧНОГО ЧАСУ В УМОВАХ ВОЄННОГО СТАНУ

В умовах збройної агресії російської федерації існує потреба забезпечення та контролю управління передаванням еталонних сигналів часу та частоти (далі – ЕСЧЧ), оскільки навіть короткочасне виведення з ладу, внаслідок постановки перешкод або підміни координат сигналу глобальних навігаційних супутникових систем (далі – ГНСС), може призвести до зниження ефективності або, взагалі, невиконання бойових завдань. Безперечно, ГНСС здатна забезпечувати високу точність під час вимірювання частоти, фази та часу, однак її використання супроводжується низкою недоліків, серед яких:

зниження продуктивності через погані погодні умови; вразливість до перешкод, що призводить до інтерференції сигналу, та поганий прийом в разі обмеженого огляду неба. Відсутність належної завадостійкої апаратури приймачів сигналів та контролю навігаційного поля обумовлює використання в якості основного ешелону передавання еталонних сигналів від еталонів часу та частоти через волоконно-оптичні лінії зв'язку.

Для успішного вирішення проблеми, в умовах ведення сучасних бойових дій, пропонується розглянути питання проведення територіального розподілу елементів системи частотно-часового забезпечення Збройних Сил України, шляхом створення пунктів цілодобового контролю та управління передаваням ЕСЧЧ в регіональних метрологічних військових частинах, в якості резерву, з єдиним центром управління у військовій частині А0785. Механізм взаємодії суб'єктів передбачено здійснювати за допомогою транспортних протоколів UDP та TCP/IP, оптоволоконною мережею рівня L2 або радіоканалів, що захищені методами сучасної криптографії, за умов використання серверу точного часу Microsemi Timeprovider 4100. Дослідження, проведені в рамках науково-дослідних робіт підтверджують можливість передавання еталонних сигналів часової та частотної синхронізації із застосуванням оптоволоконних технологій від військового еталону одиниці часу та частоти до обладнання, встановленого в Головному інформаційно-телекомунікаційному вузлі ЗС України, з похибкою передавання менше ніж 10 мкс на відстань 600 км. Тому, пропонується провести дослідження можливостей передавання еталонних сигналів за допомогою протоколу PTP IEEE1588v2 на маршруті Харків – Біла Церква (в/ч А4533) з оцінюванням похибки, за умов розповсюдження пакетів даних, використовуючи асинхронні канали передавання та близько 15 вузлів комутації.

Відповідно до Плану виконання заходів з реалізації першого етапу Концепції створення та розвитку системи контролю частотно-часового забезпечення Збройних Сил України, здійснюється формування проміжного переліку споживачів ЕСЧЧ. Слід зазначити, що в умовах сьогодення існує нагальна потреба оперативного контролю та забезпечення даними сигналами: серверів цифрових систем і засобів зв'язку, автоматизованих систем управління, передавання і обробки інформації, систем оперативного управління військами, випробувально-вимірювальних комплексів та геопросторового забезпечення. На даний час, від Держспецзв'язку отримано запит про нарощування спроможностей та розгортання Центру обробки даних ядра захищеної мультисервісної IP-платформи, внаслідок чого виникає потреба в передаванні еталонного сигналу часу та частоти серверам ЦОД Управління. Процес формування ускладнюється через відсутність нормативної основи системи контролю частотно-часового забезпечення ЗС України, що, в свою чергу, визначає необхідність розроблення низки нормативних документів, які будуть регламентувати порядок взаємодії суб'єктів та реалізацію політики використання ЕСЧЧ та сигналів ГНСС.

УДК 621.39

Ваврічен О.А., Городиський Р.О.

ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ ВОЛЗ ПРИ СТВОРЕННІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У зв'язку з особливостями технології обміну даними, характером сигналів та умовами передачі, волоконно-оптичні лінії зв'язку (ВОЛЗ) вважаються найбільш захищеними від зовнішнього втручання системами з підвищеною конфіденційністю. Це пояснюється повним внутрішнім відображенням електромагнітного випромінювання при проходженні через оптичне волокно і закономірним зменшенням інтенсивності поза його

межами, що легко виявити. На даний час існують дві основні категорії несанкціонованого підключення до ВОЛЗ, відомі як «fiber tapping». Перша категорія включає способи, що передбачають відрізання оптичного волокна для подальшого підключення через спеціальний пристрій для зчитування інформації. Друга категорія включає методи, які порушують передачу сигналу в оптичному волокні, що призводить до переривання потоку даних без обов'язкового відрізання волокна.

Після аналізу цих методів стає очевидною необхідність розробки та впровадження засобів захисту для уникнення несанкціонованого доступу до ВОЛЗ, що є важливою науковою задачею [1].

Кожен з методів несанкціонованого зняття інформації має свої слабкі сторони, які дозволяють оперативно визначати і локалізувати точки стороннього впливу на ВОЛЗ. При використанні пасивних методів зловмисники використовують посилення тієї невеликої частини розсіяного випромінювання, яка природним чином проникає за межі волокна. Проте несанкціонований доступ за таким підходом можливий лише на обмеженій кількості ділянок волокна з посиленим бічним випромінюванням: місця вигинів, зварювання, з'єднань волокон зі стаціонарним обладнанням в комутаційних центрах.

Активні методи передбачають фізичні зміни стану волокна, щоб змінити параметри передаваних сигналів. Наприклад, це може включати шліфування, механічне згинання, підключення розгалужувачів, вдавлення зондів, безконтактне під'єднання, розчинення оболонки. Ці зміни ведуть до зміни енергетичних, структурних і хвильових характеристик сигналу і хвиль (падіння потоку, відбиття хвиль, зміна модової структури хвиль), що спрощує виявлення несанкціонованого доступу за допомогою спеціальних діагностичних і систем безпеки для ВОЛЗ.

При виявленні зниження рівня потужності оптичних сигналів, що може вказувати на виникнення несанкціонованого доступу, приймається рішення про перенаправлення інформаційних потоків на інші маршрути передачі. Це важливо для забезпечення точності методу, і для цього необхідно підтримувати постійний рівень потужності оптичних сигналів у волоконно-оптичних лініях зв'язку, використовуючи певний тип кодування, який не залежить від характеру передаваної інформації.

Зниження контрольованого рівня потужності оптичних сигналів спричиняє спрацювання аварійної сигналізації. Ефективним способом виявлення несанкціонованого підключення до волоконно-оптичних ліній зв'язку є використання оптичних рефлектометрів, які дозволяють аналізувати розсіяне випромінювання в зворотному напрямку. Рефлектометричний метод полягає в тому, що в ОВ подається короткий імпульс, а потім реєструється випромінювання, яке розсіялося на різних неоднорідних ділянках ОВ. Це дозволяє визначати розподілені втрати потужності оптичного сигналу на всій його довжині до 120 км. Порівняння еталонних рефлектограм з поточними дозволяє забезпечити контроль захищеності ВОЛЗ з точністю до локального відхилення рефлектограм не більше ніж на 0,1 дБ.

Ще один варіант захисту інформації у ВОЛЗ базується на використанні волокна із підвищеним коефіцієнтом гнучкості. Захист ОВ з низькими втратами і великим допустимим радіусом вигину, полягає у обмеженні високих втрат, що виникають під час згинання або проколювання волокна. Використання такого волокна також зменшує вплив витягування, перекручування та інші фізичних видів впливу на оптичне волокно [3].

Програмний метод захисту базується на використанні протоколів шифрування на третьому та другому рівнях. Протокол IPSec є прикладом шифрування на третьому рівні, яке реалізовується на приймальній стороні (стороні користувача), що може призводити до додаткових затримок у роботі телекомунікаційного обладнання. Він реалізований на стороні користувача, тому він викликає деякі затримки обробки. Протокол піднімається на початку сесії, і загальна реалізація може бути дуже складною, якщо задіяно велику кількість мережевих елементів. Використання шифрування на другому рівні звільняє елементи третього рівня від цієї функції [2].

Один із джерел шифрування на другому рівні – це технологія оптичного кодового мультиплексування CDMA (Code Division Multiple Access). Ймовірність перехоплення інформації залежить від кількох параметрів, включаючи відношення сигнал-шум, доступну системну пропускну здатність. Ймовірність успішного захоплення даних залежить від кількох факторів, таких як відношення сигнал / шум і рівень фрагментації доступної системної ємності. Збільшення складності кодування підвищує вимоги до відношення сигнал / шум, необхідного для зламання кодування лише на кілька децибел. У той же час, обробка менше ніж 100 біт з боку зловмисника може суттєво знизити відношення сигнал / шум на 12 дБ.

Перехід між довжинами хвиль та розподіл сигналу в часі, зокрема використання множинного доступу з кодовим поділом (CDMA), забезпечують достатній рівень конфіденційності, проте це високо залежить від системного дизайну та параметрів реалізації.

Також важливо відзначити метод, що базується на використанні режиму динамічного (детермінованого) хаосу. Цей метод дозволяє передавати інформацію з псевдовипадковою зміною частоти та амплітуди носійної хвилі. Це призводить до того, що вихідний сигнал стає шумоподібним, що ускладнює його розшифрування.

Методи третього типу теоретично можуть бути більш схованими. Проте їхня ефективність низька, а впровадження вимагає значних витрат. Синхронізація бічного виведення випромінювання та зворотної компенсації потужності повинна відбуватися одночасно для приховування факту вторгнення. Проте на практиці точна синхронізація через особливості розподілу параметрів волокна є практично недосяжною сучасними технічними засобами.

Для ефективного захисту волоконно-оптичних ліній зв’язку необхідно застосовувати комбіновані методи захисту оптичних інформаційних потоків, які поєднують в собі як апаратні, так і програмні засоби. Один з таких методів ґрунтується на моніторингу контрольних сигналів, що передаються по додатковим оптичним волокнам, розташованим навколо робочого оптичного волокна. Для реалізації цього методу необхідно мати додатковий волоконно-оптичний кабель, що підвищує вартість ВОЛЗ. Однак це дозволяє вести моніторинг рівня потужності оптичного сигналу, і при спробі зігнути або пошкодити цей кабель відбудеться втрата потужності контрольного сигналу, що спричинить спрацювання сигналу тривоги.

Отже волоконно-оптичний зв’язок становить серйозну загрозу національній безпеці, фінансовим інститутам, особистому життю і свободам. Після підключення до нього, отримана інформація може бути використана різними способами залежно від мотивації і технічних можливостей зловмисника. Крім отримання інформації з оптичного волокна, існують різні методи, які дозволяють вставляти в нього інформацію, такі як поділ на неоднорідні хвилі, а також можливість викликати помилкову інформацію або додавати неправдиві дані. Легкість прослуховування fiber вимагає прийняття певних запобіжних заходів.

Список використаних джерел

1. Манько О, Шматок О., Петренко А. Використання пасивних оптичних пристроїв для захисту інформації у волоконно-оптичних лініях зв’язку та мережах. *Захист інформації.* 2017. том 19, №2, квітень-червень. С 143–147.

2. Мохунь І. І., Вікторовська Ю. Ю., Галушко Ю. К. Оптичні технології в інформаційній техніці. Чернівці: Чернів. нац. ун-т, 2021. 301 с.

3. Рахимов Н. Р. Сучасні методи розробки інформаційної безпеки ВОЛЗ. *Автоматика та програмна інженерія.* 2015. №4. С. 85–89.

Васильцова Н.В.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВИРІШЕННЯ ЗАДАЧІ ВЕДЕННЯ СТАЖУ РОБОТИ СПІВРОБІТНИКІВ ВІЙСЬКОВИХ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

В сучасних політичних і економічних умовах, в яких існує наша держава, велике значення приділяється розвитку військової освіти, яка є складовою частиною загальнодержавної системи освіти. Система військової освіти складається з органів управління та мережі вищих військових навчальних закладів (ВВНЗ), військових навчальних підрозділів закладів вищої освіти (ВНП ЗВО), закладів фахової передвищої військової освіти (ЗФПВО) і військових ліцеїв [1].

Освітня діяльність у ВВНЗ, ВНП ЗВО, ЗФПВО та військових ліцеях здійснюється відповідно до вимог національного законодавства, європейських стандартів та євроатлантичних стандартів щодо забезпечення якості освіти.

До ЗВО, які здійснюють військову підготовку, включаються: ЗВО із специфічними умовами навчання, що належать до сфери управління Міністерства внутрішніх справ України; ЗВО Державної прикордонної служби України, ЗВО Державної служби України з надзвичайних ситуацій; ЗВО Національної гвардії України [2].

В умовах функціонування ЗВО ключове становище у ресурсному потенціалі управління займає персонал (кадри), який визначає успіх таких закладів у досягненні їх цілей. Кадровий потенціал управління державними ЗВО є складовою, що знаходиться в постійному розвитку, з відкритою структурою, що об'єднує працівників з різними професійно-кваліфікаційними характеристиками, зі складною системою вертикальних і горизонтальних взаємозв'язків між елементами структури. Тому вирішення проблеми управління таким складним об'єктом, яким є персонал ЗВО, вимагає реалізації сучасних методів управління, що ґрунтуються на всебічній інформатизації, і є ключовим моментом усієї перебудови системи управління ЗВО.

У сучасних ЗВО процеси обґрунтування, вироблення, прийняття та реалізації управлінських рішень з урахуванням сучасних технологій управління персоналом насамперед потребують повнофункціонального інформаційного забезпечення системи управління персоналом (СУП), яке полягає у здійсненні процесів збору, обліку, систематизації та вивченні відомостей, що характеризують систему управління. Автоматизація даних процесів у межах інформаційного забезпечення СУП визначає основні якісні та кількісні характеристики всього процесу управління персоналом [3].

Аналіз СУП різних організацій показав, що у теперішній час склалася типова структура управління персоналом, що включає підсистему загального та лінійного керівництва, функціональні підсистеми. Однією з функціональних підсистем, що широко розвиваються, є підсистема інформаційного забезпечення СУП [3], [4].

Функції щодо реалізації інформаційного забезпечення СУП у будь-якій великій організації зазвичай виконуються відділами кадрів (службами управління персоналом). Однак на цей підрозділ найчастіше не покладається рішення цілого ряду завдань з управління персоналом, до яких входять: завдання оцінки та підбору кандидатів на вакантні посади, аналіз кадрового потенціалу та потреби в персоналі, планування та контроль ділової кар'єри. Однак саме цей підрозділ здійснює основні інформаційні функції, пов'язані з обліком кадрового складу та веденням його статистики, на основі яких приймаються управлінські рішення щодо персоналу організації [4].

Аналіз кадрової роботи великої організації, якою є державний ЗВО, показав, що задачі обліку кадрів, прийому на роботу, звільнень та переведень, переміщення співробітників у рамках трудової діяльності потребують першочергової автоматизації. Формально облік, аналіз та контроль трудової діяльності співробітника є складовою задачі розрахунку, аналізу та контролю стажу (ведення стажу) роботи. Найчастіше задачі розрахунку, аналізу та контролю стажу в існуючих інформаційно-управляючих системах

ЗВО вирішується таким чином. Облік переміщення працівників у межах трудової діяльності та розрахунок стажу здійснюється працівником відділу кадрів один раз на певну дату. Подальший розрахунок може здійснюватись вручну або автоматизованим способом шляхом додавання відповідної кількості днів до дати проведення першого розрахунку. Цей алгоритм є простим, проте досить жорстким щодо аналізу переміщень співробітника у межах діяльності. Він не дозволяє здійснити контроль розрахунку стажу, а також розрахунок стажу співробітника на ту дату, яка є меншою за дату першого розрахунку.

Задача розрахунку, аналізу та контролю стажу співробітника ЗВО є однією з основних обліково-розрахункових задач, а також є однією з основних функціональних елементів підсистеми інформаційного забезпечення СУП. Аналіз існуючих способів автоматизованого розв'язання цієї задачі в рамках інформаційних систем організацій показав низькі якісні характеристики її практичного використання через відсутність формального підходу до вирішення.

Специфіка діяльності ЗВО, які розглядаються в роботі, вимагає здійснювати автоматизований розрахунок, контроль та аналіз одночасно кількох видів стажу співробітника (загального стажу; стажу роботи, пов’язаного з військовою службою; педагогічного і науково-педагогічного стажу; стажу роботи в даній організації; стажу роботи для оформлення листа непрацездатності тощо), використовуючи типовий підхід (алгоритм розрахунку стажу) та визначену інформаційну технологію. Вирішення задачі таким способом має дозволити проводити гнучкі розрахунки стажу співробітника на будь-яку дату, призначену користувачем.

Задачу ведення стажу пропонується вирішувати у два етапи. Перший етап пов'язаний із прийняттям рішення про віднесення заданого виду діяльності (трудова діяльність в організації, військова служба, навчання у ЗВО тощо) до певного виду стажу, а також безпосереднього розрахунку даного виду стажу.

Однією з проблем, що потребує вирішення на даному етапі, є існування різних за формою та змістом видів «первинних» документів, що підтверджують діяльність людини за певний період. До таких документів належать: трудова книжка, військовий білет, диплом про освіту, дипломи, які підтверджують вчене звання та науковий ступінь тощо. Інформація (дані) про трудову діяльність зберігається у документах у неформалізованому вигляді.

В рамках інформаційної технології, що розробляється, перший етап розв'язання задачі заснований на використанні експертних оцінок. Як експерт виступає працівник відділу кадрів. Експертному оцінюванню підлягає інформація про трудову діяльність співробітника, аналіз якої дозволить сформувати вихідні дані для формалізованого розрахунку стажу.

Аналіз документів, які підтверджують трудову діяльність співробітника, показав, що з усієї інформації, що зберігається в документах, можуть бути виділені типові елементи (показники), що дозволяють проводити їх порівняння, класифікацію та розрахунок. Такими типовими показниками є дати: початку трудової діяльності на певній посаді; початку військової служби; початку навчання у навчальному закладі; переведення на іншу посаду; звільнення з посади; закінчення навчального закладу; а також посаду, яку посідав співробітник за період своєї трудової діяльності; причини звільнення з посади; статус діяльності (основна робота, робота за сумісництвом); організація чи підрозділ, у якому працював чи працює співробітник.

Аналіз сукупності типових показників, що належать до певного виду діяльності та складають запис у базі даних, дозволяє ухвалити рішення про віднесення цього запису до певного виду стажу. Цей запис маркується і може брати участь в автоматизованих розрахунках тих видів стажу, до яких вона була віднесена. Далі розрахунок стажу здійснюється звичайним способом з урахуванням порівняння відповідних дат. При зміні законів, згідно з якими розраховується певний вид стажу, або здійсненні помилки при

віднесенні запису до певного виду стажу, маркування легко може бути знято або змінено. Основний алгоритм розрахунку стажу при цьому не змінюється.

Другий етап вирішення задачі ведення стажу, у свою чергу, може бути розбитий на два підетапи, на яких відповідно вирішується дві підзадачі, і полягає в тому, що на основі інформації, що отримується при розрахунку стажу, приймається дві групи рішень щодо використання отриманих на першому етапі кількісних результатів.

Даний етап розв'язання задачі заснований на діючій в даний час кадровій політиці. Вирішення першої підзадачі пов'язане з обов'язковим виконанням загальнодержавної кадрової політики, яка виражається в існуючих юридичних законах, що закріплюють типові структури організацій, принципи підбору та розміщення кадрів, методики оцінки ефективності використання кадрів на загальнодержавному рівні. Вихідними даними для реалізації положень цих законів є певний вид трудового стажу, представлений у кількісному вигляді. До таких законів можуть бути віднесені (наприклад): закон про порядок виплати надбавок за вислугу років; закон про нарахування заробітної плати за листком непрацездатності тощо.

Особливістю вирішення першої підзадачі є закладений у структурі та змісті закону, як юридичного документа, формальний підхід до її вирішення. Формалізація у даному випадку здійснюється на змістовному рівні, проте дозволяє розробити чіткий однозначний алгоритм вирішення підзадачі.

Вирішення другої підзадачі пов'язане з внутрішньовиробничим аспектом здійснення кадрової політики, тобто з особливостями функціонування організації, з прийняттям рішень на основі традицій, інтуїції керівників, колективу, що склалися в організації.

Інформаційна технологія виконання задачі ведення стажу, що розробляється в роботі, дає можливість: здійснити візуальний контроль проведення розрахунків стажу; коригувати вихідні дані для розрахунку стажу співробітників без зміни основного алгоритму розрахунку, враховуючи існуючу загальнодержавну чи внутрішню кадрову політику. Вона призначена для проведення розрахунків та контролю всіх видів стажу роботи співробітників ЗВО та підготовки документів, що підтверджують цей стаж.

Запропонований алгоритм та інформаційна технологія вирішення задачі ведення стажу роботи співробітників ЗВО в рамках інформаційної підсистеми СУП є типовими і можуть бути використані для вирішення подібних задач у будь-якій організації. Довідник видів стажу, що розраховуються, може бути легко відкоригований відповідно до особливостей конкретних організацій і установ.

Результати вирішення цієї задачі необхідні для кадрового планування у ЗВО (планування потреби в персоналі, вивільнення або скорочення персоналу, використання персоналу, планування навчання, ділової кар'єри, службово-професійного просування, планування витрат на персонал).

Список використаних джерел

1. Міністерство оборони України. Офіційний сайт URL: https://www.mil.gov.ua/diyalnist/vijskova-osvita-na-tauka/ (дата звернення: 1.03.2024)

2. Освітньо-науковий портал Міністерство внутрішніх справ України URL: https://osvita.mvs.gov.ua/educational-institutions (дата звернення: 01.03.2024)

3. Управління персоналом: підручник / О.М. Шубалий, Н.Т. Рудь, А.І. Гордійчук та ін. Луцьк: ІВВ Луцького НТУ, 2018. 404 с.

4. Технології управління персоналом: монографія / О.А. Гавриш, Л.Є. Довгань, І.М. Крейдич, Н.В. Семенченко. Київ: КПІ ім. Ігоря Сікорського, 2017. 528 с.

УДК 621.39:623.1/.7

Викиданець В.В., Овчаренко О.Ю., Моргун Є.В., Борисов В.В.

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ПІДВИЩЕННЯ СЛІДКУЮЧИХ ВИМІРЮВАНЬ ПЕРВИННИХ КООРДИНАТ БАГАТОКАНАЛЬНОЇ СТАНЦІЇ НАВЕДЕННЯ РАКЕТ 9С32

До складу багатоканальної станції наведення ракет **(**БСНР) 9С32 входить слідкуюча координатна система (СКС). СКС призначена для автоматичної селекції (супроводження) цілей і ракет по кутових положеннях і параметрах відбитого сигналу (часової затримки τ і допплерівському зсуву частоти F_g), а також для вимірювання поточних значень координат цілей і параметрів їх руху. Встановлено, що існуюча СКС не в повній мірі відповідає вимогам щодо супроводжування сучасних повітряних цілей, а саме цілей, які різко змінюють параметри руху (висоту, швидкість, напрямок руху і так далі) [1-6].

Наведений недолік потребує усунення для більш ефективного виконання ЗРК поставлених завдань, оскільки ці питання є актуальними для підвищення ефективності радіолокаційних станцій (РЛС), і як наслідок, зенітних ракетних комплексів (ЗРК).

Досліджувались сучасні засоби слідкуючих вимірювань кутових координат, дальності та радіальної швидкості (параметрів об’єктів, що можуть бути безпосередньо виміряні РЛС) [7-14].

Встановлено, що вони дозволяють вимірювати похідні другого та більш вищого порядку параметрів об’єктів.

Разом з тим, СКС більшості ЗРК ЗРВ ПС ЗС України здійснюють супроводження цілей лише по параметрах та швидкостях їх змін. Це пов’язано з застарілістю матеріальної бази більшості комплексів, що не дозволяє в існуючих цифрових пристроях обчислення разузгодження реалізовувати похідні більш вищого ступеня.

Наведені пропозиції щодо впровадження сучасної елементної бази, що дозволяє реалізувати цифрову фільтрацію параметрів об’єктів та їх похідних більшого ступеня.

Список використаних джерел

1. Dzhus, V., Roshchupkin, Y., Kukobko, S., Herasymov, S., Drob, N., & Trofymova, M. Estimation of noise radiance point sources multichannel direction finding systems resolution by linear prediction method. Sistemi obrobki ìnformacìï. 2021. № 4(167). С. 19-26. https://doi.org/10.30748/soi.2021.167.02

2. Седишев П.Ю. Однозначне оцінювання дальності рухомої цілі при її супроводженні по швидкості й кутових координатах радіолокатором з використанням когерентних сигналів з високою частотою повторення імпульсів / П.Ю. Седишев, А.О. Подорожняк, Є.С. Рощупкін // Наука і техніка Повітряних Сил Збройних Сил України. – 2009. – № 1(1). – С. 71-74. http://nbuv.gov.ua/UJRN/Nitps_2009_1_20

3. Герасимов С.В. Оцінка параметрів руху повітряних об'єктів при об'єднанні результатів незалежних первинних вимірювань в активній багатопозиційній системі радіолокації / С.В. Герасимов, Д.М. Ізосімов, Є.С. Рощупкін, О.М. Богдановський // Системи озброєння і військова техніка. – 2010. – №3. – С. 110-113. http://nbuv.gov.ua/UJRN/soivt_2010_3_28

4. Герасимов С.В. Оценка параметров движения маневрирующих воздушных объектов в активной некогерентной системе при обработке информации от нескольких неравноточных источников с разным темпом обзора пространства / С.В. Герасимов, Е.С. Рощупкин, Г.А. Федак, Я.В. Бабий // Військово-технічний збірник. – 2012. – № 1. – С. 18-26. http://nbuv.gov.ua/UJRN/vtzb_2012_1_6

5. Асавалюк А.В. Похибки визначення повного вектора швидкості в єдиній прямокутній системі координат системою оглядових станцій радіолокації с різною точністю / А.В. Асавалюк, С.В. Герасимов, Є.С. Рощупкін // Системи озброєння і військова техніка. – 2017. – № 2. – С. 53-56. http://nbuv.gov.ua/UJRN/soivt_2017_2_13

6. Рощупкин, Е.С. (2003). Уточненный алгоритм измерения координат источника излучения при обработке пространственной фазовой структуры принимаемого разнесенной корреляционно-базовой системой сигнала. Sistemi obrobki ìnformacìï, 2(24), 90–95. https://doi.org/10.5281/zenodo.5035861

7. Рощупкін Є.С. Великоапертурна (рознесена) радіолокаційна система: пат. 148518 Україна : G01S7/42, H01Q21/00 / Є.С. Рощупкін, С.В. Герасимов, С.В. Кукобко, М.В. Борисенко, Ю.О. Крихтін, О.Ф. Галицький, Б.В. Гайбадулов, В.В. Джус, І.В. Помогаєв, В.В. Борисов, Ю.О. Чміль, А.Ю. Задорожна. – u 202100336; заявл. 29.01.2021; опубл. 18.08.2021, бюл. № 33/2021, – 7 с.

8. Крючков, Д. М., Рощупкін, Є. С., Калита, О. В., & Дранник, П. А. (2023). Пропозиції щодо підвищення ефективності відновлення сукупності різнотипних радіоелектронних засобів спеціального призначення при їх використанні в різних умовах. XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023), Kharkiv. https://doi.org/10.5281/zenodo.10257044

9. Бєляєв, Д.М. Застосування векторних аналізаторів сигналів для забезпечення електромагнітної сумісності радіоапаратури / Д.М. Бєляєв, С.В. Герасимов, С.В. Кукобко [та ін.] // Збірник наукових праць ЦНДІ ОВТ ЗС України, - 2016. №3(62), -с. 77-84.

10. Tymchenko, S., Kaplun, Y., Roshchupkin, E., Kukobko, S. (2023). Substantiation of Time Distribution Law for Modeling the Activity of Automated Control System Operator. In: Shkarlet, S., et al. Mathematical Modeling and Simulation of Systems. MODS 2022. Lecture Notes in Networks and Systems, vol 667. Springer, Cham. https://doi.org/10.1007/978-3-031-30251-0_9

11. Рощупкин, Е.С. (2007). Ошибки определения прямоугольных координат источника излучения в пассивных гиперболических измерительных системах. Збірник наукових праць Об'єднаного науково-дослідного інституту Збройних Сил, 2 (7), 156–161. https://doi.org/10.5281/zenodo.5088597

12. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2005). Организация когерентной обработки на промежуточной частоте при приеме широкополосных сигналов крупноапертурными антенными решетками и многопозиционными системами. Прикладная радиоэлектроника, (Т.4, №4), 437-440.

13. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2006). Алгоритмы когерентной обработки широкополосных сигналов на промежуточной частоте с использованием схем фазонастраивающих контуров с управляемыми дисперсионными линиями задержки в крупноапертурных антенных решетках и многопозиционных системах. Прикладная радиоэлектроника, (Т.5, №2), 250-254.

14. Рощупкін, Є. С., Гречка, О. В., Галицький, О. Ф., & Гайбадулов, Б. В. (2023). Аналіз факторів, що впливають на ефективність відновлення різнотипних радіотехнічних засобів складної системи під час виконання завдань за призначенням в екстремальних умовах. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей тринадцятої міжнародної науково-технічної конференції. Том 1: секції 1, 3, 4, Баку-Харків-Жиліна. https://doi.org/10.5281/zenodo.7868194.

УДК 621.396.96

Вітрук Д.О., Райков Р.Ю.

ВИМОГИ СУЧАСНОСТІ ДО ПРОВЕДЕННЯ ОПЕРАТИВНИХ РОЗРАХУНКІВ ПРИ ПЛАНУВАННІ БОЙОВОГО ЗАСТОСУВАННЯ РАДІОТЕХНІЧНОГО ПІДРОЗДІЛУ

Досвід відсічі збройної агресії показує, що основним способом боротьбі російських збройних формувань з засобами радіолокації радіотехнічних військ Повітряних сил є ведення оптичної, радіотехнічної та радіолокаційної розвідки з безпілотних літальних апаратів (БПЛА) різного класу та подальше вогневе ураження артилерійськими та ракетно-артилерійськими засобами і ударними БПЛА (у тому числі “дронами-камікадзе”).

Одним з способів запобіганню втрат в особовому складі та ОВТ окремого радіолокаційного взводу (зведеного радіотехнічного підрозділу, зразка РЕТ) є зміна позиції після проведеної противником розвідки. За досвідом бойового застосування радіотехнічних військ, після виявлення в районі позиції розвідувальних БПЛА вогневий удар противника з використанням ударних БПЛА типу “Ланцет” або нанесення удару ракетами класу “повітря - поверхня” настає протягом 40-50 хвилин. Кількість передислокацій на запасні позиції може досягати до 3-5 разів на добу. Крім того передислокацію на запасні позиції здійснюють також і підрозділи, що забезпечуються радіолокаційною інформацією. Загалом зміна позицій призводить до змін деяких показників бойових можливостей окремого радіолокаційного взводу.

Командир окремого радіолокаційного взводу (зведеного радіотехнічного підрозділу, зразка РЕТ) при зміні позиції зобов’язаний провести розрахунки часу на марш, витрати пального, а у разі, коли підрозділ здійснює забезпечення бойових дій зенітних ракетних військ, винищувальної авіації, засобів РЕБ, мобільних вогневих груп, підрозділів ППО Сухопутних військ – провести розрахунки щодо змін бойових можливостей підрозділу з видачі бойової та розвідувальної інформації.

Крім того, зміна дислокації, кількісного та якісного складу засобів повітряного нападу противника, зміна тактики їх застосування, вимагають від командира радіотехнічного підрозділу проведення розрахунків щодо визначення бойових можливостей повітряного противника щодо нанесення ударів по об’єктам прикриття та угрупуванню військ (сил) в зоні відповідальності.

На підставі проведених розрахунків командир радіотехнічного підрозділу проводить оцінку обстановки та приймає рішення на виконання бойового завдання та надає пропозиції щодо бойового застосування старшому командиру.

Швидкоплинність сучасних бойових дій, вимоги щодо постійної бойової готовності, потребують від командира радіотехнічного підрозділу проведення всіх видів розрахунків в найкоротші терміни, при цьому без формального підходу та з необхідною точністю та достовірністю.

Єдиним шляхом вирішення проблеми підвищення оперативності проведення розрахунків є автоматизація цього процесу. Особливостями бойового застосування окремого радіолокаційного взводу (зведеного радіотехнічного підрозділу, зразка РЕТ) є виконання завдань в польових умовах, при відсутності промислової електромережі та без доступу до мережи інтернет. Тому використання ПЕОМ зі спеціалізованим програмним забезпеченням практично неможливо.

Тому є необхідність створення програмного додатку, якій не є енергоємним, інтуїтивно зрозумілим та може використовуватися в тому числі на смартфоні. Це дозволить командиру радіотехнічного підрозділу проводити тактичні розрахунки швидка та точно, ї, відповідно, своєчасно провести оцінку бойових можливостей свого підрозділу, надати старшому

командиру пропозиції щодо бойового застосування та безумовно виконати бойове завдання в умовах обстановки, що склалась.

Vlasov K.

SMARTPHONE PROTECTION SOFTWARE TO ENSURE THE PERSONAL SAFETY OF A MILITARY SERVICEMAN

In modern conditions, a military serviceman must ensure the integrity and confidentiality of information during combat missions and be aware of his personal responsibility for conducting conversations (correspondence) of an official nature using personal devices and electronic communication networks. This becomes extremely important as today's mobile devices are one of the easiest sources of intelligence. Therefore, it is necessary to comply with the requirements and rules for the use of personal devices and relevant software in order to save the life of a serviceman during combat missions.

All threats related to mobile devices can be divided into three categories, which are analyzed at the device level, the network level, and the application level. Each of these types has its own unique characteristics and methods of protection.

Threats at the device level arise from flaws in operating systems and drivers. All smartphones have basic security, but hackers are constantly looking for ways to bypass it. For this, they use exploits - special programs that use vulnerabilities in smartphone software.

Network-level threats use control over various protocols such as Wi-Fi, Bluetooth, USB cable, SMS messages and voice calls. For example, enemy intelligence professionals can use vulnerable wireless access points to act as an intermediary between a military servicemen's device and a server.

Application-level threats include the use of malware. Every day, iOS and Android app stores block hundreds of suspicious mobile apps. In addition to malware, there is also grayware, which can also pose a threat to the privacy of sensitive data.

In the field of cyber security, there are different groups of measures such as MTD (Mobile Threat Defense), MES (Mobile Endpoint Protection) and others. They are specially designed to protect smartphones from hacker attacks of various types.

Such device-level developments track the version of the operating system, device settings and systems installed on the smartphone. The main purpose of such solutions is to detect device weaknesses, notify about incorrect security settings, and promptly detect suspicious activities.

At the network level, developments monitor the traffic of wireless and mobile networks and provide the necessary measures in case of detection of malicious activity. For example, modern mobile applications can detect and block phishing attempts in SMS messages and e-mails.

At the application level, developers detect potentially malicious software for the device. Some high-end smartphone security solutions even disassemble applications to their source code, which allows you to detect most threats with almost 100% reliability.

Therefore, mobile security is not just about installing a single application. An effective solution should cover all levels, monitor and analyze devices, quickly eliminate threats, and warn users about potentially dangerous objects, web resources, and actions.

There are different approaches to protecting mobile devices at each level of their functioning:

– mobile endpoint protection (Endpoint Protection) is used at the device level. It is a software solution that helps identify user devices and manage data access in a corporate network.

– Phishing and Content Protection measures are applied at the e-mail and information level. These systems block both known phishing sites and potentially malicious resources.

– at the application level, risk control and compliance solutions (Mobile Risk and Compliance) and embedded application protection (Embedded App Defense) are used. These programs help detect violations of corporate rules and ensure compliance with compliance requirements.

– solutions for managing vulnerabilities and patch management of mobile devices are used at the network level (Mobile Vulnerability and Patch Management). These solutions allow version control of operating systems and mobile applications for timely updates.

Hence, there are various mobile security software products, each aimed at a certain level of protection. There is no universal program that provides analysis and monitoring of all possible threats.

Вороная С.М., Самелюк В.П., Козубцов І.М.

ПРО ПОТРЕБУ УДОСКОНАЛЕННЯ ПРОЦЕСУ ОБЛІКУ МАЙНА ВВНЗ В УМОВАХ ВОЄННОГО ЧАСУ

Постановка завдання. Облік майна є одним із завдань, що вирішується постійним складом військової частини, вищим навчальним закладом. Наявність достовірної облікової інформації є ключовою вимогою керівних документів, відповідно до яких організовано облік військового майна. Це Закони України [1, 2], Постанови Кабінету Міністрів України [3], Накази Міністерства оборони України [4–8] тощо. Вони обумовлюють, що облік майна повинен здійснюватися матеріально-відповідальною особою своєчасно, бути повним, достовірним і точним, за будь-яких обставинах. Тому реалізація цих вимог можлива тільки за допомогою своєчасно обдуманих процесів, прийомів та методів обліку, використанням спеціалізованого програмного забезпечення, сканерів штрих та QR- кодів.

Аналіз наукових досліджень виявив, що особливостям обліку військового майна, присвячена невелика кількість робіт [9–12]. Зважаючи на це, можна зробити висновок, що питання обліку військового майна в умовах воєнного стану сьогодні не вивчено. Отже, вимагають удосконалення, а іноді і розробки, питання побудови раціональної організації обліку майна у військових частинах у воєнний час.

Метою доповіді є акцент на потребі удосконалення процесу обліку майна ВВНЗ в умовах воєнного часу.

До інвентарного майна належать предмети, які знаходяться в експлуатації тривалий час і застосовуються багаторазово (прилади, інструменти, техніка тощо). Через це на інвентарні предмети встановлюються відповідні терміни експлуатації. Якісний стан інвентарного майна визначається за ступенями придатності.

До витратного майна та матеріальних засобів належать предмети, які витрачаються безпосередньо одноразово під час їх використання або приходять у непридатний стан під час відносно короткочасного застосування.

Майно та матеріальні засоби ЗСУ у мирний та воєнний час є державною власністю і незалежно від джерела надходження та способу придбання підлягають обов’язковому обліку, використанню за призначенням, економному та раціональному витрачанню.

Облік військового майна ведеться у кількісних, якісних, обліково-номерних та вартісних показниках за відповідною (визначеною) номенклатурою.

Вихідними документами для постановки на облік є накладні, вимоги, відомості, акти, атестати та інші документи, які призначені для оформлення і підтвердження здійснених господарських операцій, що пов’язані з рухом і зміною вартісного та якісного (технічного) стану військового майна. Це є підставою для записів облікових даних в

облікових регістрах.

Обліковими регістрами є книги, картки обліку військового майна, картки обліку майна особистого користування та інші носії спеціального формату (паперові, електронні), які призначені для відображення наявності, руху і якісного (технічного) стану такого майна (його вартості) за визначений період.

Аналіз наукових досліджень та досвід повсякденної діяльності дозволили констатувати, що технології обліку та носії інформації, які традиційно використовуються для ведення обліку майна та матеріальних засобів в умовах війни мають низку недоліків, основними з яких є:

– значна трудомісткість процедур створення облікових і обліково-заявочних документів, а також їх аналітичної та статистичної обробки;

– значна ймовірність пошкодження (втрати, несанкціонованого доступу тощо) технічних засобів і носіїв інформації;

– суттєві затрати часу на процес передачі до вище стоячого органу відповідної інформації і низька надійність цього процесу;

– відсутність автоматизованої системи обліку майна та матеріальних засобів у воєнний час із застосуванням засобів електронної обчислювальної техніки та сканерів штрих та QR- кодів;

– тривалий відрив постійного складу ВВНЗ від основного функціонального процесу на періодичні процедури інвентаризації;

-ускладнено процес дистанційної інвентаризації майна та матеріальних засобів, що видане у тимчасове користування та перебуває на час інвентаризації за межами ВВНЗ.

Висновки. Таким чином сучасний рівень розвитку комп'ютерних та інформаційно-комунікаційних технологій, а також нові вимоги до управління ресурсами майна визначають необхідність використання захищених засобів електронно-обчислювальної техніки та спеціалізованого програмного забезпечення для обробки облікових даних. Це повинно забезпечити автоматизацію облікових операцій щодо руху різних видів майна, визначення потреби, формування звітно-заявочних документів тощо.

Список використаних джерел

1. Про правовий режим майна у Збройних Силах України: Закон України від 21.09.1999 № 1075-XIV.

2. Про бухгалтерський облік та фінансову звітність в Україні: Закон України від 16.07.1999 № 996.

3. Про затвердження Положення про порядок обліку, зберігання, списання та використання військового майна у Збройних Силах: Постанова Кабінету Міністрів України; Положення від 04.08.2000 № 1225.

4. Про затвердження Положення про військове (корабельне) господарство. Наказ Міністерства оборони України від 16.07.1997 №300.

5. Про затвердження Інструкції з обліку військового майна у Збройних Силах України: Наказ Міноборони України від 17.08.2017 №440.

6. Про затвердження Порядку списання військового майна у Збройних Силах України та Державній спеціальній службі транспорту. Наказ Міністерства оборони України від 29.03.2021 № 81.

7. Національне положення (стандарт) бухгалтерського обліку в державному секторі 121 «Основні засоби»: Наказ Мінфін України від 12.10.2010 № 1202.

8. Національне положення (стандарт) бухгалтерського обліку в державному секторі 123 «Запаси»: Наказ Мінфін України від 12.10.2010 № 1202.

9. Бенько І. Особливості діяльності установ державного сектору економіки та їх вплив на організацію обліку. Облік, оподаткування і контроль: теорія та методологія: збірник матеріалів міжнародної наук.-практ. інтернетконф. (Тернопіль, 30 черв. 2017 р.). Тернопіль: ТНЕУ, 2017. С. 93–96.

10. Dachkovskyi V. The method of the optimization of material flows for functioning of the recovery system. Journal of Scientific Papers «Social Development and Security». 2020. Vol. 10, № 2. P. 27–34.

11. Легенчук С., Грицишен Д. Розвиток бухгалтерського обліку в умовах проведення воєнних дій: історичний аналіз. Вісник ЖДТУ. 2019. Вип. 2(88). С. 121–127.

12. Флорін О., Воронін О. Аналіз можливостей застосування інформаційних систем в інтересах побудови автоматизованої системи обліку майна зв'язку в частинах та підрозділах НГУ. Збірник наукових праць НАНГ України. 2017. Вип. 2(30). С. 69–75.

УДК 621.39:623.1/.7

Вурста К.І., Крючков Д.М., Скорик А.Б., Оборонов М.І.

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ЗАСТОСУВАННЯ ОПТИЧНИХ ЗАСОБІВ ДЛЯ ОРІЄНТУВАННЯ ТА ГОРИЗОНТУВАННЯ БОЙОВИХ ЗАСОБІВ ТА МЕТОДИКИ ЩОДО ЇХ ЗАСТОСУВАННЯ

Підвищення живучості та ефективності виконання поставлених завдань підрозділів зенітних ракетних військ Повітряних Сил Збройних Сил України суттєво залежить від швидкості та точності топоприв'язки та орієнтування бойових засобів зенітних ракетних комплексів на визначених не підготовлених позиціях [1-14].

У зв'язку з наведеним було проведено аналіз особливості орієнтування зенітного ракетного комплексу (ЗРК) С300В1. Орієнтування ЗРК С300В1 здійснюється у ручному режимі - без застосування апаратури навігації, топоприв'язки та орієнтування (АНТО), або автоматизовано - з її застосуванням.

При орієнтуванні в ручному режимі (без застосування АНТО) використовуються оптичні прилади (бусолі та інше), що потребує відносно великих витрат часу та не завжди забезпечує достатню точність в стислий термін.

В ході проведеного аналізу з'ясовано, що при розгортанні на не підготовлених позиціях після здійснення маршу з великим пройденим шляхом використання АНТО не завжди отримуються вихідні данні достатньої точності щодо орієнтування бойових засобів у просторі. В АНТО для урахування кутових напрямків використовується гірокомпас, який не схильний до впливу засобів радіоелектронної боротьби, але потребує постійного коригування при веденні маневреної протиповітряної оборони, що викликає додаткові витрати часу.

Недоліками існуючих засобів орієнтування (механічних гіроскопів) є:

- відносно низька точність у порівнянні з існуючими оптичними гіроскопічними засобами;
- необхідність постійного коригування результатів, що отримуються;
- великі вага та габарити.

Лазерні гіроскопи, що використовують ефект Саньяка, дозволяють при відносно компактних ваго-габаритних характеристиках у порівнянні зі штатними засобами, отримати потрібну для орієнтування інформацію з достатньою точністю без постійного корегування.

Лазерні далекоміри дозволяють вимірювати за малий час відстань з точністю до часток міліметра, що надає можливість оцінити взаємне орієнтування засобів розрахунковими методами.

Наведені пропозиції щодо використання вказаних засобів при орієнтуванні ЗРК.

Список використаних джерел

1. Маслов, А. Ф., Рощупкин, Е. С., Хмелевский, С. И., & Селевко, В. Н. (2002). Потенциальная точность измерения времени запаздывания путем учета фазовой структуры принимаемых разнесенными аппертурами сигналов. Збірник наукових праць, 3 (41), 83–85. https://doi.org/10.5281/zenodo.5525818

2. Маслов А.Ф. Ошибки измерения координат источника излучения при обработке пространственной фазовой структуры принимаемого разнесенной корреляционно-базовой системой сигнала / А.Ф. Маслов, Е.С. Рощупкин, О.П. Колодей // Системи обробки інформації. – 2003. – № 1(23). – С. 125-138. http://nbuv.gov.ua/UJRN/soi_2003_1_21

3. Рощупкин, Е. С. (2003). Уточненный алгоритм измерения координат источника излучения при обработке пространственной фазовой структуры принимаемого разнесенной корреляционно-базовой системой сигнала. Sistemi obrobki ìnformacìï, 2(24), 90–95. https://doi.org/10.5281/zenodo.5035861

4. Бурковський, С.І., Рощупкін, Є.С., & Шрамков, А.Ю. (2004). Вплив похибок визначення координат виносних пунктів пасивної багатопозиційної системи на точність вимірювання координат джерела випромінювання. Збірник наукових праць XI ВПС, 2(11), 103–108. https://doi.org/10.5281/zenodo.5088274

5. Сухаревский О.И., А.Ю. Шрамков & Рощупкин Е.С. (2005). Высокочастотный метод расчета диаграммы направленности антенны с учетом неоднородностей рельефа местности на позиции РЛС. Моделювання та інформаційні технології, (33), 174-181.

6. Рощупкин, Е.С., & Беляев, Д.Н. (1999). Измеритель коэффициента стоячей волны в виде ответвителя дециметрового диапазона волн. Збірник наукових праць за матеріалами 3-го міжнародного молодіжного форуму "радіоелектроніка і молодь у XXI столітті" 20-23 квітня 1999 р., 1, 52–55. https://doi.org/10.5281/zenodo.5591877

7. Крючков, Д. М., Рощупкін, Є. С., Калита, О. В., & Дранник, П. А. (2023). Пропозиції щодо підвищення ефективності відновлення сукупності різнотипних радіоелектронних засобів спеціального призначення при їх використанні в різних умовах. XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023), Kharkiv. https://doi.org/10.5281/zenodo.10257044

8. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2006). Алгоритмы когерентной обработки широкополосных сигналов на промежуточной частоте с использованием схем фазонастраивающих контуров с управляемыми дисперсионными линиями задержки в крупноапертурных антенных решетках и многопозиционных системах. Прикладная радиоэлектроника, (Т.5, №2), 250-254.

9. Бєляєв, Д.М. Застосування векторних аналізаторів сигналів для забезпечення електромагнітної сумісності радіоапаратури / Д.М. Бєляєв, С.В. Герасимов, С.В. Кукобко [та ін.] // Збірник наукових праць ЦНДІ ОВТ ЗС України, - 2016. №3(62), -с. 77-84.

10. Tymchenko, S., Kaplun, Y., Roshchupkin, E., Kukobko, S. (2023). Substantiation of Time Distribution Law for Modeling the Activity of Automated Control System Operator. In: Shkarlet, S., et al. Mathematical Modeling and Simulation of Systems. MODS 2022. Lecture Notes in Networks and Systems, vol 667. Springer, Cham. https://doi.org/10.1007/978-3-031-30251-0_9

11. Рощупкін Є.С. Великоапертурна (рознесена) радіолокаційна система: пат. 148518 Україна : G01S7/42, H01Q21/00 / Є.С. Рощупкін, С.В. Герасимов, С.В. Кукобко, М.В. Борисенко, Ю.О. Крихтін, О.Ф. Галицький, Б.В. Гайбадулов, В.В. Джус, І.В. Помогаєв, В.В. Борисов, Ю.О. Чміль, А.Ю. Задорожна. – u 202100336; заявл. 29.01.2021; опубл. 18.08.2021, бюл. № 33/2021, – 7 с.

12. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2005). Организация когерентной обработки на промежуточной частоте при приеме широкополосных сигналов крупноа-

пертурными антенными решетками и многопозиционными системами. Прикладная радиоэлектроника, (Т.4, №4), 437-440.

13. Herasimov S., Roshchupkin E. (2022). Parameters of monitoring the technical condition of airspace radio engineering monitoring systems. International scientific and practical conference "Application of information technologies in the preparation and operation of law enforcement forces", Kharkiv.

14. Herasimov, S., Borysenko, M., Roshchupkin, E. et al. Spectrum Analyzer Based on a Dynamic Filter. J Electron Test 37, 357–368 (2021), https://doi.org/10.1007/s10836-021-05954-0

УДК 621.39:623.1/.7

Вурста Ю.І., Кущ П.С., Камчатний М.І., Помогаєв І.В.

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО УДОСКОНАЛЕННЯ ПРИСТРОЮ ПЕРВИННОЇ ОБРОБКИ ШЛЯХОМ ВПРОВАДЖЕННЯ СУЧАСНОЇ ЕЛЕМЕНТНОЇ БАЗИ ТА ДОДАТКОВИХ АЛГОРИТМІВ ФУНКЦІОНУВАННЯ

Аналіз застосування засобів повітряного нападу (ЗПН) росії проти України виявив, що на успішне виконання зенітними ракетними комплексами завдань з протиповітряної оборони суттєво впливає прискорення попереднього виявлення ЗПН. Найбільш ефективним є автоматичне виявлення [1-15].

Розглянуто пристрій первинної обробки (ППО) багатоканальної станції наведення ракет **(**БСНР).

За даними дослідження встановлено, що первинна обробка проводиться за алгоритмами, закладеними у програму ППО. З’ясовано, що ППО має ряд недоліків, такі як велика дискретність та обмежена кількість перевірок та алгоритмів, що використовуються.

У зв’язку з цим в доповіді розглянуті сучасні пристрої цифрової обробки, які можуть використовуватись в БСНР на заміну ППО. Розглядались мікроконтролери та мікропроцесори, що уявляють собою два типи інтегральних схем, які використовуються для обробки інформації в електронних пристроях та системах, проте вони мають різні особливості та застосування, отже вибір між ними залежить від конкретних потреб та характеристик вбудованої системи.

В доповіді наведені пропозиції щодо використання наведених пристроїв обробки сигналів високої частоти в БСНР.

Розглянуті алгоритми функціонування, що пропонуються впровадити в БСНР 9С32 при реалізації запропонованих рішень.

Список використаних джерел

1. Швидкий, А. В., Рощупкін, Є. С., Кукобко, С. В., Шулежко, В. В., & Коробков, Ю. В. (2022). Аналіз безпілотних літальних апаратів як цілей для зенітного ракетного комплексу С-300В1. XVI Міжнародна науково-практична конференція магістрантів та аспірантів "Теоретичні та практичні дослідження молодих вчених" (TPRYS-2022), Харків. https://doi.org/10.5281/zenodo.7455078

2. Туринский, А.В., Певцов, Г.В., Крючков, Д.Н., & Рощупкин, Е.С. (2020). Методы повышения достоверности и эффективности контроля технического состояния радиотехнических систем подвижных объектов. Azərbaycan dövlət dəniz akademiyasının elmi əsərləri (ISSN 2220-1025), 1, 176–182. https://doi.org/10.5281/zenodo.5035847

3. Герасимов, С.В., Гречка, А.В., Рощупкин, Е.С., Рощупкина, А.Е., & Кукобко, С.В. (2020). Адаптивный метод технической диагностики системы разнесенных радиотех-

нических устройств. Azərbaycan dövlət dəniz akademiyasının elmi əsərləri (ISSN 2220-1025), 2, 129–137. https://doi.org/10.5281/zenodo.5035853

4. Кукобко, С.В., Ветошкін, О.Г., Рощупкін, Є.С., & Джус, В.В. (2020, July 1). Автоматизове технічне обслуговування рознесених електронних інформаційних систем. Математичне та імітаційне моделювання систем (МОДС 2020), Чернігів: ЧНТУ. https://doi.org/10.5281/zenodo.5067687

5. Кузьменко Д.В., Рощупкін Є.С., & Джус В.В. (2021). Удосконалення системи управління променем багатоканальної радіолокаційної станції спеціального призначення. XV Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих науковців» (TPRYS-2021), Харків. https://doi.org/10.5281/zenodo.6791224

6. Сухаревский О.И., А.Ю. Шрамков & Рощупкин Е.С. (2005). Высокочастотный метод расчета диаграммы направленности антенны с учетом неоднородностей рельефа местности на позиции РЛС. Моделювання та інформаційні технології, (33), 174-181.

7. Рощупкин, Е.С., & Беляев, Д.Н. (1999). Измеритель коэффициента стоячей волны в виде ответвителя дециметрового диапазона волн. Збірник наукових праць за матеріалами 3-го міжнародного молодіжного форуму "радіоелектроніка і молодь у XXI столітті" 20-23 квітня 1999 р., 1, 52–55. https://doi.org/10.5281/zenodo.5591877

8. Крючков, Д. М., Рощупкін, Є. С., Калита, О. В., & Дранник, П. А. (2023). Пропозиції щодо підвищення ефективності відновлення сукупності різнотипних радіоелектронних засобів спеціального призначення при їх використанні в різних умовах. XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023), Kharkiv. https://doi.org/10.5281/zenodo.10257044

9. Бєляєв, Д.М. Застосування векторних аналізаторів сигналів для забезпечення електромагнітної сумісності радіоапаратури / Д.М. Бєляєв, С.В. Герасимов, С.В. Кукобко [та ін.] // Збірник наукових праць ЦНДІ ОВТ ЗС України, - 2016. №3(62), -с. 77-84.

10. Tymchenko, S., Kaplun, Y., Roshchupkin, E., Kukobko, S. (2023). Substantiation of Time Distribution Law for Modeling the Activity of Automated Control System Operator. In: Shkarlet, S., et al. Mathematical Modeling and Simulation of Systems. MODS 2022. Lecture Notes in Networks and Systems, vol 667. Springer, Cham. https://doi.org/10.1007/978-3-031-30251-0_9

11. Рощупкін Є.С. Великоапертурна (рознесена) радіолокаційна система: пат. 148518 Україна : G01S7/42, H01Q21/00 / Є.С. Рощупкін, С.В. Герасимов, С.В. Кукобко, М.В. Борисенко, Ю.О. Крихтін, О.Ф. Галицький, Б.В. Гайбадулов, В.В. Джус, І.В. Помогаєв, В.В. Борисов, Ю.О. Чміль, А.Ю. Задорожна. – u 202100336; заявл. 29.01.2021; опубл. 18.08.2021, бюл. № 33/2021, – 7 с.

12. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2005). Организация когерентной обработки на промежуточной частоте при приеме широкополосных сигналов крупноапертурными антенными решетками и многопозиционными системами. Прикладная радиоэлектроника, (Т.4, №4), 437-440.

13. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2006). Алгоритмы когерентной обработки широкополосных сигналов на промежуточной частоте с использованием схем фазонастраивающих контуров с управляемыми дисперсионными линиями задержки в крупноапертурных антенных решетках и многопозиционных системах. Прикладная радиоэлектроника, (Т.5, №2), 250-254.

14. Кукобко С.В., Рощупкін Є.С. (2022). Моделювання системи технічного обслуговування безпілотних літальних апаратів. Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2022): тези доповідей XII Міжнародної науково-практичної конференції, Чернігів

15. Кукобко С.В., Місценко Р.В., Бритов Д.М., Рощупкін Є.С., & Гайбадулов Б.В. (2023). Пропозиції щодо автоматизації процесу прийняття рішення при класифікації

ситуацій у повітряному просторі. Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку", Харків

УДК 658.787:(615.2:615.46)

В'яткін Ю.О.

НАВЧАЛЬНО-ТРЕНУВАЛЬНИЙ МОДУЛЬ З ПІДГОТОВКИ РОЗРАХУНКІВ 120-ММ МИНОМЕТУ «RAK»

Наприкінці 2023 року Україна отримала від Польщі самохідні міномети "Rak" калібру 120 мм. 120-мм самохідний міномет M120K "Rak" представляє собою зразок польової артилерії, який розроблено у Військово-виробничому центрі Huta Stalowa Wola S.A. й оснащений 120-мм автоматичним мінометом, встановленим на колісному шасі SMK 120, створеному на базі колісного бронетранспортеру Rosomak. СМК "Rak" здатний вести точну стрільбу на дальності від 8 до 12 км, а також окрім штатних мін може стріляти боєприпасами з кумулятивним зарядом. Час підготовки до відкриття вогню становить 2 хвилини, зміна вогневої позиції може здійснюватися протягом 15 секунд після випуску останньої міни. Машина оснащена цифровою системою управління вогнем, що складається з тепловізійної камери та лазерного далекоміру, який дозволяє ефективно виконувати вогневі завдання вдень і вночі. Дані для стрільби можуть бути отримані, серед іншого, шляхом обробки зображення з безпілотного літального апарату FlyEye. FlyEye – безпілотний літальний апарат (БПЛА) міні-класу, який успішно використовується в розвідувальних місіях, в т.ч за необхідністю забезпечення підтримки ведення артилерійського вогню. Платформа базується на новітніх рішеннях у галузі технологій розробки композитних матеріалів, системи прийому та передачі даних. Планер виготовлений за власними рішеннями авіоніки Flytronic, у тому числі розробленою з нуля системою автопілоту з алгоритмами управління і повним набором датчиків параметрів руху, що дозволяє виконувати завдання зі спостереження протягом понад двох годин майже за будь-яких погодних умов. Розроблені алгоритми управління планером забезпечують безпечний політ протягом усього часу виконання бойового завдання, включно з надзвичайними ситуаціями, такими як обертання платформи або переривання запуску, або аварійна посадка. FlyEye інтегровано з автоматизованим комплексом управління вогнем ZZKO (zautomatyzowany zestaw kierowania ogniem) TOPAZ та ін..

Самохідний міномет M120K "Rak" також має можливість вести вогонь дистанційно, як безпілотна зброя, використовуючи команди та дані, які передаються в електронному вигляді на комп'ютер машини. Оснащення мінометних підрозділів ЗС України сучасними вогневими засобами країн-партнерів потребує якісної підготовки та навченості особового складу. Вона досягається застосуванням новітніх технологій та засобів навчання. Прикладом реалізації подібного підходу є тренажерний комплекс AREX ТРАК-01 для розрахунків самохідного міномету M120K "Rak".

Процес підготовки розрахунків 120- мм СМ M120K "Rak" проводиться відповідно до навчальних програм, які передбачають поєднання набуття теоретичних знань з будови та експлуатації зразка О і ВТ з відпрацюванням практичних навичок всіма номерами розрахунку міномету. До роботи на тренажерах допускається особовий склад, який добре засвоїв будову, принципи роботи та експлуатації M120K "Rak", основи його бойового застосування в різних умовах. Після завершення теоретичної підготовки особовий склад відпрацьовує отримані знання на тренажерах. Процес підготовки розрахунків завершується практичним виконання бойових завдань безпосередньо на техніці в складі штатних підрозділів.

Навчально-тренувальний комплекс СМ "Rak" AREX ТРАК-01 забезпечує можливість реалізації повного комплексу навчання, що включає в себе виконання всього спектру вогневих завдань (стрільба з закритої вогневої позиції, стрільба напівпрямим та прямим наведенням), а також діагностику та обслуговування техніки за допомогою новітніх технологій навчання: VR (virtual reality – віртуальної реальності) та AR (augmented reality – доповненої реальності) та відтворює роботу на бойовій техніці.

Функціональність тренувального комплексу AREX ТРАК-01 забезпечена за рахунок використання нових мультимедійних технологій – VBS (Virtual Battle Space), VBS – це інтерактивне тривимірне синтетичне середовище, що створює віртуальний тренувальний полігон, пристосований для проведення широкого спектру тактичних тренувань, дисперсійного аналізу та наукових експериментів. Система віртуального середовища моделювання поля бою VBS була розроблена для моделювання тактичних навчань на рівні батальйону. VBS – середовище симулятору поля бою, далекосяжний розвиток графічного двигуна комерційної комп'ютерної гри «Operation Flashpoint», що розробляється з 2001 року для комплексного моделювання тактичної побудови підрозділів на сучасному полі бою. На теперішній час він є стандартним тактичним симулятором багатьох країн НАТО і використовується Корпусом морської піхоти США, армією США, збройними силами Великобританії, Швеції, Австралії (і Нової Зеландії), Канади, Фінляндії та іншими. Він дозволяє в реальному часі моделювати різні ситуації, що виникають на полі бою (як у повномасштабних, так і в асиметричних конфліктах), у тому числі атаки із застосуванням саморобних вибухових пристроїв (СВП), з використанням карт та техніки з бази даних, яка може бути розширено та включити додаткові необхідні елементи. Завдяки цьому можна підготуватися до бойових завдань та ознайомитися з місцевістю, провести тактичну підготовку від рівня окремого солдата до бойових груп, навчання тактичних підрозділів, рух колон, навчання спостерігачів, надання вогневої підтримки тощо.

В даний час у компанії HSW S.A. у Стальовій Волі є мобільна версія навчальної системи AREX TRAK-01 – у транспортно-тренувальному контейнері. Автономність тренажерного комплексу ТРАК-01 забезпечується його оснащенням, що дозволяє його використання в польових умовах. Мобільність системи навчання забезпечується завдяки виконавчій системі та стандартному 20-футовому контейнері, в якому монтується система ARM – 11 за допомогою системи HDS. HDS (hydrauliczny dźwig samochodowy) – це система, яка передбачає установку гідравлічного автокрана на борту вантажівки який дозволяє оператору самостійно завантажувати та вивантажувати контейнери та інші вантажі. Для транспортування тренажера також можуть використовуються автомобілі, обладнані системою мультиліфт, яка являє собою гідравлічний гаковий підіймач, що встановлюється на базовому шасі та використовується для підйому і перевезення різного роду вантажів та контейнерів. Ще один варіант – розміщення контейнеру з комплексом на базі 4-х керованих гідроопор.

Зворотній зв'язок досягається шляхом проведення тестувань на комп'ютерному обладнанні з спеціально розробленим програмним забезпеченням.

Застосування в процесі підготовки мінометників ЗС України, які мають на озброєнні 120-мм СМ М120К "Rak", навчально- тренувальних комплексів AREX ТРАК-01, дозволить суттєво підвищити бойові можливості механізованих підрозділів з нанесення ворогу втрат у живій силі, озброєнні та військової техніці.

Гера В.Я., Бондар Р.В., Фіщук І.М., Поліщук А.М.

НАПРЯМИ МОДЕРНІЗАЦІЇ КОМПЛЕКСУ ЗАСОБІВ АВТОМАТИЗАЦІЇ УПРАВЛІННЯ ВОГНЕМ АРТИЛЕРІЙСЬКИХ ПІДРОЗДІЛІВ

Протягом відбиття збройної агресії російської федерації до артилерійських підрозділів Збройних Сил України надійшла велика кількість різноманітних артилерійських систем - від найпростіших причіпних гармат до найсучасніших самохідних. Слід відмітити, значна частина цих артилерійських систем надійшла без комплексу засобів автоматизації управління вогнем, інша частина надійшла із штатною системою, яка потребує адаптації та інтегрування до системи управління вогнем артилерійських підрозділів Збройних Сил України. Також, даний комплекс управління відсутній і на радянських системах управління вогнем, що знижує ефективність їх бойового застосування. Існуючий програмний комплекс управління вогнем «Кропива», який допущений до використання у Збройних Силах України, являє собою лише засіб визначення установок для стрільби та додатково дозволяє частково автоматизувати виконання заходів підготовки стрільби і управління вогнем. Поряд з тим, комплекс засобів автоматизації управління вогнем це більш широке поняття, яке, як правило, включає в себе індивідуальні засоби топогеодезичної, метеорологічної та балістичної підготовки стрільби, засоби автоматизації наведення гармати (без використання оптичних приладів, наприклад гіроскопічним способом), засоби контролю за наведенням гармати, різноманітні датчики контролю (наявності боєприпасів, пального, виміру температури заряду та температури ствола, виміру інших життєво важливих характеристик системи), цифровий засіб визначення установок для стрільби, засоби зв'язку та інше обладнання. Таким чином, постає актуальне завдання створення сучасного комплексу автоматизації управління вогнем перспективної артилерійської системи Збройних Сил України. Даний комплекс має бути уніфікованим та дозволяти встановлення на різні типи артилерійських систем. Створення даного комплексу доцільно проводити за декількома етапами, перший - на основі аналізу можливостей існуючих моделей сучасних комплексів управління вогнем, в тому числі і під час реальної перевірки в ході ведення бойових дій, розробити склад перспективного комплексу, із вказанням обов'язкових та можливих (додаткових) компонентів.

Другий етап - скласти технічне завдання на кожну складову та на весь комплекс в цілому. На третьому етапі провести аналіз можливостей вітчизняних підприємств щодо створення компонентів перспективного комплексу управління вогнем.

Наступний етап передбачає створення дослідних компонентів - балістичних та метеорологічних станцій, цифрових систем наведення ствола гармат, наприклад гіроскопічних, систем контролю, засобів визначення установок для стрільби тощо. При відсутності можливості або доцільності створення будь-якого компонента комплексу необхідно розглянути варіанти закупівлі найбільш ефективних зарубіжних аналогів, дієвість яких перевірена під час відбиття збройної агресії російської федерації.

На четвертому етапі необхідно поєднати відібрані та створені компоненти в єдиний комплекс засобів автоматизації з підключенням до програмного забезпечення управління вогнем. Варіантом програмного забезпечення управління вогнем є вже існуючі програмні комплекси - «Кропива» або «Оболонь».

І на заключному етапі необхідно провести випробування працездатності комплексу автоматизації, за раніше розробленими критеріями оцінки, в тому числі під час проведення бойових стрільб, під час активної дії засобів радіоелектронної боротьби противника, за складних метеорологічних умов та у високих режимах ведення вогню.

Поряд з тим, необхідно пам'ятати, що чим складніша система управління, тим вища ймовірність виходу з ладу одного з компоненту, що може призвести до виходу з ладу всієї системи, тому під час розроблення перспективного комплексу засобів автоматиза-

ції необхідно закладати відповідні вимоги до її надійності, автономності, взаємозамінності компонентів та простоти в обслуговуванні. Також, слід передбачити можливість, на будь-якому етапі виконання вогневого завдання, переходу від автоматизованого управління вогнем до ручного із використанням існуючої системи визначення установок для стрільби та наведення гармати.

Таким чином, створення перспективного комплексу засобів автоматизації управління вогнем є актуальним науковим завданням, вирішення якого дозволить значно підвищити ефективність бойового застосування артилерійських систем і артилерійських підрозділів в цілому.

Гера В.Я., Корнієнко О.С., Левкович П.В., Фіщук І.М.

РОЗРОБКА ТА ВПРОВАДЖЕННЯ АВТОНОМНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ З ВІЗУАЛЬНОЮ НАВІГАЦІЄЮ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВІЙСЬКОВИХ ОПЕРАЦІЙ В УМОВАХ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Як демонструє досвід російсько-української війни безпілотні літальні апарати (БПЛА) відіграють важливу роль у виконанні різноманітних задач, починаючи від розвідки місцевості та спостереження за діями ворога, коректування вогню артилерії, та закінчуючи нанесенням вогневого ураження як спеціалізованими боєприпасами так і ураженням безпосередньо БПЛА який у своєму складі має бойову частину з підривником. Оскільки Україна не має використовує вітчизняної системи GPS, та в переважній сфері застосування ударних БПЛА противник використовує засоби радіоелектронної боротьби (РЕБ) особливо актуальним стає застосування БПЛА в районах, де відсутній доступ до сигналів GPS, що вимагає розробки надійних методів автономної навігації, яка дозволяє виконувати поставлені завдання. В цьому контексті, дана наукова робота пропонує інноваційний підхід до розробки автономного БПЛА, який використовує візуальну навігацію для орієнтування в просторі та досягнення місця призначення з метою доставки знищення цілей противника як на полі бою так і об'єктів військового промислового комплексу у тилу.

Задля реалізації цієї мети, спочатку необхідно було зібрати та обробити значний обсяг аерознімків та карт Google, що послужили основою для створення обширної бази даних зображень, з чіткою прив'язкою координат яскраво виражених об'єктів таких як: перехрестя доріг, будівель правильної форми, русел річок, інфраструктурних об'єктів, тощо. Ці зображення будуть анотовані з точними координатами, що дозволило тренувати нейронну мережу із визначення місцезнаходження на основі візуальних даних. Використання глибоких згорткових нейронних мереж (CNN) планується бути ключовим у аналізі зображень та визначенні координат БПЛА.

Програмування нейронної мережі починається з вибору архітектури CNN, яка найкраще підходить для задач візуальної навігації. Архітектури, такі як ResNet, Inception та VGG, розглядаються як потенційні кандидати завдяки їхній здатності ефективно витягувати ознаки з зображень великої роздільної здатності. Вибір конкретної моделі залежить від балансу між точністю розпізнавання та вимогами до обчислювальних ресурсів.

Наступним кроком є тренування моделі, що включає налаштування гіперпараметрів, таких як швидкість навчання, розмір пакету та кількість епох. Оптимізація мережі виконується за допомогою алгоритмів, таких як стохастичний градієнтний спуск або Adam, що дозволяє мінімізувати помилку прогнозування та покращити здатність мережі до узагальнення.

Однією з ключових задач при програмуванні нейронної мережі є забезпечення її здатності до адаптації в різних умовах, включаючи зміни в освітленості, погоді та сезонних характеристиках місцевості. Для цього використовуються техніки аугментації даних, такі як повороти зображень, зміна масштабу та зміщення, що дозволяє збільшити різноманітність навчального датасету та підвищити робастність моделі.

Для досягнення високої точності навігації, модель буде тренуватися на даних, що включали різноманітні умови освітлення, погодні умови та час доби, що забезпечує її здатність до узагальнення та адаптації до складних умов реального світу.

Для ефективної навігації безпілотника пропонується розробити спеціалізований алгоритм, який враховує отримані від нейронної мережі дані для корекції маршруту в реальному часі. Цей алгоритм дозволить БПЛА не тільки точно визначати своє розташування, але й ефективно обирати маршрут до місця призначення, уникаючи можливих перешкод. Інтеграція навігаційної системи з польотним контролером БПЛА забезпечила автономний політ безпілотника, що особливо важливо в умовах, де використання GPS неможливе або небажане.

Тим не менш, розробка такої системи стикається з рядом викликів, зокрема зі змінністю умов освітлення та погодними умовами, які можуть впливати на якість зображень. Крім того, обмежені обчислювальні ресурси БПЛА вимагають подальшої оптимізації моделі та алгоритмів для забезпечення їх ефективної роботи в реальному часі. Подальші дослідження можуть включати використання додаткових датчиків, таких як лідари або інфрачервоні камери, для покращення точності навігації та розширення можливостей БПЛА в складних умовах.

Висновково, дана робота демонструє значний потенціал використання візуальної навігації для розробки ударних БПЛА, здатних ефективно діяти в умовах обмеженого доступу до GPS-сигналів. Розроблена система відкриває нові перспективи для застосування ударних БПЛА під час нанесення ударів по цілям та об'єктам ворога, забезпечуючи надійність та автономність в складних умовах.

Гера В.Я., Сівак О.І., Бондар Р.В., Ликова І.В.

РОЗРОБКА АВТОНОМНОЇ СИСТЕМИ ДЛЯ ВОГНЕВОГО УРАЖЕННЯ ПРОТИВНИКА ЗА ДОПОМОГОЮ БЕЗПІЛОТНИКА: ІНТЕГРАЦІЯ КОМП'ЮТЕРНОГО ЗОРУ ТА АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

Створення автономної системи, яка дозволяє безпілотному літальному апарату (БПЛА) виконувати автономне наведенн’я на ціль з подальшим її ураженням, представляє собою важливий крок у розвитку технологій БПЛА з ударної частиною (БПЛА камікадзе). З огляду на сучасну ситуації у російсько-українській війні, де використання безпілотників стає все більш розповсюдженим у різноманітних бойових завданняз з ураження живої сили та техніки противника, в умовах активного застосування противником широкого спектру засобів радіоелектронної боротьби (РЕБ), потреба в автономних системах, які можуть самостійно виконувати складні завдання, стає очевидною. Однією з ключових вимог до таких систем є здатність безпілотника самостійно ідентифікувати та слідкувати за обраною ціллю для її вогневого ураження без безпосереднього втручання оператора та без використання сигналів GPS або підключення до Інтернету.

Задля реалізації такої системи використовуються передові технології в області комп'ютерного зору та машинного навчання. Серцем системи є обчислювальний модуль, що встановлюється на борту безпілотника. Платформи, такі як NVIDIA Jetson або Raspberry Pi, оснащені достатньою обчислювальною потужністю для обробки зображень в реальному часі та виконання алгоритмів глибокого навчання. Це дозволяє безпі-

лотнику аналізувати отримані відеодані безпосередньо під час польоту, ідентифікувати техніки та живої сили ворога і приймати рішення про подальші дії без зовнішнього втручання для вогневого ураження.

Основою для розпізнавання об'єктів служать попередньо навчені моделі глибокого навчання, такі як YOLO, SSD або Faster R-CNN. Ці моделі дозволяють швидко і точно ідентифікувати живу силу на зображенні, незважаючи на різноманітність умов освітлення, позицій та кутів зйомки. Додатково, можливість доналаштування та доповнення навчання цих моделей на специфічних наборах даних забезпечує високу адаптивність системи до конкретних умов та завдань.

Після ідентифікації обраного об'єкта система переходить до фази слідкування. За це відповідають спеціалізовані алгоритми слідкування, такі як KCF, MOSSE або CSRT, які забезпечують стабільне тримання об'єкта в полі зору камери безпілотника. Важливо, що ці алгоритми ефективно працюють навіть при переміщенні об'єкта або безпілотника, що є ключовим для здійснення якісної портретної зйомки.

Інтеграція розпізнавання та слідкування з системою управління польотом безпілотника є наступним кроком. Це включає передачу команд з алгоритмів до польотного контролера для автоматичного коригування траєкторії польоту, зміни висоти або положення безпілотника таким чином, щоб оптимально виконати завдання з вогневого ураження противника. Зв'язок між системами забезпечується через протоколи, як-от MAVLink, що дозволяє здійснювати плавне та координоване управління польотом.

Не менш важливим аспектом є забезпечення безпеки польоту, особливо при роботі в складних або непередбачуваних умовах. Автономні алгоритми уникнення перешкод, які використовують датчики лідару або ультразвуку, гарантують, що безпілотник може безпечно маневрувати у просторі, уникаючи зіткнень з перешкодами. Ці технології є невід'ємною частиною системи, оскільки забезпечують високий рівень надійності та безпеки польоту.

Розвиток та впровадження автономних систем управління безпілотниками для автономного ураження цілі без залучення оператора відкриває нові перспективи для використання цих апаратів. Можливість безпілотників самостійно визначати об'єкти для знищення, адаптуватися до змін умов та виконувати завдання з високою точністю без зовнішнього втручання значно розширює сфери застосування цих технологій.

Завдання створення повністю автономної системи управління безпілотником для вогневого ураження представляє собою складний інженерний виклик, що вимагає інтеграції різноманітних технологій та підходів. Розв'язання цього завдання не лише сприятиме подальшому розвитку безпілотних технологій, але й відкриє нові горизонти в їх застосуванні, роблячи безпілотники більш доступними, ефективними та безпечними для широкого на полі бою, що підвищить обороноздатність України та допоможе її перемогти у російсько-українській війні.

Гера В.Я., Сівак О.І., Левкович П.В., Ликова І.В.

РОЗРОБКА СИСТЕМИ ПАСИВНОЇ АКУСТИЧНОЇ РОЗВІДКИ ДЛЯ ВИЯВЛЕННЯ ТА ВИЗНАЧЕННЯ ЛОКАЦІЇ БПЛА 'ШАХЕД' НА ОСНОВІ АНАЛІЗУ ЗВУКУ З ВИКОРИСТАННЯМ НЕЙРОМЕРЕЖ

Сучасний світ стикається з безліччю викликів та загроз, серед яких особливе місце займає питання військових конфліктів та геополітичних змагань. Однією з країн, яка стала об'єктом агресивних дій та військового втручання, є Україна. Зокрема, зосереджуючи увагу на останніх технологічних досягненнях в галузі військової техніки, варто звернути увагу на використання безпілотних літальних апаратів (БПЛА) типу "Шахед-136", які були представлені Іраном у 2021 році.

"Шахед-136" — це дрон з вражаючими характеристиками, здатний здійснювати польоти на відстань до 2000 км, з ефективною дальністю полету від 1000 км та можливістю доставляти бойову частину масою 50 кг. За словами американських експертів, його реальна дальність складає декілька сотень кілометрів. "Шахед-136" може летіти на висотах від 60 до 4000 метрів із крейсерською швидкістю 150—170 км/год. Зазначений БПЛА оснащений 2-тактним двигуном MADO MD 550 потужністю 50 л.с., а його "мопедний" звук можна чути на відстані в кілька кілометрів.

Вага даного беспилотника складає близько 200 кг, а його розміри та конструкція — з треугольним крилом і схемою "бесхвостка" — роблять його ефективним інструментом для масового застосування проти окремих або груп цілей. Його можливість розміщення на різних транспортних засобах, включаючи грузовики, железнодорожні вагони, кораблі, збільшує його оперативну гнучкість та загрозу.

У контексті російської агресії, цей тип БПЛА може використовуватись для атак на промислові та цивільні об'єкти в Україні, створюючи серйозні виклики для національної безпеки країни. Таким чином, розробка ефективних методів виявлення та відстеження "Шахед-136" стає важливим елементом в оборонній стратегії України, а вивчення його характеристик, звукового профілю та особливостей використання допоможе у розробці тактик та технологій для протидії цій новій загрозі.

Атаки, здійснені за допомогою безпілотних літальних апаратів (БПЛА) типу "Шахед-136", відкривають новий вектор загроз для промислових та цивільних об’єктів. Використання цих БПЛА дозволяє проводити точкові удари з великої відстані, що робить традиційні методи виявлення та протидії їм менш ефективними. Особливість "Шахед-136" у його характерному "мопедному" звуку, який відрізняється від інших БПЛА. Отже, основна проблема полягає у відсутності ефективних засобів для виявлення та протидії атакам такого типу БПЛА, особливо в умовах, коли традиційні методи можуть виявитися неефективними.

Метою даної доповіді є розробка методу для виявлення БПЛА "Шахед-136" на основі аналізу звуку. Зосереджуючись на унікальному акустичному профілі цього БПЛА, ця доповідь покликана вивчити можливості використання сучасних технологій та методів для створення системи, здатної виявляти та локалізовувати "Шахед-136" на ранніх етапах його зближення. Завданням є визначення параметрів звукового сигналу, які є унікальними для даного БПЛА, та створення алгоритму, що може виявляти ці характеристики в зовнішньому середовищі. Це допоможе у розробці засобів та технік для протидії агресії з використанням "Шахед-136", зміцнюючи обороноздатність промислових та цивільних об’єктів.

Звуковий профіль ДВЗ "Шахед-136" є відзначено характерним та досить гучним, з "мопедним" тоном, що можна відрізнити на великій відстані. Двигун MADO MD 550, який встановлено на БПЛА, видає звук, що відрізняється від інших типів двигунів, дозволяючи ефективно ідентифікувати присутність "Шахед-136". Важливо визначити специфікації цього звуку, включаючи частоту, амплітуду та тембр, для точного визначення його присутності в операційному середовищі.

Для детального аналізу звуку, згенерованого "Шахед-136", можна використовувати різні методи вимірювань, такі як спектральний аналіз. Специфічні характеристики звуку можна виміряти з використанням високочутливих мікрофонів та акустичних датчиків, розміщених у ключових локаціях. Програмне забезпечення потім аналізує отримані дані, виводячи характеристики, які є унікальними для "Шахед-136". Такий підхід може дозволити виявити присутність дрону, навіть за умов високого рівня зовнішнього шуму.

Звукоприймачі, які розміщуються для виявлення БПЛА "Шахед", повинні мати специфікації, які дозволяють точно зареєструвати і аналізувати характерний "мопедний" звук двигуна дрону. Розміщення цих звукоприймачів є критично важливим, оскільки воно впливає на здатність системи точно ідентифікувати та локалізувати звук БПЛА.

Звукоприймачі розміщуються на стратегічних точках з відомими координатами, щоб забезпечити максимальне покриття та збільшити шанси на виявлення БПЛА.

Техніка та алгоритми обробки даних відіграють ключову роль у перетворенні зареєстрованого звуку на корисну інформацію. Нейромережі та інші методи машинного навчання можуть бути використані для розпізнавання шаблонів і характеристик звуку, що відрізняють "Шахед" від інших джерел шуму. Важливо ретельно навчати та оптимізувати ці моделі, щоб мінімізувати кількість помилкових виявлень та пропущених детекцій.

Пасивна розвідка пропонує значні переваги, оскільки її важко виявити. Відсутність активних сигналів або випромінювань, які можна б було виявити, означає, що ця система може безперебійно працювати, збираючи дані про можливе присутність БПЛА, не викриваючи своє місцезнаходження чи факт своєї роботи. Це робить пасивну розвідку вкрай ефективною у ворожому або конфліктному середовищі, де виявлення може призвести до знищення або збою системи.

Таким чином, комбінація стратегічно розміщених звукоприймачів, передових технік обробки даних і переваг пасивної розвідки може забезпечити потужний та ефективний інструмент для виявлення та моніторингу БПЛА "Шахед" у реальному часі.

Розробка нейромережі для аналізу звуку ДВЗ "Шахед" включає створення моделі, яка може розпізнавати характерні звукові шаблони цього дрону. Нейромережа тренується на великому наборі даних, який містить зразки звуку "Шахеда", а також інші звуки для навчання моделі відрізняти ці конкретні шуми від інших. Процес тренування вимагає часу, терпіння і точного налаштування для оптимізації точності та надійності в реальних умовах.

Результати тестування нейромережі на реальних даних важливі для визначення її здатності коректно класифікувати і ідентифікувати звуки "Шахеда". Тестування включає в себе використання звукових даних, зібраних з різних джерел та умов, щоб оцінити здатність моделі працювати в різноманітних ситуаціях і з різними рівнями шуму.

Обговорення ефективності та точності нейромережі критично важливе для оцінювання її практичної придатності. Важливо розглянути не тільки кількість правильно ідентифікованих звуків "Шахеда", але і помилкові виявлення та пропущені детекції. Ефективність та точність є ключовими параметрами, що визначають успіх системи в реальному світі, де точне та своєчасне виявлення може бути критично важливим для відгуку на загрози від БПЛА "Шахед".

В цьому дослідженні було встановлено, що аналіз звуку є вельми ефективним у виявленні БПЛА "Шахед" із його властивим "мопедним" звуком. Технічні аспекти, такі як розміщення звукоприймачів, обробка даних та впровадження алгоритмів, були успішно реалізовані для забезпечення невиявленої пасивної розвідки, що виявилося критично важливим для оборонних операцій.

Розроблена нейромережа продемонструвала значну ефективність та точність під час аналізу звукових даних у реальних умовах. Хоча були досягнуті позитивні результати, існує потреба у подальшому вдосконаленні та оптимізації для підвищення надійності та ефективності системи в умовах високого рівня фонового шуму та інших завад.

Ця система може служити важливим інструментом для захисту цивільних та промислових об'єктів від потенційних загроз та агресій, що походять від ворожих БПЛА, і вимагає подальших досліджень для забезпечення її найвищої ефективності та здатності адаптації до змінних обставин.

УДК [535.24:628.9]:623

Гера В.Я., Снітков К.І., Поліщук А.М., Долганов О.Ю.

АНАЛІЗ ЕНЕРГЕТИЧНИХ ПАРАМЕТРІВ ОПТИЧНИХ СИСТЕМ В ІНФРАЧЕРВОНОМУ ДІАПАЗОНІ ПРИ АКТИВНІЙ ЛАЗЕРНІЙ ЛОКАЦІЇ

Однією з важливих проблем, які потребують негайного вирішення при проведенні підрозділами ЗС України оборонних та контр-наступальних операцій під час повномасштабного вторгнення збройних сил російської федерації на територію України, є завдання по виявленню позиції снайпера противника [1].Причому характерною ознакою виконання снайперських операцій (завдань) є максимальне виконання вимог, пов’язаних з належним вибором позиції на місцевості та здійснення заходів маскування не тільки вогневої позиці, а й безпосередньо снайпера та снайперської гвинтівки [2]. Паралельно з цим на сьогоднішній час існує достатня кількість приладів акустичної та телевізійної розвідки [3], принцип роботи яких оснований на виявленні демаскуючих ознак, пов’язаних з роботою снайпера. Серед них можна назвати: світловий спалах з каналу ствола, характерний звук пострілу, ударну хвилю та завихрення повітря під час польоту кулі, а також значне виділення теплової енергії під час пострілу [4]. Однак попри надійну та ефективну роботу пасивних засобів (приладів) розвідки метою яких є виявлення снайперів противника їхнє використання можливе лише у випадку здійснення пострілу зі снайперської гвинтівки. Враховуючи особливості тактики снайперських груп та високу кваліфікацію стрільців противника, як правило перший постріл у 90% несе за собою ураження цілі [4].

Разом з цим, однією важливою демаскуючою ознакою, яка властива снайперам, є використання ними оптичних систем (ОС) та оптоелектронних приладів (ОЕП), тобто прицілів до стрілецької зброї (снайперський приціл). Одним із шляхів виявлення снайперських ОС та ОЕП є використання явища активної лазерної локації у інфрачервоному (ІЧ) діапазоні [5], в основу якого покладений світлореверсивний ефект (світловий блік) [6]. Враховуючи той факт, що кожна оптична лінза у тому числі і снайперського прицілу, є прозорою та оптично-рівною поверхнею з високим класом шліфування, а отже досить значна кількість світла в ІЧ діапазоні, яка потрапить на неї відіб'ється під тим же самим кутом. Також у фокальній площині усіх ОС обов’язково передбачено його конструкцією світловідблискуючі елементи такі як: призма, оптична пластина з нанесеною на неї прицільною сіткою. Тому враховуючи вище згадані твердження існує практична можливість конструювання активних лазерних систем (приладів) призначення яких буде виявлення снайперів противника до моменту здійснення ними пострілу, використовуючи принцип світлоревесного бліку від їх оптичних прицільних пристроїв.

Прикладом обладнання, що працюють за принципом лазерної локації, часто використовуються як у цивільній так і в оборонній сферах, наприклад, ІЧ лазерні детектори та системи слідкування які є ключовими компонентами багатьох сучасних систем керованої зброї та самонавідних ракетних систем **[Ошибка! Источник ссылки не найден.]**. Ці пристрої використовують технології активної лазерної локації з використанням ІЧ лазерів для підсвічування об’єктів (цілей), а також для ідентифікації ворожих оптичних активних та пасивних систем [7].

У багатьох сучасних публікаціях, наприклад [8], ґрунтовно описані принципи та засади активної та напів-активної лазерної локації, та їх практичне застосування для ідентифікації літальних апаратів по пошуку оптичного обладнання за допомогою опромінення їх ІЧ лазерним потоком. Одночасно у більшості таких публікаціях наведені теоретичні основи для розрахунку та побудови активно імпульсних приладів лазерної локації, проте не в повній мірі розкрито значення їх енергетичних параметрів та не враховано об’єкти природного походження та інфраструктури**.**

Тому, враховуючи вище вказане авторами цієї праці було розроблено математичні моделі для визначення енергетичних параметрів. Де одним з таких параметрів є сигнал ІЧ випромінення реверсивної потужності, який надходить на фоточутливий пристрій відбитий від об'єктів природного походження (інфраструктури) – P_{ab} та від оптичних пристроїв – P_{as} в залежності від дальності до них. Результат математичного моделювання цього параметру наведено на рисунку 1.

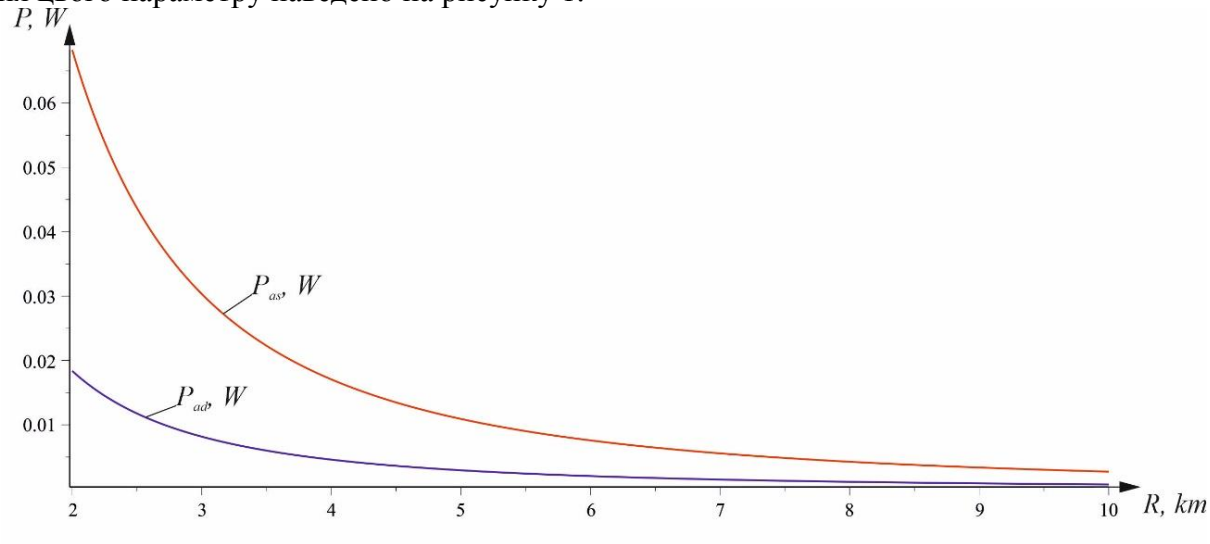


Рисунок 1 - Залежність реверсної потужності ІЧ випромінювання від дальності знаходження цілі

Наведений на рис. 1 порівняльний результат комп'ютерного моделювання енергетичної здатності виявлення цілі (об'єкту) з ефектом світлореверсного світлового бліку та цілі (об'єкту) який не має відношення до ОС (ОЕП) – P_{ab} показав, що потужність яка надходить від оптичних приладів на фоточутливий пристрій активної лазерної системи зондування у ІЧ діапазоні є в рази більшою за потужність яка отримується в наслідок об'єктів природного походження та інфраструктури – P_{as}. А отже практична реалізація та застосування пристроїв, які функціонують на основі лазерної системи зондування у ІЧ діапазоні під час виявлення позиції снайпера противника дозволять з високою точністю здійснити ідентифікацію снайперських прицілів до моменту здійснення ними пострілу, а також виявити інші оптичні прилади які використовуються у цілях розвідки та спостереження.

Список використаних джерел

1. Дробан, О.М., Жогальський Е.Ф., Федор Б.С. (2020) Визначення узагальненого показника ефективності стрілецької зброї. Військово-технічний збірник. 22 (Трав 2020), 61–65. DOI:https://doi.org/10.33577/2312-4458.22.2020.61-65.

2. Дробан, О.М., Жогальський Е.Ф., Федор Б.С. (2018). Підходи до оцінки ефективності стрільби зі стрілецької зброї. Військово-технічний збірник, (19), 19–23. https://doi.org/10.33577/2312-4458.19.2018.19-23

3. Aghil Abiri, Ali Pourmohammad (2020). "The bullet shockwave based real-time sniper sound source localization." Sensors Jornal 2020. Issue № 13. pp. 7253 - 7264. DOI 10.1109/JSEN.2020.2978814

4. Yüksel Arslan (2017). "Impulsive sound detection by a novel energy formula and its usage for gunshot recognition." Elektrik ve Elektronik Mühendisliği Bölümü 2017. Issue № 1. pp.

5. Meng Guo, Yutong Jiang, Ming-jiao Sun, Chen-xiao Zhao, Shuang Wan, Haiping Song (2020). "Research on precise positioning technology based on laser active reconnaissance."

Optical Sensing and Imaging Technology 2020. Issue № 11. pp. 33–43. DOI https://doi.org/10.1117/12.2580174.

7. Xiu-qiang Li (2019) “Design and theory analysis of infrared detector” Proceedings Volume 11023, Fifth Symposium on Novel Optoelectronic Detection Technology and Application, 2019. Issue №5. DOI https://doi.org/10.1117/12.2521432.

8. Alexandr A. Golitsyn; Natalia A. Seyfi (2020). “Digital Range-Gated Surveillance Device without an Image Intensifier.” 21st international conference on micro/nanotechnologies and electron devices edm 2020 Chemal, 2020. Issue №21. pp. 289–292. DOI 10.1109/EDM49804.2020.9153475.

УДК 623.618.51

Герасимов С.В., Базарний С.В.

МЕТОДИКА РОЗРАХУНКУ МІСЦЕЗНАХОДЖЕННЯ АГЕНТІВ СОЦІАЛЬНИХ МЕРЕЖ ПРИ ПРОВЕДЕННІ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Інформаційні операції та психологічні операції проводяться з метою протидії інформаційним операціям противника, створення сприятливих умов для застосування своїх військ (сил) і підготовки населення до боротьби з противником. До таких операцій відносяться також психологічні дії та розповсюдження підготовленої спеціальної інформації для психологічного впливу на емоції, мотиви, раціональне мислення та поведінку цільової аудиторії противника [1, 2].

Інформаційні операції передбачають здійснення спланованих дій з доведенням спеціально підготовленої інформації за допомогою засобів комунікації для впливу на емоції, мотиви, раціональне мислення та поведінку цільової аудиторії з метою досягнення політичних і військових цілей [3, 4]. Можливими засобами розповсюдження інформації під час проведення інформаційних операцій можуть бути: розсилка коротких повідомлень (SMS) на мобільні телефони в певній місцевості, радіозвернення, звукові радіостанції, друкована продукція (листівки, газети) тощо. У сучасних умовах найбільша увага приділяється приділяється засобам поширення інформації в Інтернеті, особливо в соціальних мережах [1, 5].

Ключовою умовою досягнення цілей при здійсненні інформаційних операцій є правильне визначення цільових аудиторій – груп осіб, відібраних для здійснення психологічного впливу силами і засобами інформаційних операцій [1]. Одним із головних факторів, який суттєво впливає на ефективність інформаційних операцій, є правильне визначення цільових аудиторій, для чого необхідна інформація про географічне розташування конкретних осіб або груп осіб, які відбираються для здійснення психологічної вплив. Також необхідно враховувати потенційний рівень психологічного впливу агентів соціальних мереж, які мають найбільший вплив на визначені цільові аудиторії за методикою, що базується на розрахунку рівня публікаційної активності та кількості мережевих підключень агентів у соціальних мережах [1, 3].

Визначення географічного розташування агентів соціальних мереж або геолокації агентів соціальних мереж є важливим завданням, яке необхідно вирішити при визначенні цільових аудиторій для подальшої розробки спеціальних інформаційних продуктів (інформаційних матеріалів для здійснення психологічного впливу). Визначення фактичного перебування в зоні інформаційних операцій агентів соціальних мереж є актуальним завданням через небажання агентів соціальних мереж розголошувати особисту інформацію про своє місцезнаходження. Отже, ключовою умовою досягнення цілей проведення психологічного впливу є правильне визначення цільових аудиторій, що підвищить ефективність проведення психологічного впливу.

Більшість гаджетів, які використовують агенти соціальних мереж, мають функцію визначення власного місцезнаходження за допомогою технологій супутникової навігації (GPS) або за допомогою методу тріангуляції на основі приймально-передавальних станцій мережі мобільного оператора (A-локація). Таким чином, контент, створений агентами соціальних мереж (текстові повідомлення, фотографії, відеоматеріали), може мати маркери, що вказують на географічне розташування агента соціальних мереж на момент створення (розповсюдження або розміщення) відповідного контенту, навіть якщо він, агент соцмережі, не вказав своє місцезнаходження у власному профілі соцмережі.

В налаштуваннях гаджета (мобільного телефону) агент соцмережі може самостійно заборонити використання глобальної системи позиціонування (GPS) GPS-локації, але залишити можливість використання A-локації, тоді точність геолокації зменшується. Використання технології A-location дає можливість з'єднати найближчі базові станції та їх географічні координати з гаджетом агента соціальної мережі в поточний момент часу. Використання технології A-location надає такі можливості, як:

– визначення місцезнаходження без необхідності встановлення додаткового програмного забезпечення на гаджет агента соціальних мереж, використовуючи наявну інфраструктуру мобільного зв'язку;

– не потребує згоди або інформування агента соціальної мережі про визначення його місцезнаходження;

– можна використовувати в кімнатах та інших місцях, де немає сигналу супутникової навігації GPS.

Таким чином, технологія A-локації є потенційно ефективним інструментом для вирішення проблеми визначення географічного розташування агентів соціальних мереж, який слід поєднувати з іншими підходами та методами для підвищення загальної точності геолокації. Але водночас постає питання, як вирішити проблему визначення геолокації тих агентів соціальних мереж, які з міркувань конфіденційності чи з інших причин приховують інформацію про власне місцезнаходження та заборонили використовувати GPS-локацію та A- розташування в налаштуваннях телефону.

Таким чином, розроблено перший комплексний метод визначення місцезнаходження агентів соціальних мереж на основі інтеграції баз даних геолокації IP-адрес та аналізу геотегів агентів соціальних мереж, що дозволяє підвищити надійність визначення цілі аудиторії за географічним розташуванням в інтересах проведення інформаційних операцій.

Напрямком подальших досліджень може стати розробка методів визначення цільових аудиторій на основі інших підходів, таких як аналіз мережевих зв'язків агентів соціальної мережі або аналіз додаткової інформації з контенту профілів агентів соціальної мережі. Також перспективною є розробка засобів автоматизації з використанням машинного навчання для реалізації етапів розробленого методу.

Список використаних джерел

1. S. Herasymov, A. Tkachov, S. Bazarnyi. **Complex Method of Determining the Location of Social Network Agents in the Interests of Information Operations**, *Advanced Information Systems*, 8 (1), p.p. 31-36, https://doi.org/10.20998/2522-9052.2024.1.04.

2. O. Shmatko, S. Herasymov, Y. Lysetskyi and etc. **Development of the automated decision-making system synthesis method in the management of information security channels**, *Eastern-European Journal of Enterprise Technologies*, 2023, 6(9) (126), p.p. 39-49, https://doi.org/10.15587/1729-4061.2023.293511.

3. S. Yevseiev, V. Ponomarenko, O. Laptiev and etc. **Synergy of building cybersecurity systems: monograph**, Kharkiv: PC TECHNOLOGY CENTER, 2021, 188 p., https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=4700333.

4. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.

5. S. Yevseiev, R. Hryshchuk, K. Molodetska and etc. **Modeling of security systems for critical infrastructure facilities**, Kharkiv: PC TECHNOLOGY CENTER, 2022, 196 p., https://doi.org/10.15587/978-617-7319-57-2.

УДК 355.424.3

Герасимов С.В., Базарний С.В.

ЩОДО ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕРЕЖ ПРИ ПРОВЕДЕННІ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Широкомасштабна збройна агресія російської федерації проти України супроводжується інформаційними операціями, які спрямовані на внутрішні та зовнішні цільові аудиторії із завданням виправдати свої агресивні дії та переконати власне населення та громадськість інших країн у легітимності територіальних претензій. За дослідженнями фахівців у галузі інформаційно-психологічних операцій сутність інформаційної операції визначено як "здатність у поєднанні з іншими засобами вести масовані інформаційні кампанії проти населення держав для дестабілізації суспільства та уряду, примушення держави приймати рішення в інтересах протилежної сторони".

З метою протидії інформаційним операціям противника та створення сприятливих умов застосування своїх військ (сил) Збройними Силами України проводяться інформаційні операції та психологічні операції, що включають також психологічні акції та розповсюдження підготовленої спеціальної інформації для психологічного впливу на емоції, мотиви, раціональне мислення та поведінку цільової аудиторії противника. Можливими засобами розповсюдження інформації при проведенні можуть бути: розсилка СМС на мобільні телефони у визначеному районі, радіозвернення, звукомовні станції, друкована продукція (листівки, газети) та ін. В сучасних умовах найбільша увага приділяється засобам розповсюдження інформації в мережі Інтернет, особливо – у соціальних мережах.

У досліджені розроблено метод визначення місцезнаходження агентів соціальних мереж в інтересах інформаційної операції на основі комплексного підходу. Актуальність методу обумовлюється необхідністю уточнення цільової аудиторії противника в районі проведення інформаційної операції. Запропоновано комплексний метод визначення місцезнаходження агентів соціальних мереж, який базується на поєднанні даних аналізу соціальних зв'язків визначеного агента, геотегів та часу реєстрації його друзів у соціальній мережі, баз даних IP-адрес та геолокацій агентів соціальних мереж.

Перевагою розробленого методу є можливість його застосування без безпосереднього доступу до пристроїв агентів соціальної мережі, що користуються даними супутникових систем глобального позиціонування. Запропонований комплексний метод визначення місцезнаходження агентів соціальних мереж в інтересах інформаційної операції включає такі основні етапи, як: знаходження множини друзів визначеного агенту соціальних мереж; знаходження IP кожного друга агенту соціальних мереж з визначеної множини його друзів; за знайденими IP за допомогою баз даних геолокації IP визначається цільова аудиторія, у яку входять ті друзі агенту соціальної мережі, що мешкають у тому ж самому місті; для виключення впливу помилок у базах даних геолокації IP перевіряються місця реєстрацій друзів агенту соціальних мереж (за місцем та часом), чим визначається найбільш ймовірне їх постійне місцезнаходження; за результатом уточнення цільової аудиторії методом виключення тих агентів соціальної мережі, біль-

шість реєстрацій яких є в інших місцях, формується підсумкова цільова аудиторія за ознакою однакового географічного місцезнаходження агентів соціальних мереж.

Застосування запропонованого комплексного методу визначення місцезнаходження агентів соціальних мереж дає можливість підвищити ефективність проведення інформаційних операцій за рахунок більш точного визначення цільової аудиторії противника в районі проведення операцій. Напрямком удосконалення розробленого методу може бути його інтеграція з комплексними інформаційними системами психологічного впливу, а також використання методів та алгоритмів машинного навчання.

УДК 621.396.962

Герасимов С.В., Сорока В.В.

ЩОДО ЗМЕНШЕННЯ ПОХИБКИ ВИМІРЮВАЧІВ ХАРАКТЕРИСТИК ВИПАДКОВИХ СИГНАЛІВ ПРИ ПЕРЕДАВАННІ ДАНИХ

У відомих роботах та науково-технічній літературі представлений спрощений підхід до викладання основ побудови вимірювачів характеристик випадкових сигналів при передаванні даних у системах автоматизованого управління підрозділами або інформаційного забезпечення діяльності командирів. Спрощений підхід передбачає наведення структурних схем, алгоритмів обчислення статистичних (або вибіркових) характеристик при обґрунтуванні каналів передавання даних. Однак відсутній теоретичний аналіз похибок вимірювання зазначених оцінок при цифровій обробці, що виконується у вимірювачах випадкових сигналів, які зазвичай утворюються в інформаційних каналах. При цьому слід зазначити, що похибки вимірювачів характеристик випадкових сигналів можуть суттєво впливати на результат передавання даних (у системах автоматизованого управління підрозділами та інформаційного забезпечення діяльності командира).

Обґрунтовано розповсюдження гармонічних сигналів в радіоелектронних та електричних системах передавання даних (інформаційних каналах). Таке поширення синусоїдальних сигналів пов'язане з особливостями гармонійних сигналів. Проходження гармонійних сигналів через лінійні системи змінює лише фазу та амплітуду таких сигналів, але не впливає на зміну їх частоти, при цьому не з'являються нові частотні (гармонічні) складові. У вигляді суми гармонійних сигналів із застосуванням тригонометричних функцій можна уявити різні складні сигнали (функції). Слід зазначити, що із застосуванням тригонометричних функцій можна описувати різні фізичні процеси. Показано, що гармонійні сигнали піддаються діям випадкових сигналів (особливо у вигляді перешкод).

Тому у доповіді обґрунтовано поширення характеристик випадкових сигналів щодо різних фізичних явищ, технологічних процесів і технічних об'єктів. Показано відсутність теоретичного матеріалу для аналізу похибок вимірювання характеристик випадкових сигналів під час цифрової обробки у відповідних вимірювачах. Зроблено акцент на те, що похибки вимірювачів характеристик випадкових сигналів можуть суттєво впливати на результат визначення стану технічних інформаційних систем.

Метою дослідження є розробка методу оцінювання похибки вимірювачів показників випадкових сигналів. Запропоновано метод оцінювання похибки вимірювачів характеристик випадкових сигналів, що базується на раціональних алгоритмах обчислення вибіркової дисперсії, оцінки значень похибок вимірювання статистичних характеристик випадкових сигналів, що допускаються, у тому числі оцінки впливу точності вимірювання елементів вибірки на точність цих характеристик.

У роботі визначено раціональний алгоритм обчислення вибіркової дисперсії, отримано оцінки значень похибок вимірювання статистичних характеристик випадкових сигналів, що допускаються, у тому числі оцінка впливу точності вимірювання елементів вибірки на точність їх визначення.

Для алгоритму обчислення вибіркової дисперсії випадкових сигналів запропоновано два варіанти апаратурної реалізації. Теоретично обґрунтовано, що за простотою апаратурної реалізації та швидкодії раціональнішим є другий варіант алгоритму обчислень. Цей варіант алгоритму обчислення застосовано на розрахунку незміщеної оцінки дисперсії.

Отримані результати пропонується використовувати при побудові вимірювачів характеристик випадкових сигналів при передаванні даних у системах автоматизованого управління підрозділами та інформаційного забезпечення діяльності командира.

UDC 623.9

Herasimov S., Roshchupkin Y.

SYNTHESIS OF DIGITAL GENERATORS FOR MONITORING THE TECHNICAL CONDITION OF USERS' RADIO NAVIGATION SYSTEMS

Today, radio navigation systems of various users (vehicles, water, air transport, gas transport network, cellular communication equipment, etc.) ensure not only the safety of movement, but also provide accurate coordinates in the event of emergency events (accidents). Failure of the elements of this system can lead to significant material losses: disasters, loss of cargo, increase in the duration of the route, untimely detection of damage, etc. [1 – 7]. The need for the synthesis of a digital generator of sinusoidal signals for monitoring the technical condition of users' radio navigation systems is associated with increased requirements for the means of generating sinusoidal voltage of such systems and their ability to meet the specified characteristics with high accuracy [1, 3].

Today, the main means of generating sinusoidal signals for monitoring the technical condition of users' radio navigation systems are analog generators or generators, the principle of operation of which is to convert an analog signal into a digital form. However, the digital synthesis of a signal of the required form implies a significant complexity of technical implementation compared to analog generators. Therefore, generators of sinusoidal signals based on digital methods are much more expensive than analog ones and require certain qualifications of service personnel. This shortcoming can be overcome by the use of stepwise approximation of the synthesized sinusoidal signal [2, 6].

According to the methodical error of approximation, which characterizes the degree of approximation of the generated signal to the desired one, the piecewise-staircase approximation is inferior to other types of approximation (with the same number of approximation sections), but due to simpler hardware implementation and a much smaller instrumental error, it turns out to be the most effective in general, and therefore proposed for use in digital generators [4, 5].

The paper examines the method of stepwise approximation of a sinusoidal signal and substantiates the main characteristics of such a signal. Such a signal provides the minimum value of the harmonic coefficient and the best approximation of the generated signal to a sinusoid with a given number of approximation levels per signal period. But the simplest for hardware implementation is the piecewise stepwise approximation with a uniform location of the approximation nodes in time.

We especially emphasize that this signal does not contain harmonics close to the main one, and the initial phase of the first harmonic is not always zero.

The results of the analysis of two other variants of the piecewise step signal approximating a sinusoidal signal are presented. Their main results are presented.

All three versions of the piecewise stepwise quasi-sinusoidal signal contain, in addition to the main, higher order harmonics, which depends on the number of approximation sections (steps) per signal period. For example, if the number of steps is 100, the signal will contain 99, 101, 199, 201, 299, 301, etc. higher harmonics. The amplitudes of the harmonics decrease sharply with increasing harmonic number (approximately inversely proportional to the harmonic number).

Thus, an increase in the number of approximation sections leads to an increase in the numbers and a decrease in the amplitudes of the higher harmonics in the stepwise signal. If necessary, the higher harmonics of the piece-step signal can be filtered and thus the quality of the signal is improved.

At large values of the number of steps of the piecewise step signal, the optimal approximation reduces the harmonics coefficient by 5% compared to the uniform approximation by level, and by 15% compared to the uniform approximation by time. With small values of the number of steps, this difference reaches (30 ... 50)%. Uniform approximation in level compared to uniform approximation in time gives a gain of 10%.

References

1. O. Daki, S. Herasimov and H. Zubrytskyi, **Digital Correlation Method For Power Measurement**, *Information Processing Systems*, № 4 (163), 2020, p.p. 15-26, https://doi.org/10.30748/soi.2020.163.02.

2. S. Herasimov, M. Pavlenko, E. Roshchupkin and etc. **Aircraft flight route search method with the use of cellular automata**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, is. 4, 2020, p.p. 5077-5082, https://doi.org/10.30534/ijatcse/2020/129942020.

3. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.

4. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (ISMSIT), 2022, p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.

5. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of airspace radio engineering monitoring systems**, *International scientific and practical conference* "*Application of information technologies in the preparation and operation of law enforcement forces"*, March 15, 2022, p.p. 31-32.

6. O. Brytov, D. Bieliaiev, S. Kukobko and etc. **Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects**, *Proceedings of the 3rd International Scientific and Practical Conference* "*Scientific Trends and Trends in The Context of Globalization*", UMEÅ, SWEDEN, 21-22.12.2021, p.p. 431-434, https://doi.org/10.51582/interconf.21-22.12.2021.050.

7. V. Dzhus, Y. Roshchupkin, S. Kukobko and etc. **Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction Method**, *Information Processing Systems*, 2021, Issue 4 (167), p.p. 19-26, https://doi.org/10.30748/soi.2021.167.02.

UDC 623.618.51

Herasimov S., Shmatko O.

AUTOMATED DECISION-MAKING SYSTEM FOR MANAGEMENT OF INFORMATION PROTECTION CHANNELS

Decision-making tasks when managing information security channels are not automated at a sufficient level [1, 2]. This leads to the fact that decisions to block information transmission channels are made on the basis of subjective assessments of decision makers (DMs), or using insufficiently complete information models. At the same time, in the process of functioning of information transmission channels, the results of the work of bodies identifying and blocking information leakage channels are poorly taken into account [3, 4].

Thus, managing information security channels now actually means collecting and displaying information about a possible data leak. Then influence (blocking) is assigned to each information channel separately and is carried out, in fact, manually.

The purpose of this research is to develop a method for synthesizing an automated decision-making system for managing information security channels, which takes into account uncertainty in determining information leakage channels and allows us to ensure the required level of security [5, 6].

A feature of the proposed structural diagram is that it takes into account both intellectual and technical features when making decisions when managing information security channels. Note that by intellectual features we mean the conclusions and proposals of the decision maker for managing information security channels. It is proposed to include technical features for monitoring information transmission channels and technical means for identifying (blocking) channels of possible information leakage. The proposed structure simplifies further solution of research problems.

The solution to the problem of assigning impacts when managing information security channels to cover information leakage is to determine the possibility of redirecting information through other channels. This decision depends on the method of identifying the channel of information leakage (technical channels of information leakage), the means of information leakage (technical means of espionage), the software speed of information transmission, and the information dissemination program. When solving such a problem, the time required to determine the threat and methods of influence to eliminate it is also calculated [7].

Thus, when assigning impacts on information leakage channels and areas of possible information attacks, this is a difficult logical and analytical task to solve.

The final results of solving the problem of assigning impacts to block information leakage channels are assessed qualitatively - if possible, automated control of information security channels [5].

A structural diagram of information exchange in managing information security channels has been developed. This block diagram allows you to schematically represent the order of tasks to be solved in a synthesized automated decision-making system when managing information security channels to formalize decision-making tasks. A feature of the proposed structural diagram is that it takes into account both intellectual and technical results of decision-making when managing information security channels. The implementation of the proposed scheme allows us to take into account the influence of the decision maker (a priori data) and the characteristics of technical means of monitoring information transmission channels (a posteriori data).

A comparative assessment of strategies for the planned information security process involves solving a multicriteria optimization problem. The logical-linguistic production hierarchical model is justified as a mathematical model for determining protection parameters.

The main form of recording in it is interconnected tables of linguistic rules, which are a display connecting the previous, current and future states of the described process.

The process of determining information security parameters directly in the logical-linguistic hierarchical production model is difficult to trace. Therefore, this process is described using an algebraic model that is closest to a linguistic description. If it is inappropriate to synthesize products in order to reduce the number of production rules, it is proposed to use the fuzzy identification method. The method of formalizing knowledge to determine appropriate strategies for the planned information security process has been improved. It differs from the known ones in the formation of a set of production rules taking into account parameters that, when developing recommendations under conditions of non-stochastic uncertainty, describe a fuzzy environment. The method of processing knowledge to determine appropriate strategies for the planned information security process has also been improved. It differs from the known ones in the processing of knowledge based on the developed procedure for their algebraic approximation and fuzzy identification.

The development of this research consists in substantiating a multicriteria optimization problem in a fuzzy formulation when managing information security channels. Solving this problem will make it possible to determine a rational strategy for the planned information security process using an automated decision-making system.

References

1. O. Shmatko, S. Herasymov, Y. Lysetskyi and etc. **Development of the automated decision-making system synthesis method in the management of information security channels**, *Eastern-European Journal of Enterprise Technologies*, 2023, 6(9) (126), p.p. 39-49, https://doi.org/10.15587/1729-4061.2023.293511.

2. S. Yevseiev, V. Ponomarenko, O. Laptiev and etc. **Synergy of building cybersecurity systems: monograph**, Kharkiv: PC TECHNOLOGY CENTER, 2021, 188 p., https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=4700333.

3. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.

4. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (ISMSIT), 2022, p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.

5. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of airspace radio engineering monitoring systems**, *International scientific and practical conference "Application of information technologies in the preparation and operation of law enforcement forces"*, March 15, 2022, p.p. 31-32.

6. S. Yevseiev, R. Hryshchuk, K. Molodetska and etc. **Modeling of security systems for critical infrastructure facilities**, Kharkiv: PC TECHNOLOGY CENTER, 2022, 196 p., https://doi.org/10.15587/978-617-7319-57-2.

7. S. Herasymov, A. Tkachov, S. Bazarnyi. **Complex Method of Determining the Location of Social Network Agents in the Interests of Information Operations**, *Advanced Information Systems*, 8 (1), p.p. 31-36, https://doi.org/10.20998/2522-9052.2024.1.04.

УДК 629.3

Глущенко М.О.

СИСТЕМА ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ТА РЕМОНТУ ЗБРОЙНИХ СИЛ США

Система технічного обслуговування (ТО) збройних сил (ЗС) США є складовою тилового забезпечення бойових дій поряд із системами постачання та розподілу матеріальних засобів, транспортного, медичного, інженерного, фінансового та інших видів підтримки.

Технічне обслуговування та ремонт (ТОіР) матеріальних засобів є критичним елементом у підтримці боєздатності та боєздатності збройних сил.

Нормативні документи Міністерства оборони США визначають концепцію підтримки та готовності матеріальних засобів, спрямовану на реалізацію наступних вимог:

- забезпечення високої боєздатності та боєготовності озброєння військової техніки (ОВТ) у мирний та воєнний час;
- підтримка швидкого проектування сил (забезпечення розгортання та дій експедиційних угруповань);
- визначення оптимальної структури життєвого циклу ОВТ;
- інтеграція людських, матеріальних, інформаційних та фінансових ресурсів у ході практичної діяльності.

Стратегія підтримки бойової готовності ОВТ полягає в тому, щоб забезпечити їх необхідну готовність до застосування за мінімальної вартості життєвого циклу. Реалізація цієї стратегії досягається шляхом оптимального розподілу ресурсів між розробкою, виробництвом, експлуатацією та ремонтом.

Готовність матеріальних засобів у системі тилу ЗС США полягає у підтримці встановленого коефіцієнта готовності ОВТ з урахуванням параметрів їхньої надійності та сумарних затримок часу перебування у непрацездатному стані (адміністративних, технічних та інших) при обмеженні сумарної вартості життєвого циклу виду ОВТ.

Для розрахунку та аналізу варіантів забезпечення готовності матеріальних засобів комітетом начальників штабів ЗС США затверджено єдиний набір параметрів, що застосовуються на всіх стадіях роботи ОВТ: запаси, надійність (безвідмовність), середній час простою матеріальних засобів у непрацездатному стані та витрати ЗС на підтримку їхньої готовності.

В даний час у ЗС США практикується змішана система ТОіР ОВТ, де передбачено два види обслуговування та ремонту:

- перше – сервісне обслуговування, що здійснює фірмовий виробник;
- друге – за технічним станом ОВТ, що здійснюється у військах.

Сервісне обслуговування визначається як ТО, яке виконується з метою зменшення ймовірності відмови або підтримки працездатності ОВТ. У сервісне обслуговування входить профілактичне обслуговування з напрацювання (кілометри пробігу, наліт, постріл пуску) здійснюється на етапі випробувань та підконтрольної експлуатації настановної партії ОВТ для збору статистичних даних про їх надійність.

Система ТОіР з технічного стану ОВТ включає три види обслуговування та ремонту з технічного стану:

- з контролем рівня надійності;
- з моніторингом експлуатаційних параметрів;
- комплексна система, що поєднує перші два види.

Технічне обслуговування, орієнтоване на надійність або, як правило, на безвідмовність, ґрунтується на оцінці результатів моніторингу ймовірностей відмов на інтервалі експлуатації виробу та аналізі наслідків відмов.

При цьому можуть застосовуватися два методи:

- аналіз видів та наслідків відмов – якісний метод аналізу, заснований на дослідженні можливих видів відмов та несправностей складових частин та їх вплив на виріб;
- аналіз видів, наслідків та критичності відмов – кількісний чи якісний метод аналізу, заснований на аналізі видів та наслідків відмов разом з розглядом ймовірності їх виникнення та серйозності наслідків.

Система ТОіР ОВТ станом з моніторингом експлуатаційних параметрів заснована на статистичній оцінці швидкості зміни параметрів працездатності виробу та застосовується для визначення періодичності заміни складальної одиниці ОВТ. При цьому визначальним параметром ОВТ вибирається такий спостерігаємий параметр, який однозначно характеризує її технічний стан, наприклад, потужність, точність та інші.

Концепція підтримки та готовності матеріальних засобів ЗС США, методи розрахунку готовності матеріальних засобів, система ТОіР, де передбачено два види обслуговування та ремонту – сервісне та за технічним станом сприяють підтримці необхідної готовності ОВТ до застосування за мінімальної вартості життєвого циклу шляхом оптимального розподілу ресурсів між розробкою, виробництвом, експлуатацією та ремонтом.

Gnatiuk S., Sakovich L.

DETERMINATION OF SCIENTIFIC AND TECHNICAL DIRECTIONS FOR PROVIDING PERFORMANCE INDICATORS STATE SYSTEM OF GOVERNMENT COMMUNICATION

The State Government Communication System (SGMS) of Ukraine includes an integral component — the information protection system, which is a set of organizational structures united by the goals and tasks of information protection, regulatory, legal, and material-technical base and is aimed at providing engineering and technical measures availability, confidentiality and integrity of information. It is continuously improved by the introduction of digital signal processing during the exchange of information by subscribers and the use of modern software-controlled means of communication. At the same time, the amount of software and its capabilities are constantly growing. At the same time, compared to other law enforcement agencies of Ukraine, the State System of Government Communication has rather high requirements regarding reliability: the downtime of the system should not exceed 5 minutes per year, i.e., the level of subscriber availability is 0.999999. To ensure these requirements, it is necessary to define a set of scientific and technical tasks for the modernization of the existing and the creation of a promising communication system for its functioning in modern conditions of military operations. Taking into account modern challenges and threats, it is necessary to introduce new security mechanisms of electronic communications with a corresponding increase in the reliability of their functioning [1]. This requires a comprehensive approach to increasing the operational reliability of software-controlled communication devices, improving their metrological and diagnostic support during repair and maintenance.

The analysis of the schematic and constructive construction of software-controlled means of communication allows to assign them to the class of multi-mode objects, the structure of which changes in the course of their intended use, depending on the mode of operation. That is, the resource of individual subsets of elements of software-controlled means of communication does not diverge evenly, so the real values of the reliability indicators exceed the calculated ones, which do not take this circumstance into account.

A method for estimating the values of the reliability indicators of software-controlled means of communication with a change in structure is proposed, which refines the failure

time to 33% and reduces the comprehensive reliability indicator, i.e., the failure rate to 28%, using the example of a modern software-controlled radio station [2].

Of particular importance is the assessment of software reliability, which is significantly different from the assessment of hardware reliability. A new software reliability assessment model has been proposed, which, unlike the existing ones, allows to specify the number of errors and the number of identified software deficiencies during the year of operation of the software-controlled complex "Bastion" and differs from the real number by only 3.1%.

A method of quantitative assessment of the reliability indicators of software-controlled means of communication, taking into account the quality of their software, is proposed. Its verification for 2 years of operation of the same complex showed that the value of the root mean square deviation of the calculation results from the experimental data is $0.97 \leq \sigma \leq 1.14$, which is better than when using known methods.

A new method of forming requirements for metrological support of modern software-controlled means of communication to ensure their technical maintenance and current repair is substantiated. At the same time, possible types of conditional diagnostic algorithms are considered, for each of which the choice of measuring equipment is justified with the minimum required probability value of the correct assessment of the result of the inspection during the assessment of the technical condition of software-controlled means of communication with a given accuracy [3]. An example of using the method for a modern radio relay station is given, which made it possible to reduce the average recovery time during current repairs by 6.4%.

The question of the organization of cooperation of the crews of hardware technical support and hardware communication during the restoration of software-controlled means of communication in field conditions was studied. The method of quantitative assessment of quality when using independent, compatible and zonal group search for defects is proposed, which allows in each specific case to reasonably choose a conditional algorithm that ensures the restoration of software-controlled means of communication in the shortest possible time. An example of its use for the current repair of a modern radio relay station is given, which ensures the restoration of its working capacity by two masters in 2 minutes.

Simulation of the procedure for checking the parameters of software-controlled means of communication during their maintenance by condition was also carried out. The research results are summarized in the form of a methodology. Modeling the maintenance process based on the state of software-controlled communications on a computer shows a possible reduction in the number of tested subsystems by up to 37% without reducing the probability of correctly assessing the technical state of the product.

The issue of ensuring the security of modern electronic communications of the State System of Government Communications and scientifically based measures to improve them are separately considered [4].

The use of information technologies allows you to obtain an objective assessment of the technical condition of software-controlled means of communication both during their maintenance and during ongoing repairs. For this purpose, the data base of enterprises of manufacturers of metrology centers and repair bodies includes real-time indicators of the quality of functioning of software-controlled means of communication. The processing of statistical data in the knowledge base using the given results allows to improve schematic and constructive solutions in the production process, to improve metrological and diagnostic support during the technical operation of software-controlled means of communication in combat conditions.

In this way, the goal of the research was achieved and the problem of non-compliance of the existing values of the main quality indicators of the State System of Government Communications with the requirements of application in wartime was solved by a comprehensive approach taking into account individual components [5].

References

1. Gnatiuk S. Method of Estimating the Values of Reliability Indicators of Objects with Variable Structure, CEUR Workshop Proceedings// Sergii Gnatiuk, Lev Sakovich, Yana Kuryata, Roman Odarchenko, Viktor Gnatyuk. (CEUR-WS.org/Vol-3288/paper4.pdf/pp.33-43.

2. Gnatiuk S.E. Quantitative assessment of the reliability of software-controlled means of communication / S.E. Gnatiuk, L.M. Sakovich, E.V. Ryzhov// K.:ISZZI, Collection of scientific works "Information Technology Security".-2016.-Vol. 4, No. 1, pp. 84-90.

3. Gnatiuk S. Control of the technical condition of critical infrastructure objects/ S. Gnatiuk, L. Sakovich// XIV International Scientific and practical conference “Innovations and prospect of world science//Canada, Vancouver, 2022.

4. Pyrozhkov S. I Assessing the reliability of complexsystems under uncertainty in the contextof ensuring national resilience// Pyrozhkov S. I., Reznikova O. O., Gnatiuk, S. Ye., Kuryata Ya. E/ General problems of the modern researc hand innovation policy/doi.org/10.15407/scine19.04.003. NASU Science and Innovation, №4., P.1-12, 2023.

5. Gnatiuk S. The method of estimating values of reliability indicators of objects with a variable structure// Volkov O., Gnatiuk S., Odarchenko R., Bondar S., Simachin V// ISSN 2706-8145, Control systems and computers, 2023, № 1, pp.33-53 //doi.org/10.15407/csc.2023.01.033

УДК 621.396.96

Гнойовий Д.Ю., Бакуменко Б.В.

АНАЛІЗ СТАНДАРТІВ НАТО ДЛЯ ІМПЛЕМЕНТАЦІЇ В РАДІОТЕХНІЧНОМУ ПІДРОЗДІЛІ

Досвід відсічі збройної агресії російської федерації проти України показав, що радіотехнічні підрозділи відіграють одне із найважливіших завдань в системі радіолокаційного виявлення засобів повітряного противника. Успішне виявлення повітряних цілей, особливо крилатих ракет та БпЛА, та видача про них радіолокаційної інформації вогневим засобам не тільки Повітряних Сил Збройних Сил України, а також мобільним вогневим групам, що сформовані в частинах і підрозділах інших видів Збройних Сил України та окремих родів військ, значно збільшує ймовірність їх знищення. Така ефективність бойових дій підтвердження знищенням 15 ворожих літаків А-50, Су-34 та Су-35 за 15 діб в другі половині лютого початку березня 2024 року.

Успішне виконання завдань підрозділами радіотехнічних військ як і Повітряних Сил Збройних Сил України в цілому залежить від рівня боєздатності не тільки штатного озброєння і військової техніки, а в значній мірі і отриманого від держав-членів НАТО.

Тому питання імплементації стандартів, прийнятих у арміях держав-членів НАТО, у Збройних Силах України для покращення ефективності оборонної реформи в цілому має важливе значення.

Пошук ефективних підходів до імплементації європейських і євроатлантичних стандартів у Збройних Силах України в цілому та безпосередньо в підрозділах радіотехнічних військ задля однакового їх тлумачення і застосування, наближення до принципів і стандартів, прийнятих у арміях розвинутих держав-членів НАТО.

У збройних сил держав-членів НАТО ухвалені так звані стандартизаційні угоди (англ. Standardization Agreement – STANAG), які дають змогу спільно ефективно управляти силами і засобами збройних сил, проводити спільні операції та місії, бойову підготовку, технічне оснащення армій, розробляти та виробляти необхідне озброєння і військову техніку.

Виходячи з вищесказаного та враховуючи досвід виконання завдань в ході перших днів війни, стаціонарні підрозділи в оперативній досяжності противника були знищені або понесли значних втрат. Стало зрозумілим, що для збереження боєготовності та прихованості створення і нарощування радіолокаційного поля РТВ, слід постійно змінювати позиції виконання бойового завдання.

При зміні позиції радіотехнічного підрозділу змінюється і його бойове завдання. Підготовка до виконання завдання передбачає декілька етапів один із яких відпрацювання бойових документів. Графічні документи виконуються на карті або у вигляді схеми на папері (карті). Враховуючи особливості виконання завдань, як розташування в польових умовах без промислової електромережі, виконання бойових завдань в умовах вогневого впливу противника, відпрацювання графічних бойових документів у відповідності до вимог діючих керівних наказів та вимог потребує значного часу, а в окремих випадках просто неможливе.

Тому актуальним питанням є розробка відповідного програмного забезпечення, яке дозволить відпрацювання визначених бойових документів відповідно до стандартів НАТО в електронному вигляді.

Таким чином, впровадження електронних бойових документів відповідно до стандартів НАТО значно скоротить час на підготовку до виконання завдання та є розвитком спроможностей військ (сил), який реалізується шляхом нарощування (вдосконалення) необхідних їх базових компонентів, передбачених системою DOTMLPFI, що активно застосовується в арміях держав-членів НАТО.

UDC 621.396.2

Holovan O.

APPLICATION AREA OF METEOR RADIO CHANNELS

The activities of law enforcement agencies can be carried out in hard-to-reach and remote areas, as well as under the influence of deliberate influences. The review provides data on known meteor radio communication networks that can be used on both stationary and moving objects. Their characteristics and algorithms should be taken into account when developing effective meteor radio communication systems based on modern information and telecommunication technologies.

Meteor radio communication systems (MRS) can be a low–cost alternative to satellite communication systems and are used:

- in service communication between mobile objects;
- in communication in hard–to–reach and remote areas;
- in warning systems for emergency events and natural disasters;
- in dispatching control vehicles and collecting information about the location of moving objects.

Growing concerns about the vulnerability of satellite communications and their low cost-effectiveness for transmitting low-traffic information have once again made SMR an attractive alternative method for long-distance communications [1 - 3].

One of the first, in 1952, was the creation of the JANET MRS by the Canadian Defense Research Council. The US National Bureau of Standards has approved some of the methods developed in the JANET system and enabled further experiments [4].

In 1965, the meteor communications system COMET (COMmunication by MEteor Trails) was introduced by NATO's Supreme Headquarters Allied Powers in Europe (SHAPE). This first operational military system operated between stations in the Netherlands, France, Italy,

West Germany, Great Britain and Norway. The COMET system used a signaling rate of 2000 baud and FSK with a deviation of 6 kHz. The feasibility of using COMET in various application conditions has been demonstrated [5].

The first civilian MRS system, SNOTEL, was built in the interests of the Ministry of Agriculture by Western Union. It began functioning in 1977 and provided collection of information about the state of snow cover in the mountains [6, 7].

There are several meteor radio communication systems operating in Alaska, two of which are AMBCS (Alaska Meteor Burst Communication System) and USAF (United States Air Force Meteor Burst Communication System). AMBCS, in operation since 1977, is used by several government agencies. The Federal Aviation Administration (FAA) forwards meteorological information to the AMBCS and uses it during search and rescue operations in remote areas [6]. The USAF system is used to provide redundant connections between the Regional Operations Control Center (ROCC) and 13 Long Range Radar (LRR) stations located throughout Alaska [8]. The USAF system also provides limited voice support that allows the ROCC to control interceptor aircraft via MRS.

An example of a modern integrated MRS network is the joint system of aerospace defense of the United States and Canada (NORAD) [9]. The main purpose of this meteor radio communication network is global control of strategic air transport after a nuclear strike (restoration of control). Further development of USAF meteor communications is aimed at integrating these systems into a single meteor communications system that will cover all major operational centers.

The US Federal Emergency Management Agency (FEMA) has developed a concept for the Meteor Burst Warning/Communications System (MBWCS). The FEMA MBWCS concept is complementary to the fixed National Warning System (NAWAS). It includes 10 regional meteor master station (MS) terminals, meteor transceivers at Emergency Operations Centers (EOCs) in 48 contiguous countries, and warning receivers at 5,000 designated control points (including 2,600 NAWAS control points) throughout the country [10].

Coded warning messages input from the National Warning Center (NWC) or alternate NWC are acknowledged and broadcast to nearby master stations, government EOCs, and warning receivers. MBWCS will also provide two-way point-to-point communications between adjacent master stations (MSs), as well as master stations and government EOCs in designated areas. It should be noted that this system is not adaptive.

Further improvement of meteor radio communication systems should be aimed at increasing throughput and reducing connection latency. This is possible by using adaptation in transmission speed and length of information packets depending on operating conditions, the use of smart antennas, as well as the use of large ensembles of complex broadband signals and optimal methods for processing them.

References

1. Allen, B. B. (1989). *Meteor Burst Communications For The U.S. Marine Corps Expeditionary Force* (Accession Number: ADA207831) [Master Thesis, Naval Post Graduate School Montery, CA]. https://apps.dtic.mil/sti/citations/ADA207831

2. Weitzen, J. A. (1993). Meteor Scatter Communication: A New Understanding. In D.L. Schilling (Ed.), *Meteor Burst Communications Theory and Practice*, (pp.9-58). Wiley-Interscience; 1st edition.

3. Jernovics, J. P. (1990). Meteor Burst Communications: An Additional Means Of Long-Haul Communications". https://www.globalsecurity.org/space/library/report/1990/JJP.htm

4. Forsyth, P.A., Vogan, E.L., & Hines, C.O. (1957). The Principles of JANET - A Meteor-Burst Communications System. *Proceedings of the IRE, 45*(12), 1642 – 1657. DOI**:** 10.1109/JRPROC.1957.278296

5. Bartholome, P. J. and Vogt I. M. (1968). Comet - A New Meteor Burst System Incorporating ARQ and Diversity Reception. IEEE Trans. on Comm., Vol. COM-16 No.2, pp. 268-278. DOI: 10.1109/TCOM.1968.1089833

6. Hellweg, G. A. (1987). Meteor-Burst Communications: Is This What The Navy Needs? Masters Thesis, Naval Post Graduate School, Monterey, CA, June 1987.pp. 775-771. https://core.ac.uk/download/pdf/36715588.pdf

7. Johnson, D. E. (1987). Ten years experience with SNOTEL meteor burst data acquisition system. Proc. Meteor Burst Commun. Sym., vol. SII, pp. 5-20, Nov. 1987.

8. Heacock, P. K. and Price F. D. (1984). "How the USAF Talks on a Star!" Popular Communications, (September 1984), 44-49.

9. Hoff, J.A. (1988). The Utility of Meteor Burst Communications. *IEEE Conference on Military Communications*, [MILCOM 88, San Diego, CA, October 1988, vol.2, pp. 565-570]. DOI**:** 10.1109/MILCOM.1988.13446

10. Cohen, D., Grant, W., & Steele, F. (1989). Meteor Burst System Communications Compatibility. *NTIA Report 89-241, March. 1989*. https://www.ntia.doc.gov/files/ntia/publications/89-241_ocr1_20130514113154_215619.pdf

УДК 623.644, 623.647

Горєлишев С.А., Залевський Г.С.

МОДЕЛЮВАННЯ ХАРАКТЕРИСТИК РОЗСІЮВАННЯ КОМБИНОВАНИХ ОБ'ЄКТІВ РЕЗОНАНСНИХ РОЗМІРІВ, КОНСТРУКЦІЯ ЯКИХ МІСТИТЬ МЕТАЛЕВІ І ДІЕЛЕКТРИЧНІ КОМПОНЕНТИ

Запропоновано методи моделювання характеристик розсіювання комбінованих об'єктів, зокрема безпілотних летальних апаратів, що містить металеві і діелектричні елементи конструкції. Це дозволить при обмеженої тривалості проведення розрахунків з заданої точністю розраховувати вторинні характеристики розсіювання комбінованих резонансних об'єктів у метровому і дециметровому діапазонах хвиль

Аналіз бойового досвіду та перспектив розвитку технічних радіолокаційних засобів показує, що найближчим часом радіолокаційні станції будуть основним, а при певних обставинах єдиним засобом, здатним в будь-який час року і доби, в умовах поганої оптичної видимості (туман, задимлення і запиленість атмосфери, опади, тощо) оперативно і з високою достовірністю виявляти маловисотні повітряні та наземні цілі.

Методи математичного моделювання характеристик вторинного випромінювання маловисотних повітряних та наземних радіолокаційних об'єктів визначаються складністю їх конструкції, характеристиками матеріалів, з яких виготовлені елементи конструкції об'єктів та їх електричними розмірами [1].

Так, наприклад, безпілотні летальні апарати (БПЛА) середньої і великої дальності мають фюзеляж, крила, стабілізатори і кіль, виготовлені з металу або вуглепластика. Їх поверхню із достатньою для практики точністю можна вважати ідеально-провідними, і якщо розміри БПЛА відносяться до резонансної області для розрахунку його радіолокаційного розсіювання доцільно застосовувати метод, заснований на розв'язанні інтегральних рівнянь магнітного поля (ІРМП) [2].

Тактичні БПЛА, як правило, у своєму складі мають елементи з металевою поверхнею, діелектричні елементи та радіопрозори елементи, тобто їх необхідно розглядати як комбіновані об'єкти. Розміри БПЛА і розмах крил можуть мати довжину порядку 2 м, що для метрового і дециметрового діапазону буде відповідати резонансним розмірам. Аналізуючи конструкцію таких БПЛА бачимо що фюзеляж, крила і стабілізатори,

як правило, виготовляються з діелектричного матеріалу і мають тонкі стінки (до 5 мм). Тому слід очікувати, що у метровому і дециметровому діапазонах фюзеляж БПЛА буде радіопрозорим. Про це додатково свідчить той факт, що під ним, як правило, розташовуються антени системи управління, зв'язку та передачі даних. Такі елементи конструкції як рухова установка (двигун із глушником), блоки управління і корисного навантаження є елементами з металевою поверхнею, а паливний бак, що має тонкі стінки, наповнений бензином та гвинт можна вважати однорідним діелектричним об'єктом. Розміри перерахованих елементів складають одиниці-десятки сантиметрів.

У метровому і дециметровому діапазонах хвиль для розрахунку характеристик розсіювання комбінованих об'єктів резонансних розмірів доцільно застосовувати методи, засновані на розв'язанні інтегральних рівнянь (ІР). Для розрахунку електромагнітного полю (ЕМП), розсіяних резонансними металевими елементами конструкції БПЛА, запропоновано алгоритм, заснований на застосуванні електродинамічного методу розрахунку, що передбачає обчислення щільності електричного струму на поверхнях металевих розсіювачів шляхом розв'язання ІРМП [2,3]. У випадку резонансних діелектричних елементів конструкції БПЛА запропоновано електродинамічний метод, заснований на розв'язанні системи інтегральних рівнянь Мюллера (СІРМ) для обчислення щільностей еквівалентних електричного і магнітного струмів на поверхні діелектричних розсіювачів [3].

ЕМП, розсіяне таким складним комбінованим розсіювачем, як БПЛА, необхідно обчислювати із урахуванням електромагнітної взаємодії металевих і діелектричних елементів конструкції. Базові варіанти розташування металевих і діелектричних елементів конструкції наведені на рис. 1, де V_1 – простір, який займають металеві елементи конструкції , V_n , $n=2,3$ – простір, який займають діелектричні елементи, з відповідними відносними проникностями $\varepsilon_n = \varepsilon_n' + i\varepsilon_n''$, S_n – поверхня відповідного простору.

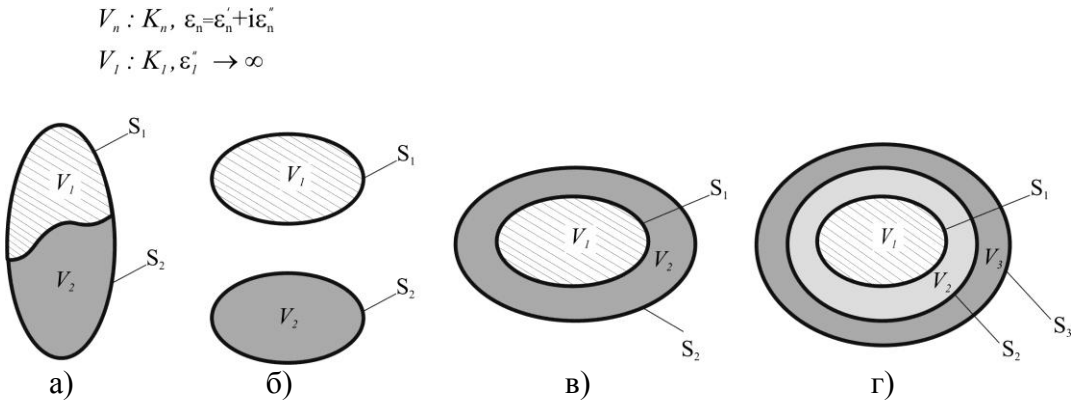


Рисунок 1 – Варіанти можливого розташування металевих і діелектричних елементів конструкції відносно один до одного

Так для варіанту а) і б) пропонується характеристики вторинного випромінювання комбінованого об'єкту у метровому і дециметровому діапазонах хвиль розраховувати як когерентну сума полів, розсіяних його металевими і діелектричними елементами конструкції. Сума розсіяних ЕМП з урахуванням їх фази за умови рівності нулю первинного поля у точці прийому $\vec{Q}_{sc}$ дозволяє врахувати електромагнітну взаємодію окремих металевих і діелектричних елементів конструкції.

$$\vec{p}^{\,sc} \cdot \vec{H}^{\,sc}\left(\vec{Q}_{sc}\right) = \vec{p}^{\,sc} \cdot \left(H_{met}^{sc}\left(\vec{Q}_{sc}\right) + H_{diel}^{sc}\left(\vec{Q}_{sc}\right)\right), \quad (1)$$

де $H_{met}^{sc}\left(\vec{Q}_{sc}\right)$, $H_{diel}^{sc}\left(\vec{Q}_{sc}\right)$ – напруженості магнітного поля, розсіяного металевими і діелектричними елементами конструкції відповідно у точці прийому $\vec{Q}_{sc}$.

Проведені дослідження електромагнітної взаємодії окремих елементів конструкції літальних апаратів [1-3,7] показують, що застосування метода розрахунку ЕМП, розсіяного комбінованим БПЛА, заснованого на використанні ІРМП, СІРМ та інтегрального подання (1) забезпечує достатньо високу точність моделювання характеристик розсіювання БПЛА, які містять металеві і діелектричні елементи конструкції у метровому і дециметровому діапазонах хвиль.

Для варіантів розташування металевих і діелектричних елементів конструкції, наведених на рис. 1 в), г) необхідно застосовувати ітераційні методи, зокрема описаний у роботах [4-6]. Використання цих методів дає більш детальне врахування електромагнітної взаємодії металевих і діелектричних елементів конструкції. У окремих випадках для більш детального врахування електромагнітної взаємодії різнорідних елементів необхідно отримати відповідну систему ІР. Застосування ітераційних методів та систем рівнянь, що описують щільності струмів на поверхнях реальних комбінованих об'єктів, пов'язані із значними часовими витратами і потрібними комп'ютерними ресурсами.

Можливі випадки, коли різні елементи конструкції повітряного об'єкту можуть належати до різних областей (релеївської, резонансної і високочастотної). У цьому випадку для отримання високої точності обчислень і прийнятного часу на моделювання характеристик розсіювання доцільно застосовувати комбіновані методи, що передбачають, наприклад, застосування асимптотичних високочастотних методів розрахунку ЕМП, розсіяних електричне великими елементами конструкції і методу, заснованого на розв'язанні ІР для компонентів, розміри яких належать до резонансної області і подальшим врахуванням електромагнітної взаємодії між зазначеними елементами конструкції.

Таким чином запропоновано методи моделювання характеристик радіолокаційного розсіювання БПЛА, що містить металеві і діелектричні елементи конструкції. Даний підхід дозволяє достатньо точно розраховувати характеристики радіолокаційного розсіювання комбінованих БПЛА у метровому і дециметровому діапазонах хвиль при прийнятній тривалості проведення розрахунків.

Список використаних джерел

1. Вторинне випромінювання безпілотних літальних апаратів (математичне моделювання): монографія / О.І. Сухаревський, І.В. Калужинов, В.О. Василець та ін. // Під ред. О.І. Сухаревського. – Х.: ХАІ, 2022. – 270 с

2. Sukharevsky O. I. Modeling of Ultrawideband (UWB) Impulse Scattering by Aerial and Subsurface Resonant Objects Based on Integral Equation Solving / O. I. Sukharevsky, G. S. Zalevsky, V. A. Vasilets // Advanced Ultrawideband Radar: Signals, Targets, and Applications / Edited by J. D. Taylor. – Boca Raton London New York: CRC Press Taylor & Francis Group, 2016. – Chapter 5. – P. 195-235.

3. Zalevsky G. S. Integral Equation Modelling of Unmanned Aerial Vehicle Radar Scattering Characteristics in VHF to S Frequency Bands / G. S. Zalevsky, O. I. Sukharevsky, V. A. Vasilets // IET Microwaves, Antennas & Propagation. – 2021. Vol. 15, No. 10. – P. 1299-1309

4. Комбинированный метод расчета характеристик рассеяния объектов сложной формы и его применение для моделирования спектров винтовой модуляции вертолетов / Г. С. Залевский, М. М. Бречка, В. А. Василец, О. И. Сухаревский // Системи обробки інформації. – 2014. – Вип. 4(120). – С. 80– 85.

5. 144.Sukharevsky O. I. Iterative Algorithm for Simulation of EM Scattering by Objects, Contained Constructive Elements of Different Electric Sizes / O. I. Sukharevsky, 268 Література G. S. Zalevsky, V. A. Vasilets // 2017 XXIInd International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED), Sept. 25 – 28, 2017: Proc. – Dnipro, Ukraine. 2017. – P. 190-193.

6. 145.Combined Calculation Method for the Scattering Characteristics of Complex Shaped Objects and Its Application to Model Helicopter Rotor Modulation Spectra / G. Zalevsky, M. Brechka, V. Vasilets, et al. // 2020 IEEE Ukrainian Microwave Week (UkrMW-2020) : 21-25 Sept., 2020 : Proc. Vol. 2, 2020 IEEE 6th International Symposium on Microwaves, Radar and Remote Sensing (MRRS). – Kharkiv, 2020. – P. 473-477.

7. Залевский Г. С. Расчет характеристик рассеяния воздушных радиолокационных объектов резонансных размеров, основанный на итерационном алгоритме / Г. С. Залевский, О. И. Сухаревский // Известия вузов. Радиоэлектроника. – 2014. – Т. 57, № 6. – С. 13-25.

УДК 621.39:623.1/.7

Горобинський М.А., Овчаренко О.Ю., Гречка О.В., Гайбадулов Б.В.

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО УДОСКОНАЛЕННЯ АЛГОРИТМІВ АВТОСУПРОВОДЖЕННЯ ПОВІТРЯНИХ ЦІЛЕЙ, ЩО РЕАЛІЗУЮТЬСЯ СПЕЦІАЛІЗОВАНОЮ ЦИФРОВОЮ ОБЧИСЛЮВАЛЬНОЮ МАШИНОЮ БАГАТОКАНАЛЬНОЇ СТАНЦІЇ НАВЕДЕННЯ РАКЕТ 9С32

Поточна російсько-українська війна характеризується різноманіттям засобів повітряного нападу (ЗПН), що застосовуються збройними силами (ЗС) рф по важливих об’єктах (в тому числі і об’єктах критичної інфраструктури) та угрупуваннях військ Сил оборони України. В умовах радіоелектронного придушення та вогневого ураження своєчасне виявлення маневру ЗПН зенітними ракетними комплексами (ЗРК) є заставою успішного наведення зенітних керованих ракет на ціль при відбитті удару та живучості ЗРК [1-15].

За результатами аналізу алгоритмів функціонування ЗРК С-300В1 при супроводженні повітряних цілей було визначено доцільним використання в його обчислювальних засобах двох додаткових алгоритмів визначення маневру.

Перший ґрунтується на аналізі прискорень, що розраховуються за результатами оцінки координатної інформації шляхом поліноміальної апроксимації координат повітряної цілі в тривимірному просторі. Крім оцінок первинних координат (азимуту, кута місця та похилої дальності) алгоритм передбачає урахування похибок їх вимірювання за результатами аналізу коефіцієнтів підсилення в блоках його автоматичного регулювання.

Другий ґрунтується на аналізі оцінки повного вектору швидкості та зміні його орієнтації у просторі при переміщенні цілі на відстань, достатню для урахування похибок вимірювання первинних координат. У якості вихідних даних використовуються оцінки азимуту, кута місця, радіальної швидкості та похибки їх вимірювання.

При цьому враховується, що в обох алгоритмах оцінки кутових координат оцінки є корельованими.

Виявлення маневру пропонується здійснювати за критерієм "*k* з *n*" де *k* обирається в залежності від похибок вимірювання координат, *n* – кількість алгоритмів, що одночасно застосовуються.

Список використаних джерел

1. Dzhus, V., Roshchupkin, Y., Kukobko, S., Herasymov, S., Drob, N., & Trofymova, M. Estimation of noise radiance point sources multichannel direction finding systems resolution by linear prediction method. Sistemi obrobki ìnformacìï. 2021. № 4(167). С. 19-26. https://doi.org/10.30748/soi.2021.167.02

2. Сухаревский О.И., А.Ю. Шрамков & Рощупкин Е.С. (2005). Высокочастотный метод расчета диаграммы направленности антенны с учетом неоднородностей рельефа местности на позиции РЛС. Моделювання та інформаційні технології, (33), 174-181.

3. Рощупкин, Е.С., & Беляев, Д.Н. (1999). Измеритель коэффициента стоячей волны в виде ответвителя дециметрового диапазона волн. Збірник наукових праць за матеріалами 3-го міжнародного молодіжного форуму "радіоелектроніка і молодь у XXI столітті" 20-23 квітня 1999 р., 1, 52–55. https://doi.org/10.5281/zenodo.5591877

4. Крючков, Д. М., Рощупкін, Є. С., Калита, О. В., & Дранник, П. А. (2023). Пропозиції щодо підвищення ефективності відновлення сукупності різнотипних радіоелектронних засобів спеціального призначення при їх використанні в різних умовах. XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023), Kharkiv. https://doi.org/10.5281/zenodo.10257044

5. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2006). Алгоритмы когерентной обработки широкополосных сигналов на промежуточной частоте с использованием схем фазонастраивающих контуров с управляемыми дисперсионными линиями задержки в крупноапертурных антенных решетках и многопозиционных системах. Прикладная радиоэлектроника, (Т.5, №2), 250-254.

6. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2005). Организация когерентной обработки на промежуточной частоте при приеме широкополосных сигналов крупноапертурными антенными решетками и многопозиционными системами. Прикладная радиоэлектроника, (Т.4, №4), 437-440.

7. Бєляєв, Д.М. Застосування векторних аналізаторів сигналів для забезпечення електромагнітної сумісності радіоапаратури / Д.М. Бєляєв, С.В. Герасимов, С.В. Кукобко [та ін.] // Збірник наукових праць ЦНДІ ОВТ ЗС України, - 2016. №3(62), -с. 77-84.

8. Tymchenko, S., Kaplun, Y., Roshchupkin, E., Kukobko, S. (2023). Substantiation of Time Distribution Law for Modeling the Activity of Automated Control System Operator. In: Shkarlet, S., et al. Mathematical Modeling and Simulation of Systems. MODS 2022. Lecture Notes in Networks and Systems, vol 667. Springer, Cham. https://doi.org/10.1007/978-3-031-30251-0_9

9. Рощупкін Є.С. Великоапертурна (рознесена) радіолокаційна система: пат. 148518 Україна : G01S7/42, H01Q21/00 / Є.С. Рощупкін, С.В. Герасимов, С.В. Кукобко, М.В. Борисенко, Ю.О. Крихтін, О.Ф. Галицький, Б.В. Гайбадулов, В.В. Джус, І.В. Помогаєв, В.В. Борисов, Ю.О. Чміль, А.Ю. Задорожна. – u 202100336; заявл. 29.01.2021; опубл. 18.08.2021, бюл. № 33/2021, – 7 с.

10 Herasimov S., Roshchupkin E. (2022). Parameters of monitoring the technical condition of airspace radio engineering monitoring systems. International scientific and practical conference "Application of information technologies in the preparation and operation of law enforcement forces", Kharkiv.

11. Рощупкін, Є. С., Гречка, О. В., Галицький, О. Ф., & Гайбадулов, Б. В. (2023). Аналіз факторів, що впливають на ефективність відновлення різнотипних радіотехнічних засобів складної системи під час виконання завдань за призначенням в екстремальних умовах. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей тринадцятої міжнародної науково-технічної конференції. Том 1: секції 1, 3, 4, Баку-Харків-Жиліна. https://doi.org/10.5281/zenodo.7868194.

13. Кукобко С.В., Місценко Р.В., Бритов Д.М., Рощупкін Є.С., & Гайбадулов Б.В. (2023). Пропозиції щодо автоматизації процесу прийняття рішення при класифікації ситуацій у повітряному просторі. Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку", Харків

14. Кукобко С.В., Рощупкін Є.С. (2022). Моделювання системи технічного обслуговування безпілотних літальних апаратів. Комплексне забезпечення якості технологіч-

них процесів та систем (КЗЯТПС – 2022): тези доповідей XII Міжнародної науково-практичної конференції, Чернігів

15. Herasimov, S., Borysenko, M., Roshchupkin, E. et al. Spectrum Analyzer Based on a Dynamic Filter. J Electron Test 37, 357–368 (2021), https://doi.org/10.1007/s10836-021-05954-0

УДК 621.39

Городиський Р.О., Вавpічен О.А.

ВРАЗЛИВОСТІ СТІЛЬНИКОВИХ МЕРЕЖ, МЕТОДИ ПОКРАЩЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ В НИХ

З інтенсивним розвитком стільникових мереж п’ятого покоління виникає проблема забезпечення безпеки в таких мережах. Незважаючи на те, що в стандартах LTE (Long-Term Evolution) передбачені вбудовані заходи безпеки, сама мережева інфраструктура недостатня для вирішення усіх проблем, пов’язаних з безпекою. Стільникова мережа LTE, на відміну від попередніх поколінь мереж, підтримує більше видів послуг та має більш широкий спектр функцій. Такі технології, як Інтернет речей (IoT), розширена реальність (AR), віртуальна реальність (VR) та машинне навчання (M2M), V2X, потребують швидкої, надійної та розгалуженої мережі, щоб не відставати від темпів розвитку. Нові підприємства та технології, які діють у епоху стільникової мережі LTE, стикаються з новими проблемами безпеки та конфіденційності. Стільникові мережі зв’язку наразі є одними з найпоширеніших у світі. Останнім технологічним вдосконаленням, що широко використовується, є стільникові мережі LTE. Ці мережі використовуються для передачі голосу, даних, підключення стаціонарних пристроїв та пристроїв Інтернету речей. Після аналізу вразливостей, що описані вище, включаючи архітектуру стільникових мереж LTE і відсутність мережевих вузлів, призначених для моніторингу кіберінцидентів, можна зробити висновок, що створення архітектури центру моніторингу та реагування на кіберінциденти у стільникових мережах LTE є надзвичайно актуальною задачею. Це допоможе продовжити розвиток цих мереж, уникнути можливих кіберінцидентів і забезпечити їхню стійкість у майбутньому [1].

Проблемам стільникових мереж, захисту інформації в них присвятили багато робіт вітчизняні та закордонні вчені: А.В. Гарист, І.А. Пількевич, В.І. Котков, Н.М. Лобанчикова, І.І. Сугоняк, В.Л. Бурячок.

Стільникові мережі зв’язку LTE не тільки успадкують уразливості мереж четвертого покоління, а й можуть обзавестися новими недоліками безпеки. Поряд з високою швидкістю, низьким енергоспоживанням і мінімальними затримками сигналу, очікується активне використання в стільникових мережах LTE технологій віртуалізації мережевих функцій (Network Function Virtualization). Заміна апаратних елементів програмними має багато позитивних ефектів, проте потенційно зробить стільникові мережі ще більш уразливими для атак зловмисників.

Незважаючи на всі існуючі переваги, в стільниковій мережі LTE є також ряд недоліків, серед яких предметом розгляду даної наукової праці є вразливості від кібератак. Перша загроза – атаки DoS (Denial of Service) на мережу. Ємність радіоканалу в стільниковій мережі LTE передбачається велика, але все ж вона має обмеження, а тому може бути повністю вичерпана. Наступним класом загроз є вірусні атаки. Хоча таким атакам піддаються пристрої, а не мережі, LTE надають можливість підвищити швидкість поширення шкідливого програмного забезпечення. Проблеми починаються при установці користувачами додаткових прошивок або при отриманні повного доступу до мобільного пристрою, коли при неправильній конфігурації зловмисникам стають доступні всі

ресурси телефону через протокол SSH (Secure SHell). Третя небезпека – атаки на додаткові сервіси. Власне, LTE розроблялося не тільки для забезпечення доступу до Інтернету мобільних користувачів, а радше як платформа для впровадження нових послуг: відео, ігрових і багатьох інших. Ці сервіси також можуть бути уразливі до найрізноманітніших атак – як з Інтернету, так і з боку мобільної мережі.

Стільникові мережі 5 п'ятого покоління є, по суті своїй, еволюцією мереж 4-го покоління LTE. Ядро стільникової мережі не зазнало значних змін, на відміну від технологій радіодоступу. Тому, архітектура безпеки стільникової мережі повинна бути розроблена з упором на перевикористання відповідних технологій, прийнятих в стандарті 4G LTE.

Таким чином, можна виділити найбільш небезпечні види атак, до яких чутливі абоненти стільникових мереж: сніффінг – використання програми або пристрою для перехоплення і аналізу мережевого трафіку; витік персональних даних, SMS і голосових дзвінків; витік даних про місцезнаходження; спуфінг (FakeBTS або IMSI Catcher) – в контексті безпеки мережі, це випадок, коли особа або програма маскується під іншу за допомогою фальсифікації даних, і тим самим отримує незаконну перевагу; віддалене захоплення SIM – карти, виконання довільного коду (RCE); відмова в обслуговуванні (DoS).

Захист стільникових мереж відрізняється тим, що там є дві бази даних або, як їх називають, регістри. Один з них – HLR (домашній регістр місцеперебування) – містить інформацію про абонента, його телефонний номер, ідентифікатор обладнання, перелік послуг і місце розташування в поточний момент часу. Інший – VLR (Visitors Location Register) – містить інформацію про те, яка кількість активних абонентів знаходиться в зоні дії та дозволяє ідентифікувати їх за номером чи кодом IMEI мобільного пристрою. Саме для захисту регістрів використовуються програмні методи та алгоритми шифрування. Забезпечення належного рівня безпеки є обов'язковим для постійно змінних видів загроз та атак на системи безпеки у мережах LTE. Для посилення безпеки та захисту даних користувачів, модель безпеки має відповідати наступним вимогам та параметрам:

1) Конфіденційність: в моделі безпеки стільникової мережі конфіденційність даних є однією з основних вимог безпеки; властивість, яка може захистити передачу даних від розголошення її стороннім особам та від пасивних атак (тобто, прослуховування та підслуховування). Враховуючи архітектури 4G-LTE та 5G, будь-які дані користувача повинні бути конфіденційними та захищеними від несанкціонованих користувачів.

2) Цілісність: запобігання втручанню та втраті інформації під час її переміщення з однієї точки в іншу. У 5G NR цілісність захищена бездротовим трафіком даних на рівні протоколу конвергенції пакетних даних (PDCP). У 4G LTE захищеність цілісності забезпечується лише для шару (рівня) без доступу (NAS) та шару доступу (AS).

3) Доступність: у області доступності стільникової мережі – це забезпечення доступності мережевих ресурсів тоді, коли вони будуть потрібні законним користувачам, оскільки доступність впливає на репутацію постачальника послуг. Іншими словами, доступність забезпечує високу ймовірність ефективності мережевої інфраструктури. Вона також вимірює стійкість мережі проти активних атак, наприклад, DoS-атак.

4) Централізована політика безпеки: архітектури безпеки 3GPP 4G не можуть безпосередньо застосовуватися для використання в стільникових мережах, оскільки вони присвячені традиційній моделі довіри оператор-абонент. Тому для підтримки нових інновацій (таких як NFV та SDN) існує потреба у централізованій системі управління політикою безпеки, яка забезпечує зручність доступу користувачів до додатків та ресурсів. Для цього можна використовувати структуру управління безпекою на основі політик для підтримки централізованого управління безпекою для стільникової мережі.

Крім того, оператори можуть включити Security-as-a-Service (SaaS) як потенційне рішення проблем з безпекою для ряду клієнтів, наприклад таких як вендори IoT.

5) Видимість: дозволяє ефективно вирішити основні проблеми мережі для забезпечення безпечного середовища. Мережам 5G необхідно використовувати комплексні стратегії наскрізного (end-to-end) захисту які повинні охоплювати всі рівні мережі. Для реалізації такого всебічного механізму безпеки оператори повинні мати повну видимість, перевірку та контроль над усіма рівнями мережі. Покращення видимості дозволяє запобігти загрозам, що керують даними, знаходити та ізолювати заражені пристрої до того, як вони вчинили атаку на мережу.

Отже на сьогоднішній день вдалося зменшити ризики витоку інформації про мережу і абонента завдяки впровадженню системи SMS Home Routing, яка здійснює фільтрацію повідомлень. Зараз мережі мобільного зв'язку використовують системи фільтрації і блокування сигнального трафіку. Однак лише комплексний підхід до вирішення проблем безпеки, включаючи регулярний аналіз захищеності, підтримання параметрів мережі в актуальному стані, постійний моніторинг сигнального трафіку і вчасне виявлення нелегітимної активності, може забезпечити високий рівень захисту від злочинців.

Список використаних джерел

1. Гарист А. В. Вразливості мереж стільникового зв'язку. Дослідження інновацій та перспективи розвитку науки і техніки у XXI столітті: матеріали Міжнар. наукю-практ. конф. Рівне: Видавн. дім «Гельветика», 2021. Ч. III. С. 19–21.

УДК 623.9

Гречка О.В.

ПРОПОЗИЦІЇ ЩОДО ПІДВИЩЕННЯ НАДІЙНОСТІ РАДІОЕЛЕКТРОННОЇ АПАРАТУРИ РАДІОТЕХНІЧНИХ СИСТЕМ

Для контролю технічного стану радіоелектронної апаратури радіотехнічних систем використовуються різні засоби контрольно-вимірювальної техніки, сукупність яких утворює контрольно-перевірочну систему. Відомі два методи забезпечення надійної експлуатації будь-якої технічної системи, у тому числі радіотехнічної та радіоелектронної [1–6]:

– підвищення та підтримання надійності кожного її елементу;

– створення інформаційної надмірності шляхом апаратурного або часового резервування.

Для підвищення надійності радіоелектронної апаратури складних технічних систем у процесі їх експлуатації проводяться періодичні перевірки (контроль технічного стану) і ремонтні роботи, спрямовані на підвищення надійності окремих складових і засобів у цілому [1, 2]. З тією ж метою зменшують інтервал контролю технічного стану радіоелектронної апаратури радіотехнічних систем. Проте при цьому не лише зменшується коефіцієнт готовності такої апаратури, але й створюється ситуація, коли переважна більшість такої апаратури, що поступають для контролю технічного стану, є дійсно справними [3, 4]. При цьому витрачається ресурс радіоелектронної апаратури радіотехнічних систем на зайві операції контролю. При цьому час збільшення інтервалу контролю технічного стану викликає зниження надійності зразків радіоелектронної апаратури, особливо модернізованих [5, 6]. Для вирішення вказаного протиріччя запропонований метод підвищення надійності модернізованих зразків радіоелектронної апаратури радіотехнічних систем.

Метою даної роботи є розробка методу підвищення надійності модернізованих зразків радіоелектронної апаратури радіотехнічних систем, який заснований на інформаційній надмірності. Ця інформаційна надмірність досягається за рахунок введення кон-

трольних проміжних перевірок, що проводяться впродовж інтервалу контролю технічного стану. Такі контрольні перевірки направлені на визначення технічного стану тільки окремих блоків (скорочений контроль) для радіоелектронної апаратури радіотехнічних систем, та додаткових блоків (елементів) для модернізованої апаратури.

Припустимо, що після кожного встановленого циклу визначення технічного стану радіоелектронної апаратури радіотехнічних систем проводяться наступні контрольні вибіркові перевірки тих засобів, які за результатами попередніх контрольних або поточних перевірок визнавалися несправними та були відремонтовані (відрегульовані). Після закінчення інтервалу контролю технічного стану проводиться черговий контроль усіх зразків модернізованої апаратури радіотехнічних систем, що знаходиться в експлуатації до кінця інтервалу контролю технічного стану.

Таким чином, проведення контрольних перевірок разом з черговими періодичними перевірками модернізованих зразків радіоелектронної апаратури радіотехнічних систем дозволяє істотно підвищити різні показники ефективності їх експлуатації. Метод контрольних перевірок може бути також використаний для вирішення такого актуального завдання, як коригування інтервалу контролю технічного стану у процесі експлуатації модернізованих зразків радіоелектронної апаратури радіотехнічних систем, особливо при експлуатації за технічним станом.

Запропонований метод забезпечує підвищення надійності модернізованих зразків радіоелектронної апаратури радіотехнічних систем за рахунок створення інформаційної надмірності про їх поточний технічний стан. Ця надмірність досягається проведенням додаткових контрольних перевірок, які характеризуються високим рівнем імовірності виявлення відмови. У запропонованому методі варійованим параметром є часовий інтервал між двома контрольними перевірками. Застосування цього методу не потребує значних додаткових апаратурних і фінансових витрат, при цьому істотно збільшує коефіцієнт використання справних модернізованих зразків радіоелектронної апаратури.

Список використаних джерел

1. С.В. Герасимов, Л.В. Гаценко. **Моделювання генерації сигналів спеціальної форми для контролю технічного стану радіоелектронного обладнання**, *Комплексне забезпечення якості технологічних процесів та систем* (КЗЯТПС – 2022): матеріали тез доповідей XI Міжнародної науково-практичної конференції, Чернігів: НУ «Чернігівська політехніка», 2022, Т. 2, С. 176.

2. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.

3. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (ISMSIT), 2022, p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.

4. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of airspace radio engineering monitoring systems**, *International scientific and practical conference* "*Application of information technologies in the preparation and operation of law enforcement forces"*, March 15, 2022, p.p. 31-32.

5. O. Brytov, D. Bieliaiev, S. Kukobko and etc. **Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects**, *Proceedings of the 3rd International Scientific and Practical Conference* "*Scientific Trends and Trends in The Context of Globalization*", UMEÅ, SWEDEN, 21-22.12.2021, p.p. 431-434, https://doi.org/10.51582/interconf.21-22.12.2021.050.

6. V. Dzhus, Y. Roshchupkin, S. Kukobko and etc. **Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction**

Method, *Information Processing Systems*, 2021, Issue 4 (167), p.p. 19-26, https://doi.org/10.30748/soi.2021.167.02.

УДК 623.5

Григоренко І.В., Ольховіков Д.С.

МЕТОД ДИСКРЕТИЗАЦІЇ СИГНАЛІВ ЗА МІНІМУМОМ ПОХИБКИ ВІДНОВЛЕННЯ В ЗАСОБАХ КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ ЗРАЗКІВ ОЗБРОЄННЯ

При контролі технічного стану зразків озброєння застосовується різноманітні зразки вимірювальної техніки [1, 2]. При цьому слід виділити цифрові засоби контролю. Такі засоби контролю дозволяють контролювати технічний стан основних блоків (систем) зразків озброєння: елементів систем автоматичного керування, блоків керування роботи двигунів, засобів зв'язку та радіонавігації, систем енергозабезпечення тощо. Вихід з ладу одного з зазначених блоків (систем) зразків озброєння може привести до не виконання бойового завдання. Тому постійно зростають вимоги до характеристик таких засобів контролю [3, 4]. До таких характеристик належать: відповідність форми синтезованого сигналу до заданої; збільшення характеристик точності та підвищення стабільності параметрів синтезованого сигналу; скорочення часу перехідних процесів; автоматизація управління режимами роботи; можливість інформаційного з'єднання із системними приладами і засобами обчислювальної техніки [5, 6].

Задача про оптимальний вибір інтервалу або частоти дискретизації при аналого-цифровій обробці сигналів не втрачає своєї актуальності у вимірювальній техніці, в тому числі при відновленні сигналів у засобах контролю технічного стану зразків озброєння.

У класичній постановці задача про вибір частоти дискретизації аналогового сигналу добре відома та вирішується теоремою Шеннона-Котельникова [3]. Однак у вимірювальної практиці має місце одна принципова особливість, яка робить безпосереднє застосування теореми Шеннона-Котельникова та сучасних методів оптимізації частоти дискретизації аналогових сигналів за мінімумом похибки відновлення не цілком адекватними [2, 6]. Отже, при синтезі апаратури контролю технічного стану зразків озброєння необхідно враховувати, що частота дискретизації вимірювального сигналу впливає як на похибку апроксимації, так і на завадову складову похибки відновлення інформаційного сигналу. З підвищенням частоти дискретизації похибка апроксимації зменшується, а завадового складова похибки – збільшується. Тому для кожного класу вхідних сигналів, при відомих значеннях передавальної функції еквівалентного аналогового блоку та статистичних характеристиках завади у вихідному сигналі аналого-цифрового перетворювача, може бути визначена оптимальна частота дискретизації. Для цього можна використовувати, наприклад, або критерій мінімуму сумарної похибки відновлення, що включає обидві зазначені складові похибки. Або критерій мінімуму однієї складової похибки відновлення при заданому рівні іншої складової похибки, або інформаційний критерій (максимум інформації в вимірювальному сигналі, яку можна отримати за дискретного сигналу).

Існування та визначення оптимальної частоти дискретизації, завищення якої, як і заниження збільшує похибку відновлення вимірювального сигналу, складає сутність запропонованого методу. Незалежно від критерію для визначення оптимальної частоти дискретизації необхідно знайти оцінки обох складових похибки відновлення в функції частоти дискретизації. Для цього слід отримати розв'язок відповідного рівняння, тобто за відомим дискретним сигналом знайти вимірювальний сигнал. Запропоноване рів-

няння при цьому має безліч рішень. Рішення, що володіє найменшою нормою та не містить апріорної інформації про вимірювальний сигнал, є сигналом, який апроксимується (скелетним).

Підкреслимо, що навіть у тому випадку, коли відновлення вимірювального сигналу за дискретним сигналом не проводиться, апроксимуючий сигнал потенційно містить у сигналі інформацію про вимірювальний сигнал залежно від частоти дискретизації та дозволяє обґрунтовано визначити її.

Зменшення частоти дискретизації нижче оптимальної призводить до збільшення похибки апроксимації та втрати частини інформації про вимірювальний сигнал пристрою аналого-цифрової обробки сигналу. Разом з тим і невиправдане завищення частоти дискретизації, ускладнюючи технічну реалізацію пристрою, не приносить користі. Це пов'язано з тим, що завищення частоти дискретизації не тільки не збільшує інформацію про вхідний сигнал, але й при необхідності його відновлення призводить до її зменшення за рахунок збільшення впливу завад у вихідному сигналі на точність відновлення вхідного сигналу.

Список використаних джерел

1. С.В. Герасимов, Л.В. Гаценко. **Моделювання генерації сигналів спеціальної форми для контролю технічного стану радіоелектронного обладнання**, *Комплексне забезпечення якості технологічних процесів та систем* (КЗЯТПС – 2022): матеріали тез доповідей XI Міжнародної науково-практичної конференції, Чернігів: НУ «Чернігівська політехніка», 2022, Т. 2, С. 176.

2. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.

3. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (ISMSIT), 2022, p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.

4. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of airspace radio engineering monitoring systems**, *International scientific and practical conference* "*Application of information technologies in the preparation and operation of law enforcement forces"*, March 15, 2022, p.p. 31-32.

5. O. Brytov, D. Bieliaiev, S. Kukobko and etc. **Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects**, *Proceedings of the 3rd International Scientific and Practical Conference* "*Scientific Trends and Trends in The Context of Globalization*", UMEÅ, SWEDEN, 21-22.12.2021, p.p. 431-434, https://doi.org/10.51582/interconf.21-22.12.2021.050.

6. V. Dzhus, Y. Roshchupkin, S. Kukobko and etc. **Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction Method**, *Information Processing Systems*, 2021, Issue 4 (167), p.p. 19-26, https://doi.org/10.30748/soi.2021.167.02.

Даник Ю.Г.

ОСОБЛИВОСТІ РЕГУЛЮВАННЯ РОЗВИТКУ І ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В РІЗНИХ КРАЇНАХ СВІТУ

Важливим елементом забезпечення національної безпеки і оборони та розвитку суспільства є створення, застосування і використання технологій штучного інтелекту (ШІ) в різних сферах людської діяльності.

Розвиток технологій ШІ має лавиноподібний, і дуже часто навіть стрибкоподібний характер. За даними Всесвітньої організації інтелектуальної власності, від 1998 до 2017 року у США було подано приблизно 50 000 патентних заявок на ШІ, а в Китаї - близько 41 000, зараз кількість подібних заявок зростає багатократно.

На саміті в Мадриді в жовтні 2021 року 17 країн-членів НАТО підписали угоду про створення інноваційного фонду розвитку технологій ШІ на 1 млрд євро.

Тільки в США у період з 2016 по 2020 роки було виділено 18 мільярдів доларів на створення та розвиток автономної зброї з ШІ.

Німеччина, яка має найбільший сектор досліджень ШІ в ЄС, оновила свою національну стратегію ШІ в грудні 2020 року. Вона оголосила про збільшення інвестицій у цей сектор з 2,4 млрд доларів США до 5,9 млрд доларів США до 2025 року.

Інтенсивна діяльність Великої Британії в галузі ШІ спрямована на вихід, протягом 10 років, на передові позиції в світі в цій царині. У вересні 2021 року британський уряд завершив розробку плану, який передбачає випередження США і Китаю в сфері штучного інтелекту. Документ "Національна стратегія розвитку штучного інтелекту" має на меті просування використання ШІ в бізнесі, залучення міжнародних інвестицій в британські компанії в цій галузі та формування нового покоління британських талантів в технологічній сфері. Основна увага приділяється розв'язанню питань національної безпеки і оборони. Аналогічна активність в цій сфері спостерігається у переважній більшості держав світу до чого активно долучається приватний сектор.

Кількість напрямків розвитку ШІ також постійно зростає. Так, якщо Командування підрозділу Сухопутних військ США, відповідальне за технологічне забезпечення та модернізацію військ (Army Futures Command (AFC)), після аналізу сфер застосування ШІ кілька років тому вибрало 11 найбільш перспективних напрямків для проведення досліджень у найближчі п'ять років, то на цей час можна виділити вже біля двох десятків напрямків, які мають безпосереднє відношення до сфери національної безпеки і оборони.

А саме: представлення знань (Knowledge representation), машинне навчання (Machine learning), візуалізація (Visualization), обробка «природною» мовою (Natural language processing), глибоке навчання (Deep learning), генерування природньої мови (Natural language generation), глибокі системи запитань і відповідей (Deep Q&A systems), віртуальні особисті помічники (Virtual personal assistants), графічний аналіз (Graph analysis), аналіз соціальних мереж (Social network analysis), датчики/Інтернет речей (Sensors/internet of things), робототехніка (Robotics), рекомендаційні системи (Recommender systems), імітаційне моделювання (Simulation modelling), «м'яка» робототехніка (Soft robotics), аналіз аудіомовлення (Audio/speech analytics), аналітика зображень (Image analytics), машинний переклад (Machine translation) тощо.

У сфері розвитку ШІ все більше задіюються високотехнологічні досягнення з різних галузей науки і техніки. З аналізу досягнень і напрямків розвитку технологій можна прогнозувати використання не лише електронних, але й квантових, біо- та інших комп'ютерів, а також їх комбінацій, як базових елементів для реалізації технологій ШІ. Це дозволить значно збільшити швидкість обчислень та вирішити завдання, які не можуть бути повністю розв'язані на класичних комп'ютерах.

Одним з важливих напрямів стало створення багатоагентних систем ШІ, в яких багато агентів взаємодіють між собою та з навколишнім середовищем для досягнення певних цілей. Це може включати розробку систем контролю та управління, мережевих технологій тощо.

Поява на початку 21-го століття теорії та практики створення нейромереж і розробка технологій глибокого навчання та інших методів машинного навчання [1-5], комп’ютерного зору тощо стали важливими елементами у розвитку таких систем зі штучним інтелектом, як автономні наземні, надводні (підводні) та повітряні платформи, здатні працювати і застосовувати зброю в різних середовищах. На цей час як дер-

жавні так і приватні структури по всьому світу вкладають значні кошти в дослідження та розробку автономної зброї зі штучним інтелектом.

Але цей бурхливий розвиток супроводжується не тільки позитивними наслідками, але й несе в собі значні загрози і ризики [6-9]. Особливо, коли йдеться про використання ШІ в інтересах національної безпеки і оборони, а тим більше в деструктивних цілях різноманітними кримінальними структурами.

Таким чином, розвиток штучного інтелекту, поряд з новими можливостями, які він надає, одночасно формує нові етичні, соціальні і безпекові проблеми, пов'язані з його використанням,. Одне з актуальних питань полягає в тому, як забезпечити, щоб ШІ залишався під контролем людини, не створював загроз та був безпечним.

Для цього необхідно ретельно враховувати етичні та правові аспекти використання штучного інтелекту, взаємодії з ним людини, у тісному взаємозв'язку з прогностичним аналізом розвитку технологій і зростанням можливостей ШІ та здійснювати превентивні заходи щодо всебічного, регулювання всього кола пов'язаних з цим питань.

Питання прозорості та обліковості прийнятих рішень, а також відповідальності за можливі негативні наслідки від використання ШІ, і нормативно-правового регулювання створення, розвитку та використання продуктів ШІ в різних сферах життєдіяльності людини і суспільства об'єктивно переходять до категорії життєвоважливих. Тому, в провідних країнах світу вже проводиться інтенсивна робота щодо нормативно-правового регулювання використання технологій у сфері ШІ [10]. Наприклад, 21 квітня 2021 року Європейською комісією був прийнятий регламент ЄС "Proposal for a Regulation laying down harmonised rules on artificial intelligence", який передбачає усунення можливих ризиків та забезпечення прозорого використання ШІ з обов'язковим дотриманням прав та демократичних цінностей [11]. У цьому регламенті визначено чотири категорії ризику використання штучного інтелекту, проте він не застосовується до військових цілей. В Канаді введений в дію The Artificial Intelligence and Data Act (AIDA), який врегульовує питання захисту даних, нормативні вимоги до оцінки ризиків. Закон зосереджується на системах ШІ з високим рівнем впливу і розглядає індивідуальну шкоду, колективну шкоду та інші важливі питання. В КНР прийнятий Нормативно-правовий акт «Тимчасові заходи з управління службами генеративного штучного інтелекту» (Interim Measures for Generative Artificial Intelligence Service Management). Він врегульовує питання розробки, експлуатації та надання послуг генеративного штучного інтелекту, забезпечення безпеки та етичного його використання, захист прав та інтересів користувачів. Питання розвитку та використання штучного інтелекту, етичні принципи його використання та пріоритетні напрямки розвитку в США введені в дію Указом Президента США "Про безпечний, надійний та гідний довіри розвиток та використання штучного інтелекту" (Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence), а в Великій Британії розглянуті в Білій книзі про штучний інтелект (Artificial Intelligence White Paper). На засіданні 2 грудня 2020 року Кабінет Міністрів України затвердив концепцію розвитку ШІ в Україні до 2030 року, яка визначила основні напрями розвитку сфери ШІ в Україні та створення правового поля використання ШІ у відповідності до міжнародних стандартів.

Питання стосовно автономних систем зі ШІ розглядається і досліджується на всіх рівнях протягом багатьох років. Особливості розроблення й застосування автономної зброї та ШІ розглядались на рівні Європейського Союзу у 2018 р. про що повідомляла у своїх виступах Ф. Могеріні. В 2023 році Організація Об'єднаних Націй інтенсифікувала діяльність щодо оцінки ризиків пов'язаних з розвитком і застосуванням ШІ та створила консультативну раду для проведення аналізу та розробки рекомендацій щодо міжнародного управління в цій сфері, з метою розв'язання питань, щодо створення міжнародних стандартів, які стосуються всіх аспектів пов'язаних із ШІ. До складу ради увійшли представники урядових органів, наукових груп і бізнесу, включно з керівництвом відомих компаній, таких як Google й OpenAI.

Проте, існують невирішені протиріччя між швидким розвитком ШІ та його використанням, особливо в сфері безпеки і оборони, і необхідністю передбачати виклики, ризики і загрози, пов'язані з його розвитком. Наразі відсутні обґрунтовані системні підходи до зниження, запобігання і нейтралізації цих загроз, особливо того, що стосується автономних систем.

Такі дослідження, зважаючи на особливості ШІ мають міжгалузевий та міждисциплінарний характер. Вони повинні враховувати особливості взаємодії в системах: людина (користувач) ШІ –ШІ і у зворотному зв'язку ШІ – людина; ШІ – суспільство; ШІ – держава; ШІ – кібер-фізична(і) система(и) (КФС). А також системи більш високої складності і рівнів взаємодії. Таких як: особа (група осіб, суспільство)1- ШІ 1 – ШІ 2 - особа (група осіб, суспільство) 2; структура (інституція, організація, держава)1- ШІ 1 – ШІ 2 - структура (інституція, організація, держава) 2, ШІ 1 – КФС 1 - КФС 2 - ШІ 2 тощо. А також різноманітних комбінацій багатокомпонентних систем, які можуть організовуватись різними акторами та самоорганізовуватись.

Результати досліджень представлені в доповіді комплексно розглядають особливості регулювання розвитку і використання ШІ в різних країнах світу з врахуванням існуючих трендів і прогнозів високотехнологічного та інноваційного розвитку соціотехнічних систем, які передбачають всебічну і різнорівневу взаємодію людини і кіберфізичних систем зі ШІ, у взаємозв'язку з розвитком нормативно-правового забезпечення, яке врегульовує діяльність в сфері розвитку та використання ШІ в США, ЄС, Україні тощо.

Список використаних джерел

1. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

3. Schmidhuber, J. (2015). Deep learning in neural networks: An overview. Neural Networks, 61, 85-117.

4. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255-260.

5. Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., Van Den Driessche, G., ... & Hassabis, D. (2016). Mastering the game of Go with deep neural networks and tree search. Nature, 529(7587), 484-489.

6. Artificial intelligence: threats and opportunities. https://www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities

7. Opportunities of Artificial Intelligence. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf

8. Artificial Intelligence and National Security. https://sgp.fas.org/crs/natsec/R45178.pdf

9. AI and National Security: Major Power Perspectives and Challenges. https://www.idsa.in/issuebrief/ai-and-national-security-ssharma-120922

10. Proposal for a Regulation laying down harmonised rules on artificial intelligence, 2021. URL: https://ec.europa.eu/newsroom/dae/redirection/document/7578

11. UN E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development. Retrieved from URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

УДК 004.056.53+005.94

Данилов А.Д.

ОГЛЯД МЕТОДІВ ЗАХИСТУ ДАНИХ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ В ОРГАНІЗАЦІЇ

Розвиток сучасних технологій призвів до глобальної інформатизації суспільства. Життя сучасної людини нерозривно пов'язане з використання інформаційних технологій. Кілька років тому пересічні користувачі використовували в своєму житті лише прості інструменти та системи, але суспільство та технології розвиваються та потреби користувачів збільшуються. Зараз ведення профілю в соціальних мережах та використання інформаційних технологій у сфері державних послуг є звичкою.

Зі збільшенням обсягу використання інформації та впровадженням інформаційних технологій та систем збільшується потреба в захисті інформації та персональних даних. Все частіше поширюються випадки незаконного отримання, накопичення, використання, видалення, розповсюдження персональних даних, проведення незаконних фінансових операцій та махінацій у мережі Інтернет. Для забезпечення захисту інформації доцільно використовувати комплексний підхід.

Розглянемо деякі методи та інструменти захисту даних.

Data Leak Prevention (DLP) − це набір інструментів і процесів, які використовуються для захисту інформаційних ресурсів. Зокрема сюди входять функції захисту конфіденційних даних від втрати та запобігання їх використання для вчинення шкідливих дій, або ж отримали доступу сторонніми особами. Втрата, витік, або порушення цілісності конфіденційних даних може призвести до серйозних наслідків[1].

Програмне забезпечення, що відноситься до класу DLP дозволяє відстежувати та контролювати діяльність кінцевих точок, фільтрувати потоки даних у корпоративних мережах та відстежувати дані в хмарі, з метою захисту інформації у будь-кому стані. Крім того DLP-система надає звіти для відповідності законодавчим нормам та вимогам аудиту, дозволяє визначити слабкі місця і аномалії, що можна ефективно використовувати для підвищення ефективності розслідувань експертів-криміналістів та реагування на інциденти [1].

Інструменти, що використовуються для моніторингу та фільтрації мережного трафіку, наприклад Брандмауери, які дозволяють забезпечити передачу даних або доступ до них лише авторизованим користувачам

Шифрування даних. Виділяють симетричне, асиметричне та гібридне шифрування. Доступ до файлу можливо отримати лише використовуючи заздалегідь заданий пароль та ключ шифрування. До переваг шифрування можна віднести умовний захист даних навіть у разі викрадення, крім отримання доступу до інформаційних ресурсів зловмисник також повинен розшифрувати отримані данні, що іноді є занадто складним та знецінює важливість отриманої інформації.

Видалення не потрібних або не актуальних даних. Важливим процесом є знищення застарілих, або непотрібних даних. Використовуючи такий тип даних зловмисник може ввести в оману потенційних жертв, або спричинити серйозні проблеми для функціонування організації. Таким чином, збереження такого типу файлів є обтяжливим для інформаційної структури організації та несе потенційні ризики використання інформації зловмисниками.

Створення систем відмовостійкості в рамках програмного та апаратного забезпечення інформаційної системи організації для забезпечення безпеки у разі надзвичайних ситуацій, або навмисного нанесення системі шкоди. В залежності від типу інформаційної системи організації її відмовостійкість можна забезпечувати на різних рівнях та за допомогою різних інструментів.

Резервне копіювання даних. Для забезпечення збереження та цілісності інформації доцільним є резервне копіювання даних, що дозволяє уникнути, або мінімізувати шкоду у разі збою або стороннього впливу. Для цього формуються плани резервного копіювання. При резервному копіюванні можна використовувати окремі фізичні диски, хмарні технології тощо.

Для повноцінного захисту організацій важливо запровадити структуру захисту даних, що містить рекомендації щодо захисту всіх робочих процесів. Така структура допоможе організації забезпечити захист і розумне використання даних та інформаційних ресурсів, що зберігаються на серверах або використовуються організацією. Також це дозволить керівництву своєчасно виявляти потенційні ризики та вносити зміни до інформаційні структури для їх попередження.

Розробка ефективної стратегії захисту веб-ресурсів є нетривіальною задачею та повинен включати одночасне здійснення системного, евристичного та статистичного аналізу вразливостей веб-ресурсу, що дозволяє здійснити якісний захист від зловмисників, які використовують декілька типів атак.

Методи незаконного вилучення інформації можуть бути дуже різноманітними і складними, тому потрібно розробляти ефективні методи протидії. Для цього необхідно розуміти потенційні загрози та використовувати відповідні методи захисту даних, щоб забезпечити їх конфіденційність, цілісність та доступність. Також важливо постійно оновлювати методи протидії відповідно до нових загроз та викликів, які постійно змінюються[2].

Нажаль, ніхто не захищений від злому баз даних, що містять персональну інформацію, простих помилок та людської необачності. Наприклад, реєструючись або авторизуючись на сайті через соціальну мережу, ви дозволяєте сайту отримати особисті дані, і точно невідомо, як вони в подальшому будуть використані. Так само будь-який ваш дзвінок (авторизоване звернення) у магазин або будь-яку організацію автоматично зберігає ваш номер у базі користувачів. Тому захист та збереження даних є необхідністю.

Для забезпечення ефективного захисту інформації в організації та забезпечення її стійкого функціонування, доцільно використовувати системнологічний підход [3, 4] до формування системи функціонування організації, що дозволить побудувати ефективну систему захисту та буде мати прогностичний характер. Такий підхід дозволить виявити потенційні загрози, спрогнозувати наслідки втрати або знищення інформації та своєчасно вносити зміни в структуру організації та інформаційну систему для їх попередження.

Список використаних джерел

1 Запобігання втраті даних. https://octava.ua: веб сайт URL https://octava.ua/zapobigannya-vtrati-danyh (дата звернення: 29.02.2024).

2 Іващенко Д.О., Данилов А.Д. Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VII Міжнар. наук.-практ. конф. (м. Дніпро, 17 бер. 2023 р.). - Дніпро : ДДУВС, 2023. – с. 558.

УДК 355.424

Деменко М.П., Савельєв А.М., Воронін В.В., Масолов В.М., Пасічник А.В.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-РОЗРАХУНКОВОЇ СИСТЕМИ "АРГУМЕНТ–2023" ДЛЯ ОРГАНІЗАЦІЇ ТА ПІДТРИМКИ ВЗАЄМОДІЇ ВІЙСЬКОВИХ ЧАСТИН (ПІДРОЗДІЛІВ) ЗРВ У СКЛАДІ МІЖВИДОВОГО (МІЖВІДОМЧОГО) УГРУПОВАННЯ СИЛ ТА ЗАСОБІВ ППО

В доповіді розкрито особливості використання інформаційно-розрахункової системи "Аргумент–2023" для організації та підтримки взаємодії військових частин (підрозділів) зенітних ракетних військ у складі міжвидового (міжвідомчого) угруповання сил та засобів протиповітряної оборони.

Постачання озброєння та військової техніки (ОВТ) іноземного виробництва країн-членів НАТО в Україну призвело до якісної зміни бойового складу міжвидового (міжвідомчого) угруповання сил та засобів протиповітряної оборони (ППО) під час операції (бойових дій), ефективність виконання завдань яких, залежить від організації взаємовідносин між ними та іншими складовими сил оборони.

В цілому, найбільше розходження у алгоритмах планування операцій у Збройних Силах (ЗС) України та НАТО припадає на етап аналізу завдання (організації оперативного планування). Умовно, проблеми організації та підтримання взаємодії зведені у групи, як такі, що пов'язані з вирішенням питань правового характеру, теоретичного плану, організаційного і технічного характеру та розглянуто їх зміст.

Одним із головних завдань повітряного компоненту має бути підвищення рівня його оперативної сумісності з силами та засобами ППО ЗС країн-членів НАТО. Особливості організації і підтримання взаємодії військових частин (підрозділів) зенітних ракетних військ (ЗРВ) пов'язані з відмінностями бойового застосування військових частин (підрозділів) різних видів і родів військ (сил) зведених в угруповання сил та засобів ППО для сумісного виконання бойового завдання.

Запропоновано створення ефективної системи міжвидової (міжвідомчої) підготовки сил та засобів ППО з метою сприяння вирішенню зазначених проблем. Окрім цього, удосконалено інформаційно-розрахункову систему (ІРС) (Аргумент-2023) для оцінювання ефективності організації взаємодії частин та підрозділів ЗРВ Повітряних Сил ЗС України, з урахуванням застосування зенітних ракетних комплексів (ЗРК) іноземного виробництва [1-4]. З цією метою в ІРС удосконалено наступне:

- програмний модуль моделі засобів повітряного нападу (ЗПН) противника;
- програмний модуль моделі застосування частин та підрозділів радіотехнічних військ (РТВ);
- програмний модуль моделі бойового застосування частин та підрозділів авіації;
- програмний модуль моделі бойового застосування частин та підрозділів ЗРВ та ППО Сухопутних військ (СВ);
- програмний модуль моделі функціонування пункту управління авіації та ППО командного пункту міжвидового угруповання військ в реалізації можливих варіантів взаємодії зенітних ракетних частин (підрозділів) у бойових діях.

У програмному модулі моделі бойового застосування частин та підрозділів ЗРВ та ППО СВ враховані підрозділи, що озброєні ЗРК NASAMS, IRIS-T SLM, SAMP-T, "Patriot", а також FlaK-Panzer Gepard, Crotale NG, Stormer HVM,AN/TWQ-1 "Avenger".

Низка програмних удосконалень дозволила у ІРС реалізувати основні способи взаємодії підрозділів та частин ЗРВ з підрозділами (частинами) інших родів військ. При цьому, виникла можливість обирати варіанти взаємодії з урахуванням відповідних способів та здійснювати оцінку ефективності кожного обраного варіанту.

Розроблено рекомендації щодо використання ІРС при оцінці ефективності взаємодії зенітних ракетних частин (підрозділів) з урахуванням застосування зенітних ракетних комплексів іноземного виробництва.

Для використання ІРС "Аргумент-2023" при оцінюванні ефективності взаємодії зенітних ракетних частин (підрозділів) міжвидового угруповання військ у бойових діях необхідно:

– задати склад та бойові порядки частин та підрозділів ЗРВ, ефективність взаємодії яких необхідно оцінити;

– задати склад та бойові порядки частин та підрозділів РТВ, з якими взаємодіють ЗРВ, війська ППО СВ та авіація;

– задати склад і розміщення аеродромів частин авіації;

– задати склад та бойові порядки частин та підрозділів військ ППО СВ;

– задати склад сил та ЗПН противника, а також варіант повітряного удару (маршрути польоту ЗПН);

– задати спосіб взаємодії з авіацією, підрозділами ППО СВ.

– провести моделювання бойових дій (по отриманим результатам оцінити ефективність взаємодії зенітних ракетних частин (підрозділів) міжвидового угруповання військ в ході бойових дій).

Таким чином, проводячи моделювання бойових дії з різними способами взаємодії та оцінюючи ефективність бойових дій є можливість вибрати найбільш ефективний спосіб взаємодії зенітних ракетних частин (підрозділів) міжвидового угруповання військ з урахуванням застосування ЗРК іноземного виробництва. Обрати такий варіпнт, при якому досягається найбільша ефективність бойових дій частин (підрозділів) ППО міжвидового угруповання військ.

Список використаних джерел

1. Савєльєв А.М., Коломійцев О.В., Опенько П.В., Новіченко С.В., Третяк В.Ф. Актуальні аспекти управління оборонними ресурсами сектору безпеки та оборони: монографія / за ред. І. М. Ткач. 2023. С. 150-164

2. Модель універсального командного пункту в інформаційно-розрахунковій системі «Аргумент–2022» / А. Савельєв та ін. InterConf. 2022. № 25(125). С. 258–270. URL: https://doi.org/10.51582/interconf.19-20.09.2022.024 (дата звернення: 03.03.2024).

3. Аналіз напрямків розвитку військової техносфери країн НАТО / О. Коломійцев та ін. InterConf. 2023. № 37(171). С. 379–397. URL: https://doi.org/10.51582/interconf.19-20.09.2023.033 (дата звернення: 03.03.2024).

4. Структура інформаційно-розрахункової системи підтримки прийняття рішення «АРГУМЕНТ–2021» / А. Савельєв та ін. InterConf. 2021. С. 631–642. URL: https://doi.org/10.51582/interconf.7-8.04.2021.069 (дата звернення: 03.03.2024).

5. Бурцев, В., Воронін, В., Волювач, С., Запара, Д., Коломійцев, О., Савельєв, А., Новіченко, С., Деменко, М., Возний, О., Третяк, В., Кривчун, В., & Довгалюк, Д. (2023). Підходи щодо оцінки живучості підрозділів зенітних ракетних військ. *Scientific Collection «InterConf»*, (154), 538–542. Retrieved from https://archive.interconf.center/index.php/conference-proceeding/article/view/3387.

6. Запара, Д., Коломійцев, О., Савельєв, А., Новіченко, С., Воронін, В., Деменко, М., Третяк, В., Крук, Б., Кривчун, В., & Довгалюк, Д. (2023). Особливості розрахунку показників та критеріїв оцінки ефективності в інформаційно-розрахунковій системі «Аргумент–2023». *Scientific Collection «InterConf»*, (146), 396–403. Retrieved from https://archive.interconf.center/index.php/conference-proceeding/article/view/2706.

Дуболазов Ю.О.

ПЕРЕВАГИ ВИКОРИСТАННЯ СИСТЕМИ PROZORRO ДЛЯ ЗАКУПІВЕЛЬ ВИМІРЮВАЛЬНОЇ ТЕХНІКИ

З плином часу розвиток вимірювальної техніки, як і техніки і технологій взагалі не стоїть на місці. В останні роки тенденції в її розвитку мають наступні ознаки: перехід від аналогових приладів до цифрових, зменшення розмірів і ваги без втрати точності і функціональності, вдосконалення сенсорів та датчиків, вдосконалення інтерфейсів для підключення до комп'ютерів та інших приладів тощо.

Отже застосування новітніх засобів вимірювальної техніки на робочих місцях та еталонній базі має вдосконалити як процес повірки (калібрування) так і потенційно розширити номенклатуру засобів, що обслуговуються на них.

Відповідно до Закону України «Про публічні закупівлі», який набув чинності у 2016 році з'явилась можливість проводити закупівлі через авторизовані електронні майданчики за допомогою процедур закупівель. Цей інструмент дозволяє оновлювати в тому числі і засоби вимірювальної техніки на більш досконалі. З кожним роком замовники, які купують товари, роботи і послуги на Prozorro економлять велику кількість державних коштів за рахунок використання авторизованих електронних майданчиків. Наведемо лише деякі аспекти такого підходу до закупівель.

Прозорість та конкуренція. Відкритий доступ до інформації про тендери змушує постачальників конкурувати, пропонуючи кращі ціни та умови. Тобто потенційні постачальники можуть вивчити опис тендеру, деталі щодо гарантійних зобов'язань, які саме використовуються кваліфікаційні критерії, наприклад щодо досвіду поставок аналогічних засобів вимірювальної техніки. Це стимулює зниження цін та може призвести до значних економії державних коштів.

Електронний аукціон. Функція електронного аукціону дозволяє замовникам отримувати більш вигідні пропозиції в режимі реального часу, що також сприяє зниженню вартості закупівлі. Неодноразово відбуваються випадки суттєвого зниження вартості закупівлі, особливо якщо в аукціоні брали участь велика кількість учасників.

Детальний опис тендеру. Замовники мають можливість детально описати предмет закупівлі, включаючи технічні специфікації та вимоги до якості, що допомагає отримати пропозиції, які максимально відповідають потребам.

Ефективна система оцінки. Prozorro використовує чіткі та прозорі критерії оцінки тендерних пропозицій, що дає можливість замовникам обирати найекономічнішу пропозицію, що відповідає його потребам. Замовник має змогу обирати як цінові так і нецінові (такі, як наприклад вартість життєвого циклу) критерії оцінки з тією чи іншою питомою вагою. До того ж є можливість використовувати один або декілька кваліфікаційних критеріїв оцінки пропозиції учасника (потенційного постачальника): наявність матеріально-технічної бази та технологій, наявність працівників відповідної кваліфікації, які мають необхідні знання та досвід, наявність документально підтвердженого досвіду виконання аналогічного за предметом закупівлі договору, наявність фінансової спроможності, яка підтверджується фінансовою звітністю. Наведені критерії дозволяють відхилити пропозиції недобросовісних постачальників і як наслідок економити державні кошти, що виділені для закупівлі засобів вимірювальної техніки.

Можливість оскарження. Prozorro гарантує можливість оскарження результатів тендерів, що запобігає корупції та зловживанням. Завдяки тому що процес відбору постачальника за умовами які були оголошені публічно і заздалегідь відбувається у відкритій площині у інших постачальників є можливість оскаржити результати кваліфікації учасників.

Головне, що застосування такого ефективного інструменту як Prozorro значно підвищує рівень довіри як до замовників так і постачальників і як наслідок це створює

передумови для формування повноцінного та конкурентоспроможного ринку засобів вимірювальної техніки.

УДК 004.415.53

Дудар З.В., Лановий О.Ф.

ВИКОРИСТАННЯ ШІ В ТЕСТУВАННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Тестування програмного забезпечення є основним способом перевірки відповідності програмного забезпечення певним вимогам. Програмне забезпечення за своєю суттю представляє функцію перетворення вхідної інформації у вихідну в багатовимірному просторі. До такої математичної моделі досить легко застосувати методи нечіткої логіки, тобто нейронні мережі. Штучна нейронна мережа (ШНМ) – це математична модель штучного інтелекту (ШІ), заснована на когнітивних процесах мозку. Так само, як і мозок, нейронна мережа складається з вузлів (нейронів) і змінних зв'язків між ними.

Однією з основних перешкод на шляху використання методів ШІ в тестуванні ПЗ є відповідь на питання – які вимоги повинно висувати використання ШІ до процесу розробки ПЗ та до команди розробників.

Припустивши, що після внесення виправлень в програмний продукт існуючий функціонал не зміниться, можна очікувати, що при однакових вхідних даних ШНМ і реальний програмний додаток дадуть ідентичні результати. За допомогою порівняння можна буде зробити висновок, чи є коректним результат тестування програми [1]. Вказану методику тестування представлено на рис. 1.

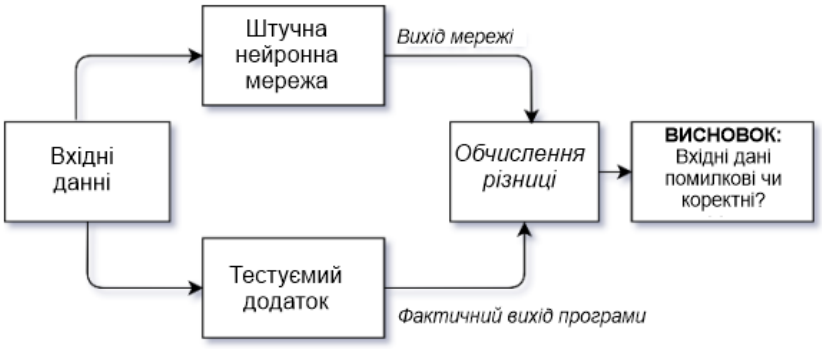


Рисунок 1 – Методика тестування з використанням ШНМ

Використання моделі ШНМ починається з етапу навчання. На цьому етапі (рис. 2) вектор введення (тестовий приклад) для кожного тест-кейсу генерується випадковим чином, відповідно до специфікації програми. Кожен вхідний вектор подається на вхід програми, яка генерує відповідний вихідний вектор.

Вхідні та вихідні вектори програми використовуються для навчання нейронної мережі. Навчена ШНМ може використовуватись у якості автоматизованого «оракула» для тестування наступних версій програми в процесі регресійного тестування [2].

На етапі тестування (рис. 3) кожен тестовий випадок подається як вхідний вектор одночасно і на вхід програмної системи, що підлягає тестуванню, і на вхід навченої ШНМ. Для кожного вхідного вектору інструмент порівняння обчислює абсолютну відстань між виходом ШНМ та відповідним значенням виходу програми.

Всі виходи є числами від нуля до одиниці. Обчислена відстань потрапляє в один із трьох інтервалів, визначених двома пороговими значеннями в діапазоні [0, 1]. Якщо передбачення мережі та вихід програми однакові, а обчислена відстань потрапляє в

інтервал між 0 і низьким порогом відмінності (відстань дуже мала), то це означає, що передбачення мережі відповідає виходу програми, і обидва результати, ймовірно, будуть правильними. У цьому випадку інструмент порівняння повідомляє, що вихід програми правильний. З іншого боку, якщо результат прогнозування мережі відрізняється від виходу програми і відстань між виходами дуже велика (потрапляє в інтервал між високим порогом і 1), то інструмент порівняння повідомляє про помилку програми (неправильний вихід). В обох випадках висновок ШНМ буде правильним, і він є достатньо надійним для оцінки правильності вихідних даних програми. Однак, якщо відстань розміщується в інтервалі між низьким і високим порогом, вихід мережі вважається ненадійним. В цьому випадку засіб порівняння повідомляє про помилку програми лише в тому випадку, якщо передбачення мережі повністю ідентичне виходу програми.

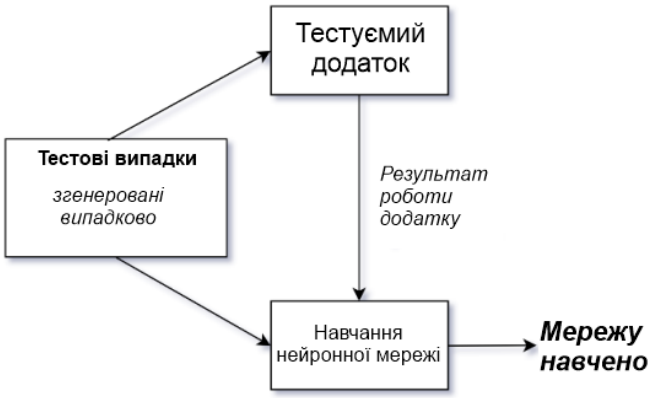


Рисунок 2 – Фаза навчання ШНМ

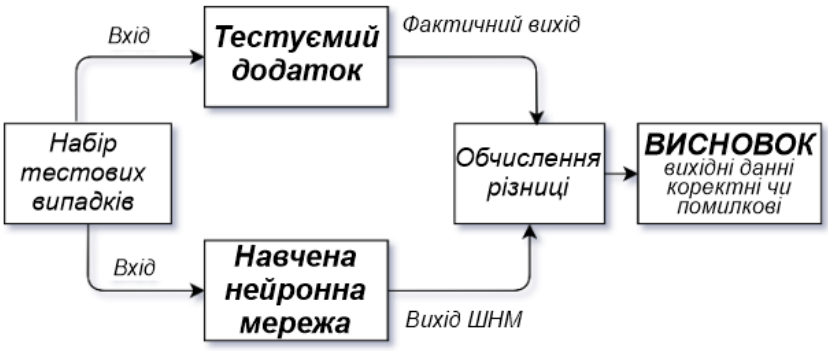


Рисунок 3 – Фаза тестування

Інструмент порівняння може використовуватись як незалежний метод порівняння результатів моделювання ШНМ та результатів тестування ПЗ. Оскільки ШНМ є лише моделлю реальної програмної системи, деякі її результати можуть бути неправильними. З іншого боку, сама програма, що тестується, може містити дефекти, виявлення яких і є основною причиною процесу тестування. Якщо вихід ШНМ вважати правильним, а вихід програми – невірним, то оцінка інструменту порівняння класифікується як дійсно негативний результат – визначення того факту, що результат роботи програми містить фактичну помилку [3].

На підсумку слід зазначити, що в роботі проведено дослідження та аналіз сучасних методів, засобів і технологій, які застосовуються для тестування ПЗ в використанням елементів ШІ. Так, наприклад, фахівці з автоматизації фірми Eggplant в жовтні 2020 року запустили нову платформу для тестування програмного забезпечення на базі ШІ Digital Automation Intelligence (DAI) Eggplant, яка має наступні характеристики [4]:

- наскрізна автоматизація на основі хмари;
- моніторинг: додавання даних і показників розширеного взаємодії з користувачем (UX), що дозволяє клієнтам порівнювати продуктивність UX своїх додатків.

Подальші дослідження в цій галузі будуть спрямовані на проведення експериментів з ШНМ з підтримки процесів тестування ПЗ за допомогою множинних інтелектуальних агентів, що відстежують процес тестування.

Список використаних джерел

1. Meinke, K. & Bennaceur, A., 2018. Machine Learning for Software Engineering: Models, Methods, and Applications. Gothenburg, Sweden, IEEE. URL: https://www.researchgate.net/publication/321807797_Machine_Learning_for_Software_Engineering_Models_Methods_and_Applications (дата звернення: 20.02.2024).

2. Kraus, D. (2018). Machine Learning and Evolutionary Computing for GUI-based Regression Testing. arXiv preprint arXiv: 1802.03768. (дата звернення: 18.02.2024).

3. Лановий О.Ф. Про один підхід до функціонального тестування web-додатків // Поліграфічні, мультимедійні та web-технології. Т1. Тез. доповід. 2-ї Міжнарод. наук.-техн. конф. (16-22 травня 2017) / редкол.: В.Ф. Ткаченко, І.Б. Чеботарьова та ін. – Харків: ХНУРЕ, 2017. – с. 246.

4. Eggplant Test. Deliver faster with model-based, AI-powered test automation (назва з екрану). URL: https://www.keysight.com/us/en/product/EG1000A/eggplant-test.html (дата звернення: 20.02.2024).

УДК 004.01

Душкін В.Д., Глушко П.Г., Федорчук І.І.

МАТЕМАТИЧНА МОДЕЛЬ ДИФРАКЦІЇ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ НА ДВОШАРОВІЙ СИСТЕМІ СМУГ

Електродинамічні структури в якості складової містять багатошарові періодичні вздовж одного з напрямків системи смуг, довжина яких значно перевищує їх ширину. Процес взаємодії електромагнітних хвиль із такими структурами можна описати за допомогою крайових задач для рівняння Гельмгольця з крайовими умовами першого, другого роду, або імпедансними граничними умовами. Для розв’язання таких задач існує велика кількість підходів. У випадку наявності великої кількості різних стрічок довільної ширини варто використовувати підходи, що не залежать від кількості смуг не періоді, їх ширини та взаємного розташування. Таким вимогам задовольняє підхід, що ґрунтується на зведенні початкових рівнянь до системи граничних інтегральних рівнянь за допомогою методу параметричних подань сингулярних та гіперсингулярних операторів [1-5]. Для знаходження наближених розв’язків систем граничних інтегральних рівнянь можна використовувати модифікації методу дискретних особливостей [6]. Завдяки використанню цього методу наближена система граничних рівнянь зводиться до пошуку розв’язків систем лінійних рівнянь, через які виражаються основні фізичні характеристики електродинамічних процесів.

Досліджувана структура складається з двох систем стрічок що лежать у паралельних площинах. Кількість стрічок, їх ширина та відстань між ними може бути довільною. На цю структуру згори падає Е-поляризована хвиля. В результаті застосування методу параметричних подань сингулярних операторів початкова задача зводиться до системи граничних інтегральних рівнянь, яка відрізняється від аналогічної системи граничних інтегральних рівнянь задачі розсіювання Е-поляризованих хвиль на екранованій системі стрічок підінтегральними виразами.

Здійснено комп'ютерну реалізацію отриманої математичної моделі за допомогою MathCAD 15. Для різних значень параметр структур, що містять від двох до п'яти елементів на кожному шарі було отримано числові значення коефіцієнтів Фур'є а також мапи ліній рівня поля над та під структурою. Числовий експеримент довів, що для отримання числових розв'язків із точністю достатньою для побудови графіків достатньо взяти до десяти точок інтерполяції на кожному з відрізків, який відповідає одній зі смуг структури. Слід відзначити, що при розгляді структури що містіть п'ять елементів на кожній стрічці необхідно було розв'язувати системи, що складались з тисячі лінійних рівнянь. Засоби MathCAD 15 успішно справлялись з такою задачею, однак час виконання обчислень для одного значення хвильового числа був достатньо довгим и складав 10-15 хвилин. Таким чином для проведення комп'ютерного моделювання у широкому діапазоні значень фізичних та геометричних параметрів реалізації має сенс використовувати комп'ютерні реалізації із застосуванням більш потужних за швидкістю обчислень програмних продуктів.

Список використаних джерел

1. Гандель Ю.В., Душкин В.Д. Математические модели двухмерных задач дифракции: сингулярные интегральные уравнения и численные методы дискретных особенностей. – Харьков: Ак. ВВ МВД Украины. – 2012. – 544 с.

2. G. I. Zaginaylov, V. D. Dushkin, V. Korostyshevski and P. V. Turbin, "Modeling the beam excitation of planar waveguide with rectangular irregularities," *MMET Conference Proceedings. 1998 International Conference on Mathematical Methods in Electromagnetic Theory. MMET 98 (Cat. No.98EX114)*, Kharkov, Ukraine, 1998, pp. 409-410 vol.1, doi: 10.1109/MMET.1998.709993.

3. Gandel' Yu. V., Dushkin V. D., 2012, Mathematical models based on SIE 2D diffraction problems on reflective multilayer periodic structures. Part II. The case of H polarization. Scientific statements. Series: Mathematics. Physics. Vol. № 5 (124) issue of 26. pp. 88

4. Dushkin V. D. Application of the Singular Integral Transform Method to the Solution of the Two-Dimensional Problem of Diffraction of Electromagnetic Waves from a Superconducting Layer with Rectangular Waveguide Channels // Telecommunications and Radio Engineering. – 2001. – V. 56. – N. 2. – P. 78 – 86.

5. V. D. Dushkin, S. V. Zhuchenko and O. V. Kostenko, "Computational Simulation of E-Waves Diffraction on Periodic Multielement System of Impedance Strips," *2020 IEEE Ukrainian Microwave Week (UkrMW)*, Kharkiv, Ukraine, 2020, pp. 625-629, doi: 10.1109/UkrMW49653.2020.9252606.

6. S. M. Belotserkovsky, I.K. Lifanov Method of Discrete Vortices, CRC Press, 1992. - 464p.

УДК 681.5.015

Дядюн С.В.

ОЦІНКА АДЕКВАТНОСТІ МАТЕМАТИЧНИХ МОДЕЛЕЙ ФУНКЦІОНУВАННЯ СКЛАДНИХ СИСТЕМ

Проблема побудови адекватних математичних моделей функціонування складних і великих систем завжди є однією з найбільш складних задач, і вирішальною при дослідженні та впровадженні науково-практичних розробок на реальних об'єктах.

У випадку, якщо імітаційна модель є адекватною, її можна використовувати для прийняття рішень щодо системи, яку вона відображає, як начебто ці рішення були здійснені на основі реальних експериментів з реальною системою. Модель складної систе-

ми може лише наблизитися до оригіналу, незалежно від того, наскільки багато зусиль було витрачено на її розробку, оскільки абсолютно адекватних моделей не існує.

Модель завжди розробляється для конкретного набору цілей і це свідчить про те, що модель, яка є адекватною для одного визначеного завдання, може не бути такою для іншого. Важливо відзначити, що адекватна модель не обов'язково є достовірною, і навпаки. Модель може бути достовірною, але при цьому не використовуватись для прийняття рішень. Наприклад, хоча достовірна модель може відтворювати реальність, вона може бути недостатньою для прийняття рішень у певних галузях та сферах з характерних причин.

Перевірка адекватності є необхідною умовою для переходу від дослідження об’єкта до дослідження моделі і подальшого перенесення результатів на об’єкт моделювання. Якщо формулювати визначення, то можна сказати, що адекватність – це відтворення моделлю, з необхідною повнотою, всіх властивостей об’єкта, важливих для цілей даного дослідження. Як правило, адекватність моделі визначається на підставі статистичних оцінок розбіжностей значень вихідних змінних моделі та об’єкта при однакових значеннях вхідних змінних, розрахованих за результатами серії експериментів на об’єкті моделювання.

Для перевірки адекватності моделі використовуються дані іншої серії експериментів, ніж для параметричної ідентифікації.

Саме відмінність значень виходу моделі та об’єкта може бути зумовлена наступними причинами:

- велика спрощеність моделі;
- похибка чисельних методів;
- похибка вимірювальних пристроїв;
- обчислювальна похибка, пов’язана з переходом на різні системи обчислення та особливостями комп’ютерних обчислень.

Якщо модель не задовольняє критеріям адекватності, необхідно крок за кроком перевірити коректність розробки на всіх етапах:

- умови проведення експерименту та правильність вимірювання і фіксування його результатів;
- правильність програмної реалізації алгоритмів;
- адекватність результатів параметричної ідентифікації;
- обґрунтованість вибору методу розв’язання моделі;
- коректність математичного опису явищ та характеристик об’єкта;
- адекватність концептуальної моделі.

Після побудови математичної моделі необхідно визначити її адекватність, для чого використовуються формальні й неформальні процедури. У першому випадку результати моделювання порівнюють з емпіричними даними, що відповідають тим самим значенням вхідних параметрів, межових і початкових умов. У цьому разі залишки моделі, тобто різниці між емпіричними даними й результатами, що розраховані за моделлю, мають бути нормально розподіленими випадковими величинами з близьким до нуля середнім арифметичним. Не має бути часової, просторової або будь-якої іншої кореляції між цими залишками. Крім того, має бути певна відповідність масштабів між стандартними відхиленнями залишків і похибок емпіричних даних. Неформальні процедури зазвичай передбачають якісне порівняння типових залежностей, передбачуваних моделлю, з наявними емпіричними даними та результатами, що одержані на інших вже апробованих моделях. Вони також мають встановлювати відповідність моделі більш загальним теоретичним законам і принципам, сформульованим у певній предметній області.

За результатами перевірки адекватності моделі приймають рішення щодо можливості її використання. Результатом перевірки може бути висновок про необхідність доробки (корегування) та оптимізації моделі. При корегуванні уточнюють перелік суттєвих

параметрів, обмеження, функціональні зв’язки між параметрами тощо. Інколи для перевірки адекватності треба залучати незалежних експертів, які не брали участі в розробці моделі. Після успішної перевірки адекватності модель може бути практично застосована.

Під оптимізацією розуміють спрощення моделі при збереженні заданого рівня її адекватності. Основними критеріями оптимальності є витрати часу, апаратних та інших ресурсів при використанні моделі. Як правило, основним критерієм оптимальності є співвідношення між можливими втратами, пов’язаними з неточністю моделі, й додатковими витратами, необхідними для їх усунення.

В цілому можна говорити про адекватність моделі оригіналу, якщо поведінка моделі досить точно збігається з поведінкою системи, що моделюється в однакових ситуаціях, і модель переконливо представлена щодо тих властивостей системи, які прогнозуються за допомогою моделі. Оцінка адекватності моделі полягає у перевірці ступеня збігу моделі та реальної системи.

Порушення адекватності моделі може визначатися багатьма факторами, які можна зарахувати до однієї з двох груп. Перша група факторів, що породжують так звану випадкову похибку, обумовлена деякою невизначеністю постановки задачі, пов’язаної з неповнотою вихідної інформації, відсутністю точних відомостей про зовнішні впливи, зневагою до деяких випадкових параметрів. Друга група факторів, що породжує систематичні похибки, є наслідком прийнятих припущень та обмежень при розробці концептуальної та математичної моделі – виключення тих чи інших параметрів, апроксимація, інтерполяція, припущення та гіпотези, заміна нелінійних елементів лінійними, ідеалізація режимів функціонування системи.

Результат моделювання в значній мірі залежить від адекватності вихідної концептуальної (описової) моделі, від отриманого ступеня подібності опису реального об'єкта, кількості реалізацій моделі та багатьох інших факторів. У ряді випадків складність об'єкта не дозволяє не тільки побудувати математичну модель об'єкта, а й дати досить близький кібернетичної опис, і перспективним тут є виділення частини об'єкта, що найбільш важко піддається математичному опису, і включення цієї реальної частини фізичного об'єкта в імітаційну модель. Тоді модель реалізується, з одного боку, на базі засобів комп’ютерної техніки, а з іншого - є реальна частина об'єкта. Це значно розширює можливості і підвищує достовірність результатів моделювання.

В доповіді розглядаються приклади успішної побудови адекватних математичних моделей функціонування складних і великих систем та їх впровадження на реальних об’єктах народного господарства країни та за кордоном.

УДК 681.5.015

Дядюн С.В., Новикова О.О.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Як і всі інші органи державного управління, правоохоронні служби у своїй поточній повсякденній діяльності все активніше впроваджують інформаційні та комп'ютерні технології, насамперед складання звітів та обробку різноманітної документації, обслуговування різних баз даних, архівів, а також використання Інтернету з питань, пов'язаних із виконанням професійних обов'язків. Використання сучасних технологій вимагає від співробітників органів внутрішніх справ (ОВС) володіння не лише основами інформаційних технологій, а й знання спеціального програмного забезпечення та програм, які застосовуються на державній службі. Майбутні фахівці ОВС мають отримати найваж-

ливіші навички застосування інформаційних технологій, спеціального програмного забезпечення та програм, необхідних для ефективної роботи.

В останні роки використання науково-технічних засобів у діяльності правоохоронних органів значно активізувалося. Впровадження нових інформаційних технологій у діяльність правоохоронних органів здійснюється через побудову локальних, регіональних та загальнодержавних галузевих обчислювальних мереж. Одним із основних компонентів інформаційних обчислювальних мереж загального користування є банк криміналістичної інформації. На практиці такі банки даних реалізовані у вигляді автоматизованих інформаційних систем (АІС), масиви яких ув'язані у єдине інформаційне поле.

Ефективність боротьби зі злочинністю визначається рівнем організації оперативної, слідчої, профілактичної роботи, яку проводять ОВС. У свою чергу, результати цієї роботи залежать від якості інформаційної підтримки, оскільки основні зусилля практичних працівників у розслідуванні, розкритті та запобіганні злочинам так чи інакше пов'язані з отриманням необхідної інформації. Саме ці функції покликана забезпечити система інформаційно-аналітичного забезпечення органів внутрішніх справ, яка підтримує значний обсяг інформації.

Загалом в органах внутрішніх справ в автоматизованому режимі за допомогою комп'ютерів обробляються завдання оперативно-розшукового та довідкового призначення з кількістю запитів, що постійно надходять, а також завдання обліково-статистичного, управлінського та виробничо-економічного призначення. Запорука успішного здійснення оперативно-розшукових заходів у тому, що стратегію і тактику виявлення і розкриття протиправних діянь необхідно будувати з урахуванням знань специфіки складу якихось злочинів. Співробітники правоохоронних органів повинні мати знання в галузі комп'ютерних технологій, кібернетики, психології, психолінгвістики. На жаль, нині такий підхід реалізувати не досить легко через недостатню підготовку більшості співробітників ОВС у галузі сучасних інформаційних технологій.

У діяльності підрозділів ОВС можна використовувати як універсальне, так і спеціальне програмне забезпечення. Універсальні програми (інформаційно-пошукові системи, редактори, електронні таблиці тощо) загального призначення не лише підвищують продуктивність праці та ефективність роботи з виявлення, розкриття і розслідування злочинів, а й піднімають її на якісно новий рівень. Спеціалізовані програми можуть бути орієнтовані на безпосереднє їх застосування під час здійснення оперативно-розшукових заходів у напрямі боротьби з інформаційною (у т.ч. комп'ютерною) злочинністю.

Інформаційно-аналітичне забезпечення діяльності правоохоронних органів є системою, яка включає в себе дві взаємопов'язані компоненти, що вимагають постійної уваги. Перша - це інформаційне забезпечення, яке полягає у вивченні інформаційного попиту споживачів, підтримці сталого стану інформаційних зв'язків, збиранні, накопиченні, обробці, зберіганні та видачі інформації споживачам у максимально короткі терміни. Друга - аналітичне забезпечення, яке полягає у дослідженні кримінальних загроз, виявленні причин та умов, що впливають на формування обстановки, прогнозування її розвитку, вивчення проблемних ситуацій у сфері протидії організованій злочинності.

Наразі в органах внутрішніх справ накопичено значний масив оперативно-розшукової та довідкової інформації, необхідної працівникам правоохоронних органів для проведення оперативно-слідчих та розшукових заходів, а також для вирішення інших службових завдань. Оперативно-аналітичний пошук інформації правоохоронними органами можуть забезпечити лише сучасні інформаційні технології. Підвищення ефективності роботи правоохоронних органів щодо розкриття та розслідування злочинів у сфері високих технологій на даний час неможливе без інтеграції в їхню діяльність нових інформаційних технологій, без розробки та повсюдного впровадження інформаційно-аналітичних систем.

Підвищення рівня інформатизації системи МВС на основі єдиної інформаційної інфраструктури ОВС має на меті забезпечити: оперативність формування, достовірність та повноту відомостей, що містяться в автоматизованих банках даних ОВС; підвищення ефективності інформаційної підтримки оперативно-службової та службово-бойової діяльності на всіх рівнях управління системи МВС за рахунок реалізації безпосереднього доступу користувачів до інформації, що зберігається та обробляється, створення єдиних алгоритмів та засобів обміну інформацією між взаємодіючими системами за рахунок використання електронної документації. У процесі інформатизації постійно відбувається вдосконалення процедур та регламентів міжвідомчої та відомчої інформаційної взаємодії, уніфікація даних, скорочення їх надмірності та виключення дублювання первинного введення інформації, зниження обсягу паперового документообігу; підвищення ефективності організаційно-управлінської діяльності за рахунок впровадження електронної документації та інформаційної підтримки управління силами та засобами; забезпечення аналітичної підтримки оперативно-службової діяльності, у тому числі скорочення часу, підвищення результативності та якості прийнятих рішень із використанням сучасних аналітичних методів обробки інформації. Крім того, інформатизація ОВС покликана забезпечити реалізацію вимог щодо комплексного захисту інформації, кібербезпеки; забезпечити необхідний рівень стійкості, безперервності, оперативності та скритності управління ОВС, підвищити якість управлінських рішень та скорочення тривалості управлінського циклу на основі ефективного використання інформаційно-технологічних та аналітичних можливостей ситуаційних центрів; підвищити якість та доступність наданих послуг громадянам та організаціям в електронному вигляді, інформаційну відкритість та прозорість механізмів управління у системі ОВС.

У доповіді розглядаються передові, уже працюючі в ОВС інформаційно-аналітичні системи, висловлюються пропозиції щодо їх подальшого розвитку, вдосконалення, розповсюдження по всім містам та населеним пунктам, та їх прив’язки з урахуванням специфіки кожного об’єкту та місцевості.

Єфімов Г.В., Івахів О.С., Поступальський С.Л., Касаткін Є.В.

ПРОБЛЕМИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УПРАВЛІННІ СИЛОВИМИ СТРУКТУРАМИ СКЛАДОВИХ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ ДЕРЖАВИ

Управління силовими структурами складових сектору безпеки і оборони (СБтаСО) держави пов'язане з добуванням і обробкою інформації. Отже, підвищення її якості нерозривно пов'язане з використанням передових інформаційних технологій. На сьогоднішній день досягнення максимальної ефективності застосування силових структур при вирішенні поставлених завдань стає неможливим без комплексної автоматизації управлінської діяльності органів управління.

Водночас необхідно чітко бачити протиріччя, які пов'язані з впровадженням автоматизованих систем управління (АСУ) силовими структурами. З одного боку, автоматизація процесів збору, передачі, обробки, зберігання і відображення інформації істотно підвищує можливості органів управління, а відповідно можливості застосування сил та засобів силових структур, а з іншої – зростає залежність стійкості управління від надійності функціонування комплексів засобів автоматизації.

Під час робіт пов’язаних з підвищенням стійкості системи управління, на наш погляд, недостатньо уваги приділяється питанням безвідмовності програмного забезпечення і апаратних засобів не в традиційному трактуванні технічної надійності, а з точки зору протидії можливим «інформаційно-технологічним диверсіям» противника. Завдання полягає в тому, щоб при виробництві компонентів АСУ не допустити викорис-

тання технічних і програмних засобів, не перевірених на наявність вбудованих «пасток», «вірусів» тощо. Нехтування цією проблемою може звести нанівець усі зусилля із автоматизації управління силовими структурами. Проблема загострюється ще більше із-за випадків експлуатації неліцензійних копій програмного забезпечення різних фірм-виробників. Це не лише суперечить встановленим нормам, але і створює труднощі при використанні різних розроблених ліцензійних програм. Крім того, відомо, що фірми-розробники, з метою боротьби з нелегальним використанням своїх програмних продуктів, застосовують механізми захисту. Їх запуск може привести до збоїв в роботі і навіть до втрати інформації, що зберігається в пам'яті засобів електронно-обчислювальної техніки (ЕОТ), а отже, до порушення управління.

Ми вважаємо, що для успішного вирішення зазначених проблем необхідно здійснювати наступні заходи. По-перше, при створенні (розробці, удосконаленні) автоматизованих систем управління різновідомчими силовими структурами враховувати, що вибір програмних засобів є одним з ключових моментів ще на ранніх стадіях проектування. Це особливо важливо при розробці АСУ в системі територіальної оборони, оскільки ці системи взаємодіють не лише по військовій, але і по цивільній лінії, фактично між всіма складовими СБтаСО. По-друге, удосконалювати єдину політику в області вибору, тестування, розробки і застосування програмних засобів (продуктів). Закуповувати програми для використання в АСУ тільки після ретельного тестування, уникаючи при цьому зволікання, оскільки «старіння» інформаційних технологій відбувається надзвичайно швидко. По-третє, посилити роботу зі створення систем програмування і загального програмного забезпечення гарантованої надійності. Розробку програмного забезпечення для потреб складових СБтаСО здійснювати під чітким контролем органів Служби безпеки та кібербезпеки держави. З цього приводу цікавим є досвід вирішення даних питань за кордоном. Суттєвим є те, що сталися істотні зміни в поглядах керівництва розвинених країн світу на роль і місце нових інформаційних технологій в системах управління. Про це, зокрема, свідчить прийнятий в США план масштабної реорганізації тих структур, які пов'язані з розробкою інформаційних технологій.

Останніми роками зарубіжні країни активізували дослідження в області теорії і практики застосування інформаційних дій проти комп'ютеризованих інформаційних систем, АСУ військами і зброєю, об'єктами життєзабезпечення, використання телекомунікаційних систем в ході розвідувальної діяльності та можливостей комп'ютерних зламів в інтересах спецслужб противника.

Водночас в організації управління є проблеми, що вимагають всебічних теоретичних досліджень, обґрунтування нових методологічних підходів до їх вирішення. Одна з них – автоматизація функції передбачення (прогнозування), а також процесу ухвалення рішення. Можливість заздалегідь отримати інформацію про наслідки реалізації того або іншого варіанту рішення є вкрай важливою і необхідною.

Один з шляхів прогнозування результатів рішень ґрунтується на використанні в АСУ такого ефективного методу, як моделювання спільних дій різновідомчих силових структур. Існуюча нині схема «досліджуваний процес - модель процесу - програмна реалізація на ЕОМ» вимагає коригування, яке викликане специфікою завдань управління складовими ТрО, їх складністю і важливістю. Недостатність одностороннього підходу до моделювання очевидна, оскільки практика розробки універсальних моделей показала, що неможливо охопити усе різноманіття умов і способів виконання завдань в системі ТрО. На нашу думку в АСУ повинен бути втілений автоматизований синтез моделей, що передбачає також їх подальше зберігання. Це, у свою чергу, пов'язано з необхідністю розробки моделей предметних областей. Методологічною основою тут служить концепція баз даних і баз знань.

Значну увага при вдосконаленні управління варто приділяти підвищенню оперативності і обґрунтованості ухвалення рішень, забезпеченню можливості їх вироблення, реалізації і контролю виконання у будь-яких умовах обстановки. Також необхідно до-

магатися гнучкості процедур управління, відмовитися від шаблонних рішень. Характерно, що при переході на більш високі рівні управління різко знижується кількість завдань, що вирішуються в автоматизованому режимі.

Кардинальних змін в цих питаннях можна досягти за рахунок: оптимізації збору, систематизації, обробки і зберігання, а також передачі інформації про обстановку; прогнозування результатів ухвалення рішень на основі завчасного моделювання і планування спеціальних (бойових) дій, оперативного коригування варіантів рішень при зміні ситуації; широкого застосування обчислювальних мереж, розподіленої обробки інформації; активного впровадження процедур підготовки пропозицій для ухвалення оптимальних рішень, які ґрунтуються на теорії ситуаційного управління, методах штучного інтелекту; раціональній інтеграції інтелектуальних здібностей посадовців штабів і обчислювальних можливостей ЕОМ, що враховує психофізіологічні особливості і можливості людини; використання мобільних компактних засобів обробки і передачі інформації. Головною складовою процесу інформатизації стає інтелектуалізація.

В основі виконання сучасних вимог до управління міжвідомчими силовими структурами лежить системний підхід до побудови АСУ, які повинні мати багатофункціональні робочі місця, об'єднаних в локальні обчислювальні мережі з розподіленою обробкою інформації. Особливості таких АСУ полягають в наступному. Їх технічні і програмні засоби дозволяють створювати інтегровану систему моделювання завдань управління, що в іноземній літературі визначається як моделюючий центр. До складу цієї системи входять модель предметної області, засоби автоматизованого синтезу моделей завдань управління на основі нових інформаційних технологій, засобу багатоваріантного експериментування, а також система підтримки ухвалення рішень. Програмне забезпечення будується за принципом інваріантного динамічного ядра, яке при необхідності можна адаптувати до конкретних вимог.

Таким чином, підходи до комплексної автоматизації функцій управління, розробки і створення засобів автоматизації, що ґрунтуються на використанні традиційних схем і методів, вичерпали свої можливості і не дозволяють радикально підвищити ефективність управління міжвідомчими структурами. Реалізувати ті жорсткі вимоги, які пред'являються до управління сьогодні, неможливо без впровадження сучасних інформаційних технологій. Для цього потрібні фахівці, що впевнено орієнтуються в питаннях оперативного мистецтва, тактики і спеціального (бойового) застосування різновідомчих сил та засобів, твердо володіють методами математичного моделювання, глибоко знають основи теорії управління, теорії систем, системного аналізу, дослідження операцій і ухвалення рішень.

УДК 351.865

Живило Є.О.

ОЦІНКА КІБЕРРИЗИКІВ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ МОДЕЛЕЙ КІБЕРЗАХИСТУ

Через швидкий розвиток технологій, зростання цифровізації, проведення превентивних наступальних операцій та деструктивних дій у кіберпросторі, об’єкти критичної інформаційної інфраструктури (Далі – ОКІІ) можуть зазнати підвищених ризиків в системах захисту інформації та кібербезпеки (Далі – КБ), що може негативно позначитися на цілях організації, відповідальної за центри інформаційної інфраструктури. Таким чином, організації повинні ефективно управляти ризиками КБ. Оцінка ризиків КБ є невід’ємною частиною процесу управління ризиками в організації.

Проводячи оцінку ризику КБ на ОКІІ необхідно [1]:

- визначити, які технологічні процеси можуть зазнати негативного кібернетичного впливу, що в подальшому безпосередньо вплине на стале функціонування такого ОКІІ;

- визначити рівні ризику, яким вони піддаються (добре зрозуміти рівні ризику, що в свою чергу дозволить розподілити адекватні дії та ресурси для управління найвищими пріоритетами).

При оцінці ризику можна виявити наступні небезпеки:

- невірне формулювання сценаріїв ризику;

- варіанти сценаріїв ризику, які описують події пов'язані з кібернетичним впливом, що мають розмитий і загальний характер, не містять конкретних подій загроз, вразливостей, активів та наслідків. Як результат, важко зрозуміти ступінь ризиків та пов'язати їх із організаційним контекстом або визначити цілеспрямовані заходи щодо їх усунення;

- визначення ризиків із використанням підходу, орієнтованого на відповідність – виявлення ризиків з точки зору оцінки заходів безпеки (або їх відсутності), подібно до проведення аудиту відповідності або аналізу невідповідностей на основі нормативно-правових актів. Підхід до оцінки ризиків відповідності визначає поведінку контрольного списку, створюючи хибне відчуття безпеки, що ОКІІ не піддається жодним ризикам, якщо вона відповідає всім відповідним вимогам;

- визначитись з відсутністю факторів толерантності до ризику. Часто плани управління ризиками КБ ОКІІ не включаються до програми управління ризиками організації чи установи. Як результат, толерантність до ризиків КБ на організаційному рівні часто ігнорується, і керівництву установи важко визначити відповідний рівень ризику для досягнення своїх цілей;

- визначення ймовірності ризику на основі історичних або передбачуваних подій;

- неточність визначеного підходу. Зазначене може статись внаслідок одночасного фіксування **n**-ої кількості випадків. За таких умов, можна припустити, що подія сталася раніше, особливо у випадку відсутності інформації про минулі події КБ. У контексті безпеки ймовірність події КБ не залежить від частоти минулих подій;

- обробка ризиків за допомогою неслушного контролю заходів. При використанні загального підходу з розробки заходів контролю потенційних ризиків, багатьма організаціями доволі часто пом'якшується алгоритм виявлення ризиків КБ. В свою чергу, це призводить до впровадження засобів контролю, які не повністю усувають першопричину [2]. Ця проблема часто пов'язана з поганим розумінням або формулюванням сценаріїв ризику.

Як показано на рисунку 1, процес управління ризиками, пов'язаний з безпекою ОКІІ може бути ітеративним. Ітераційний підхід до процесу оцінки кіберризиків може мати форму підвищення рівня деталізації кожної ітерації або зупинки процесу. Після кожної фази/етапу є точки прийняття рішення (продовження, завершення, повернення). Ітераційний підхід забезпечує вигідний баланс між скороченням часу, зусиллями, необхідними для певних засобів контролю, та впевненістю у правильній оцінці кіберризику.

За цих умов, встановлення контексту ризику є важливою передумовою для подальшої оцінки кіберризику. Даний крок гарантує, що внутрішні та зовнішні зацікавлені сторони, які беруть участь у процесі оцінки ризику, мають загальне розуміння того, як формується ризик, прийнятність ризику до розгляду та відповідальність власника ризику.

Припустимо, що ризик КБ (R) визначається як функція:

- ймовірності (P) того, що ця загроза впливає на вразливість активу;

- результуючий вплив (V) виникнення загрози.

$$R(t) = F(P, V) \quad (1)$$

Пропонується визначити кожен із факторів ризику окремо.

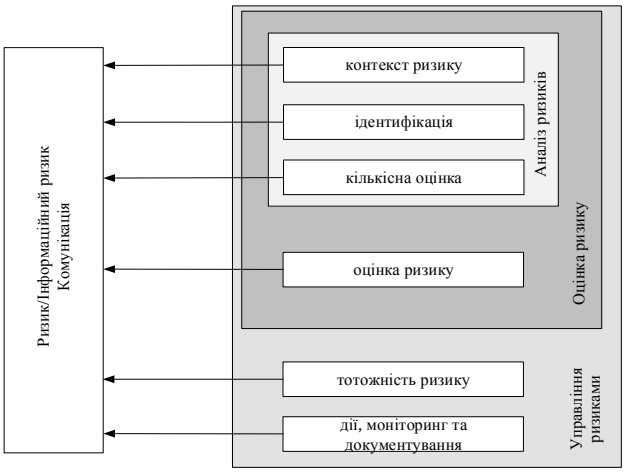


Рисунок 1 – Модель процесу управління кіберризиками

Загроза – це будь-яка подія, під час якої зловмисник, використовуючи вектор загрози, діє проти активу таким чином, що він потенційно може заподіяти йому шкоду. У контексті КБ загрози можуть характеризуватися тактикою, методами та процедурами, що застосовуються зловмисниками.

Уразливість – дефект у розробці, впровадженні та експлуатації активу, або у внутрішньому контролі процесу.

Ймовірність – це можливість того, що дана загроза здатна використати дану вразливість (або сукупність вразливостей). Ймовірність може бути виведена з таких факторів, як: виявлення, придатність для використання та відтворюваність.

Вплив – це розмір збитку, спричиненого загрозою, яка використовує вразливість (або сукупність уразливостей). В таких умовах розмір шкоди може бути оцінений з точки зору держави, організації чи окремої людини.

Толерантність до ризику визначається як рівень прийняття ризику, прийнятний для досягнення конкретної мети. Визначення толерантності до ризику дозволяє чітко сформулювати, який ризик готова прийняти організація. У таблиці 4 статті [3] наведено приклад врахування толерантності до ризику, який можна адаптувати відповідно до контексту кожної організації.

Отже, оцінка ризиків складається з виявлення ризиків, характерних для навколишнього середовища, та визначення рівня виявлених ризиків. Основними етапами оцінки ризику є ідентифікація ризику, кількісна оцінка ризику (що є елементами аналізу ризику) та якісна оцінка ризику [4].

Кількісна оцінка ризику складається з аналізу елементів, які включають кожен сценарій ризику окремо, з метою визначення ймовірності виникнення сценарію ризику та впливу (тобто величини шкоди) в результаті виникнення сценарію ризику.

Попередньо проведений аналіз засвідчує, що цілеспрямоване або неочікуване виникнення події традиційно використовується як метрика для вимірювання ймовірності ризику. Однак використання такої метрики для вимірювання ймовірності ризику КБ може бути недоцільним через динамічний характер загроз КБ. Якщо штатне функціонування системи не було порушено раніше, то зазначене не означає, що вона не буде порушена в майбутньому. Імовірність ризиків КБ повинна оцінюватися з точки зору загроз та вразливостей системи. Тому для визначення ймовірності ризику КБ системи необхідно враховувати наступні фактори: виявленість, можливість використання та відтворюваність.

При цьому необхідно враховувати, що прояв сценарію ризику може порушити конфіденційність, цілісність та/або наявність активів (наприклад, інформації, обладнання,

операцій). Будь-яка компрометація активів призведе до негативних наслідків на всіх організаційно-технічних рівнях.

Як висновок необхідно зазначити, що складність кіберфізичних відносин у функціонуванні ОКІІ полягає у несвідомих системних залежностях. Водночас точна оцінка ризику вимагає розробки моделей, які забезпечують основу для аналізу залежності та кількісної оцінки ризиків. За цих обставин зв'язок між характеристиками ОКІІ сприяє процесу аналізу ризиків та пом'якшенню їх наслідків.

Отже, зазначений підхід до оцінки ризиків КБ може бути застосований в інформаційно-аналітичній системі "Система управління безпекою"[5], яка забезпечує виявлення вразливостей та оцінку ризиків (потенціал ризику) та спрощує розробку управлінських рішень для запобігання подіям, що впливають на КБ.

Список використаних джерел

1. Постанова Кабінету Міністрів України "Про затвердження Положення про організаційно-технічну модель кіберзахисту" від 29 грудня 2021 р. № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text.

2. Information security, Cybersecurity and the IEC 62443 series of standards (2022). Available at: https://ikmj.com/en/information-security-cybersecurity-and-the-iec-62443-series-of-standards/

3. Yevhen Zhyvylo, Vladyslav Kuz Risk Management of Critical Information Infrastructure:Threats-Vulnerabilities-Consequences // Vol. 5 No. 2 (2023): Theoretical and Applied Cyber Security. P. 68–80.

4. Svitlana Onyshchenko, Yevhen Zhyvylo, Anna Cherviak, Stanislav Bilko Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security // Vol. 5 (13 (125)) (2023): Eastern-European Journal of Enterprise Technologies. P. 65–76.

5. Mokhor V., Bakalynskyi O., Bohdanov O., Tsurkan V. Interpretation of the simple risk level dependence of its implementation in the terms of analytic geometry. Information technology and security. 2017. V. 5. № 1. P. 71–82.

УДК 623.4.017

Задерей К.С., Юзова І.Ю., Худов Г.В.

АНАЛІЗ ДОСВІДУ ЗАСТОСУВАННЯ КРИЛАТИХ РАКЕТ ТИПУ «КАЛІБР» В РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ

З першого дня повномасштабного вторгнення війська рф ведуть ракетний терор у містах України. Спочатку для ударів використовували високотехнологічні та дорогі ракети Х-101, Х-30 або Х-32, а також "Калібр" та "Іскандер". Попри те, що влада рф запевняла, ніби цілями їхньої "високоточної" зброї будуть виключно об'єкти військової інфраструктури, від ракетних ударів постраждало багато цивільних об'єктів.

Наразі, за даними українського Генштабу, росіяни активно використовують проти України крилаті ракети "Калібр", а також оперативно-тактичний ракетний комплекс "Іскандер".

Сучасні високоточні крилаті ракети, такі як "Калібр", мають здатність змінювати траєкторію, висоту польоту, напрямок руху та швидкість, що ускладнює для сил ППО розрахунок траєкторії та прогнозування місцеположення ракети. У певному сенсі "Калібри" можна порівняти із безпілотниками - тільки вони летять значно швидше, а ефект від їх застосування більш руйнівний. Низька висота та зміна напрямку ускладнюють захоплення цілей. Розроблялися вони переважно як озброєння кораблів та підводних

човнів, але існують варіанти і для їхніх пусків з літаків ("Калібр-А"), а також наземних пускових установок, зокрема і з тих же комплексів "Іскандер".

Особливість "Калібрів" у їхній універсальності. Це озброєння можна запускати як з кораблів та підводних човнів, так і з літаків та наземних пускових установок.

На озброєнні у росії є:

– ракетні комплекси Калібр для озброєння підводних човнів (Калибр-ПЛЭ, експортне позначення Club-S);

– ракетні комплекси для озброєння бойових надводних кораблів (Калибр-НКЭ, експортне позначення Club-N);

– мобільні ракетні комплекси Калібр-М (експортне позначення Club-M);

– комплекси ракетної зброї авіаційного базування Калібр-А (експортне позначення Club-A).

Але Україна вже навчилась ефективно протистояти ракетам "Калібр". Завдяки допомозі та підтримці західних партнерів, українське ППО покращилось у рази, разом з цим зріс і відсоток збиття ворожих повітряних цілей. Співпрацюючи з партнерами, Україна отримала комплекси ППО NASAMS та IRIS-T.

Завдяки тому, що "Калібр" більшу частину траєкторії рухається з дозвуковою швидкістю, її можна збивати звичайними ручними ракетними комплексами, такими як радянська "Ігла", чи їх американським аналогом "Stinger". Річ у тому, що швидкість польоту ракет, випущених з цих комплексів, становить близько 750 метрів за секунду (2700 км/год), або більше 2 Мах, чого повністю достатньо для того щоб наздогнати "Калібр". Україна вже сформувала окремі батальйони, які спеціалізуються на перехопленні подібних ракет у місцях, де враження ракети і падіння її уламків не становлять загрози для мирного населення й інфраструктури.

Вкрай важливим аспектом у зменшенні кількості обстрілів України за допомогою цих ракет є поступова ліквідація їх кораблів-носіїв у тимчасово окупованому Криму. Близько 33% бойових кораблів Чорноморського флоту рф Україна вивела з ладу за час широкомасштабного вторгнення.

Тому напрямком подальших досліджень є прогнозування польоту крилатої ракети типу "Калібр" для розрахунку зони радіолокаційної інформації радіотехнічних підрозділів.

УДК 621.396.96

Закарлюка К.А., Сердюк О.В.

АНАЛІЗ ТАКТИЧНИХ ТА ТАКТИКО-ТЕХНІЧНИХ ХАРАКТЕРИСТИК РЛС «СНОВ»

На сьогодні технології безпілотних літальних апаратів (БПЛА) не тільки значно розширюють функціональні можливості авіаційної складової збройних сил, а також можуть мати переваги перед традиційною авіацією. Тому подальший розвиток БПЛА, закупка та постановка їх на озброєння в збройних силах різних країн обумовили:

− необхідність перерозподілу задач між пілотованою та безпілотною авіацією;

− застосовування при виготовленні БПЛА нових композитних матеріалів, які разом з відносно невеликими розмірами й спеціальною формою забезпечують порівняно малі значення ЕПР ніж у пілотованих літальних апаратів;

− забезпечення розвитку БПЛА, який пов’язаний зі збільшенням корисної ваги, дальності бойового застосування, висоти і тривалості польоту та розширенням діапазону швидкостей, покращенням автономності роботи БПЛА;

− проведення досліджень та робіт щодо розширення функціональності й універсальності БПЛА, з удосконалення форм та способів їх застосування, зі збільшення обсягів обробки отриманих розвідувальних них даних на борту БПЛА (впровадження удосконалених алгоритмів автоматизації процесів виявлення, розпізнавання та ідентифікації об'єктів розвідки) перед передачею їх на наземні станції;

− перехід до використання великих угруповань БПЛА в рамках концепції "рій", "зграя" під керівництвом штучного інтелекту;

− цілеспрямовану роботу з модернізації БПЛА, яка спрямована на адаптацію апаратури БПЛА до виконання бойових завдань в умовах впливу завад та протидії противника;

− здійснення розвитку функціональних можливостей БПЛА одночасно з удосконаленням (або створенням) комплексної системи розвідки, інформаційного забезпечення військ, адаптивної системи управління.

Зазначені вище особливості розвитку БПЛА вимагають здійснювати дієві кроки щодо протидії існуючим мережецентричним системам, які утворились при інтеграції БПЛА, дронів-камікадзе та високоточної зброї різних родів військ, в першу чергу, це стосується задачі своєчасного та гарантованого виявлення БПЛА.

Бажано відмітити, що тактичні мікро-БПЛА не виявляються сучасними РЛС, але такі БПЛА мають малий радіус бойової роботи, (12−15) км, і суттєво обмежені можливості по збору розвідданих, тому наразі концентрувати зусилля для забезпечення ви- явлення таких безпілотників недоцільно. На даний час більш важливим бачиться вирішення завдання ефективного виявлення оперативних й оперативно-тактичних БПЛА, які в змозі вирішувати задачі оптичного, радіотехнічного, радіолокаційного спостереження великих територій тривалий час.

Найбільш прямолінійним варіантом рішення задачі щодо покращення якості виявлення БПЛА є закупівля найсучасніших РЛС іноземного виробництва. Наприклад, новітня багатофункціональна РЛС TPS-77 виробництва корпорації Lockheed Martin (США) призначена у тому числі для виявлення та спостереження БпЛА. Однак такий шлях є нераціональним, оскільки Україна має повний цикл виробництва власних РЛС.

Наступним шляхом рішення задачі щодо покращення якості виявлення БПЛА є розробка нових типів радіолокаторів, які призначені для отримання інформації про такі цілі. Такий шлях вимагає великих фінансових вкладень, значних працевитрат та займає тривалий час. Тобто це робота на віддалену перспективу, керування якою повинне проводитись органами державного і військового управління.

Наступним напрямом рішення задачі щодо покращення якості виявлення БПЛА є модернізація існуючих зразків радіолокаційного озброєння, в яких задача виявлення БПЛА здійснюється краще. Одним з таких варіантів є радіолокаційний комплекс 1РЛ220УК виробництва казенного підприємства "Науково-виробничий комплекс "Іскра" (м. Запоріжжя). Досвід випробувань цього комплексу свідчить про високу якість виявлення й спостереження артилерійських снарядів калібру 120 мм і 152 мм. На думку авторів, радіолокаційний комплекс 1РЛ220УК може бути достатньо швидко переорієнтований для рішення задач виявлення малорозмірних, маловисотних та малошвидкісних цілей.

Розглянемо можливості виявлення безпілотних літальних апаратів радіолокаційними станціями старого парку. Радіолокаційні засоби, які перебувають на озброєнні РТВ Повітряних Сил Збройних Сил України, здатні виявляти БПЛА різного призначення в межах своїх тактико-технічних характеристик. Максимально можливі дальності виявлення БПЛА з різною ЕПР за допомогою оглядових РЛС РТВ за досвідом ведення бойових дій наведені в табл. 1.

Таблиця 1 – Максимально можливі дальності виявлення БПЛА різних класів за допомогою РЛС РТВ

Висота польоту БПЛА, м	Дальність виявлення БПЛА, км								
	РЛС 19Ж6 (35Д6, 35Д6М)			РЛС П-18 "Малахіт" (П-18)			РЛС П-19 (П-19МА)		
	"Форпост", "Орион" (σ=0,1 м2)	"Тахион" "Орлан10" (σ=0,01 м2)	Mavic-PRO "Квадрокоптер" (σ=0,001 м2)	"Форпост", "Орион" (σ=0,1 м2)	"Тахион" "Орлан10" (σ=0,01 м2)	Mavic-PRO "Квадрокоптер" (σ=0,001 м2)	"Форпост", "Орион" (σ=0,1 м2)	"Тахион" "Орлан10" (σ=0,01 м2)	Mavic-PRO "Квадрокоптер" (σ=0,001 м2)
100	40	31	22	13	12	10	25	18	12
200	50	37	25	22	18	14	34	26	18
500	75	37	25	30	25	21	50	20	13
1000	90	37	25	42	35	28	65	29	17

При цьому виявлення БПЛА на малих та гранично малих висотах здійснюється в зоні дії потужних пасивних завад у вигляді віддзеркалень від місцевих предметів. Радіус цієї зони для середньопересіченої місцевості, яка є характерною для зони проведення бойових дій, становить 30…40 км. Тобто можливості оглядових РЛС РТВ щодо виявлення БПЛА на малих та гранично малих висотах обмежені.

В Україні створені декілька радіолокаційних засобів, які призначені для виявлення цілей з малою ефективною площею розсіювання (БПЛА).

Малогабаритна автоматизована РЛС "Снов" здатна виявляти повітряні, наземні й надводні цілі на відстані в 60 км і на висоті від 20 до 5000 метрів. Призначена саме для виявлення малорозмірних та маловисотних цілей.

Холдингова компанія «Укрспецтехніка» (входить до складу ГС «Ліга оборонних підприємств України») продовжує удосконалювати лінійку малогабаритних радіолокаційних станцій. Чергове досягнення в цьому напрямку — оглядова автоматизована РЛС «Снов», що створена на базі цифрової антенної решітки. Ця радіолокаційна станція призначена для ведення радіолокаційної розвідки та видачі радіолокаційної інформації про повітряні об'єкти. Управління нею здійснюється дистанційно. Вона здатна виявляти малорозмірні цілі на відстані до 50 км на висотах від 20 до 5000 метрів.

Нещодавно завершено її державні випробування, під час проведення випробувань така РЛС добре себе зарекомендувала саме під час виявлення низьколітаючих і малорозмірних цілей з малою ефективною відбиваючою поверхнею, з ідентифікацію та спостереженням за якими деколи не можуть ефективно впоратись застарілі РЛС, виготовлені за радянських часів. Тактико-технічні характеристики наведені в таблиці 2.

Таблиця 2 - Тактико-технічні характеристики РЛС

Частотний діапазон:	L-діапазон
Дальність виявлення:	до 50 км
Огляд за кутом місця:	- 10°..+30°
Огляд за азимутом:	0°..360°
Висота виявлення:	20...5000 м
Період огляду зони виявлення:	2...5 с

Управління станцією здійснюється дистанційно. Здатна виявляти малорозмірні цілі на відстані до 50 км на висотах від 20 до 5000 метрів. Радар може працювати й видавати інформацію в автоматизованому режимі й встановлюватися як стаціонарно (на позиції), так і на автомобілі або причепі.

РЛС Х1- М "Око" призначена для виявлення малорухомих наземних об'єктів на фоні місцевості, низьколітаючих малорозмірних ЛА, визначення координат цілі (азимуту і

дальності), радіальної швидкості і ширини допплерівського спектру. Тактико-технічні характеристики наведені в таблиці 3.

Таблиця 3 – Основні ТТХ РЛС Х1-М “Око”

Найменування характеристики	Значення
Інструментальна дальність, км	0,3 – 30
Імпульсна потужність передавача, Вт	30
Сектор огляду по куту місця, °	30
Азимутальний сектор огляду, °	360
Точність:	
– по дальності, м;	5
– по азимуту, °	1
Радіальна швидкість, м/с	0,1
Максимальна швидкість цілі, що супроводжується, м/с	60
Дальність виявлення при С/Ш, більше 15 дБ:	
– БЛА (0,01 м2), км;	7
– людина (0,5 м2), км;	18
– автомобіль, літак, (1 м2), км	25
Споживана потужність, Вт	300
Вага, кг	65

Таким чином, радіолокаційні засоби, які перебувають на озброєнні РТВ Повітряних Сил Збройних Сил України, потенційно здатні виявляти оперативно-тактичні БПЛА в межах своїх тактико-технічних характеристик. Використання оглядових РЛС РТВ для виявлення тактичних міні-БПЛА є недоцільним і невиправданим. Недоцільним – через надзвичайно низькі можливості з виявлення означеного типу цілей, а невиправданим – через невідповідність масштабів задач, для вирішення яких первісно проектувались і розроблялись РЛС РТВ. Новітня РЛС «СНОВ» та «Око» більш ефективні, для виявлення БПЛА, ніж радіолокаційні станції старого парку.

УДК 004.056

Здоренко Ю.М., Хакімов М.Е., Масловський А.В.

МЕТОДИ ЗАХИСТУ ВЕБ-РЕСУРСІВ ВІД ІН’ЄКЦІЙНИХ АТАК НА ОСНОВІ ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ

У сучасному світі використання власних веб-ресурсів є необхідною складовою забезпечення повсякденної діяльності установ та організацій. Цифрова трансформація комерційних та державних секторів відкриває безліч можливостей для швидкого та ефективного доступу до необхідних документів та послуг. Поряд з цим зростає рівень загроз від здійснення кібернетичних атак на веб-ресурси. Деякі атаки можуть відбуватися непомітно (без явних ознак) для користувачів, але мають значний негативний вплив на роботу інформаційних систем та можуть стати причиною витоку даних.

Одним з найпоширенішим способів проведення кібератак на веб-ресурс є ін’єкційні атаки [2]. До них відносять: XSS-ін’єкції (Cross-Site Scripting) та SQL-ін’єкції. Ін’єкційні атаки можуть реалізуватися, коли зловмисники використовують уразливості у веб-додатках, які можуть приймати ненадійні дані. Так, внаслідок додавання зловмисного коду у поля введення форм, можуть бути виконані неавторизовані команди, отриманий доступ до конфіденційних баз даних та отриманий повний контроль над веб-ресурсом. Також необхідно враховувати, що переважна більшість потенційних вразливостей в інформаційних системах виникає через людський фактор. Наприклад, випадкове надання доступу до баз даних особам, які не повинні мати доступу, може стати

причиною несанкціонованого втручання або витоку конфіденційної інформації. Також недбале тестування програмного забезпечення на етапах розробки та використання неперевіреного коду при оновленнях програмного забезпечення веб-ресурсу є передумовою вразливостей, які можуть бути використані зловмисниками для атаки на інформаційну систему. Тому важливо вдосконалювати процеси контролю доступу, навчання персоналу з питань кібербезпеки та ретельно перевіряти програмний код перед впровадженням на веб-ресурсі.

Для виявлення ін'єкційних атак можуть бути використані методи на основі використання інтелектуальних підходів. Так, в роботі [1] запропоновано визначати тип атаки JS(HTML)/ScrInject на основі використання нечіткої системи логічного виводу. Однак даний підхід ґрунтується на налаштуваннях вхідних параметрів на основі експертних знань (оцінок) та потребує періодичного перенавчання таких систем. Тому для визначення факту проведення ін'єкційної атаки та вчасного вжиття запобіжних заходів пропонується удосконалити зазначений підхід та використати нейро-нечітку систему. Такий тип інтелектуальних систем дозволяє поєднати можливості нечітких систем логічного виводу для визначення класу атаки та нейронних мереж - для налаштування значень параметрів систем логічного виводу та їхнього перенавчання. Використання такого підходу дозволить забезпечити надійний захист веб-ресурсів та забезпечити захист від нових атак в майбутньому.

Список використаних джерел

1. Здоренко Ю.М., Фесьоха О.В., Субач І.Ю. Методика виявлення кібератак типу JS(HTML)/ScrInject на основі застосування математичного апарату теорії нечітких множин / Збірник наукових праць ВІТІ № 4, – 2018, м. Київ.

2. OWASP top 10 vulnerabilities. Veracode. URL: https://www.veracode.com/security/owasp-top-10 (date of access: 23.02.2024).

УДК 37.09

Зеленюх О.М., Кузьменко Р.В., Канчуга М.К.

ТЕНДЕНЦІЇ У ПІДГОТОВЦІ ВОДІЇВ АВТОМОБІЛЬНОЇ ТЕХНІКИ

Традиційне навчання водіїв відбувається в один етап, до того, як водій отримує посвідчення водія. Дійсно, основною метою навчання водіїв є підготовка початківців до здачі іспитів на отримання посвідчення водія, а більшість видів навчання вважаються успішними, якщо навчаємі досягають навчальних цілей і успішно складають іспит. Проте очікується, що навчання водінню змінить їхню подальшу поведінку настільки, що це матиме вимірюваний вплив на аварійність. Ґрунтуючись на тривалій історії оціночних досліджень, більшість фахівців скептично ставляться до переваг водійської підготовки з точки зору безпеки руху. Саме навчання водінню стало дуже різноманітним, і створення стратегічного вдосконалення є досить складним завданням. Це важлива галузь у всьому світі, хоча вона залишається дуже фрагментованою.

Сучасне навчання водіїв має на меті зменшити фактори ризику для водіїв-початківців. Зростає розуміння того, що безпечне водіння передбачає зміну навичок і звичок, які визначають фактичну поведінку за кермом. Ненавмисні помилки і неправильні дії, ймовірно, сприяють підвищеному ризику для водіїв-початківців, хоча, можливо, і не в однакових пропорціях для всіх випадків.

Щоб досягти значного підвищення безпеки за допомогою навчання водіїв-початківців, стало досить загальновизнаним, що необхідно впроваджувати більш ком-

плексні підходи до досліджень і розробки програм, а також встановлювати зв'язки між навчанням водіїв та іншими факторами, що впливають на безпеку руху.

У навчанні водіїв простежується багато новітніх тенденцій, що розвиваються, адже підвищення рівня освіти завжди є популярним рецептом для покращення безпеки. Проте, продемонстрована ефективність покращення показників безпеки виключно за допомогою навчання у будь-якій формі є відносно незначною. Навчання може сприяти розвитку кращих когнітивних і психомоторних навичок, однак кращі навички не призводять автоматично до підвищення рівня безпеки, що залежить як від навичок, так і від поведінки. Вплинути на поведінку з метою зменшення ризику набагато важче, ніж прийнято вважати.

Перспективною тенденцією є зростаюче визнання необхідності більш сильнішої теорії та складання логічної програми. Теоретичні підходи ґрунтуються на ієрархічному впорядкуванні широкого спектру характеристик водія, його рис, психічних станів, навичок водіння, мотивації, цінностей, навичок самоконтролю та поведінки під час кермування.

Ще однією загальною тенденцією у сфері безпеки дорожнього руху є визнання того, що активні та пасивні заходи безпеки потребують і можуть бути надалі розвинені. Поступова видача водійських посвідчень є ініціативою з безпеки дорожнього руху, а післядипломна освіта водіїв, є обґрунтована теоретичними засадами. Цілком зрозуміло, що не всі навички, які необхідні водієві, можуть бути засвоєні за один раз. Тому навчання повинно бути розподілене в часі, через початкову неготовність навчаємого до навчання або недостатню його когнітивну здатність.

У провідних країнах світу помітно зростає інтерес до коротких післяліцензійних навчальних програм для розвитку навичок і мотивації нових водіїв. Вони включають в себе комп'ютерне навчання, навчання в автомобілі (поза дорогами) або навчання на симуляторах.

Майбутнє ринку симуляторів водіння виглядає багатообіцяючим. Зростаючий попит на ефективні та безпечні програми навчання водіїв, прогрес у технологіях симуляції та зростання кількості молодих водіїв є ключовими факторами його зростання. Симулятори на основі штучного інтелекту можуть аналізувати поведінку водія, персоналізувати навчальні модулі та забезпечувати зворотний зв’язок у режимі реального часу, роблячи процес навчання ефективнішим і результативнішим.

Отже, сучасні тенденції, що стосуються підготовки водіїв автомобільної техніки, спрямовані в більшій мірі на поступове отримання посвідчення водія, що включає в себе декілька етапів навчання до та після отримання посвідчення водія, яке в свою чергу має покращити результативність і, відповідно, підвищити рівень безпеки на дорогах.

УДК 621.396

Зубков А.М., Андреєв І.М., Красник Я.В., Онищенко В.А., Прокопенко В.В.

СПОСТЕРЕЖЕННЯ ПОВІТРЯНИХ ОБ’ЄКТІВ, ЩО НИЗЬКО ЛЕТЯТЬ, НА ОСНОВІ ДІЮЧОЇ МЕРЕЖІ МОБІЛЬНОГО ЗВ’ЯЗКУ

Спостереження повітряних об’єктів, що низько летять (перш за все малорозмірних типу БпЛА, крилата ракета), в межах міської інфраструктури традиційними методами радіо, теплової та оптичної локації ускладнено через екрануючу дію будівель. Показано, що альтернативою такому підходу є застосування методів “просвітної” радіолокації. Причому в якості “підсвітлюючого” джерела радіохвиль доцільно використовувати випромінювання базових станцій мобільного зв’язку. Визначені граничні можливості такого способу за дальністю дії. Практична реалізація розробленого спо-

собу не вимагає впровадження в апаратно-програмну частину системи мобільного зв'язку і допускає гнучку зміну місцезнаходження чергової радіолокаційної станції. Підхід, що пропонується, є оптимальним за критерієм "ефективність/вартість".

Актуальність роботи обумовлена необхідністю пошуку науково-практичних шляхів забезпечення ефективного захисту від високоточної зброї повітряного базування об'єктів в межах міської інфраструктури. Метою роботи є збільшення дальності виявлення місцеположення атакуючих малорозмірних повітряних цілей, що низько летять, в умовах екрануючої дії міської інфраструктури. Ключовим елементом запропонованого науково-технічного підходу є спосіб бар'єрного виявлення на основі використання "підсвітлюючого" сигналу базових станцій мобільного зв'язку в рамках методу напівактивної радіолокації.

Ефективними шляхами подолання рубежу ППО являються:

– політ літальних апаратів (ЛА) на гранично низьких висотах;

– зниження ефективної поверхні розсіювання (ЕПР) в напрямку польоту і в бокових плоскостях шляхом придання аеродинамічній конструкції спеціальної форми і використання для її виготовлення спеціальних композитних матеріалів і пластика.

Другий шлях фізично оснований на перерозподілі розсіяної формоутворюючою поверхнею потужності зондуючого сигналу в вертикальній плоскості. Ця обставина дає можливість підвищити енергетику радіолокаційного каналу спостереження при установці приймальної апаратури чергової РЛС на земній поверхні і обробці ехо-сигналів "підсвітки", що формуються базовими станціями сотового зв'язку [1].

Являє собою безсумнівно теоретичний і прикладний інтерес оцінка граничних можливостей методу "просвітної" радіолокації за дальністю виявлення маловисотних цілей з врахуванням енергетичних показників сигналів базових станцій сотового зв'язку.

Комплекс бар'єрного виявлення формує слабонаправлене поле радіолокаційного виявлення в зеніті "на просвіт", а відеокамерою – додаткове оптико-електронне поле видимості з метою підвищення надійності виявлення цілі. При цьому в радіолокаційному каналі реалізується вищевказаний ефект максимізації ехо-сигналу в нижню напівсферу.

Гостро направлена антена опорного каналу орієнтована строго в напрямку базової станції сотового зв'язку. При цьому орієнтація слабоспрямованої антени повинно забезпечувати співпадання поляризації діаграми направленості з поляризацією діаграми спрямованості антени базової станції.

Інформація відеоспостереження з відеокамери разом з радіолокаційною інформацією, отриманою цільовим і просвітним каналами, поступає споживачу у вигляді відеозображення цілі.

Для оцінки граничних можливостей методу, що пропонується, шляхом трансформації основного рівняння "просвітної" радіолокації для малих висот польоту цілі показано:

– збільшення дальності бар'єрного виявлення може бути досягнуто тільки збільшенням коефіцієнту підсилення слабоспрямованості антени "просвітного" каналу, але це зменшує час спостереження цілі і, як наслідок, приводить до підвищення ймовірності її пропуску. Причому, наявність оптико-електронного каналу вночі і при метеорологічних осадках цю ймовірність не збільшує;

– одночасне отримання радіолокаційного і оптичного зображень цілі, що низько летить, полегшує її ідентифікацію для вогневого ураження;

– суцільна зона радіолокаційного прикриття об'єкту в границях міської інфраструктури може бути забезпечена раціональним розташуванням дешевих радіозасобів, які працюють тільки на прийом, чим досягається їх висока завадостійкість і скритність.

Розрахунковим шляхом показано, а експериментальним підтверджено, що при ефективній поверхні розсіювання повітряної цілі в передньому і боковому ракурсах спостереження 0,01 $м^2$ в нижньому ракурсі спостереження "на просвіт" вона складає (0,1-1)

м^2. Ця обставина дозволяє при коефіцієнті підсилення антени “просвітного каналу ”14 *дБ* для типової потужності випромінювання базової станції розташувати радіолокаційний комплекс бар’єрного виявлення на відстанях понад 1,3 км від базової станції і значно підвищити площу території, яка захищається від БпЛА, що низько летять, і крилатих ракет.

Висновки:

1. Запропонований і проаналізований ефективний і малозатратний метод виявлення маловисотних малорозмірних повітряних цілей в границях міської інфраструктури на основі використання існуючої сітки мобільного зв’язку.

2. Виконано аналіз досягаємих характеристик радіолокаційного виявлення маловисотних малорозмірних цілей, що низько летять, на основі запропонованого методу.

3. Запропонований науково-технічний підхід є альтернативою до існуючих методів виявлення маловисотних малорозмірних повітряних цілей стосовно цілефонової обстановки, яка супутня до протиповітряної оборони об’єктів міської інфраструктури.

Список використаних джерел

1. Демидюк Е.В., Фомин А.В. Патент RU261598C1. Способ и комплекс барьерного зенитного радиолокационного обнаружения малогабаритных летательных аппаратов на базе сетей сотовой святи – 2015.

2. Аверьянов В.Я. Разнесенные радиолокационные станции и системы – Минск: Наука и техника, 1978.

УДК 621.396

Зубков А.М., Онофрійчук А.Я., Петлюк І.В., Сірий Ю.І., Цицик М.В.

ПІДВИЩЕННЯ ДИНАМІКИ І БЕЗПЕКИ ІНЖЕНЕРНОЇ РОЗВІДКИ МІСЦЕВОСТІ МЕТОДОМ ЛОКАЦІЙНОГО ГЕОМОНІТОРИНГУ

Розроблено новий метод неконтактного пошуку замаскованих ґрунтом мін на основі локаційного зондування замінованої ділянки в міліметровому діапазоні спектру електромагнітних хвиль. Незалежність ефективності пошуку і точності місцевизначення від матеріалу формоутворюючої поверхні мін (метал, діелектрик або їх поєднання) досягається одночасним взаємноюстованим за напрямком прийманням ехо-сигналів в радіолокаційному і теплових сигналів в радіометричному каналах. Новизна і можливість технічної реалізації методу підтверджена патентами і результатами експериментальних досліджень.

Ефективність гуманітарного розмінування рішучим чином залежить від точності, динаміки і безпеки інженерної розвідки місцевості. Забезпечення сукупності вищеперерахованих вимог можливе тільки при безконтактному моніторингу замінованої території. Одночасно інструмент інженерної розвідки повинен забезпечувати:

– мінімальні габаритовагові показниками для доступу в любу точку замінованої території, включаючи будови і елементи їх архітектури, і допускати управління одним оператором;

– сканування взаємоюстовано за напрямком і взаємосинхронно за часом замінованої ділянки поверхні в міліметровому діапазоні (ММД) електромагнітних хвиль (ЕМХ) в режимах активної і пасивної (радіотеплової) локації для виключення впливу фізичних і геометричних властивостей формоутворюючої поверхні міни на ефективність їх пошуку і місцевизначення;

– гнучку зміну структури і параметрів зондуючого сигналу в режимі активної радіолокації для адаптації під геометричний розмір міни;

– адаптивну зміну параметрів радіо теплового каналу для узгодження з цілефоновою обстановкою.

В роботі [1] розглянуті фізичні передумови локаційного моніторингу, ефективність якого інваріантна до електродинамічних характеристик конструкції формоутворюючої поверхні міни:

– переважно відбиваючі ЕМХ, які мають в складі формоутворюючої конструкції в основному металеві компоненти;

– переважно поглинаючі ЕМХ, які мають в складі формоутворюючої конструкції в основному діелектричні компоненти.

Тоді при одночасному спостереженні в радіолокаційному і радіотепловому (радіометричному) каналах появляється можливість розглядати металеві і діелектричні об’єкти як “позитив” і “негатив”, відповідно.

В роботі [2] запропонована і обґрунтована структурна схема системи неконтактного виявлення і визначення місцезнаходження замаскованих в ґрунті мін. Забезпечення інваріантності системи до фізичних характеристик формоутворюючої поверхні мін досягається паралельним використанням радіолокаційного і радіометричного каналів.

В роботі [3] попередні дослідження в області радіолокаційного геомоніторингу для гуманітарного розмінування розповсюджені на любі геометричні і фізичні характеристики формоутворюючої поверхні міни і оточуючого ґрунту. Інструментом є структурно-параметрична адаптація каналів радіолокатора підземного зондування (РЛПЗ) під цілефонову обстановку на основі критерію максимуму правдоподібності [4].

Мета дослідження: підвищення достовірності виявлення мін з одночасним забезпеченням безпеки незалежно від фізико-хімічних властивостей маскуючого ґрунту і профілю місцевості.

Методика дослідження: порівняльний взаємосинхронний по часу аналіз ехо-сигналів в режимах активної радіолокації і сигналів в режимі радіометрії від замінованої ділянки поверхні для формування признаків виявлення і розпізнавання.

Сформульовані цілі досягаються:

– шляхом адаптивної перебудови параметрів міношукача під цілефонову обстановку;

– за рахунок адаптації часового контакту міношукача з міною (для досягнення максимуму енергетичного контрасту цілі).

Практична цінність підходу, що пропонується, визначається наступними обставинами:

– мінімальні масогабаритні показники міношукача що допускають його експлуатацію однією людиною;

– доступність до замінованої ділянки незалежно від її територіального розташування (відкрита місцевість, міські будови, ліс, кущі);

– простота експлуатації і простота навчання в зв’язку з можливістю чіткої фізичної інтерпретації принципу роботи;

– можливість розширення функцій шляхом установки міношукача на різних об’єктах в якості датчика.

Висновки:

1. Розроблені методологія застосування і апаратурна реалізація радіолокатора підповерхневого зондування для гуманітарного розмінування.

2. Розширення умов експлуатації для пошуку мін любої конструкції і мінімізація габаритовагових характеристик РЛПЗ дозволяє ефективно його застосовувати в фоноцільовій обстановці, що динамічно міняється, при управлінні одним оператором.

3. Технічна структура допускає практичну реалізацію на доступних для вітчизняного розробника елементній базі і матеріалах.

Список використаних джерел

1. Зубков А.Н. Самонаведение ракеты на наземную цель при знакопеременном целефоновом контрасте / А.Н. Зубков, В.А. Юнда, И.З. Залуцкая, А.П. Коленников // Військово-технічний збірник. – 2013 – № 2(9). – С. 31-35.

2. Зубков А.М., Красник Я.В., Мартиненко С.А., Цицик М.В. і ін. Патент на корисну модель № 144081 Спосіб неконтактного виявлення і визначення місцезнаходження замаскованих в ґрунті мін із системою для його реалізації / А. Зубков, Я. Красник, С. Мартиненко, М. Цицик і ін.; пріоритет 25.08.2020.

3. Зубков А.М. Аналіз ефективності інтеграції радіолокаційного і радіометричного каналів геомоніторингу в інтересах гуманітарного розмінування / А. Зубков, Я. Красник, В. Прокопенко, С. Каменцев, М. Цицик // Матеріали МНТК "Геофорум-2023". – С. 118-120.

4. Вопросы статистической теории радиолокации / П.А. Бакут и др.: под общ. ред. Г.П. Тартаковского. М.: Сов. радио. – т. 1 – 1963.

Івченко М.М., Глобін А.В., Карабань О.В., Цимбал І.В., Шугалій О.О.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВПРОВАДЖЕННЯ НОВІТНІХ ТЕХНОЛОГІЙ ПОБУДОВИ МЮОМЕТРИЧНОЇ БЕЗДРОТОВОЇ НАВІГАЦІЙНОЇ СИСТЕМИ

В епоху стрімкого розвитку інформаційних технологій, коли використання засобів радіоелектронної боротьби дозволяє блокувати діючі супутникові сигнали від радіонавігаційних систем, є також ряд факторів, поєднання яких впливає на точність визначення місцеположення об'єктів, а саме:

1. Вплив засобів РЕБ на радіонавігаційні системи. Радіопередавач відповідної потужності та частоти, розміщений поблизу захищеної цілі, заважає приймачам GPS отримувати правильні дані. Виробники супутників намагаються боротися з цим, розробляючи все більш стійкі до перешкод сигнали, якими оснащуються останні версії обладнання. Однак перевага на боці руйнівників. Вони можуть швидше адаптуватися та реагувати на зміни завдяки меншим витратам та більшим можливостям. Адже супутники не змінюються за тиждень.

2. Неоднорідність іоносферних і тропосферних шарів Земної атмосфери. Точність вимірів залежить від сталої швидкості поширення радіохвиль, яка через різноманіття неоднорідностей в атмосфері може змінюватися. Як наслідок, виникають іоносферні та тропосферні помилки у визначенні відстаней до супутників.

3. Багатопроменева природа поширення радіохвиль. Приймач СНС приймає не тільки прямі радіохвилі, а й відбиття від будь-яких об'єктів – земля, водна поверхня. Відбиті сигнали створюють додаткові перешкоди, які впливають точність виміру.

4. Помилки синхронізації. Для точного виміру затримки сигналу від супутника використовується синхронізація приймача із супутниковим сигналом.

5. Неточність розрахунку становища супутника у просторі, тобто ефемеридні помилки (помилки зміни орбіти).

6. Геометричний чинник. (GDOP – Geometrical delusion of precision). У момент, коли супутники, на які проводиться обсервація, знаходяться під кутами близькими до прямих, точка перетину кіл орбіт може бути обчислена з меншою похибкою, ніж у випадку, коли супутники знаходяться під гострими кутами.

7. Сонячна активність. Спалахи на сонці супроводжуються викидами гігантських мас сонячної речовини, що породжують різкі зміни властивостей магнітосфери й іоносфери Землі. Такі спалахи циклічні та під час їх появи помилки у позиціонуванні зростають.

8. Виборча точність позиціонування шляхом кодування сигналів, що передаються із супутника. Комерційний короткий код дозволяє отримати точність гірше, ніж довгий код для військових потреб.

Детально проаналізувавши вищезазначені фактори слід зауважити що використання системи GPS у збройних силах країн блоку НАТО виходить на другий план. Затухання і блокування супутникових сигналів стає все більш поширеним явищем, і як результат, точне озброєння, засноване лише на космічних даних, перестало бути таким же ефективним, як раніше. Проблема стосується не тільки самої зброї, а й літаків, кораблів, наземних транспортних засобів та будь-яких інших пристроїв, які оснащені GPS-приймачем.

Іншою стратегією, заснованою на камерах, є навігаційна система, яка використовує топологічне уявлення простору і ансамбль нейронних мереж для управління наприклад роботизованим комплексом у внутрішньому просторі (прикладами є NEURO-NAV13,14 і FUZZY-NAV15). Як приклад можливостей цих методів навігації на основі камер можна навести FINALE (оснащений високопродуктивною камерою в оптимальних умовах), щоб керувати роботизованим комплексом у русі із середньою швидкістю 17 м/хв, використовуючи звичайний алгоритм самопозиціювання на основі персонального комп'ютера, який обробляє зображення на основі даних камери. Однак помилки накопичуються в міру подовження часу сеансу навігації роботизованого комплексу, і для задовільної роботи необхідні повторні корекції за допомогою зовнішнього пристрою. Крім того, оскільки ці методи оцінюють місцеположення робота на основі спостереження за орієнтирами, встановленими в навколишньому середовищі, ці методи не можуть бути використані, коли орієнтири не спостерігаються, наприклад, в умовах низької освітленості або в середовищі, де навколишнє світло та перешкоди, що екранують, можуть поставити під загрозу здатність камер точно відображати зображення на основі даних камери.

Технології радіочастотної ідентифікації (RFID) і ZigBee дають змогу досягати точності позиціювання на відстані 10-30 м і 10-200 м відповідно з невеликою витратою заряду батареї. Однак RFID вимагає створення центру управління, що містить сервери, принтери, монітори та інші компоненти, а ZigBee вимагає великомасштабної мережі Wi-Fi з кількома вузлами. Мертвий розрахунок (DR) часто використовується як алгоритм позиціювання всередині приміщень, який дозволяє користувачам оцінити загальну відстань, пройдену від початкової точки. Його недолік полягає в тому, що помилки оцінки DR також накопичуються з плином часу, якщо для корекції не використовуються зовнішні опорні сигнали.

Проблематику існуючих методів позиціювання можливо успішно вирішити завдяки використання властивостей космічного випромінювання для навігації.

На противагу існуючим радіонавігаційним системам, для орієнтування в зонах, куди не можуть проникати сигнали глобальної навігаційної супутникової системи (GNSS),японськими вченими було розроблено перспективну технологію, яку назвали “мюометричною бездротовою навігаційною системою**” (**Muometric wireless navigation system (MuWNS)). Цей принцип дії оснований на відстеженні руху потоків мюонів з використанням відповідних детекторів, тобто частинок, що легко проникають крізь щільні матеріали, куди не може потрапити радіосигнал. Цей тип навігації може стати незамінним інструментом для орієнтації всередині заплутаних споруд, під землею, в глибині води і т.д.

Мюони формуються, коли космічні промені досягають земної атмосфери. Там вони зіштовхуються з різними частинками, що викликає каскади вторинних частинок – мюонів. Цей процес відбувається неперервно і з великою інтенсивністю, на кожен квадратний метр поверхні нашої планети припадає близько 10 000 мюонів. Мюони космічних променів однаково падають на Землю і завжди рухаються з постійною швидкістю, незалежно від того, яку матерію вони перетинають.

Вже існують детектори мюонів, які дозволяють через аналіз руху потоків частинок виявити приховані об’єкти. За допомогою цієї технології можна синхронізувати роботу пристроїв, розділених перешкодою, непрозорою для інших видів випромінювання. Так, наприклад, проведені дослідження щодо адаптації даної технології для визначення місцезнаходження людини з детектором всередині будівель.

Це проривне відкриття може не тільки революціонізувати сучасні системи навігації, але й відкрити нові можливості для дослідження складних об’єктів або пошуку осіб у складних умовах. Мюометрична навігація може стати важливим інструментом як для вдосконалення способів пошуку в роботі рятувальних команд у надзвичайних ситуаціях, таких як обвал будівлі так і при розробці роботизованих морських підводних безекіпажних апаратів різного цільового призначення тощо.

Ільницький І.Л., Рудковський О.М.

БЕЗПІЛОТНІ СИСТЕМИ ЯК НОВИЙ РІД СИЛ У ЗБРОЙНИХ СИЛ УКРАЇНИ

Повномасштабна війна дала поштовх до розвитку і застосування нових форм і способів ведення збройної боротьби, а саме створення та впровадження в тактику дій СВ наземних роботозованих комплексів. Це сприяло підвищенню ефективності застосування військ, трансформації, відкрило нові форми ведення бою. Крім того наземні роботезовані комплекси (НРК) відіграють важливу роль у збереженні життя, скорочення втрат серед військовослужбовців.

Провідні країни світу такі як США, Німеччина, Велика Британія, Японія, Китай - визначились щодо характеру ведення майбутних війн, збройні конфлікти - це війни роботів (роботизованих комплексів). Основним напрямком розвитку сучасних роботизованих систем є впровадження в них новітніх інноваційних технологій, зокрема штучного інтелекту. США сьогодні в авангарді розробок, щодо застосування НРК, про що свідчать нові програмні розробки, щодо стратегії роботизованих і автономних систем армії США (RAS) до 2035р. Ведучими фахівцями в цієї нової галузі проаналізовано стратегію армейських роботизованих і автономних систем. Операційна концепція армії США до 2040 року. Наземний роботизований комплекс - це безпілотна роботизована платформа,на якій встановлено пункти дистанціонного управління, мережа керування і контролю та інші елементи , що дають змогу автоматично виконувати певний перелік бойових завдань.

Наймасовішим американським військовим роботом є TALON було випущено (понад 3 тис. одиниць).TALON розроблений компанією Foster-Mille. Після военної компанії в Іраку (версія була застосована з кулеметом) в 2007 року фірма отримала замовлення на 80 машин. Найбільшим бойовим роботом на сьогодні є американський Biak Knight, розроблений компанією BAE Systems. Бойовий робот на гусеничному ходу озброєний 30 мм автоматичною гарматою М242 та спареним із нею 7,62-мм кулеметом., машина обладнана телекамерами, тепловізорами, РЛС, системою супутникової навігації, а управляється Biak Knight зі спеціальної командної машини. Американська компанія Textron Systems розробила чотири прототипи НРК RCV-L, в 2021 році отримала четвертий прототип середньої безпілотної бойової машини (RCV-M) Ripsaw M5 у 10-тонній версії, який пройшов польові випробування у 2023році. На озброєні автоматична гармата 30мм Mk.44 Bushmaster II, оснащена гранатаметом CROWS-J з протитанковими снарядами або ракетами «земля – повітря», а також обладнений інфочервоною камерою. Відомі американські військові роботи сімейства Pack Bot, були застосовані для розмінування, а також для роботи TAGSi Red Owl. У Ізраїлі, Великої Британії, Німеччини знайшли військове застосування, рухомі гусеничні роботи для розвідки, розмінування та знищення вибухових пристроїв різного типу. Армія США під час бойових дій і полі-

цейських операцій в Іраку з успіхом використовувала вогнепальну зброю на малогабаритних роботозованих комплексі, як в наступальних так і розвідувальних операціях. Загальна кількість військових роботів використаних армією США в Іраку досягла кількох тисяч одиниць.

В 2022 році пройшла випробування роботизована платформа для танків Type-X (Естонська компанія MilIren Robotics). Вона пройшла перші випробування на мобільність, продемонструвала стрільбу з платформи автоматичною гарматою Bushmaster калібр 30мм, частина алгоритмів в роботі використовує штучний інтелект, крім того платформа підтримує функцію Indirect Drive, з елементами передбачення , що дозволяє керувати діями машини на високих швидкостях. Тому вже є має попит на закупівлю в Скандинавських країнах в арміях: США, Німеччини, Франції, Австралії, Італії, Нідерландів, Норвегії, Іспанії , Великої Британії. Акціонерне товариство «Укроборонпром» підписали угоду з естонською компанією «MilIren Robotics», про створення роботизованих оборонних систем нового покоління. Були зроблені перші кроки у рамках угоди – налагодження стратегічного співробітництва з метою визначення потреб Сил оборони України. З часом будуть інтегровані у бойовий досвід наших військових фахівців до вже наявних в активів «MilIren Robotics»систем, та в по-дальшему створювати нові вироби. У вересні 2022 році Естонія поставила нашій країні 15 одиниць безпілотних гусеничних бронетранспортерів The MIS. Згодом«MilIren Robotics» та німецька оборонна компанія Kraus-Maffei Wegmann (KMW) підписали контрактна поставку в Україну 14 безпілотних наземних апаратів (UGV) The MIS.У червні 2023 році Німеччина передала сім гусеничних платформ The MIS для захисту від російської агресії.

З початку 2014 року автоматизація і роботизація стала одним з перспективних напрямків розвитку Збройних Сил України. Вітчизняні винахідники і науковці пройшли не простий шлях. Застосування наземних роботизованих комплексів дозволяє зберегти життя кожного українського бійця. Наземні роботизовані комплекси мають великій потенціал: від знищення противника із засідок й до евакуації поранених з зони обстрілу, доставки боєприпасів на позиції переднього краю. Це сприяло у визначенні пріоритетів їх розвитку, в центріалізованій закупівлі «Укроборонпромом», поступове забезпечення ними підрозділів ЗСУ, починаючи з нулевої позиції .

Розробники державних та приватних компаній в 2016 році представели декілька макетних зразків. Фахівці видання Defense Express визначили відому «п’ятірку» наземних роботозованих комплексів, де кожний НРК представлений на виставці мав унікальний зразок. Перший НРК «Мисливець» (РВСВК-М3») пройшов ряд випробувань на полігонах та бойових умовах.(КБ «Роботікс»). Другий зразок роботизовані платформи «Ласка-2»та «Скорпіон-2» «Інфоком Лтд» (м. Запоріжжя.) Третій зразок розробила Львівська приватна компанія GIobaI Dynamscs (нине Roboneers) на дистанційно керованій платформи є з гібридним приводом, компанія працює над створенням трьох бойових машин. Четвертий зразок тактичний багатофункціональний транспортний засіб «Фантом», виконаний як багатофункціональна платформа з колісною формулою 6х6 для розвідки, спостереження, вогневої підтримки, апарат озброєний 12,7мм кулеметом, запас ходу до 20 км, корисне навантаження -350 кг. А також «Фонтом-2»з колісною формулою 8х8. П’ятим зразком був Бойовий дистанційний комплекс «Піранья» на гусеничній платформі, розроблено київським ПАТ («Кузня на Рибальському»), проект був не вдалим,тому був заморожений.

Досвід створення, експлуатації та застосування НРК у США, та провідних країн світу, показує ,що розроблення окремих відповідних зразків не є досить складним, але їх комплексне виробництво з відповідною бойовою, економічною та технологічною ефективностью для України є проблематичною. Управління веденням бойових дій НРК повинно здійснюватися з використанням автоматизованої системи управління. Система зв’язку та управління НРК має включати інтегровані засоби зв’язку та автоматизацію управління, в тому числі і програмні засоби, які забезпечать їх взаємодію . Тому спи-

раючись на досвід провідних країн світу, досвід в зоні бойових дій можна визначити як основні напрямки щодо виробництва та подальшого застосування НРК в ЗС України. Основою військово-технічної політики повинна стати реалізація курсу на високий технологічний рівень озброєння Збройних Сил . Подальше військове-технічне співробітництво з країнами НАТО, що дозволить створити в Україні виробництво вітчизняних високотехнологічних систем озброєння.

Цей рік повинен стати вирішальним у багатьох аспектах, І очевидно,- на полі бою дрони- безпілотні системи - довели свою ефективність у боях як на суходолі ,так і на морі. Завдяки дронам Україна реально змінила безпекову ситуацію в Чорному морі.

Завдання і для армії, і для Міністерства оборони та уряду загалом. І щоб дати необхідну координацію в Силах оборони, забезпечити належний рівень планування та якість логістики, у структурі Збройних Сил будуть створені Сили безпілотних систем .

Президент України Володимир Зеленський розпорядився створити у Збройних Силах окремий рід сил, який займатиметься дронами. З метою нарощування спроможностей Збройних Сил України щодо використання безпілотних та роботозованих повітряних, морських та наземних систем, забезпечення готовності до застосування таких систем за призначенням постановою Кабінетом міністрів із залученням Генерального штабу Збройних сил прийнято рішення про створення у структури Збройних Сил України Сил безпілотних систем, як окремого роду сил та за результатами опрацювати внести відповідні пропозиції на розгляд Ради національної безпеки і оборони України.

Сьогодні вітчизняні винахідники формують нову реальність на полі бою, у пошуках місця в строю для роботизованих наземних платформ, яскравим прикладом є підсилення підрозділу наземною роботизованою платформую «Рись», яка пройшла випробування в бойових умовах,з бойовим модулем, з кулеметом ПКТ. Як недолік не було передбачено рухової теплової камери, а також виникло питання, щодо покращення прохідності та маневру на базі гусеничної або колісної системи. У військах нарощується та удосконалюється, збільшення дальності управління такої зброї. Імплементація стандартів НАТО це можливість зробити прорив у військово-технічному співробітництві, саме запровадження стандартів НАТО з огляду на їхню ефективність і перспективи використання в майбутньому в архітектурі світової та європейської систем безпеки, цей напрямок стане складовою частиною оборони у ході російсько-української війни .

Іохов О.Ю., Манько А.В.

АДАПТАЦІЇ СИСТЕМИ РАДІОЗВ'ЯЗКУ МОБІЛЬНОЇ КОМПОНЕНТИ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ ДО УМОВ ВПЛИВУ НАВМИСНИХ ЗАВАД ПРИ ВИКОНАННІ ЗАВДАНЬ ІЗ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ

Адаптація систем радіозв'язку до умов впливу навмисних завад - це важлива задача, оскільки радіочастотний спектр може бути підданий різноманітним перешкодам, таким як електромагнітні перешкоди, інтерференція, шум, блокування сигналу та інші. Враховуючи досвід ведення бойових дій при відсічи збройної агресії з боку російської федерації можна впевнено стверджувати, що сучасні системи радіозв'язку військового призначення не завжди, а деколи взагалі неспроможна протистояти навмисним завадам засобів РЕБ російської федерації.

Ось деякі стратегії:

– Частотне планування: Використання алгоритмів частотного планування, щоб уникнути частот, які піддані інтерференції або зайняті іншими системами.

– Техніки модуляції і кодування: Використання ефективних технік модуляції та кодування, які забезпечують більшу стійкість до шуму та інтерференції.

– Адаптивні антени: Використання адаптивних антен, які можуть автоматично адаптувати напрямок та властивості сигналу для зменшення впливу навмисних завад.

– Фільтрація сигналів: Використання фільтрів та схем підсилення для підвищення відношення сигнал-шум і відфільтрування небажаних сигналів.

– Часове розмежування (Time Division Multiplexing - TDM): Розподіл доступу до каналу в часі, щоб уникнути конфліктів та інтерференції між різними користувачами.

– Криптографічне захист: Використання шифрування та інших криптографічних методів для захисту передачі даних від незаконного доступу та перехоплення.

– Системи забезпечення стійкості до перешкод: Використання спеціальних алгоритмів та апаратних засобів для виявлення та компенсації навмисних завад.

Ці стратегії можуть застосовуватися окремо або в поєднанні, в залежності від конкретних умов експлуатації та вимог до системи радіозв'язку.

Враховуючи той факт, що в умовах військового стану, браком фінансування, а саме головне використання в секторі безпеки та оборони закордонного парку радіозасобів унеможливлює використання згаданих стратегій адаптації систем радіозв'язку до навмисних завад.

Найбільш прийнятним на даний час є використання механізмів адаптивних антен у поєднанні з методами їх просторово розташування.

Це вимагає від науковців вирішення наукового завдання яке полягає у забезпеченні завадозахищеності засобів радіообміну в умовах зміни завадової обстановки та дії радіотехнічної розвідки при виконанні завдань із забезпечення державної безпеки, за рахунок використання спеціалізованих спрямованих антен як елементів захисту радіозасобів, оптимізації їх параметрів і просторового розміщення.

Вирішення поставленогшо наукового завдання можливо за рахунок удосконалення методу адаптації системи радіозв’язку мобільної компоненти тактичної ланки управління в умовах впливу навмисних завад, який на відміну від відомих враховує орієнтацію спрямованих антен засобів радіообміну, просторове розташування постановників завад та особливості середовища розповсюдження радіохвиль та дозволяє розрахувати коефіцієнт придушення та адаптувати орієнтації імпровізованих (нестандартних) антен та ФАР системи радіозв’язку до умов зміни завадової обстановки.

Метод адаптації системи радіозв’язку мобільної компоненти тактичної ланки ґрунтується на оптимізації параметрів засобів антен та дозволяє визначити реальні зони розміщення засобів активного радіомаскування з урахуванням параметрів засобів радіообміну, особливостей оперативного розташування радіозасобів, характеристик наявних антенних пристроїв постановників завад маскування, а також максимізувати кількість подавлених точок розміщення або траєкторії пересування засобу радіоелектронної розвідки противника.

UDC 355.551

Iokhov O., Liwång H., Krahn U.

PROSPECTS OF USING STEEL BEASTS SIMULATION SYSTEMS IN THE TRAINING OF TACTICAL LEVEL OFFICERS AT THE NATIONAL ACADEMY OF THE NATIONAL GUARD OF UKRAINE

The experience of using simulation modeling systems to conduct command and staff exercises at the operational level allows us to confidently declare that the training of officers of the management staff, headquarters and units has been improved several times with minimal expenditure of human and material resources. This testifies to the importance of the implementation of simulation modeling systems not only in the training of units and parts of

the National Guard of Ukraine, but also in the training of applicants for higher education at the National Academies of the National Guard of Ukraine.

Today there are many simulation systems: MILES, STEEL BEASTS, SPECTRUM, JCATS and others. Steel Beasts, presented by Swedish partners in 2023, deserves special attention among the mentioned programs. Steel Beasts is a computer military simulation game that simulates combat operations using armored vehicles. The game was developed for PC and has realistic models of tanks, armored personnel carriers and other combat vehicles. It is used for military training, as well as an entertainment product for fans of military simulations. This is a virtual simulation of modern armored and mechanized combat with the use of combined arms and a focus on the tactics of small units, which corresponds to the educational and professional training programs of officers of the tactical branch of the National Academies of the National Guard of Ukraine.

With its ability to engage NATO-standard military maps, the ability to perform post-simulation analysis makes it suitable for constructive simulation training up to brigade level.

There are two versions of Steel Beasts Professional: a personal version (SB Pro PE) and a class version (SB Pro). As the name suggests, SB Pro PE is intended for personal use and has some limitations on the number of players and functionality. At the moment, our partners from Sweden provide free access to the personal version (SB Pro PE), which provides an opportunity to quickly introduce these programs into the educational process.

Implementation of Steel Beasts Professional will allow:

1. To conduct command and staff exercises with the use of combat simulation simulations with the military command and control units of the National Guard of Ukraine.

2. Conduct command and staff exercises and practical training activities using simulation tools:

– with students of the academy of various types of training in various specialties (specializations);

– students of advanced training and professional level courses;

– students of departments of military training.

3. Increase the effectiveness of student training by practicing the practical skills of commanding troops in the conditions of a constantly strengthening environment.

Thus, the introduction of Steel Beasts Professional into the educational process of the National Academies of the National Guard of Ukraine is a priority task of the simulation center of the Academy.

Iokhov O., Stratiychuk I.

APPLICATION OF RADIO CONTROLLED AMMUNITION DESTRUCTION MEANS ON VEHICLES AND ARMORED VEHICLES DURING THE PERFORMANCE OF STATE SECURITY TASKS

The experience of conducting combat operations in repelling armed aggression by the Russian Federation has shown that protection against radio-guided munitions (RCBMs) is a difficult task, since these munitions can be used to attack and inflict damage in various areas, including military targets and personnel, which is involved in the performance of tasks to ensure state security.

Here are some possible ways to protect against radio-guided munitions:

Signal Encryption: The use of cryptographic techniques to protect against unauthorized access and interception of signals controlling radio-guided munitions.

Frequency Planning: planning and managing frequencies to avoid interference and conflicts between different radio control systems.

Active Protection: The use of electronic devices that can interfere with, intercept, or block radio control signals.

Detectors and blocking systems: the use of systems for detecting and blocking radio-controlled signals that can activate munitions.

Signal Filtering and Verification: Use of specialized filters and software to verify the legitimacy and integrity of signals entering radio-guided munitions.

Physical protection: The application of physical barriers and defenses that impede access to radio-guided munitions, such as shielding against electromagnetic interference or mechanical safeguards.

Intelligence and deterrence development: active intelligence and analysis of potential threats, as well as development of warning and response capabilities for radio-guided munitions.

These measures can be used alone or in combination to protect against radio-guided munitions in various scenarios and operating conditions.

In turn, the destruction of radio-controlled munitions is a complex and dangerous process, as it requires specialized equipment and skills, and can also lead to explosions and other dangerous situations. Here are some methods that can be used to destroy radio-guided munitions:

Controlled Detonation: Under the most controlled conditions, munitions can be destroyed by controlled detonation. This may involve the use of explosive charges or destructive devices to safely defuse the munition.

Manual destruction: In some cases where it is not possible to use explosive devices, specially trained crews can independently remove and destroy radio-controlled munitions.

Robotic systems: The use of special robotic systems with manipulators to destroy radio-controlled munitions that provide remote control and reduce the risk to all personnel involved in the performance of national security tasks.

Controlled burning or destruction: Application of special installations for controlled burning or destruction of radio-controlled munitions.

Electronics Deactivation: The use of special devices to deactivate the electronics and radio frequency devices in radio-controlled munitions to prevent them from being remotely controlled.

In any case, the safe destruction of radio-guided munitions requires great attention to detail, experienced personnel, and the use of specialized equipment to ensure the safety of all personnel involved in national security missions.

Taking into account the experience of conducting hostilities in repelling armed aggression by the Russian Federation, it can be confidently asserted that at this stage the most dangerous and widespread are radio-controlled munitions that are used against cars and armored vehicles during the performance of tasks to ensure state security. The most acceptable at present is the use of special radio means of neutralizing radio-controlled munitions installed on cars and armored vehicles when performing tasks to ensure state security.

This requires scientists to solve the scientific task, which consists in the development of a scientific and methodological apparatus for determining the procedure for the use of radio-controlled munitions disposal means on cars and armored vehicles of the security and defense sector of Ukraine, as well as typical algorithms for the use of radio-controlled munitions disposal means on cars and armored vehicles.

The solution of the scientific task is possible due to the creation of a methodology for the application of radio-controlled munitions disposal systems on armored vehicles, which, unlike the known ones, uses the properties of digital antenna arrays to generate a zone of damage around the device and allows creating a continuous layer of destruction of radio-controlled munitions.

УДК 372.862

Казіміров О.О.

АНАЛІЗ ЗАСТОСУВАННЯ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ ЗБРОЙНИМИ СИЛАМИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ У ХОДІ ЗБРОЙНОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

У сучасних війнах далеко не все вирішує суто військова міць в її традиційному сенсі. Щоб обеззброїти противника, достатньо порушити роботу його радіоелектронних засобів, «засліпити» і «оглушити» його, зробивши безпорадним на сучасному високотехнологічному полі бою. На сьогодні, коли в світі повсюдно присутні цифрові технології, роль засобів радіоелектронної боротьби (РЕБ) у збройному конфлікті важко переоцінити, а динаміка їх розвитку – одна з найбільших з усіх сучасних видів озброєнь.

Під час воєнної реформи збройних сил Російської Федерації (РФ) впродовж останніх десяти років значна увага приділялася саме системам РЕБ. Їх розвиток відбувався за двома основними напрямами. Перший напрям – це зведення наявних систем РЕБ в окремі з'єднання, частини та підрозділи та введення них до складу військових округів, загальновійськових армій та дивізій (бригад). Другий напрям – технічне переоснащення з'єднань, частин та підрозділів РЕБ більш сучасними засобами та системами. Експерти американського дослідницького центру RAND зазначають, що щороку Росія витрачає близько 450 млн. доларів на переозброєння військ РЕБ.

Із самого початку повномасштабної війни проти України РФ активно застосовує різні зразки засобів радіоелектронної боротьби, що створює певні проблеми нашим захисникам, та вимагає пошуку засобів симетричної або ж асиметричної протидії. Але перш ніж шукати такі засоби, потрібно розібратись в реальних можливостях засобів РЕБ, що стоять на озброєнні армії РФ, і заодно простежити еволюцію їх розвитку, а також проаналізувати як російські окупанти використовують свої засоби радіоелектронної боротьби у війні проти України.

Майже усі зразки сучасних систем РЕБ Росія випробувала ще під час вторгнення на Сході України навесні 2014 року. Американські експерти стверджують, що саме активна фаза боїв на Донбасі стала головним для Росії тестовим майданчиком для перевірки нових систем РЕБ.

Майже кожні два-три тижні новітні російські системи РЕБ потрапляють у матеріали звітів Спеціальної моніторингової місії ОБСЄ. За даними міжнародної волонтерської спільноти InformNapalm, яка проводить розслідування щодо наявності російської військової техніки на сході України, на даний час ідентифіковано декілька зразків сучасних засобів РЕБ, які використовуються збройними силами РФ в бойових діях на території України. Серед таких засобів є: комплекси РЕБ «Леер-3», «Борисоглебск-2», «Житель», «Торн», «Р-934Б», "Красуха-2", "Красуха-4", "Ртуть-БМ" , «Шиповник-Аэро».

Комплекс аеродинамічно закидуємих передавачів перешкод РБ-341В "Леер-3" призначений для виявлення, ідентифікації, визначення місцеположення та скритого радіоелектронного подавлення (РЕП) абонентських терміналів в мережах стільникового зв'язку стандартів GSM 900, GSM-1800 на основі імітування роботи базової станції.

Комплекс РЕБ "Борисоглебск-2" призначений для РЕП систем рухомого короткохвильового (КХ)та ультракороткохвильового (УКХ) радіозв'язку. Він здатний виявляти, визначати місця розташування та здійснювати РЕП радіомереж і ліній радіозв'язку тактичної ланки управління

Автоматизована станція перешкод Р-330Ж "Житель" призначена для: виявлення, пеленгування та радіоелектронного подавлення переносних мобільних станцій, систем пересувного супутникового зв'язку "Inmarsat" та "Iridium"; виявлення, пеленгування і

РЕП базових станцій систем стільникового зв’язку стандартів GSM 1900; РЕП приймачів користувачів систем супутникової навігації NAVSTAR (GPS).

Автоматизований мобільний комплекс радіорозвідки “Торн-МДМ” призначений для пошуку, аналізу та реєстрації сигналів у КХ та УКХ діапазонах, а також пеленгування та визначення місцеположення джерел радіовипромінювання, які знаходяться на відстані до 70 км.

Автоматизована станція перешкод Р-934Б призначена для РЕП засобів зв’язку авіаційних наземних та повітряних цілей, а також наземних радіоліній, які працюють на фіксованих частотах або у режимі псевдовипадкового переналаштування робочої частоти (ППРЧ).

Станція РЕП 1Л269 “Красуха-2” може застосовуватися у складі окремих батальйонів РЕБ для прикриття об'єктів від авіаційних радіолокаційних станцій (РЛС) типу “AWACS”.

Для прикриття стаціонарних об’єктів від бортових радіолокаційних станцій (БРЛС) радіолокаційної розвідки літаків Е- 8С “Джистарс”, багатофункціональних БРЛС літаків ударної авіації, розвідувальних і розвідувально-ударних БпЛА “Глобал Хок” і “Предатор”, БРЛС штучних супутників землі “Лакросс” може використовуватися широкодіапазонна станція потужних шумових перешкод 1РЛ257 “Красуха-4”.

Станція перешкод радіопередавачам артилерійських боєприпасів 1Л29 СПР-2 “Ртуть-Б”/1Л262 СПР-2М “Ртуть-БМ” призначена для захисту особового складу та бойової техніки від вогню артилерійських боєприпасів масового застосування, що оснащені радіопідривачами. Цю задачу станція виконує шляхом створення перешкод для підриву на безпечній висоті або їх блокування.

Комплекс РЕБ з БпЛА “Шиповник-Аеро” призначений для радіоподавлення (блокування) каналів управління БпЛА.

Автоматизований комплекс РЕП КХ ліній радіозв'язку ГТ-01 “Мурманск-БН” призначений для виявлення, пеленгування і створення перешкод лініям КХ радіозв'язку в оперативно-стратегічних і оперативно-тактичних ланках управління противника.

Одночасно з технічним удосконаленням своїх засобів РЕБ Росія удосконалює і способи їх застосування. Окрім придушення каналів радіозв’язку засоби РЕБ активно застосовуються збройними силами РФ для боротьби з БПЛА та для створення фальшцілей засобам ППО ЗСУ.

Таким чином, Росія має потужні засоби РЕБ, розташовані по всій лінії бойового зіткнення. Їх застосування є ключовим фактором, що ускладнює контрнаступ Збройних Сил України. Тому, вогневе ураження систем та комплексів радіоелектронної боротьби збройних сил Російської Федерації являється важливим завданням.

УДК 681.3:681.5

Калачова В.В., Місюра О.М., Карманний Є.В., Павлій В.О., Закіров З.З., Ткачик В.Д., Шигімага Н.В.

ОСНОВНІ ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВНІ НАПРЯМКИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ВІЙСЬКОВОЇ ОСВІТИ В УКРАЇНІ В УМОВАХ ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ТА ПІСЛЯ ПЕРЕМОГИ

Минуло два роки від початку повномасштабного вторгнення російсько-фашистських окупаційних військ на територію України і десять років російсько-української війни. Масштаби, скоєних рф за цей період воєнних злочинів, нечувані: сума прямих збитків, нанесених інфраструктурі України в ході тільки двох років повномасштабної війни,

станом на січень 2024 року, сягнула близька 155 млрд. доларів, а непрямих – в п’ять разів більше [1]! На кінець лютого 2024 року внаслідок війни в Україні повністю зруйновані майже 400 закладів освіти, а понад 3,5 тисячі - зазнали тих чи інших пошкоджень. Світовий банк оцінює вартість відновлення освітньої інфраструктури України у близька 14 мільярдів доларів. Водночас, частина пошкоджених закладів відновленню не підлягає [2]. Лише станом на 1 серпня 2022 року, згідно з інформацією Міністерства освіти і науки (МОН) України, в результаті повномасштабного вторгнення рф на територію України серед повністю зруйнованих закладів освіти України було вже 7 закладів вищої освіти (ЗВО). Чисельна більшою була кількість пошкоджених ЗВО та закладів післядипломної педагогічної освіти. Ця кількість сягала 49. Найбільше пошкоджень зазнали на той момент ЗВО в Харківській (21) і Донецькій (6) областях (разом 58,7 % загальної кількості пошкоджених ЗВО). Найбільших обсягів руйнувань і пошкоджень своїх об’єктів нерухомості зазнали Харківський національний університет ім. В. Каразіна, Національний університет «Чернігівська політехніка», Державний податковий університет (м. Ірпінь), Харківський національний педагогічний університет ім. Г. Сковороди, Маріупольський державний університет, Приазовський технічний університет (м. Маріуполь), Луганський національний університет ім. Т. Шевченка (новозбудований корпус у м. Рубіжному Луганської області), Національний аерокосмічний університет ім. М. Жуковського «Харківський авіаційний інститут» та інші [3]. Аналогічних інфраструктурних руйнувань зазнали і вищі військові навчальні заклади (ВВНЗ) України, які після стабілізації обстановки були передислоковані в пункти тимчасової дислокації та відновили навчальний процес.

Руйнування освітньої інфраструктури порушує доступ дітей і молоді до освіти, що впливає на якість їх навчання, соціалізацію й інтегрованість у суспільство. На допомогу в рішенні проблеми налагодження в умовах війни освітнього процесу в навчальних закладах країни, приходять найсучасніші інформаційні технології, які мають великий потенціал щодо можливостей організації навчання в нестандартних умовах і на відстані (що було доведено в 2020-2021 роках під час пандемії короновірусної інфекції COVID-19) та забезпечують, при порівняно незначних витратах, високий рівень надання освітніх послуг в звичайному, змішаному та дистанційному форматах, роблячи при цьому процес отримання знань максимально сучасним, наочним, інтерактивним, цікавим і, головне, безпечним для життя здобувачів освіти, викладачів та тих, хто його забезпечує. Тому, задача дослідження основних тенденції та перспективних напрямків застосування інформаційних технологій (ІТ) для підготовки здобувачів вищої військової освіти в Україні в умовах дії правового режиму воєнного стану та після ПЕРЕМОГИ є як ніколи актуальною.

Після повномасштабного вторгнення рф, МОН України звернулося до відомих світових корпорацій і компаній у сфері цифрової індустрії, по допомогу в організації відновлення освітнього процесу в навчальних закладах країни в умовах дії воєнного стану. Результатами цих перемовин стало: надання корпораціями Google і Microsoft доступу до своїх освітніх програмних пакетів та супроводження процесів забезпечення освітян України додатковими пристроями для навчання; безкоштовний доступ до продуктів компанії ZOOM; досягнення домовленості з лідерами ринку онлайн-навчання – платформами Coursera, Udemy та edX про надання безкоштовного доступу до курсів українським студентам; здійснення запуску е-документів про освіту в мобільному застосунку «Дія» задля забезпечення рівних можливостей доступу до освіти та працевлаштування всіх громадян України за підтримки проєкту EU4DigitalUA (Академія електронного урядування (e-Governance Academy)); безкоштовне надання виробниками комп’ютерного обладнання - компаніями HP, Microsoft, Phineo своїх пристроїв навчальним закладам України; підписання згоди з Vodafone, Lifecell та Київстар про надання безлімітного, нетарифікованого доступу до сервісів ДН і таке інше [3].

Великий потенціал щодо активного застосування при підготовці здобувачів освіти в ВВНЗ України мають як вітчизняні, так і закордонні ІТ для сфери освіти (сервіси, платформи, програмні додатки) [4]:

1) програмні додатки для проведення відеоконференцій і вебінарів - Microsoft Teams, ZOOM, Google Meet, BigBlueButton: платформа BigBlueButton активно використовується для організації вебінарів по вивченню дисциплін за дистанційною формою навчання та відеоконференцій Національним університетом оборони (НУО) України ім. І. Черняховського та Харківським національним університетом Повітряних Сил ім. І. Кожедуба (ХНУПС)); додатком ZOOM, в цих же цілях, активно користуються ДНУ «Інститут модернізації змісту освіти» та Національна академія сухопутних військ (НАСВ) ім. гетьмана П. Сагайдачного; потужні можливості програмного продукту Google Meet з 2020 року використовує Харківський національний університет радіоелектроніки (ХНУРЕ) для прийняття в дистанційному режимі іспитів, проведення лабораторних і практичних робіт на відстані, захисту курсових і кваліфікаційних робіт бакалаврів та магістрів;

2) системи управління навчанням (LMS) (Moodle, Google Workspace for Education/Google Suite for Education, Microsoft Office 365 Education від відомих світових виробників програмного забезпечення для комп'ютерного і дистанційного навчання та розроблені фахівцями ВВНЗ/ЗВО України, власні унікальні LMS-системи, які, враховуючи всі нюанси і особливості організації навчального процесу саме у власному навчальному закладі, роблять свій програмний продукт максимально зручним, для його користувачів (наприклад, LMS-системи «СІМ» та «Веб-клас ХПІ», створені в Національному технічному університеті «ХПІ»; LMS-система «ДІАЛОГ» та «КАСКАД» (ХНУПС). Найбільшим попитом в ВВНЗ та ЗВО України користується LMS Moodle, яка має вбудовану систему тестування з автоматизованою миттєвою перевіркою, можливостями аналізу і виправленням своїх помилок здобувачами освіти, оцінюванням та видачою коментарів до оцінки з кожного питання;

3) розроблений фахівцями ХНУРЕ навчальний відео-контент, заснований на застосуванні сучасних технологій відео з ефектом присутності дозволяє користувачеві під час лабораторних робіт з технічних дисциплін, що проводяться в дистанційному форматі, і де при звичайному очному навчанні потрібне використання складного апаратного забезпечення, відчувати максимально можливий рівень наочності та реалістичності процесів при роботі на складному обладнанні з макро- та мікро- оглядом, демонстрацією роботи різних приладів окремо один від одного та всіх разом. Панорамне відео, яке лежить в основі цього контенту, надає можливість тому, хто здійснює ДН, працювати не в полі зору оператора, який знімає навчальний чи комп'ютерний клас, навчальну аудиторію чи лабораторію, а у власному полі. Контент, що базується на ви-користанні сучасних технологій відео з ефектом присутності, є об'єднанням новітніх технологій та пояснень крейдою на класній навчальній дошці. Під час такого заняття досягається справжній ефект присутності в аудиторії, де є викладач, що демонструє і пояснює принципи роботи апаратури, та студенти за своїми робочими місцями у віртуальному просторі. Розробка цього відео-контенту, дозволила ХНУРЕ потрапити до світового рейтингу ЗВО – Times Higher Education University Impact Rankings;

4) Шолом (VR-окуляри) віртуальної/доповненої реальності, що дозволяє не просто переглядати зображення (відео), а й поринути в події за допомогою 3D – зображення. Процес отримання нових знань змінюється від простого «вивчення» теми до її «переживання наживо». Поєднання ж віртуальних окулярів з відповідним технічним обладнанням із застосуванням додаткового ПЗ, дозволяють створювати цілі навчально-тренажерні комплекси, які успішно застосовуються різними навчальними закладами при відпрацюванні практичних навичок роботи зі складними технічними пристроями, і, навіть, з військовою зброєю та технікою, наприклад, в НАНГУ відточують навички стрільби з протитанкових та зенітно-ракетних комплексів на спеціальних тренажерах,

складовою яких є віртуальні окуляри і створених на базі різних типів ПТРК та ПЗРК і моделюючих реальні бойові умови;

5) імітаційні моделі об'єктів і процесів (3-D моделі, flesh-анімація, навчально-пізнавальні анімаційні ролики, навчальні інтерактивні комп'ютерні ігри тощо) дозволяють візуалізувати складні та динамічні об'єкти та процеси навчального матеріалу, що вивчається та зробити електронний навчальний контент будь-якого навчального курсу, максимально наочним та зрозумілим здобувачеві освіти, незалежно від ступеню складності матеріалу, що потребує засвоєння та підвищити його інтерес до знань (інтерактивне освітнє програмне забезпечення mozaBook, математичні програмні додатки GeoGebra, засіб для створення інтерактивного навчального контенту H5P, додаток створення інтерактивних анімаційних відео та презентацій Genially-Powtoon);

Таким чином, на сьогоднішній день на ринку IT-продуктів існує велика кількість додатків, платформ, сервісів, які дозволяють в умовах дії воєнного стану зробити освітній процес максимально сучасним, наукоємним, насиченим на емоції, що сприяє підвищенню вмотивованості здобувачів освіти до отримання нових знань і веде до високих показників якості освіти, як зараз, так і в після нашої неминучої ПЕРЕМОГИ!

Список використаних джерел

1. Прямі збитки від зруйнованої внаслідок війни інфраструктури АПК оцінюють у $8.7 млрд. URL: https://agrotimes.ua/agromarket/pryami-zbytky-vid-zrujnovanoyi-vnaslidok-vijny-infrastruktury-apk-oczinyuyut-u-8-7-mlrd/. (дата звернення: 28.02.2024).

2. Кожна сьома школа в Україні пошкоджена через війну – МОН. URL: https://life.pravda.com.ua/society/v-ukrajini-cherez-viynu-poshkodzheni-ponad-3-5-tisyachi-zakladiv-osviti-300221/. (дата звернення: 28.02.2024).

3. Шкарлет С., Вітренко А., Рогова В., Костюченко О., Даниленко С. та інші Освіта України в умовах воєнного стану. Інформаційно-аналітичний збірник. Київ: МОН України, Інститут освітньої аналітики, 2022. 358 с.

4. Kalachova V., Misiura O., Shcherbinin S., Sizon D., Pylypenko V.,. Karmannyi Y, Khvorost O., Kiriienko I., Honchar R., Niziienko B., Tretiak V., Dudenko S., Kolomiitsev O., Zakirov Z. Analysis of role of information technologies in the organization of the educational process in Higher Educational Institutions of Ukraine in the conditions of martial law. Scientific Collection «InterConf+». 2023. № 35(163). P. 306-326.

УДК 004.056

Калмиков Д. І., Данилов А.Д.

MICROSOFT DEFENDER ЯК ЗАСІБ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

Робота присвячена аналізу використання Microsoft Defender в якості засобу для захисту кінцевих точок від сучасних кібератак. В тезах проаналізовані переваги використання Defender ATP.

В сучасному цифровому світі загрози кібербезпеці стають все більш складними та розповсюдженими. Кіберзлочинці використовують новітні технології для виявлення можливих точок входу. Безперечно, бізнес починає все більше замислюватися над якістю власної кібербезпеки та які передові технології допоможуть захищатися від кібератак. Коли мова йде про захист кінцевих точок, одразу приходить на думку використовувати XDR&EDR рішення, але маючи велике різноманіття поставщиків, виникає питання: «А кого обирати?».

Defender ATP - провідне рішення від Microsoft. Microsoft Defender for Endpoints – це платформа безпеки кінцевих точок, яка допомагає організаціям захистити свою цифрову власність за допомогою провідного механізму виявлення і реагування на основі штучного інтелекту. За статистикою від Microsoft за день Defender повідомляє про загрози понад 65 трильйонів разів [1]. В 2023 Microsoft Defender отримав нагороду «Leaders» від Gartner Magic Quadrant в номінації «Endpoint Protection Platform», що ще раз показує якість продукту.

Це секрет, що численна більшість організацій мають інфраструктуру на базі Windows, будь то on-premises, cloud чи hybrid це не так важливо. Головне те, що Microsoft надали Defender можливість нативної інтеграції зі всіма своїми рішеннями де б вони не були розгорнуті. Зручна консоль керування, перегляду аналітики – також є величезним плюсом використання Defender. До речі, MacOS та Linux також можна покрити агентами Defender і мати чітке розуміння про захищеність систем.

Використовуючи Microsoft Defender, ви отримуєте[2]:

– Core Defender Vulnerability Management, який використовує сучасний підхід, заснований на оцінці ризиків, для виявлення, оцінки, встановлення пріоритетів і виправлення вразливостей кінцевих точок і неправильних конфігурацій;

– Attack Surface Reduction забезпечує першу лінію захисту в стеку. Забезпечуючи належне налаштування параметрів конфігурації та застосування методів запобігання експлойтам, можливості протистоять атакам і експлуатації;

– захист нового покоління призначений для виявлення всіх типів нових загроз;

– EDR виявляює, досліджує і реагує на розширені загрози, які могли подолати перші два стовпи безпеки. Розширений пошук надає інструмент пошуку загроз на основі запитів, який дозволяє завчасно знаходити порушення та створювати спеціальні виявлення.

– автоматизоване розслідування та виправлення допомагають зменшити кількість сповіщень за лічені хвилини;

– Microsoft Secure Score for Devices допомагає динамічно оцінювати стан безпеки вашої корпоративної мережі, виявляти незахищені системи та виконувати рекомендовані дії для підвищення загальної безпеки вашої організації;

– Microsoft Threat Experts забезпечує проактивний пошук, визначення пріоритетів, а також додатковий контекст і аналітику, які ще більше допомагають центрам безпеки (SOC) швидко й точно виявляти загрози та реагувати на них.

Будь-які рішення мають свої недоліки, Microsoft Defender не виняток:

– хоча й заявлено, що існує інтеграція з MacOS та Linux, але функціонал не такий широкий. Наприклад, такі функції як Device Control, Network Protection, Attack Surface Reduction мають певні обмеження через специфіку операційних систем;

– обмежений функціонал безкоштовної версії. Безкоштовна версія не здатна задовольнити потреби централізованого управління, EDR та аналізу поведінки. Вона не надає функціонал для централізованого керування, налаштовування політики та інші речі.

Працюючи в компанії, яка надає послуги з кібербезпеки, особисто мав досвід, коли правильно налаштований Microsoft Defender For Endpoints врятував під розповсюдження вірусу по корпоративній мережі. Був інцидент пов’язаний з фішинговою розсилкою з вірусом всередині. Коли зрозуміли, щоб була фішингова атака на компанію, 6 користувачів вже вивантажили собі архіви та розпакували файли. В цей момент агент Defender помітив нелегітимну активність і зробив 3 головні дії :

– вбив процес, який запустив вірус;

– відправив в центр керування IoC, за рахунок чого ці файли більше не можна було розпакувати іншим користувачам;

– ізолював хости від корпоративної мережі.

Після проведення розслідування виявилось, що вірус нічого не встиг зробити, ніяких комунікацій назовні не відбулося.

За результатами проведеного аналізу можна прийти до висновку, що Microsoft Defender ATP можна використовувати як ключовий інструмент в боротьбі з кіберзагрозами на кінцевих точках. За допомогою своїх технологій та інновацій, він дозволяє організаціям забезпечити ефективний захист своєї інформації та інфраструктури в умовах постійно зростаючих загроз. Його потужність у виявленні та реагуванні на загрози, а також можливості інтеграції з іншими системами, роблять його незамінним інструментом для будь-якої компанії, що прагне забезпечити безпеку своєї інформації та інфраструктури.

Список використаних джерел

1 Microsoft is named a Leader in the 2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms. https://www.microsoft.com/en-us/security/blog/2024/01/12/microsoft-is-named-a-leader-in-the-2023-gartner-magic-quadrant-for-endpoint-protection-platforms/: веб сайт URL https://www.microsoft.com/en-us/security/blog/2024/01/12/microsoft-is-named-a-leader-in-the-2023-gartner-magic-quadrant-for-endpoint-protection-platforms/ (дата звернення: 27.02.2024).

2 Microsoft Defender for Endpoint. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide#compare-microsoft-endpoint-security-plans-1 веб сайт URL https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide#compare-microsoft-endpoint-security-plans-1 (дата звернення: 27.02.2024)

Каляєв О.О., Турик Р.Р., Бондар Р.В., Корнієнко О.С.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ ТА ДІЯЛЬНОСТІ СИЛОВИХ СТРУКТУР

В Україні існує багато програм для інформаційно-аналітичного забезпечення силових структур. Деякі з цих програм є автоматизованими за допомогою штучного інтелекту та використовують аналітичні алгоритми для оптимізації обробки даних

Основними задачами інформаційно-аналітичних підрозділів є: ведення автоматизованої бази інтегрованої оперативно-розшукової інформації й видачу довідкової інформації; аналітичні дослідження і прогнозування; програмно-технічне забезпечення і захист інформації; виконання інших завдань і функцій, що стоять перед підрозділами.

Існує багато програм, які використовуються силовими структурами для інформаційно-аналітичного забезпечення. Деякі з найпоширеніших програм: Системи обліку та документообігу: "Автоматизована система документообігу", "Система електронного документообігу". Системи аналітики: "Система аналізу даних про розвідку", "Система аналізу даних про оперативну обстановку", "Система аналізу даних про бойові дії". Системи візуалізації: "Система геоінформаційних систем", "Система візуалізації даних про розвідку", "Система візуалізації даних про оперативну обстановку". Використання програм для інформаційно-аналітичного забезпечення дозволяє: "Підвищити ефективність роботи.", "Покращити якість прийняття рішень.", "Зменшити ризики помилок.", "Підвищити рівень безпеки.".

Важливим завданням є подальший розвиток та вдосконалення програмного забезпечення для інформаційно-аналітичного забезпечення всіх силових структур. Це дозволить їм більш ефективно виконувати свої завдання та забезпечувати оборону України.

Ось програми які успішно застосовують ЗСУ для планування та орієнтування бойових підрозділів, автоматизованого управління військами, а також розвідки та спостереження за діями противника, а в подальшому аналіз і збір даних про них: "Дельта", "Візир", "Кронос", "Кропива".

Одною з найуспішніших програм створених спеціально для потреб: ЗСУ, НГУ, ДПСУ, ССО і тд., являється: "Кропива", сотні і навіть тисячі завдань які було виконано завдяки цій програмі. "Кропиву" використовують 90–95% підрозділів РВіА, дякуючи цій розробці час розгортання батареї зменшився більш ніж у п'ять разів, час на ураження незапланованої цілі – у три рази, а час на відкриття контрбатарейного вогню – у десять разів. Раніше координати цілі передавались за допомогою радіостанції, артилерист сідав за стіл з лінійкою, олівцем та калькулятором і розраховував дані по цілі 15–20 хвилин. З часом додаток почали оновлювати і в ньому з'явились функції не тільки для артилеристів а і для механізованих, танкових, розвідувальних та інженерних підрозділів. Кожного дня оновлюється лінія фронту, військовослужбовець може побачити: де стоять ворожі підрозділи, а де дружні війська, обмінюватися позиціями, розвідданими, комунікувати з командним пунктом. У функціях програми є також GPS навігація, карта з точними координатами, височинами і низовинами, визначення дальності від одного об’єкта до іншого, обчислення далекобійності по цілям: реактивних систем залпового вогню, ракетних пускових установок, гармат та інших артилерійських систем. Додаток, який керується "Армія SOS", не єдиний, який застосовують силові структури, подібних програм є біля десяти. Багато військових використовують "Кропиву". Хтось застосовує "Delta", хтось "GIS Arta". А підрозділи ППО – "Віраж-планшет".

Проблемними питаннями застосування радіотехнічних і телевізійних систем та електронних комунікаційних мережах є: Недостатня підготовка кадрових військовослужбовців: війська потребують кращої підготовки кадрів для роботи з телевізійними, електронно комунікаційними та радіотехнічними мережами. Це збільшить швидкість та функціональність їх роботи і зменшить ризик виникнення помилок. Термін експлуатації обладнання вичерпано: велика кількість радіотехнічних і телевізійних систем, а також електронних комунікаційних мереж, які застосовуються нашими силовими структурами, застаріли. Це може призвести до проблем з їх продуктивністю в порівнянні з новими зразками обладнання, а також безпекою адже чим новіші тихнології тим тяжче від них щось приховати. Недостатня координація: існує потреба в кращій взаємодії між різними силовими структурами, які використовують телевізійні, електронно комунікаційні та радіотехнічні мережі. Недостатня захищеність: є ймовірність перехоплення та дешифрування даних противником, які передаються за допомогою радіотехнічних, телевізійних та електронно комунікаційних мереж. Це може призвести до витоку інформації та шкоди для національної безпеки.

Перспективні напрямки в застосуванні радіотехнічних і телевізійних систем та електронних комунікаційних мережах є: Застосування безпілотних літальних апаратів: дрони і БПЛА могли б використовувати для розвідки, нагляду та передачі даних у реальному часі з віддалених районів, що дозволяє збільшити обсяг інформації, доступної підрозділам силових структур. Захист від кібератак та електронного вторгнення: розвиток розробок протидії кібератакам та електронного вторгнення. Використання супутникових технологій: супутниковий зв'язок та навігаційна система набувають все більшого значення для силових структур. Завдяки супутникам нашим військам вдається добувати та передававти інформацію з різних регіонів, обходячи РЕБ. Розвиток мереж 5G: впровадження технології 5G збільшить швидкість та пропускну спроможність комунікаційних мереж для силових структур. Це допоможе передавати великі обсяги даних у реальному часі та забезпечити практично миттєвий обмін інформацією. Мережі зв'язку на основі штучного інтелекту: штучний інтелект може використовуватися для отримання даних від радіотехнічних та телевізійних систем, а також для автоматичної обробки цих

даних. Це дасть командирам підрозділів збільшити якість та швидкість прийняття рішень в бойових умовах.

Технології захисту інформації та кібербезпека: Навчання та освіта користувачів: навчання співробітників, щодо правил безпеки та потенційних загроз кібербезпеці. Аутентифікація: вибір кількох методів аутентифікації, таких як пароль, підтвердження пошти, номеру телефону і тд., зменшує ризик непланового доступу до даних та системи. Шифрування даних: сучасні шифрувальні алгоритми забезпечують високий рівень безпеки, навіть у разі прехоплення даних вони всеодно залишаються захищеними. Резервне копіювання та відновлення даних: регулярне копіювання даних та розробка планів їх відновлення забезпечують доступність та цілісність інформації в разі виникнення аварійних ситуацій. Захист мережевого трафіку: використання мережевих проксі-серверів та інших засобів дає можливість контролювати та фільтрувати трафік, що надходить до інформаційної системи. Моніторинг і виявлення вторгнень: дозволять виявляти та відбивати атаки на інформаційну систему в реальному часі.

УДК 539.3

Камак Д.О., Тітов І.В., Сидоренко І.І.

ПІДВИЩЕНЯ ЕФЕКТИВНОСТІ ВИПРОБУВАНЬ ЗРАЗКІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ ЗА РАХУНОК ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

Запропоновано один із можливих шляхів підвищення ефективності проведення випробувань нових та модернізованих зразків озброєння та військової (спеціальної) техніки за рахунок впровадження інформаційно-комунікаційної системи супроводження випробувань. Підвищення ефективності, що очікується, може бути досягнуте за рахунок покращення показників точності та об'єктивності результатів випробувань, зменшення часу на підготовку та обробку даних, оптимізацію комунікації між усіма особами, що задіяні у випробувальних процесах та ін.

Створення та модернізація с передбачає проведення різноманітних випробувань на певних етапах їх життєвого циклу. В процесі таких випробувань, в залежності від їх виду, може проводитись експериментальне визначення кількісних та (або) якісних характеристик властивостей об'єктів в певних умовах застосування; вибір найкращих режимів застосування або характеристик об'єкту та як наслідок дії на нього під час його функціонування; контроль якості виробів; перевірка відповідності характеристик дослідних зразків вимогам тактико-технічного завдання та ін. [1]. Все це неодмінно пов'язано із великими обсягами різнопланової інформації, що має оперативно і якісно оброблятись, та доставлятись великій кількості її внутрішніх і зовнішніх споживачів.

Суттєвого підвищення ефективності всіх етапів випробувань зразків озброєння та військової (спеціальної) техніки можна досягти за рахунок впровадження інформаційно-комунікаційної системи, яка має забезпечувати комплексний супровід випробувань озброєння та військової техніки, включаючи автоматизацію процесів збору, обробки та аналізу даних, а також оптимізацію комунікацій між всіма учасниками випробувального процесу [2]. Така система перш за все повинна відповідати сучасним вимогам до безпеки зберігання та передавання даних, мати можливість за потреби бути масштабованою, а також інтегруватись із іншими інформаційними системами силових відомств та цивільних структур.

Призначенням зазначеної системи супроводження випробувань є надання всебічної автоматизованої інформаційної підтримки інженерам-випробувачам, науковим праців-

никам, керівному та допоміжному персоналу на всіх етапах проведення випробувань зразків ОВТ:

- планування випробувань (розробка програми, методик, планів проведення випробувань, призначення бригади інженерів-випробувачів, підготовка та навчання бригади інженерів-випробувачів, планування та підготовка лабораторно-вимірювального комплексу, вибір полігонної бази, документальний супровід етапу тощо);

- проведення випробувань (надання інформаційних довідок щодо методів та методик вимірювань, підготовка конкретного експерименту під час конкретного випробування, оцінка відповідності фактичних умов його проведення вимогам програми і методики проведення випробувань, автоматизований збір вимірюваної інформації, її обробка тощо);

- підготовки результатів випробувань (агрегування результатів та складання звітних документів);

- управління випробуваннями (технічний супровід оформлення необхідної документації, управління ризиками, контролю за ходом випробувань, аналіз успішності функціонування випробувальних бригад та випробувальної організації в цілому.

Основними завданнями системи, що пропонується до впровадження є збір та обробка результатів випробувань; контроль за ходом проведення випробувань та збір даних вимірювань та телеметрії; фіксація та формалізація результатів випробувань, з подальшим формуванням звітних документів і надання їх зацікавленим сторонам; введення, зберігання та відображення документації щодо проведення випробувань; сполучення зі всіма типами обладнання, що використовуються на випробувальному полігоні; безпечне зберігання даних та забезпечення їх захисту від несанкціонованого доступу, втрати або знищення.

Результатом впровадження такої інформаційно-комунікаційної системи стане суттєве підвищення ефективності проведення випробувань нових та модернізованих зразків озброєння та військової (спеціальної) техніки.

Список використаних джерел

1. ДСТУ 3021-95. Випробування і контроль якості продукції. Терміни і визначення. Київ: Держстандарт України. С. 71.

2. Корнієнко І.В. Щодо можливих функціональних компонент інформаційної системи супроводження випробувань ОВТ ЗСУ / І.В. Корнієнко, С.П. Корнієнко, Д.О. Камак, С.М. Казначей, О.В. Жирна // Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. – Чернігів : ДНДІ ВС ОВТ, 2020. – Вип. № 4(6). – С. 52-61.

УДК 621.396

Каменцев С.Ю., Зубков А.М., Красник Я.В., Мартиненко С.А., Файфура М.В.

МАЛОГАБАРИТНА РЛС РОЗВІДКИ ПОЛЯ БОЮ

На основі аналізу тенденцій розвитку вітчизняних і закордонних аналогів і елементної бази обґрунтовані структурно-функціональна схема і варіанти застосування малогабаритної РЛС пошуку, виявлення, вимірювання координаті і розпізнавання наземних цілей. В якості конструктивних обмежень при інженерному синтезі структури РЛС прийняті:

– мінімальні масогабаритні показники апаратури, що дозволяють транспортувати і експлуатувати РЛС розрахунком із двох осіб;

– максимальні енергетична скритність роботи РЛС і завадостійкість;

– інваріантність до наявності чи відсутності руху об'єктів, що спостерігаються.

Ефективним інструментом інструментального забезпечення всепогодного, цілодобового моніторингу оточуючої обстановки в умовах відсутності оптичної прозорості приземного шару атмосфери є радіолокаційні засоби. Область їх застосування розширяється на цивільні (зв'язок, транспорт, метеорологія, картографія) і спеціальні (артилерійська розвідка, об'єктова протиповітряна оборона) завдання. Однако при любих застосуваннях ключовими питаннями практичної ефективності РЛС є:

– дальність дії і точність вимірювання координат;

– маса і габарити апаратури;

– завадозахищеність;

– незалежність від швидкості руху цілі (включаючи нульову).

Практичними шляхами мінімізації маси і габаритів РЛС розвідки наземних цілей є [1]:

– робота в міліметровому діапазоні (ММД) радіохвиль (в "вікнах прозорості" приземного шару атмосфери (36 або 95 ГГц));

– повністю твердотільне апаратне виконання;

– реалізація дальністної (не більше 0,5 м) і допплерівської (не більше 300 Гц) роздільних здатностей;

– реалізація кутової роздільної здатності не більше одного кутового градуса.

В роботах [1, 2] розглянуті методи виявлення і розпізнавання наземних цілей на основі дальністних, допплерівських і поляризаційних признаків в ММД і виконана оцінка їх ефективності.

Незважаючи на велику кількість досліджень і розробок в області створення РЛС спостереження наземних цілей [3, 4] актуальними питаннями, що вимагають вирішення, остаються:

– зняття обмежень на наявність або відсутність руху об'єктів, які спостерігаються, оскільки саме нерухомі об'єкти являються найбільш небезпечними потенціальними джерелами вогневого впливу;

– об'єднання режимів виявлення і розпізнавання наземних об'єктів, які спостерігаються, для підвищення інформативності геомоніторингу;

– підвищення точності пеленгації об'єктів, які спостерігаються, при обмежених розмірах апертури антени РЛС.

Основні конструктивно-функціональні особливості побудови апаратури РЛС:

– приймально-передавальна антена – скануюча з моноімпульсною обробкою ехо-сигналів;

– когерентно-імпульсний передавач – твердотільний на базі імпульсних лавинно-прольотних діодів (ЛПД);

– приймач – супергетеродинний на основі безперервних ЛПД (гетеродин) і діодів з бар'єром Шотткі (змішувач);

– зондуючий сигнал імпульсний когерентний з реалізацією двох режимів черезперіодної і черезпачкової перебудови несучої частот для забезпечення інваріантності до наявності чи відсутності руху об'єкту спостереження і завадозахищеності.

Вага і габарити РЛС дозволяють транспортувати, розгортати і експлуатувати розрахунком із двох людей.

Розрахунково-експериментальним шляхом підтверджені можливості виявлення наземної техніки (одиночні об'єкти) на дальність до 5 000 м, колони техніки на дальність до 10 000 м незалежно від часу доби, погоди (дощ інтенсивністю до 4 мм/год, туман з оптичною видимістю до 100 м, сніг з густиною до 0,35 мг/см^3), що недосягаємо в оптичних і теплових каналах спостереження наземних цілей.

Перспективними напрямками подальших досліджень є:

– уточнення сигнатурних інформативних признаків типових наземних цілей (солдат, танк, БМП, БТР, пускова установка…);

– уточнення інформативних признаків що пов’язані з динамікою руху наземних цілей;

– уточнення цілефонової і завадової обстановки, яка супутня спостереженню наземних цілей, з урахуванням можливого застосування противником активних завад;

Висновки:

1. Запропоновані і обґрунтовані технічні шляхи підвищення інформативності локаційного спостереження наземних об’єктів для підвищення точності їх місцевизначення і класифікації.

2. Виконано інженерний синтез структури малогабаритної твердотільної РЛС спостереження наземної обстановки і визначені її граничні можливості.

3. Всі елементи синтезованої структури РЛС реалізується на загальнодоступній вітчизняній і імпортній елементній базі.

Список використаних джерел

1. Зубков А.Н. (2005) Системы радиовидения миллиметрового диапазона. / А.Н. Зубков // Радиоэлектроника. – 2005. – № 9, С. 3-16; 2005. – № 10, С. 3 – 10.

2. Нефедов С.И., (2010) Перспективы применения миллиметровой радиолокации для обнаружения и распознавания неподвижных и движущихся объектов на фоне подстилающей поверхности / С.И. Нефедов, М.И. Ониашвили, А.А. Лаговиер, М.Е. Голубцов // IV Всероссийская конференция “Радиолокация и радиосвязь” – ИРЭ РАН, 29 ноября – 3 декабря 2010. с. 237-242.

3. Kulemin G.P. (2003) Millimeter-Wave Radar Targets and Clutter. Artech House, 2003. 417 p.

4. Нефедов С.И. (2012) Экспериментальные исследования радиолокационных портретов различных типов целей в миллиметровом диапазоне длин волн / С.И. Нефедов, В.Н. Скосырев, С.А. Растворов, А.Б. Восторгов, М.И. Ониашвили, А.В. Шумов // 2012 – НИИ РЭТ МГТУ им. Н.Э. Баумана. http://www.technomag.edu.ru/doc/253065.html

УДК 004.91

Канчуга М.К., Дуфанець І.Б.

ВИКОРИСТАННЯ ІНФОРМАЦІНИХ ТЕХНОЛОГІЙ В УМОВАХ СЬОГОДЕННЯ

Інформатизація навчального процесу є одним з найважливіших завдань перебудови та формування системи освіти відповідно до вимог суспільства. Завдяки використанню комп'ютерних мереж та онлайн-технологій навчальні заклади мають можливість поширювати новий матеріал у спосіб, що відповідає унікальним потребам кожного навчаємого.

Використання інформаційних технологій у навчальному процесі має на меті розвивати мислення навчаємих, вміння розв'язувати проблеми, аналізувати інформацію. Тому, необхідність розвитку професійних навичок у викладачів, щодо доцільності вивчення та використання інформаційних технологій, не викликає сумнівів [1].

Проте жорсткі та непередбачувані умови воєнного стану вносять свої корективи в життя в цілому. Враховуючи можливості інформаційних технологій для освіти, важливим є вивчення їх застосування для навчання, вплив на подолання стресу, ефективність для навчання, доступність.

Інформаційні технології допомагають навчаємим самостійно вивчати матеріал, поповнювати свої знання та навички, розвивати творчі та конструктивні здібності, вчитися самостійно вирішувати проблеми .

Зокрема, платформа для навчання MOODLE (Modular Object-Oriented Dynamic Learning Environment), яка забезпечує викладачів та навчаємих необхідним набором інструментів, котрі надають можливість використовувати навчальний матеріал в будь якому місці та у будь який час, проводити контроль засвоєння рівня знань навчального матеріалу та дають можливість опрацьовувати навчальний матеріал самостійної підготовки у вільний час.

Не менш важливим є також економічний фактор та доступність платформи MOODLE. Ця система повністю безкоштовна і не потребує жодних інших платних програмних забезпечень. Також вона є найбільш розповсюдженою платформою для навчання у всьому світі, що робить її однією з найбільш доступних [2].

Отже, використання інформаційних технологій є предиктором успішної роботи. Використання інформаційних технологій в Україні в умовах воєнного стану дає можливість не зупиняти освітній процес та пристосувати його до вимог сучасності.

Список використаних джерел

1. Жанга, К., Аслан, А. (2021). Технології штучного інтелекту для освіти: останні дослідження та майбутні напрямки. Комп'ютери та освіта: штучний інтелект.

2. Система електронного навчання ВНЗ на базі MOODLE: Методичний посібник / Ю. В. Триус, І. В. Герасименко, В. М. Франчук // За ред. Ю. В. Триуса. - Черкаси, 2012. - 220 с.

УДК: 378.14

Каршень А.М., Стаднічук О.М., Кропивницька Л.М.

ОСОБЛИВОСТІ ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ІННОВАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ВИКЛАДАННІ СПЕЦІАЛЬНИХ ДИСЦИПЛІН

Сучасний етап розвитку українського суспільства визначає основні завдання для системи освіти, серед яких необхідність підвищення якості освіти, академічної мобільності та доброчесності, інтеграція у світовий науково-освітній простір тощо. Одним із ефективних шляхів вирішення цих завдань є інформатизація освіти, що охоплює всі складові освітнього процесу. Удосконалення технічних засобів зв'язку призвело до значного прогресу в обміні інформацією. Поява нових інформаційних технологій, пов'язана з розвитком комп'ютерної техніки та телекомунікаційних мереж, дозволила створити якісно нове інформаційно-освітнє середовище як основу розвитку та вдосконалення системи освіти. Використання інформаційно-комунікаційних технологій (ІКТ) є важливим і неминучим для проведення інтерактивного заняття, оскільки сприяє інноваціям і оновленню інституцій, забезпечує підвищення ефективності та результативності. Однак, більшість сприймають інтерактивне навчання виключно як навчання з використанням інтернет-ресурсів, а ІКТ – як інструмент для створення презентації, тоді як насправді кожен, хто задіяний в освітньому процесі (адміністрація, викладач, курсант), робить власний внесок у процес спільної діяльності, обмінюючись знаннями, ідеями, формами та способами дій для формування професійних фахівців.

Ефективність реалізації завдань і очікуваних результатів при вивченні військово-спеціальних дисциплін суттєво впливає на професійну компетентність майбутніх військовослужбовців. Зважаючи на реалії сьогодення, сучасний офіцер повинен відповідати

трьом основним критеріям: бути кваліфікованим у своїй спеціальності, мати достатні навики у роботі з комп'ютером та Інтернетом та володіти кількома іноземними мовами. Інформаційні технології відіграють також важливу роль для курсантів як засіб підвищення ефективності навчання та особистого розвитку професійної, мовної та інформаційно-технологічної компетентностей. Крім того, ІКТ дозволяють курсантам самостійно вдосконалюватись, розвивати ініціативу та здатність до самостійного отримання інформації, ідей та досвіду [1, 2].

Дослідження, проведені під час педагогічного експерименту у Національній академії сухопутних військ з використанням стратегії проблемного навчання, де матеріал, який потрібно вивчити, спершу формується як проблема, що надалі забезпечує мотивацію та контекст для роботи, вказали на важливість ІКТ. Курсанти і викладачі віддають перевагу як активній участі в освітньому процесі, так і активній обробці інформації. Сучасні засоби ІКТ мають добре побудовану нелінійну систему навігації у вигляді гіпертекстів та складаються з візуального або звукового фрагмента. Основними ознаками таких засобів є *комунікативність* (забезпечує можливість безпосереднього спілкування, оперативність подання інформації, швидкий доступ до освітніх ресурсів в мережі Інтернет в режимі on-line), *інтерактив* (розвиває активні форми навчання, дозволяє маніпулювати та змінювати зміст навчальних об'єктів), *мультимедіа* (представляє навчальні об'єкти різними способами для забезпечення реалістичного уявлення об'єктів і процесів), *моделінг* (реалізує візуалізацію, моделювання об'єктів і досліджуваних процесів) та *продуктивність* (збільшує швидкість пошуку інформації, посилює ефективність навчання). Відповідно, більшість курсантів факультету Сил підтримки віддають перевагу наступним способам сприйняття інформації:

- *сенсорному* (баченню, звукам, фізичним відчуттям, практичному, орієнтоване на факти та інтуїтивному мисленні);
- *візуальному* (через фото, малюнки, діаграми, блок-схеми, графіки, демонстрації);
- *активному* (через залучення до фізичної активності чи обговорення, роботу в групах);
- *послідовному* (як лінійний процес мислення, навчання *step by step*, тобто невеликими поступовими безперервними кроками).

Водночас, *інтуїтивне* (можливість, сприйняття, передчуття, абстрактне мислення, інноваційне, орієнтоване на теорії), *вербальне* (письмові чи усні пояснення), *рефлекторне* (через самоаналіз, роботу наодинці чи в сталій парі) та *глобальне* (процес цілісного мислення, навчання великими стрибками) розуміння інформації сприймається важче і задовольняє не більше 10% курсантів, що брали участь в експерименті.

Для викладачів важливим є стиль викладання на який впливає тип інформації: конкретна (фактологічна), абстрактна (концептуальна, теоретична); форма її презентації: візуальна (наочне зображення, схеми, відеоподкасти, демонстрації), вербальна (усна бесіда, читання, дискусія); спосіб участі курсантів: активний (курсанти говорять, рухаються, розмірковують), пасивний (курсанти дивляться та слухають) та бачення на інформацію, що подається: послідовна (step by step), глобальна (релевантна). Опитані викладачі обирають різні стратегії навчання, комбінуючи їх, проте надають перевагу *послідовному* викладу інформації незалежно від типу заняття чи завдання, що вирішується [3].

Так, сучасна лекція – аудиторна чи дистанційна – це динамічний діалог між викладачем і курсантами, основним інструментом якої є якісна інтерактивна презентація, вдало підібрані відео- та аудіопідкасти українською та англійською мовами. Досвід проведення таких лекцій показує, що вони дозволяють оптимально активізувати сприйняття матеріалу, дають можливість наочності навіть при вивченні тем, які враховують просторові та часові масштаби.

Практична складова (практичні, групові заняття) потребують від ІКТ не лише демонстрації інформації, але й можливості нею оперувати. Наприклад, вивчати, розбира-

ти на складові різні типи мін чи вибухонебезпечних предметів, створених за допомогою 3D-моделювання, проєктувати нові зразки мостів, доріг, враховуючи дані інженерної розвідки (крутизни берегів, глибини водної перешкоди тощо). Співпрацювати у нових програмних продуктах можуть як викладачі так і курсанти. Для прикладу, використання безкоштовного програмного забезпечення Open eLearning з різними інструментами (захоплення екрана, редагування зображень) дозволяє створювати навчальні курси та інтерактивні навчальні посібники у формі гри (геймифікація). Ще одним безкоштовним інструментом електронного навчання, який дозволяє створювати інтерактивні посібники, презентації та інші навчальні матеріали є CourseLab з середовищем WYSIWYG без програмування. Контент, створений у CourseLab, сумісний із деякими системами керування навчанням, зокрема Moodle. Для курсантів цікавими є 3D-програми, що дозволяють самостійно працювати і створювати 3D-моделі. Найбільш популярними є Blender, Google Sketchup, DesignWorkshop Lite (дозволяє проєктувати 3D-моделі для занять, що як правило пов'язані з фортифікацією) чи FreeCad (пакет програм 3D-CAD для вивчення геометрії, кінематики, динаміки, вібрації, механізмів, моделювання руху). Цілеспрямоване використання цих програмних засобів сприяє ефективному засвоєнню курсантами навчального матеріалу та формуванню у них мотиваційної готовності використовувати набуті знання, уміння та навички в практичній діяльності. У багатьох випадках віртуальна практична складова є доречною та ефективною. Залучення курсантів до проведення таких практичних робіт із спеціальних військових дисциплін можна шляхом включення цих завдань до тематики курсових та кваліфікаційних робіт. Очевидно, що на етапі проведення занять ІКТ дозволяють: економити час; естетично подавати матеріал; оптимізувати процес навчання; індивідуалізувати навчання; зосередити увагу на найважливішій проблемі заняття; повернутися до знайомого матеріалу в будь-який момент; самостійно використовувати курсантами навчальний матеріал.

Ще однією складовою освітнього процесу, що спонукає до розвитку навичок самоосвіти та формування креативного мислення, є самостійна робота курсантів. Виконання ситуативних комплексних завдань, що поєднують кілька тем або дисциплін, у формі проєктів, що включає: постановку проблеми, планування проєкту, вивчення стану питання, формулювання результатів і висновків, розробку презентації та захист передбачає використання ІКТ. Організація такого виду самостійної роботи дозволяє курсантам гнучко, у формах і обсягах, що відповідають індивідуальній ситуації, оволодіти цими матеріалами, урізноманітнює та оптимізує форми роботи, робить процес навчання та оцінювання знань контрольованим та «прозорим», і суттєво впливає на якість освітнього процесу.

Втім, використання ІКТ у системі військової освіти має також певні проблеми та завади. Перешкодами або предикторами прийняття інтеграції ІКТ визначаються намірами користувача та/або фактичним використанням технології. До них можна віднести:

- очікуваний результат – найважливіший предиктор використання ІКТ, це результат внутрішніх переконань і установок щодо використання ІКТ, що вимірюється прийнятною корисністю та простотою використання;

- відповідність технології до завдання – це ступінь, до якого технологія допомагає людині виконувати поставлені завдання. Фактично, користувач приймає технологію через її потенційні переваги, наприклад, підвищення продуктивності, незалежно від їхнього ставлення до цієї технології;

- соціальний вплив або домінуючий соціальний фактор – це різновид соціальної норми, що визначається як прийнятий соціальний тиск щодо поведінки і має значний позитивний вплив на індивідуальні переконання щодо корисності технологій і позитивно впливає на використання ІКТ;

- особисті фактори, що включають самоефективність роботи з комп'ютером і схильність до вивчення та використання технологічних інновацій. До таких факторів курсанти відносять:

- дуже насичену діяльність, що втомлює і знижує їхню мотивацію до навчання;
- брак вільного часу для саморозвитку, наприклад, використання Інтернету для отримання нових навичок або просто пошук рекомендацій для навчання;
- тиск з боку інших курсантів, нездорова конкуренція, що сповільнює розвиток професійної, мовної та інформаційно-технологічної компетенції;
- заборона користування мобільними телефонами під час навчання тощо.

Отже, комп'ютеризація навчання створює особливе інформаційне середовище, яке стимулює інтерес до військових спеціальних дисциплін та піднімає професійну підготовку на новий рівень. Курсанти і викладачі вважають, що вдало адаптовані ІКТ для використання в "авдиторії" підвищуватимуть ефективність навчання та сприятимуть покращенню професійної військової підготовки. Це полегшує розуміння та розв'язання багатьох проблем, сприяє розкриттю закладених можливостей і здібностей до пізнання, творчої ініціативи, розвитку особистості кожного курсанта. Роль викладача при цьому є визначальною (оскільки він відповідальний за розміщення комплексу матеріалів, включно з презентаціями, завдань, інструкцій та коментарів до їх виконання), але процес навчання курсанта – індивідуалізований.

Список використаних джерел

1. L.A.B. dos Santos, N.A.R.S. Loureiro, J.M.M. do Vale Lima, J.A. de S. Silveira, R.J. da S. Grilo Military higher education teaching and learning methodologies: an approach to the introduction of technologies in the classroom. *Security and Defence Quarterly*. 2019. Vol. 24 (2). P.123-154. https://doi.org/10.35467/sdq/108668

2. Duzhyi R.V., Derkach T. M. Learning styles of the Armed Forces of Ukraine personnel undergoing English language courses. *Educational Technology Quarterly.* 2024. https://doi.org/etq.659

3. Стаднічук О., Фтемов Ю., Каршень А., Надос В., Кропивницька Л. Впровадження методів активного навчання на прикладі викладання навчальної дисципліни "Військові мости і шляхи" *Військово-технічний збірник.* 28. 2023. С.124-132. https://doi.org/10.33577/2312-4458.28.2023.124-132

УДК 351.746.1:314:355.232 (477)

Катеринчук І.С., Бабарика А.О.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ВИБОРУ РАЦІОНАЛЬНИХ ПАРАМЕТРІВ СИСТЕМИ ПРОТИДІЇ НЕЗАКОННІЙ МІГРАЦІЇ НА ДЕРЖАВНОМУ КОРДОНІ

Розширення масштабів незаконної міграції та загострення проблем, які з нею пов'язані викликають серйозну занепокоєність керівництва і громадськості країни. Адміністрацією Державної прикордонної служби України та іншими органами управління ведеться активна робота щодо створення дієвої система протидії незаконній міграції (СПНМ) на державному кордоні. Однак, незважаючи на заходи, які вживаються силами та засобами ДПСУ у взаємодії з іншими правоохоронними органами, продовжують функціонувати канали незаконної міграції територією України. При в'їзді в Україну виявляються 65-70 % незаконних мігрантів, біля 10 –15 % – затримуються та передаються в Україну прикордонною охороною Польщі, Словаччини та Угорщини. Одною із основних причин цього є недостатнє врахування при організації оперативно-службовій діяльності причинно-наслідкових зв'язків між параметрами міграційної загрози та елементами системи протидії незаконній міграції. На рівень міграційної загрози може впливати багато чинників: економічні, політичні, соціальні, екологічні тощо.

Наявний науково-методичний апарат надає можливості оцінити окремі параметри процесу незаконної міграції та ефективність застосування типових елементів охорони державного кордону.

Система протидії незаконній міграції на державному кордоні може включати різноманітні елементи, спрямовані на запобігання незаконному перетину кордону та контроль за міграційними процесами. Головними із них є прикордонний контроль (включає пункти пропуску, прикордонну охорону, патрулювання та моніторинг кордону для виявлення та зупинки незаконних перетинів); технологічні засоби (інженерно-технічні засоби моніторингу державного кордону (РЛС, камери відеоспостереження, теплові камери, БПлА та інші технічні засоби для виявлення незаконних перетинів та підвищення ефективності контролю за кордоном); інформаційні системи (системи обміну інформацією між правоохоронними органами, міграційними службами та іншими зацікавленими сторонами для обміну розвідувальною інформацією та координації дій); нормативно-правова база (законодавчі акти, які встановлюють правила та процедури щодо в'їзду, перебування та виїзду осіб через державний кордон, а також санкції за порушення міграційного законодавства); співпраця (взаємодія) з міжнародними партнерами та інші. Оцінка ефективності системи протидії незаконній міграції на державному кордоні може здійснюватися за допомогою різноманітних критеріїв, які враховують як технічні, так оперативно-тактичні аспекти цієї системи.

Незаконна міграція і контрабанда товарів тривалий час залишаються одними з основних загроз національній безпеці України на державному кордоні. В умовах обмеженості людських, технічних, матеріальних та фінансових ресурсів органам охорони державного кордону необхідно мати гнучку систему протидії незаконній міграції, адекватну рівням міграційної загрози.

Для досягнення мети дій органів охорони державного кордону щодо протидії незаконній міграції необхідно створити систему протидії, яка була б адекватною параметрам міграційної загрози. Складовими СПНМ є підсистеми протидії незаконній міграції в пунктах пропуску, поза пунктами пропуску та оперативної протидії незаконній міграції. Авторами пропонуються інформаційні технології вибору раціональних параметрів системи протидії незаконній міграції на державному кордоні, які ґрунтуються як на загальнонаукових методах (аналіз, синтез), так спеціальних методів прикладної математики (теорії графів, алгебри кортежів, багатопараметричної оптимізації).

Стан СПНМ на державному кордоні можна оцінити кортежем показників, які характеризують підсистеми протидії незаконній міграції: у пунктах пропуску; поза пунктами пропуску та оперативної протидії незаконній міграції.

У свою чергу кожна підсистема характеризується відповідним кортежем власних показників. Так, показник підсистеми протидії незаконній міграції у пунктах пропуску містить часткові показники ефективності типових елементів прикордонного контролю: перевірки документів; огляду транспортних засобів, вантажу та іншого майна; спостереження за транспортними засобами; режиму в пунктах пропуску. Аналогічним чином формуються кортежі показників протидії незаконній міграції поза пунктами пропуску та оперативної протидії незаконній міграції. Показники ефективності окремого елементу прикордонного контролю розраховуються за показниками оперативності та якості заходів протидії незаконній міграції.

Показники ефективності підсистеми протидії незаконній міграції поза пунктами пропуску включає оцінку таких елементів: показник ефективності виявлення незаконних мігрантів, який розраховується як відношення площі ділянки, на якій забезпечується виявлення незаконних мігрантів, до площі всієї ділянки, що охороняється прикордонним формуванням; ефективність затримання незаконних мігрантів, розраховується як відношення довжини ділянки гарантованого затримання до усієї ділянки, що охороняється прикордонним формуванням; ефективність контролю за порядком перебування іноземців в межах контрольованих прикордонних районів, розраховується як відношення кількості

маршрутів, пунктів, районів, у яких здійснюється контроль силами й засобами ООДК, і взаємодіючих органів, до загальної кількості об'єктів, на яких необхідно здійснювати контроль з урахуванням часу несення служби.

Для досягнення мети дій ООДК щодо протидії незаконній міграції необхідно залежно від рівня та типу міграційної загрози забезпечити у відповідних місцях (районах) та у визначений час такий рівень значень показників кортежів у пунктах пропуску; поза пунктами пропуску та оперативної протидії незаконній міграції, який би забезпечив виявлення та затримання незаконних мігрантів. У той же час надлишковий рівень значень показників призведе до перевитрат сил та засобів охорони державного кордону. Інформаційна технологія надає можливості вибору раціональних значень параметрів СПНМ, що адекватні рівням міграційної загрози.

На відміну від відомих результатів, у моделі та методиці вперше враховані параметри міграційної загрози, а саме: рівень, тип, місце, форма вияву загроз на державному кордоні та обмеження на використання персоналу й технічних засобів, витрати часу на виконання завдань протидії незаконній міграції в пунктах, поза пунктами пропуску та заходів оперативної протидії. Методика забезпечує раціональне використання сил та засобів за рахунок підвищення рівня протидії в місцях найбільш імовірного прояву загроз та його зменшення, де загроза менша.

В подальших дослідженнях за даним напрямком доцільно розробити програмні засоби для оцінки ефективності та визначення достатніх значень параметрів підсистеми оперативної протидії незаконній міграції.

УДК 614.84

Катунін А.М., Коломійцев О.В.

АКТУАЛЬНІСТЬ ОЦІНЮВАННЯ ПОЖЕЖНОЇ НЕБЕЗПЕКИ КАБЕЛЬНИХ ВИРОБІВ ЗІ СТРУМОВІДНИМИ ЖИЛАМИ З РІЗНИХ МАТЕРІАЛІВ

В доповіді розкрито застосування відомих математичних моделей для визначення діапазонів нагріву кабельних виробів для різних матеріалів ізоляції. Представлено результати математичного моделювання отриманих діапазонів та різних матеріалів струмовідної жили.

Сучасні електроприлади з одного боку – поліпшують та полегшують життя людства, з іншого боку – мають велику пожежонебезпеку. Електротехнічні вироби, враховуючи їх значне горюче навантаження, можуть сприяти поширенню пожежі, і, крім того, бути й причиною її виникнення. Найбільш пожежонебезпечними з них вважаються електричні кабелі, проводи та шнури, які, маючи значне горюче навантаження, підтримують горіння та сприяють поширенню вогню на значну відстань. Найбільшою причиною загоряння кабельної продукції є короткі замикання та перевантаження електромережі. При короткому замкненні сила струму у провідниках стрімко зростає та досягає сотень і тисяч ампер. Тому, по усій довжині кабелю (проводу) виділяється теплова енергія, величина якої сягає десятків і сотень кДж, що призводить до займання горючих ізоляційних матеріалів. До того ж, перевантаження мережі прискорює процес старіння ізоляції. Інтенсивність нагрівання залежить від величини та часу дії електричного струму на провідник та площі його поперечного перерізу. Підвищення температури провідників скорочує термін їх експлуатації. Старіння (знос) ізоляції супроводжується зміною її захисних та механічних якостей. Вона стає крихкою, здатною ламатися та тріскатися, що може призвести до її пробою та короткого замикання. Таким чином, одним із актуальних завдань є проведення профілактичних заходів, які забезпечать необхідну експлу-

атацію мережі, починаючи вже з її проектування, монтажу та експлуатації. Проблеми забезпечення надійності та безпеки систем електропостачання України при аварійних ситуаціях на енергетичних, промислових та цивільних об'єктах на сьогодні вирішуються в умовах жорстких фінансових вимог, що висуваються до вартості відповідних технічних рішень.

В Україні необхідність щодо застосування вогнезахисних засобів для кабелів і будівельних конструкцій на енергетичних підприємствах регламентована наступними нормативними документами: НАПБ В.01.056-2013/111 Правила будови електроустановок. Пожежна безпека електроустановок. Інструкція; НАПБ 05.028-2004 Протипожежний захист енергетичних підприємств, окремих об’єктів та енергоагрегатів. Інструкція з проектування і експлуатації; НАПБ В.01.061-2011/111 Протипожежний захист машзалів електростанцій. Правила проектування та експлуатації протипожежного устаткування; НАПБ В.05.023-2005 Інструкція щодо застосування вогнезахисних покриттів для кабелів у кабельних спорудах тощо.

Таким чином, необхідно проводити комплексні наукові та практичні роботи щодо визначення методів зниження пожежної небезпеки окремих складових систем електропостачання, які будуть мати невисоку вартість. Особливе значення набуває порівнювальне оцінювання пожежної небезпеки кабельних виробів зі струмовідними жилами із різних матеріалів, серед яких найпоширеними є мідь та алюміній.

На даний час світова ціна 1 тони міді більш ніж у 3,5 рази дорожча за 1 тонну алюмінію. При цьому, значення електричного опору алюмінію вище, ніж міді у 1,64 рази. Тому, температура нагрівання кабелю з алюмінієвою жилою, при проходженні по ньому електричного струму, буде вищою у порівнянні з температурою нагрівання кабелю з мідною жилою в аналогічних умовах. Жили кабельних виробів виготовляються з електролітичної міді М0 та М1, яка відрізняється певною чистотою – 99,95 % та 99,90 % – відповідно. Різні домішки до міді потенційно спроможні знижувати її провідну здатність, збільшувати міцність або надавати певний комплекс змін властивостей. Наприклад, мідь з домішкою кисню має кращу пластичність, ніж мідь марок М1 і М0, з домішкою миш'яку – знижену електричну провідність, з домішкою сурми – знижені теплопровідність, електропровідність та пластичність.

Також, струмовідні жили виробляються на основі алюмінію марок А1 та А2, які характеризуються наявністю незначних домішок заліза та кремнію. Дані домішки погіршують провідність жили. До інших небажаних елементів у складі жил відносять: титан, ванадій, марганець та магній. Температура струмопровідної жили як з міді, так і з алюмінію залежить від сили струму, що протікає, від температури навколишнього середовища, діаметра жили та ізоляції провідника, теплообміну з навколишнім середовищем, питомого опору матеріалу провідника, часу роботи тощо. Діелектричні властивості ізоляції кабельних виробів швидко втрачаються за високих температур: ізоляційний полівінілхлоридний пластикат витримує нагрів до +70 °С; гумова ізоляція – до +80 °С; кремнійорганічна ізоляція – до +180 °С. У процесі експлуатації можуть досягатися значення температури, які призводять до займання ізоляції кабельного виробу, що може спричинити пожежу. Отже, визначення діапазону нагріву кабельних виробів зі струмовідними жилами з різних матеріалів дозволяє оцінювати пожежну небезпеку цих виробів.

Таким чином, за результатами отриманих розрахунків можливо оцінити вплив домішок у матеріал жили на температуру нагрівання кабелів та проводів, а також визначити додаткові напрямки застосування кабельних виробів з алюмінієвими жилами, які є більш дешевими, ніж аналогічні вироби з мідними жилами.

Список використаних джерел

1. Катунін А.М., Коломійцев О.В., Лазня О.О., Кожушко М.І. (2023). Оцінка впливу матеріалу ізоляції проводу на його температуру нагрівання в процесі експлуатації. *Міжнародний науковий журнал «Грааль науки» № 28* (червень, 2023) : за матеріалами І

Міжнародної науково-практичної конференції «Science in motion: classic and modern tools and methods in scientific investigations», що проводилася 9 червня 2023 року ГО «Європейська наукова платформа» (Вінниця, Україна) та ТОВ «International Centre Corporative Management» (Відень, Австрія). С. 151-156. https://doi.org/10.36074/grail-of-science.09.06.2023.

2. Катунін А.М., Коломійцев О.В., Коломійцев В.О. Дослідження впливу матеріалу ізоляції на температуру кабельного виробу в процесі експлуатації. *XXXI Міжнародна науково-практична конференція MicroCAD-2022. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я.* 17-20 травня 2023 р. – Харків: НТУ «ХПІ». – 2023. – С. 1171. http://repositsc.nuczu.edu.ua/handle/123456789/18811.

3. A. Katunin, O. Kolomiitsev, O. Kulakov, H. Heiko and I. Rudakov, "Information technologies for calculating the effect of wire thickness and insulation material on its heating temperature during operation," *2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek)*, Kharkiv, Ukraine, 2023, pp. 1-5, doi: 10.1109/KhPIWeek61412.2023.10311586.

4. Катунін А.М. Оптимізація задач зниження пожежної небезпеки кабельної продукції / А.М. Катунін, О.В. Коломійцев // Проблеми інформатики та моделювання (ПІМ–2023) : тези 23-ї міжнар. наук.-техн. конф., Харків – Одеса, 20-22 вересня 2023 р. / наук. ред. В. Д. Дмитрієнко ; Нац. акад. наук України [та ін.]. – Харків : Контраст, 2023. – С. 57. URI https://repository.kpi.kharkov.ua/handle/KhPI-Press/70163.

УДК 623.5:623.4

Качуровський Г.М., Оборонов М.І., Ставицький О.М., Косенко Г.П., Константинов С.О.

ВИКОРИСТАННЯ КІЛЬЦЕВИХ ПРИЦІЛІВ ДЛЯ ВЕЛИКОКАЛІБЕРНИХ КУЛЕМЕТІВ, ЯКИМИ ОЗБРОЄНІ МОБІЛЬНІ ВОГНЕВІ ГРУПИ ПО ПРОТИДІЇ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТАМ

В доповіді представлено пропозиції щодо підвищення дійсності стрільби по безпілотним літальним апаратам мобільних вогневих груп озброєних великокаліберними кулеметами з використанням кільцевих прицілів в якості прицільних засобів.

У ході повномасштабної збройної агресії російської федерації проти України, противником масово застосовуються в якості засобів повітряного нападу безпілотні літальні апарати (БпЛА) різних типів, які несуть реальну загрозу озброєнню та особовому складу частин та підрозділів ЗС України.

На поточний момент одними з типових БпЛА являються "Орлан-10", "Шахед-136". Дані БпЛА являються малорозмірними цілями з малими кутовими розмірами в картинній площині стрільби (КПСтр).

Поширене застосування великокаліберних кулеметів (ВКК) на зенітних кулеметних установках (ЗКУ), в якості озброєння мобільних вогневих груп (МВГ) для протидії нальотам БпЛА, потребує оцінки ефективності застосування та розгляду шляхів з її підвищення.

Обмеженням дальності виявлення та наведення по кутам являється статична роздільна здатність людського ока в 1 кут. хв. Обмеженням для дальності оцінки результатів стрільби (роздільне розрізнення трас куль та цілі) складає ~5 кут. хв (з врахуванням впливу контрастної чутливості при осліпляючій дії яскравості фону). В зворотному випадку навідник ЗКУ не зможе відрізнити факт наведення, влучання, промаху в КПСтр.

Тому, є доцільним у якості прицільного пристрою використовувати оптичні прилади зі збільшенням видимого зображення замість штатних, які є без збільшення.

Аналіз впливу похибок наведення свідчить про безпосередній вплив на дійсність стрільби та неможливість компенсації коректурою під час стрільби. Тому даний тип похибок завжди потребує мінімізації. Використання оптичних приладів зі збільшенням видимого зображення дозволяє кратно зменшити похибки наведення.

У більшості випадків зенітним прицілом в ЗКУ являється реалізація одного із типів кільцевого прицілу: горизонтально розташований, ракурсний.

Для вказаних типів прицілів, для підвищення дійсності стрільби, окрім похибок наведення, необхідна мінімізація наступних похибок: визначення швидкості; визначення курсу та розрахунку ракурсної швидкості; прицільної дальності.

Похибку визначення швидкості можливо зменшити шляхом перерахунку шкал кільцевих прицілів для актуальних швидкостей БпЛА (на поточний момент шкали градуюванні для швидкостей кратно більших).

Похибки визначення курсу та розрахунку ракурсної швидкості визначаються безпосередньо типом кільцевого прицілу.

При горизонтальному положенні площини кілець переднього візира завдання зустрічі кулі з ціллю вирішується відповідно до гіпотези, що протягом упереджувального часу рух цілі горизонтальний, прямолінійний та рівномірний.

Для ракурсного прицілу (кільцевий візир встановлений перпендикулярно до віссі візування) завдання зустрічі вирішується відповідно до гіпотези, що протягом упереджувального часу рух цілі прямолінійний і рівномірний в будь-якій площині.

Основною перевагою стрільби з горизонтальною установкою кільцевого візира є здійснення врахування курсу цілі в процесі самого наведення шляхом вибору відповідної точки візування на самому кільці, тому окрім визначення курсу цілі окремі розрахунки відносно курсу (ракурсу) цілі не потрібні.

При використанні ракурсного прицілу необхідно окрім визначення курсу цілі провести розрахунок ракурсної швидкості шляхом перемноження дійсної швидкості цілі на визначений ракурс цілі з подальшим вибором точки прицілювання на відповідне кільце сітки прицілу.

Гіпотеза, що протягом упереджувального часу рух цілі горизонтальний, прямолінійний та рівномірний цілком відповідає характеру руху БпЛА типу “Орлан-10”, “Шахед-136”. Тому для таких цілей горизонтальне розташування площини кілець переднього візира є доцільним та нівелює похибку в розрахунку ракурсної швидкості, врахування курсу цілі здійснюється в процесі самого наведення шляхом вибору відповідної точки візування. Використання горизонтально розташованого кільцевого прицілу сприяє зменшенню вимог до навичок навідника в прицілюванні.

Поширеність застосування прицільних сіток, що відповідають випадку горизонтального розташування кільцевого візира з фіксованим (найбільш очікуваним) кутом місця цілі пов’язана з простотою реалізації прицілу і швидкістю виконання прицілювання. Внесені похибки усуваються коректурою стрільби.

Швидкоплинність протиповітряного бою, відсутність автоматичного визначення і врахування у прицільних засобах дальності до цілі призвело до відмови від ручного введення в приціл дальності до цілі Прицільні засоби виконуються з фіксованою розрахунковою дальністю до цілі. Внесену похибку, між дійсною дальністю і розрахунковою, швидше і практичніше усунути коректурою стрільби, ніж зміною налаштування прицілу за дальністю під час бою.

Окремим чинником зменшення похибок наведення є порядок спорядження боєприпасів. В зв’язку з низькою (для зенітної стрільби) скорострільності більшості ВКК (до 800 пострілів на хвилину), стандартний порядок споряджання трасуючих та не трасуючих куль в пропорції 1:4 недостатній для швидкої коректури стрільби навідником в умовах швидкоплинності протиповітряного бою. Пропонується змінити пропорцію на

1:1 (1:2).

На дійсність стрільби суттєво впливає номенклатура застосованих боєприпасів. Застосування куль з осколково-фугасною дією (тип кулі МДЗ) підвищує дійсність стрільби, при всіх інших рівних.

Таким чином, проведено аналіз та розроблено пропозиції з підвищення дійсності стрільби ЗКУ, озброєних ВКК, по БпЛА типу “Орлан-10”, “Шахед-136”, а саме:

- використання оптичних приладів зі збільшенням видимого зображення для кратного зменшення похибок наведення;
- перерахунок шкал швидкості кільцевих прицілів відносно актуальних швидкостей БпЛА для зменшення похибок визначення швидкості;
- використання горизонтально розташованого кільцевого прицілу для нівелювання похибок розрахунку ракурсної швидкості та зменшення вимог до навичок навідника ЗКУ;
- порядок споряджання трасуючих та не трасуючих куль встановити в пропорції 1:1 (1:2) для швидкої коректури стрільби навідником;
- використання в номенклатурі застосованих боєприпасів куль з осколково-фугасною дією.

УДК 621.396.96

Квашенко В.Р., Пастушенко М.С

ТЕХНІЧНІ ЗАХОДИ ВИЯВЛЕННЯ ТА УСУНЕННЯ СИНТЕЗОВАНОГО ГОЛОСУ В СИСТЕМАХ ГОЛОСОВОЇ АВТЕНТИФІКАЦІЇ

В умовах постійного розвитку технологій голосова автентифікація зайняла провідне місце серед методів біометричної автентифікації. Так і як з більшістю нових відкриттів, також було створено системи, які можуть обходити голосові системи автентифікації, використовуючи синтезований голос [1-3].

Проблема з виявленням синтезованої мови є особливо складною через широкий арсенал доступний методів генерації синтезованого голосу. Синтезована мова може бути отримана простими методами конкатенації звукових хвиль з існуючого голосового зліпку, можна знайти готові рішення з підробки голосу в мережі інтернет з відкритим вихідним кодом і використати згенеровані голосові зліпки для видачі себе за іншу людину під час голосової автентифікації.

У цій роботі розглядається метод розпізнавання синтетично згенерованої мови. Полягає задача, за наявним аудіозаписом, у визначенні чи є він синтезований, тобто, сгенерований, за допомогою певних алгоритмів, або ж ні. Для цього пропонується набір дескрипторів заснованих на короткостроковому та довгостроковому аналізу зміни сигналу з часом. Так як голосові сигнали можна програмно інтерпретувати, тому можна відокремити важливу інформацію вивчаючи зв’язок попарно порівнюючи фрагменти аудіозразків. Для порівняння використовується процес, що поєднує короткостроковий і довгостроковий аналіз мовних сигналів.

Короткостроковий аналіз – ця частина процесу зосереджена на аналізі мовного сигналу протягом коротких сегментів, які зазвичай охоплюють лише кілька мілісекунд. Мета полягає в тому, щоб зафіксувати спектральні властивості мови, які швидко змінюються з часом, наприклад, частоти та амплітуди звукових хвиль, що виробляються голосовим трактом людини. Короткостроковий аналіз часто включає в себе розрахунок помилки короткострокового прогнозування, яка вимірює, наскільки добре модель мовного сигналу може передбачити майбутні патерни на основі минулих патернів в межах цих коротких сегментів. Це має вирішальне значення для ідентифікації швидко змінних

характеристик мови, які можуть вказувати на те, чи є вона синтетичною чи справжньою.

Довготривалий аналіз –досліджує мовний сигнал протягом більш тривалих періодів, часто від декількох десятків мілісекунд до декількох секунд. Цей аналіз має на меті зафіксувати особливості мовлення, які є більш стабільними в часі, такі як висота тону (основна частота) і гармонійна структура, які вказують на голос мовця і його мовленнєві патерни. Довгостроковий аналіз може включати розрахунок помилки довгострокового прогнозування, яка оцінює, наскільки добре можна передбачити мовний сигнал протягом цих довших сегментів. Це допомагає визначити періодичність та інші довгострокові характеристики, які характерні для людського мовлення, але можуть бути відсутніми або відрізнятися в синтезованій мові.

Таким чином, даний алгоритм зможе зменшити кількість успішних авторизацій з використанням синтезованого голосу , після імплементації в голосові системи автентифікації.

Для досягнення максимальної ефективності алгоритму критично важливим є вибір оптимальних дескрипторів та параметрів класифікації, що потребує глибокого аналізу характеристик мовного сигналу та експериментування з різними методами вирізнення таких характеристик. Такий підхід забезпечить ефективне розрізнення справжнього та синтетичного голосу, а дослідження методів вирізнення характеристик мовного сигналу стане логічним продовженням досліджень у цій області.

Список використаних джерел

1. Pastushenko, M., Pastushenko, V., Pastushenko, O. (2019), "Specifics of Receiving and Processing Phase Information in Voice Authentication Systems", International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kyiv, Ukraine, 2019, pp. 621-624**.** DOI: 10.1109/PICST47496.2019.9061260

2. Pastushenko, M., Krasnozheniuk, Ya., Lemeshko, O. (2020), Analysis of voice signal phase data informativity of authentication system // Zaporizhzhia, Ukraine, April 27-May 1, 2020. Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020). PP 1040-1053.URI: http://openarchive.nure.ua/handle/document/11843

3. Pastushenko, M., Krasnozheniuk, Ya., Zaika, M. (2020), "Investigation of Informativeness and Stability of Mel-Frequency Cepstral Coefficients Estimates based on Voice Signal Phase Data of Authentication System User," International Conference "Problems of Infocommunications. Science and Technology" (PIC S&T′2020), pp. 1-5. DOI: 10.1109/PICST51311.2020.9468083

УДК: 355.451:004.7

Кізло Л.М., Пашковський В.В., Перемибіда Д.О., Жук О.В.

ТРАНСФОРМАЦІЯ СИСТЕМИ КІБЕРЗАХИСТУ В УКРАЇНІ В УМОВАХ ПОВНОМАСШТАБНОЇ РОСІЙСЬКОЇ АГРЕСІЇ: ОСОБЛИВОСТІ, ТЕНДЕНЦІЇ

Після початку повномасштабної агресії рф проти України українські кіберфахівці перебувають на передовій кібервійни де пріоритетом для держави є безпечний кіберпростір. Держава зацікавлена, щоб послуги були безпечними, саме тому важливо забезпечити дотримання усіма (об’єктами і суб’єктами) достатнього рівня кіберзахисту.

У теперішній час війна в Україні відбувається не лише на фізичному фронті, а й у інформаційному полі. Загарбники здійснюють кібератаки не лише на урядові структури – жертвами зламів і викрадення даних стають і пересічні громадяни. Ворог намагається

отримати доступ до персональних даних та державних реєстрів через приватні комп'ютери чи мобільні телефони. Українці масово отримують листи із шкідливою програмою, яка викрадає паролі й файли.

Реалії українського сьогодення зумовили створення та постійне нарощення вітчизняних кібервійськ з метою як захисту критичної інформаційної інфраструктури від кібератак, так і задля реалізації превентивних наступальних кібероперацій (до прикладу, DDoS-атаки на корпоративні, інформаційні та державні сайти противника, виведення з ладу критично важливих об’єктів інфраструктури росії, компрометація баз даних телекомунікаційних, роздрібних та урядових організацій, й інше).

Російські хакери не тільки збільшили кількість атак проти України (у 2,8 рази, порівнюючи 2022 та 2023 рік), а й атакують також Європу та весь цивілізований світ. Тому Європа особливо детально вивчає наш досвід і вже зараз посилює повноваження власних відповідальних органів у зв'язку зі збільшенням кількості атак і зміною тактики російських хакерів. Україна теж рухається у цьому фарватері та вдосконалює свою діяльність в умовах війни. Ворог теж вчиться, якщо раніше агресор намагався безпосередньо атакувати об'єкти критичної інфраструктури за допомогою фішингу, то з другої половини 2022 року вони почали намагатися використовувати технічні вразливості установ, які надають послуги операторам критичної інформаційної інфраструктури.

Враховуючи вищезазначене правомірно стверджувати, що кібербезпека є складовою національної безпеки країни, а кіберстійкість – основою її гарантування. В умовах війни питання безпеки кіберпростору стає особливо важливим, оскільки ворог перестає керуватися моральними принципами. Їх головна мета – дестабілізація ситуації в країні, знищення "незручної" для них інформації, знищення або замороження техніки, інформації. До того ж доцільно пам’ятати, що загрози щоденно змінюються, тому слід постійно удосконалювати систему захисту.

Побудувати систему захисту один раз і сподіватися, що вона завжди допомагатиме – не найкраща стратегія. Варто пам’ятати, що ефективна кібербезпека складається з багатьох компонентів, серед яких важливу роль відіграє інформування співробітників та службовців. Адже значна частина атак починається через те, що люди не знають та не дотримуються правил кібергігієни, не кажучи вже про здатність швидко й правильно реагувати на нестандартну ситуацію в кіберпросторі. Проте, у теперішній час інформаційний простір дозволяє людині бути на зв'язку з рідними, дізнаватись останні новини з фронту, хоч якось контролювати те, що відбувається навколо. Для підлітків Інтернет залишається світом розваг та спілкування з друзями. Але важливо пам'ятати, що за позначкою геолокації на пості чи фотографії, веселим відео в соціальній мережі чи одним повідомленням може ховатися справжня небезпека. Особливо під час війни, коли інфопростір використовують окупанти для військових нападів на українські міста. Тому, для більшості країн світу важливим стало створення і постійне зміцнення вітчизняних кіберкордонів, нарощення кіберсил та інформування власних громадян щодо застосування цифрової грамотності, дотримання цифрового етикету та правил кібергігієни.

Реалізація цих та інших завдань ІТ спрямованості в умовах воєнного стану набуло для України особливого стратегічного значення. Національна система кібербезпеки України перебуває лише в процесі становлення, однак російським кіберзагарбникам досягти стратегічної мети й завдати значної шкоди критичній інфраструктурі нашої країни не вдається. Правда в тому, що росія недооцінила Україну не тільки у військовій, але й у кібергалузі. Створення кіберсил – це наступний важливий крок, навіть попри те, що ще з початку війни фахівці в сфері ІТ -технологій з усієї країни долучилися до кіберполіції, чим обумовили створення вже діючої кіберармії.

Вже з перших днів російсько-української війни добровольча ІТ-армія України налічувала 175 тис учасників з усього світу: від білих хакерів та хактивістів до представників різних технологічних компаній, серед яких, зокрема, SpaceX, а також міжнародна сітка активістів і “хакеристів” Anonymous Collective. Парадокс ситуації, що склалася,

полягав у тому, що досі жодному уряду в світі не вдавалося завербувати незалежних іноземних суб'єктів (кандидатів) до настільки глобального волонтерського кіберутворення та ще й добровільно. Незважаючи на те, що в Збройних силах України вже є кібервійська, котрі реально працюють, утім досі перебувають на етапі формалізації у правовому полі та складаються, здебільшого, із самоорганізованих добровольців та представників різних держорганів.

В умовах повномасштабної війни проти України зі значною гібридною складовою цифрові засоби масової комунікації та соціальні Інтернет-сервіси широко використовуються противником для здійснення деструктивного інформаційно-психологічного та кібервпливу на військово-політичне керівництво, особовий склад та населення країни, в цілому. Кожна сучасна соціально активна людина і в світі і в Україні використовує мобільні пристрої та користується Інтернетом, державні органи переходять на електронний документообіг, стабільна діяльність банківського сектору, залізниці й авіатранспорту, великих підприємств залежить від стабільності кіберпростору, з яким вони працюють, та базується на комунікації за допомогою електронних засобів зв'язку. Отже, аналіз вразливості окремого користувача, залежно від розміщеної ним у соціальних мережах інформації, є актуальним, а розроблення методів захисту від деструктивного кібервпливу дозволятиме створити ефективну систему виявлення та протидії їм.

Тема кіберзахисту важлива в наш час як для України, так і глобально, враховуючи світові тренди та агресивну війну, яку розв'язала росія. Щодня ворог атакує нас у кіберпросторі. Тож особливо цінними є рекомендації фахівців, які можуть поділитися корисними знаннями та цікавими думками і допомогти захистити себе, бізнес та держструктури від кібератак".

До того ж, регулярні консультації та тренінги створення надійної політики безпеки можуть обмежити виток конфіденційної інформації через працівників. Тому, для забезпечення інформаційної захищеності під час війни слід дотримуватися таких простих організаційних або управлінських правил, а саме:

1. Пересвідчитись, що співробітники мають доступ до надійних та перевірених джерел інформації щодо поточної ситуації і є обізнаними щодо ризиків фішингу та шахрайських вебсайтів з тематики війни в Україні.

2. Надавати поради з кібербезпеки для співробітників, що знаходяться в місцях потенційного ризику, працюють у правоохоронних органах або на державних посадах у секторі оборони.

3. Забезпечити термінове додаткове підтримання управління звичайними функціями безпеки, аналізу збільшеного обсягу сповіщень, особливо в умовах військового стану, тощо.

Утім говорити сьогодні про перемогу в кібервійні в Україні ще зарано, і надалі потрібно докладати більше спільних зусиль, щоб результативно протидіяти кіберзагрозам. Кіберстійкість країни багато в чому залежить саме від злагодженої взаємодії означених вище суб'єктів національної системи кібербезпеки на всіх рівнях. Водночас, наявність міцного законодавчого підґрунтя та вчасна адаптація останнього до нових кібервикликів сучасності, очікувано, підвищить спроможність України ефективно стримувати деструктивні дії в кіберпросторі.

Ці та інші питання особливо актуалізуються для нашої держави зараз – у період війни, саме тому потрібно докласти зусиль для реформування вітчизняного законодавства в кіберсфері, з метою наділення його здатністю гнучко адаптуватися до нових змін безпекового середовища, що в свою чергу, гарантуватиме злагоджене функціонування національного сегмента кіберпростору в цілому. Для цього потрібно оптимізувати процес взаємодії між основними суб'єктами національної системи кібербезпеки України, а також налагоджувати конструктивне і швидке міжнародне співробітництво, активно працюючі з інноваціями, які розвиваються щодня.

Нині Україна перебуває на передовій кібервійни. І хоча ці обставини негативно впливають на наше життя, їх можна використати для тестування нових ідей та технологій у галузі захисту інформації. Досвід, який ми здобуваємо в боротьбі з ворогом, робить наших кіберспеціалістів лідерами галузі на світовому ринку а державна політика у сферах національної безпеки й оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо. Правові норми, орієнтовані на забезпечення національної кібербезпеки як пріоритетного напряму реалізації національної політики України, мають публічно-правову природу й становлять міжгалузевий правовий інститут у системі права України, який регулює інформаційні суспільні відносини в секторах національної інформаційної безпеки, виборчої системи, медицини, оборони, транспорту, фінансово-банківської сфери тощо та забезпечує інформаційний суверенітет держави як суб'єкта міжнародного права загалом.

Отже галузь кіберзахисту у нашій державі і надалі активно зростатиме та залучатиме нові таланти, і настане час, коли ми зможемо повноцінно поділитися набутим знаннями зі світом. Варто підкреслити, що виконання зазначених шляхів стосовно нарощення кіберпотужностей і захисту кіберпростору здатне вивести Національний індекс кіберезпеки (NCSI) України у лідируючі позиції в світі.

Таким чином, основними напрямами, які негативно впливають на рівень кіберстійкості України, правомірно визначити низький рівень захисту цифрових послуг, недостатній рівень внеску у глобальну кібербезпеку та нерозвинений напрям військових кібероперацій. Водночас, враховуючи, що у 2022 році Україна прийнята до складу Об'єднаного центру передових технологій з кібероборони НАТО як учасник-контрибутор, відмічаючи активний процес формування кібервійська доцільно відмітити значний потенціал країни у сфері кібербезпеки та можливості його реалізації в майбутньому.

Кільдеров Д.Е., Приходько Ю.І., Скворок І.М.

АКТУАЛЬНІ ПРОБЛЕМИ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ В УМОВАХ ВОЄННОГО СТАНУ

Важливим завданням розвитку вищої освіти є її трансформація у сектор безпеки та оборони відповідно до доктринальних підходів та принципів НАТО. Трансформація сучасної системи військової освіти передбачає професіоналізацію Збройних Сил та інших складових сил оборони, інтеграцію органів управління військовою освітою, мережі військових навчальних закладів, діючих стандартів освіти, професійних стандартів і нормативно-правової бази в єдиний комплекс складових системи військової освіти для забезпечення сил оборони військовими фахівцями [1; 6].

Професіоналізація військової освіти передбачає формування сучасної моделі професійної військової освіти, що забезпечує підготовку військових фахівців на основі їх безперервного професійного розвитку, враховує загальні тенденції розвитку системи національної та міжнародної безпеки, зміни принципів та способів ведення збройної боротьби, нові вимоги до якості військової освіти, формування доброчесності на основі стандартів НАТО.

Підготовка військових фахівців, яка мала місце в умовах мирного часу, має оперативно трансформуватись в умовах агресії РФ проти України в напрямах нагальних потреб Збройних Сил (далі – ЗС) України, які ведуть бойові дії [5]. В першу чергу, це стосується диверсифікації системи підготовки військових фахівців усіх категорій і освітніх ступенів, запровадження прискорених моделей їх підготовки з метою достатнього забезпечення ЗС України кадровим персоналом і ведення ними бойових дій з високою ефекти-

вністю, що, на нашу думку, пов'язано з такими чинниками: 1) оптимізацією організаційно-штатних структур і діяльності вищих військових навчальних закладів (далі – ВВНЗ), навчальних центрів (далі – НЦ), наукових установ з дослідження сучасних проблем ЗС України, системи військової освіти і науки, воєнного мистецтва тощо; 2) переглядом організаційних, процесуальних засад і термінів підготовки військових фахівців, змісту їх теоретичного та практичного навчання.

Окреслимо узагальнені напрями (підходи, моделі) підготовки військових фахівців усіх категорій і освітніх ступенів: 1) фундаментальний, дослідно-конструкторський з перспективою служби в наукових і конструкторських установах з розроблення озброєння та військової техніки наступних поколінь (офіцери; ВВНЗ); 2) експлуатаційний – з новітніх систем озброєння та військової техніки (офіцери; ВВНЗ, НЦ); 3) прискорена підготовка за різними термінами (офіцери; ВВНЗ); 4) підготовка, допідготовка офіцерів запасу (ВВНЗ, НЦ); 5) підготовка сержантського складу (ВВНЗ, коледжі); 6) підготовка рядового та сержантського складу (НЦ); 7) підготовка усіх категорій військових фахівців у військових навчальних закладах і навчальних центрах країн-партнерів.

З окреслених напрямів особливого значення набуває запровадження підготовки військових фахівців з вищою освітою з фундаментальних, військово-технічних знань за спеціальностями (спеціалізаціями) дослідницької, конструкторської діяльності з акцентом на перспективні наукові технології з розроблення нових зразків озброєння та військової техніки. На теперішній час практично всі фахівці у ВВНЗ готуються в основному на базі застарілих і модернізованих зразків озброєння та військової техніки, а також на окремих зразках озброєння та військової техніки країн-членів НАТО. Як тимчасовий вихід, – з цим можна погодитись. Щодо перспективи – це шлях в нікуди, адже збройні сили провідних країн світу засвоюють озброєння та військову техніку 4-5 поколінь на основі нових фізичних принципів із використанням квантових, інформаційних, космічних, гіперзвукових, кібербезпекових, біологічних технологій, а також технологій у сфері штучного інтелекту, створення нових матеріалів, робототехніки та автономних безпілотних апаратів. Пройде небагато часу і ЗС України досягнуть такого стану, але до цього треба готуватись заздалегідь. Саме тому проблема підготовки зазначених вище фахівців у ВВНЗ видів ЗС України, родів військ, спеціальних військ потребує нагального вирішення, а саме: формування переліку спеціальностей (спеціалізацій); розроблення військових освітніх стандартів, освітньо-професійних програм, програм навчальних дисциплін; розроблення всебічного наукового, інформаційного, технологічного, навчально-методичного забезпечення; створення матеріально-технічної бази.

В умовах протистояння збройній агресії РФ зростають вимоги до організаційних засад підготовки офіцерів запасу у ВВНЗ, військових навчальних підрозділах закладів вищої освіти (далі – ВНП ЗВО) [2; 3; 4], а саме :

– оптимізувати замовлення на підготовку офіцерів запасу відповідно до потреб ЗС України в умовах воєнного часу;

– впровадити обов'язковий для проходження курс з процедур планування та прийняття рішень за стандартами НАТО на тактичному рівні (TLP, MDMP)

– переглянути програми підготовки офіцерів запасу за військово-обліковими спеціальностями, які затребуванні на теперішній час для поповнення потреб мобілізаційного ресурсу в офіцерському складі військових частин, що ведуть бойові дії. В першу чергу, це стосується таких напрямів [5]: створення системи кібероборони для ведення протиборства в інформаційному просторі (включаючи кіберпростір); здатність до забезпечення ефективного кіберзахисту власної інформаційної інфраструктури (критичної інформаційної інфраструктури); проведення превентивних дій щодо виявлення, реагування на кібератаки та інциденти кібербезпеки, усунення їх наслідків в умовах ведення противником кіберрозвідки та інтенсивного кібервпливу (кібератак); здатність до ведення кіберрозвідки та кібердорозвідки в інформаційно-телекомунікаційних мережах та системах; здатність організовувати підготовку та проводити кібердії (кібервпливи, кі-

бератаки) із застосуванням усіх видів кіберзброї або захоплення (виведення з ладу, отримання контролю), заподіяння шкоди (каскадний ефект), порушення функціонування об'єктів критичної та інформаційної інфраструктури противника з одночасним приховуванням слідів своєї діяльності в кіберпросторі;

– спрямувати підготовку фахівців механізованих і танкових військ на вивчення не лише тактики лінійних загальновійськових підрозділів, але й мотопіхотних, стрілецьких, штурмових підрозділів та підрозділів Сил територіальної оборони ЗС України;

– здійснювати завершальну частину підготовки офіцерів запасу зі специфічних військово-облікових спеціальностей на базі спеціалізованих навчальних центрів;

– оптимізувати терміні підготовки офіцерів запасу на період воєнного стану, ведення протистояння російській агресії, зокрема, перейти на річну програму підготовки офіцерів запасу із застосуванням модульної системи навчання;

– застосовувати сучасні інформаційно-комунікаційні і кібербезпекові технології;

– здійснювати підтримання рівня теоретичних знань та практичних навичок офіцерів після завершення навчання та під час перебування у резерві на основі програми перепідготовки офіцерів, яка передбачатиме проведення періодичних навчальних зборів офіцерів запасу перед кожним їх призначенням на вищу посаду чи підвищенням у військовому званні;

– ефективніше застосовувати контрольно-діагностичні, моніторингові процедури при оцінюванні якості підготовки офіцерів запасу та освітнього процесу;

– провести модернізацію матеріально-технічної бази ВВНЗ, ВНП ЗВО, що здійснюють підготовку громадян України за програмою підготовки офіцера запасу, сучасними національними та іноземними зразками озброєння та військової техніки, комп'ютерними навчальними комплексами на основі штучного інтелекту.

На теперішній час зростають вимоги до якості підготовки офіцерів запасу, а саме :

– підготовка компетентних, психологічно стійких військових фахівців з лідерськими якостями, здатних керувати підлеглим особовим складом як у мирний, так і у воєнний час;

– здобуття офіцерами глибоких теоретичних знань та практичних навичок з експлуатації та застосування новітніх систем озброєння та військової техніки, зокрема, безпілотних літальних апаратів;

– вироблення у фахівців готовності до прийняття самостійних рішень на ведення бою за непрогнозованих змін тактичної обстановки, застосування противником різних типів озброєння та готовності нести відповідальність за прийняте рішення;

– створення умов для здобуття навченості офіцерами аналізувати бойову обстановку, організовувати виконання бойових завдань, здійснювати всебічне забезпечення особового складу;

– вироблення у офіцерського складу творчого підходу, гнучкості, критичного аналізу при оцінці бойової обстановки з урахуванням сучасних поглядів на форми і способи застосування військ (сил);

– набуття офіцерами вмінь знаходити й узагальнювати інформацію для прийняття оптимальних рішень.

Список використаних джерел

1. Концепція трансформації системи військової освіти : Постанова Кабінету Міністрів України від 15 грудня 1997 р. № 1410 (в редакції Постанови Кабінету Міністрів України від 30 грудня 2022 р. № 1490). URL: https://zakon.rada.gov.ua/laws/show/1410-97-%D0%BF#Text

2. Камалов Є.В. Обгрунтування рекомендацій з підвищення ефективності військової підготовки громадян України : дисертація доктора філософії. Київ: Національний університет оборони України імені Івана Черняховського, 2021.

3. Кас’яненко М. Аналіз проблем професійної підготовки громадян України за програмою підготовки офіцерів запасу. Social Development and Security. Vol. 10, No 5., Kyiv, 2020. С. 161–168.

4. Про основи національного спротиву. Закон України від 16.07.2021 р. № 1702-IX. Відомості Верховної Ради (ВВР), 2021, № 41. Ст.339 (Із змінами, внесеними згідно із Законами України 2022-2023 рр.).

5. Стратегічний оборонний бюлетень України: Указ Президента України від 17 вересня 2021 р. № 473/2021. URL: https://zakon.rada.gov.ua/laws/show/473/2021#n17

6. Стратегія менеджменту військової освіти: Затверджена Міністром оборони України 12.12.2023 р. URL: https://www.facebook.com/photo?fbid=672850318365064&set=pcb.672850445031718

УДК 621.39:623.1/.7

Кісіль О.А., Коробков Ю.В., Резніченко О.А.

ПРОПОЗИЦІЇ ЩОДО ПРИСТРОЮ ВИЯВЛЕННЯ БАЛІСТИЧНИХ ЦІЛЕЙ ПРИЙМАЧА ВИЯВЛЕННЯ СИГНАЛУ 1Б БАГАТОКАНАЛЬНОЇ СТАНЦІЇ НАВЕДЕННЯ РАКЕТ ЗЕНІТНОГО РАКЕТНОГО КОМПЛЕКСУ С-300В1

Ведення сучасних бойових дій характеризується впливом противника балістичними ракетами на важливі об’єкти [1-12].

За результатами аналізу балістичних засобів нападу, можна зробити наступні висновки:

а) оцінка локальних війн та збройних конфліктів сучасності показала суттєве зростання ролі балістичних ракет у вирішенні завдань високоефективного вогневого ураження;

б) з досвіду російсько-Української війни слідує широке застосування рф балістичних та аеробалістичних засобів для ураження об'єктів військової та цивільної інфраструктури;

в) огляд характеристик балістичних та аеробалістичних засобів ураження рф показав, що данні типи озброєння можуть бути цілю для ЗРК С-300В1

Приймальний пристрій виявлення сигналом 1Б призначений для посилення й обробки імпульсного сигналу 1Б тривалістю 360 мкс, передбаченого для роботи по балістичних цілях у режимі БРБ. Вихідна інформація при цьому видається в СЦОМ-2 і використовується для грубої цілевказівки по швидкості при переході на виявлення сигналом ІІТ. Апаратура приймального пристрою виявлення сигналом 1Б складається з канальної і загальної частини. Канальна частина прийомного пристрою включає блок обробки сигналу 1Б.

За результатами аналізу роботи ЗРК С-300В1 при виявленні та супроводжені балістичних цілей можна зробити наступні висновки:

а) під час виявлення балістичних цілей використовується як сигнал ІБ, так і сигнал ІІТ;

б) сигнал ІБ використовується для грубої оцінки швидкості балістичної цілі з метою установки слідкуючих систем по швидкості в заданому діапазоні;

в) інформація про дальність балістичної цілі в подальшому не використовується в зв’язку з великими похибками оцінки, які пов’язані з формуванням лише двох стробів на великий діапазон дальності;

За результатами проведених досліджень отримані наступні пропозиції:

а) запропоновано спосіб визначення швидкості цілі та її дальності;

б) запропонована схема, що дозволяє реалізувати знайдене рішення;

в) встановлена можливість суттєвого підвищення точності оцінювання швидкості, при цьому мається можливість отримати оцінку дальності з достатньо високою точністю;

г) наведений варіант розміщення запропонованого пристрою в приймальному тракті БСНР.

В доповіді наведені можливі варіанти реалізації запропонованих рішень

Список використаних джерел

1. Крючков Д.М., Рощупкін Є.С., Титаренко Р.В., & Шулежко В.В. (2019). Шляхи підвищення можливостей засобів протиповітряної оборони при роботі з об'єктами, що рухаються по балістичній траєкторії. Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів, 104-105. https://doi.org/10.5281/zenodo.5651545

2. Кузьменко Д.В., Рощупкін Є.С., & Джус В.В. (2021, December 8). Удосконалення системи управління променем багатоканальної радіолокаційної станції спеціального призначення. XV Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих науковців» (TPRYS-2021), Харків. https://doi.org/10.5281/zenodo.6791224

3. Сухаревский О.И., А.Ю. Шрамков & Рощупкин Е.С. (2005). Высокочастотный метод расчета диаграммы направленности антенны с учетом неоднородностей рельефа местности на позиции РЛС. Моделювання та інформаційні технології, (33), 174-181.

4. Рощупкин, Е.С., & Беляев, Д.Н. (1999). Измеритель коэффициента стоячей волны в виде ответвителя дециметрового диапазона волн. Збірник наукових праць за матеріалами 3-го міжнародного молодіжного форуму "радіоелектроніка і молодь у XXI столітті" 20-23 квітня 1999 р., 1, 52–55. https://doi.org/10.5281/zenodo.5591877

5. Гайбадулов, Б.В., Джус, В.В., Коробков, Ю.В., Крючков, Д.М., & Рощупкін, Є.С. (2019, September 3). Тренажні імітаційні комплекси зенітного ракетного озброєння – досвід використання, проблемні питання та пропозиції щодо їх розв'язання. Спільні дії військових формувань і правоохоронних органів держави: Проблеми та перспективи, Одеса. https://doi.org/10.5281/zenodo.5067126

6. Крючков Д.М. Удосконалення підготовки персоналу для обслуговування радіотехнічних засобів контролю повітряного простору шляхом урахування питань технічної експлуатації в тренажних імітаційних комплексах / Д.М. Крючков, Є.С. Рощупкін, В.В. Джус, Р.В. Титаренко // Сучасні інформаційні системи. – 2020. – Т. 4, № 3. – С. 89-93. http://nbuv.gov.ua/UJRN/adinsys_2020_4_3_14

7. Петрук С.М, Крючков Д.М., Джус В.В., & Чміль Ю.О. (2020). Вдосконалення технічної експлуатації при проведенні тренувань, відпрацюванні питань використання за призначенням та підтриманні технічного стану радіотехнічних засобів протиповітряної оборони бойовими обслугами. Проблеми координації воєнно-технічної та оборонно-промислової політики в Україні. Перспективи розвитку озброєння та військової техніки, 174, 175. https://doi.org/10.5281/zenodo.5651579

8. Крючков Д.М., Мірюгін В.І., Титаренко Р.В., & Чміль Ю.О. (2020, August 26). Пропозиції щодо удосконалення існуючих тренажних імітаційних комплексів вогневих засобів ураження протиповітряної оборони. Створення та модернізація озброєння і військової техніки в сучасних умовах, ДНДІ ВС ОВТ, Чернігів. https://doi.org/10.5281/zenodo.5578770

9. Меленті Є.О. Розрахунок поля електричного диполя в тропосферному хвилеводі / О.І. Сухаревський, С.В. Кукобко, Є.С. Рощупкін // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2012. – № 4(33). – С. 93-98. http://nbuv.gov.ua/UJRN/ZKhUPS_2012_4_19

10. Герасимов, С.В., Кадубенко, С.В., Рощупкін, Є.С., & Ліцман, А.М. (2020). Контроль частотного розподілення радіосигналів при управлінні зенітними керованими ра-

кетами. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я (MicroCAD-2020), Харків: НТУ "ХПІ". https://doi.org/10.5281/zenodo.5067901

11. Tymchenko, S., Kaplun, Y., Roshchupkin, E., Kukobko, S. (2023). Substantiation of Time Distribution Law for Modeling the Activity of Automated Control System Operator. In: Shkarlet, S., et al. Mathematical Modeling and Simulation of Systems. MODS 2022. Lecture Notes in Networks and Systems, vol 667. Springer, Cham. https://doi.org/10.1007/978-3-031-30251-0_9

12. Кукобко С.В., Місценко Р.В., Бритов Д.М., Рощупкін Є.С., & Гайбадулов Б.В. (2023). Пропозиції щодо автоматизації процесу прийняття рішення при класифікації ситуацій у повітряному просторі. Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку", Харків

Кобзєв В.Г., Яковлєв С. В., Назаров О.С., Назарова Н.В., Горішня К.О.

МОДИФІКАЦІЇ МЕТОДУ ОПОРНИХ ВЕКТОРІВ ДЛЯ КЛАСИФІКАЦІЇ ТА ВИЯВЛЕННЯ АНОМАЛІЙ У ЗАДАЧАХ ОБРОБКИ ЗОБРАЖЕНЬ

Сучасний аналіз накопичених та доповнюваних у часі даних у багатьох прикладних галузях передбачає дослідження різноманітних зображень (космічних, медичних, топографічних і т.п.) з метою виявлення існуючих в них закономірностей [1]. Для задач Data Mining, що використовуються при такому аналізі, важливе значення мають методи класифікації та виявлення аномалій як для сталих даних [1], так і для часових рядів [2].

У переважній кількості прикладних досліджень розглядається розділення наявної сукупності деяких об’єктів на дві частини за певним співвідношенням їх просторових ознак, а також виявлення об’єктів, які суттєво відрізняється набором значень своїх характеристик від інших елементів сукупності. Метод опорних векторів використовує попереднє навчання та визначення правила класифікації об’єктів і дає можливість вирішувати ці задачі у взаємозв’язку.

Метод опорних векторів (англ. – Support Vector Machine, SVM) [3] для навчальної сукупності, яка задана множиною векторів (x_1, x_2, …, x_n) у гіперпросторі R^k, здійснює визначення таких значень координат нормального вектору $\boldsymbol{w}$ та константи b, які дають можливість подати рівняння розділяючої гіперплощини H двох класів у вигляді:

$$\boldsymbol{w}^T \bullet \boldsymbol{x} + b = 0. \quad (1)$$

Параметр зсуву b співпадає з координатою точки перетину гіперплощини з віссю x, вектор $\boldsymbol{w}$ є вектором ваг, які обираються так, щоб виконувалася рівність (1). Така гіперплощина знаходиться на рівновіддаленій відстані від найближчих у просторі представників двох різних класів у навчальній сукупності, які відіграють роль опорних векторів.

Відстань від початку координат до гіперплощини H дорівнює $|b|/||\boldsymbol{w}||$, де знаменник означає Евклідову норму (довжину) вектора $\boldsymbol{w}$. Дві гіперплощини H_1 та H_2, що містять згадані найближчі об’єкти різних класів, є паралельними гіперплощині H. Відстань поміж H_1 та H_2 (ширина межі або зазор, що розділяє два класи) дорівнює $\rho = 2/||\boldsymbol{w}||$. Якщо згадати, що $\left|\left|\boldsymbol{w}\right|\right| = \sqrt{\boldsymbol{w}^T \bullet \boldsymbol{w}}$, то бажання максимізувати в міру можливості ширину зазору ρ призводить до необхідності мінімізації квадратичної функції при лінійних обмеженнях. Задача квадратичної оптимізації — це добре вивчена математична задача оптимізації, для рішення якої запропоновані спеціалізовані методи квадратичного програмування для реалізації саме методу опорних векторів.

При використанні такого методу класифікації нові об’єкти, що у просторі не перетинають гіперплощину H_1 у напрямі до H_2, відносять до першого класу. До другого класу відносять об’єкти, що у просторі не перетинають гіперплощину H_2 у напрямі до H_1, відповідно. В той же час, об’єкти, координати яких у просторі потрапляють у проміжок

поміж гіперплощинами H_1 та H_2 (не відносяться до жодного з двох класів), можна вважати аномальними.

Викладений підхід придатний для задач дуже великої розмірності, які допускають лінійний поділ об'єктів на класи, що у загальному випадку не виконується. Якщо ця умова і виконується, то перевага все рівно віддається тому рішенню, яке краще розділяє основну масу даних, ігноруючи невелику кількість незвичайних шумових об'єктів.

Якщо навчальна множина не є лінійно роздільною, то звичайно при побудові широкого розділового зазору (межі) може статися деяка кількість помилок (окремі точки — аномальні екземпляри — можуть лежати як усередині зазору, так і на невірній стороні). За кожен невірно класифікований екземпляр буде накладатися штраф, що залежить від того, наскільки сильно порушуються умови, накладені на зазор.

За таких умов у задачу оптимізації вводять фіктивні змінні $\xi_i \geq 0$. Узявши фіктивне значення $\xi_i > 0$, ширину зазору для точки x_i можна зробити менше одиниці, але при цьому доведеться заплатити штраф $C\ \xi_i$. Сума величин ξ_i визначає верхню границю кількості помилок при навчанні. Кількість помилок при навчанні за рахунок ширини зазору мінімізує метод опорних векторів з м'яким зазором (soft-margin SVM). При цьому рішення оптимізаційної задачі носить компромісний характер: воно встановлює баланс між шириною зазору і кількістю точок, що довелося б перемістити, для того щоб забезпечити цю ширину. Параметр C дає змогу керувати перенавчанням: якщо він стає великим, то небажано ігнорувати дані за рахунок зменшення геометричного зазору; якщо його значення невелике, то за допомогою фіктивних перемінних неважко врахувати деякі точки й одержати розмір зазору, що моделює основну масу даних.

Як правило, опорні вектори складають невелику частину навчальної множини. Час навчання в методі опорних векторів в основному визначається часом вирішення відповідної задачі квадратичного програмування, тому теоретична й емпірична складність даного етапу залежить від способу розв'язування цієї задачі. Залежність часової складності стандартного рішення задачі квадратичного програмування від обсягу навчальних даних прийнято вважати кубічною. Понадлінійна емпірична складність традиційних алгоритмів опорних векторів утруднює і може унеможливити їхнє застосування до великих наборів навчальних даних. Усі новітні роботи з методу опорних векторів спрямовані на зниження цієї складності, причому найчастіше за рахунок заміни точного розв'язку наближеним.

Один зі способів рішення задачі класифікації у випадках, коли набори даних не допускають лінійний поділ, полягає у відображенні даних у простір більш високої розмірності з наступним застосуванням лінійного класифікатора в цьому просторі. Відомі приклади, коли лінійний класифікатор легко розпізнає дані при використанні квадратичної функції або полярних координат для відображення даних у двовимірну площину. Основна ідея полягає у відображенні вихідного простору ознак у простір ознак більш високої розмірності, у якому навчальна множина виявляється лінійно роздільною. Безумовно, при цьому бажано зберегти релевантну розмірність відношень між точками даних так, щоб отриманий класифікатор узагальнював вихідні дані.

Якщо задача не має властивості лінійної роздільності чи зазор малий і множина невірно класифікованих точок чи точок, що лежать усередині зазору, буде достатньо великою, то в нелінійному випадку це може виявитися основним фактором зниження уповільнення методу опорних векторів на етапі класифікації нових даних.

Викладені варіанти методу опорних векторів можуть застосовуватися у різних прикладних сферах, зокрема там, де можна поділити досліджувані об'єкти на два типи, наприклад, свій – чужий, здоровий – хворий і т.п. У роботі [4] викладений приклад використання лінійного методу опорних векторів у задачі класифікації стану тяжких захворювань в медичних дослідженнях.

Список використаних джерел

1. L Han, Jiawei. Data mining: concepts and techniques / Jiawei Han, Micheline Kamber, Jian Pei. – 3rd ed., Morgan Kaufmann Publishers is an imprint of Elsevier, 2012, 740p.
2. Kirichenko, V Kobziev, Y Fedorenko. Data Mining methods for detection of collective anomalies in time series // Міжн. наук.-практ. конф. “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” / Збірник тез доповідей. - Харків, 2021, - с. 106.
3. Steinwart, Ingo; and Christmann, Andreas; Support Vector Machines, Springer-Verlag, New York, 2008.
4. Горішня К., Кобзєв В. Метод опорних векторів для виявлення і класифікації тяжких захворювань в медичних дослідженнях // Комп’ютерні науки, інформаційні технології та системи управління: матеріали Міжн. наук.-техн. конф. - Івано-Франківськ: Прикарпатський національний університет ім. В. Стефаника, 2023. - с. 137-139.

УДК 004.852

Козирєв А.Д.

МЕТОД ЛОГІЧНОЇ КЛАСИФІКАЦІЇ ДЛЯ АНАЛІЗУ АКАДЕМІЧНИХ ХАРАКТЕРИСТИК

У доповіді розглядається метод логічної класифікації, який може бути використаний для ідентифікації груп студентів з подібними академічними потребами та характеристиками. Аналізуючи різноманітні академічні індикатори, методу логічної класифікації як засобу для ефективного розподілу ресурсів та індивідуалізації академічного супроводу студентів.

Застосування технологій у сфері освіти, включно з усіма аспектами індивідуального навчання, відбувається з високою швидкістю. Розвиток нових інформаційно-комунікаційних технологій уможливив обробку об'ємних масивів даних в освітній сфері. Це сприяло тому, що освітні установи аналізують наявні дані про взаємодію зі студентами, щоб виводити узагальнення для поліпшення навчального середовища.

Поняття "великі дані" може бути охарактеризоване як злиття структурованих даних з баз даних та неструктурованих даних з нових джерел, таких як соціальні мережі, мобільні девайси, сенсори, розумні вимірювальні пристрої та фінансові системи. Сучасні методи дозволяють організаціям збирати та аналізувати дані будь-якого типу, об'єму чи швидкості передачі, щоб робити більш обґрунтовані управлінські рішення на їх основі.

Для аналізу обширного масиву даних все більше застосовуються два ключові підходи, знані як Видобування Даних (Data Mining) та Аналіз Великих Даних (Big Data). Видобування даних, що також відоме як виявлення знань у базах даних [1], є методом розкриття прихованої інформації з великих наборів даних. Цей процес включає аналіз підмножин даних для виявлення повторюваних моделей поведінки чи встановлення прогнозованих моделей на основі обробленої інформації.

Видобування даних займається пошуком та виявленням прихованих знань у необроблених даних за допомогою машинних алгоритмів та інструментів штучного інтелекту, виявляючи невідомі раніше, нетривіальні та практично значущі інформації, які можуть бути інтерпретовані людиною. Початково використовуваний з економічною метою, його потенціал дозволив розширити застосування до освітньої сфери.

Серед основних методів видобування даних та їх застосувань: класифікацію даних у групах з однаковими характеристиками та дає змогу знати загальні моделі для студентів, які знаходяться в тій же групі. Методи логічної класифікації знаходять застосуван-

ня у вирішенні завдань, що виникають у широкому спектрі областей, включаючи біологію, фізику, метеорологію та інші [2]. Особливості цих методів виявляються на стадії розробки математичної моделі, при цьому особлива увага приділяється характеристикам даних, що обробляються. Традиційно у випадках застосовують логіку висловлювань [3]. У цьому дослідженні пропонується використовувати підхід, що базується на алгебрі кінцевих предикатів.

Розглянемо структуру задач, які базуються на використанні предикатних рівнянь. Змінні, як $y_1, y_2, \ldots, y_l$, відображають певні характеристики об'єктів. Це може включати, як варіант, структуроване уявлення критеріїв для оцінки ситуації, наприклад, згідно з нормами оцінки якості або категоризації суб'єкта за рівнями значущості. Відмінно від булевих змінних, які приймають лише два значення, предикатні змінні можуть приймати різноманітні значення з власних дискретних областей значень.

Розглянемо випадок, коли дискретні змінні $x_1, x_2, \ldots, x_n$ представляють собою характеристики, за якими ми можемо оцінити потенційні значення характеристик об'єктів. Ці характеристики та ознаки можуть бути взаємопов'язані через складні логічні відносини [3], що дозволяє формулювати їх через предикатні рівняння:

$$P(y_1, y_2, \ldots, y_l;\ x_1, x_2, \ldots, x_n) = 1 \quad (1)$$

Основні характеристики, які визначають процес виконання практичних завдань студентами, включають:

– унікальний ідентифікатор студента, рівень освіти (курс або показник завершення навчального закладу);

– загальну кількість завдань, які студент розв'язав;

– відсоткове відношення правильно розв'язаних завдань до всіх спроб розв'язання;

– середню кількість спроб, необхідних студенту для вирішення одного завдання;

– середній рівень складності завдань, які студент брав до виконання та успішно вирішив.

Ці параметри можна витягти з бази даних тестового середовища за допомогою простих SQL-запитів.

Завдання класифікації полягає в побудові множини

$$C = \{c_1, c_2, ..., c_k, ..., c_g\}, \quad (2)$$

де c_k – клас, що містить схожі один на одного об’єкти з множини I

$$c_k = \{i_j, i_p \mid i_j \in I, i_p \in I \upsilon d(i_j, i_p) < \sigma\}, \quad (3)$$

де $d(i_j,i_p)$ – міра близькості між об’єктами, звана відстанню, σ – величина, яка визначає міру близькості для включення об’єктів в один клас (в ході експерименту її значення було підібрано емпірично).

Таким чином, завдання полягає в тому, щоб групувати студентів на основі їхніх академічних характеристик для подальшого аналізу. Визначення кількості класів (m): Ми можемо вирішити розділити студентів на, скажімо, 3 класи: ті, хто відмінно вчаться (високий середній бал), середнього рівня студенти (середній бал), та студенти, яким потрібна додаткова допомога (низький середній бал).Вибір атрибутів для класифікації: Можна використовувати середній бал і кількість взятих кредитів як атрибути для групування студентів. Застосування методу класифікації: Використовуючи метод k-середніх, ми ініціюємо алгоритм з трьома центрами класів і ітеративно призначаємо кожного студента до класу, центр якого найближчий за вибраними атрибутами. Оцінка якості класифікації: Якість класифікації можна оцінити, використовуючи внутрішньокласову відстань (сума квадратів відстаней між об'єктами і центром їхнього класу) і міжкласову відстань (відстань між центрами класів).

Список використаних джерел

1. John Walker S. Big data: a revolution that will transform how we live, work, and think. *International journal of advertising*. 2014. Vol. 33, no. 1. P. 181–183. URL: https://doi.org/10.2501/ija-33-1-181-183 (date of access: 02.03.2024).

2. Kash B. R. P., Thappa D. M. H., Kavitha V. Big data in educational data mining and learning analytics. *International journal of innovative research in computer and communication engineering*. 2014. Vol. 02, no. 12. P. 7515–7520. URL: https://doi.org/10.15680/ijircce.2014.0212044 (date of access: 02.03.2024).

3. Kozyriev A., Shubin I. Method for solving quantifier linear equations for formation of optimal queries to databases. *CEUR workshop proceedings*. 2023. Vol. 3396, no. 449-459.

Козлов Ю.В., Дубровіна Л.В.

МЕТОД КІЛЬКІСНОГО ОЦІНЮВАННЯ РІВНЯ ВИВЧЕНОСТІ СУБ'ЄКТА НАВЧАННЯ

Прийнятим і пропонованим до вжитку методам і системам оцінювання вивченості суб'єктів навчання (СН) притаманні недоліки, пов'язані з використанням різноманітних шкал, відсутністю чітких критеріїв їх застосування, надмірна «заматематизованість».

Під вивченістю будемо розуміти показник (бажано інтегральний), що характеризує проміжний або кінцевий результат навчання як рівень засвоєння суб'єктом навчання знань, умінь та навичок у певній галузі людської діяльності, що дозволяє також отримати рейтинговий список групи СН.

Для оцінювання рівня вивченості в системі освіти будь-якої розвинутої країни має існувати так звана система оцінювання знань (СОЗ) як найважливіший елемент освітянського процесу.

Система оцінювання знань суб'єктів навчання у закладах освіти України передбачає використання чотирибальної, десятибальної, дванадцятибальної, двадцятибальної, накопичувальних стобальної та двохсотбальної шкал порядку, а також декларованих у рамках Болонського процесу рейтингової стобальної шкали (РСШ) і відповідної їй ECTS шкали та їх різновидів, прийнятих у закладах вищої освіти (ЗВО), включаючи ЗВО авторів. Відмітимо, що збільшення довжини шкали зумовлено потребою поліпшення якості розрізнення СН.

Подання результатів вимірювань із залишенням двох знаків після коми відповідає відомому з метрології методу ноніуса розмірністю 1/100; абсолютна похибка при цьому не перевищить ±0,010. З тих же міркувань кожна з поділок будь-якої із цифрових шкал може бути додатково поділена на п'ять, десять, двадцять і більше поділок.

Введемо до розгляду і застосування удосконалену чотирибальну шкалу (УЧШ) з ноніусом 1/100, що робить недоцільними до вжитку десяти-, дванадцяти- та двадцятибальної шкал і дозволяє використовувати прийняті у викладацькій практиці оцінки типу 2^+ або 4^-, еквівалентом яких в УЧШ будуть оцінки 2,33 та 3,66. У разі утруднень з визначенням відповідного бала (назвемо це "ефектом буріданова віслюка") експерт виставляє оцінку, що дорівнює середині інтервалу між оцінками або, взагалі, середині шкали, тобто 3,50.

Контроль рівня вивченості може бути усним, тестовим, у вигляді письмового опитування або контрольної роботи тощо. Його результат оцінюють шляхом розрахунку частки повернутої СН інформації:

$$q = n_в / n_з. \qquad (1)$$

де $n_в$ –кількість вірних відповідей на запитання, правильно виконаних завдань або розв'язаних задач; $n_з$ – загальна кількість запитань (завдань, задач).

Значення q може бути використано як деякий коефіцієнт подібності, що характеризує виражену у відсотках долю засвоєної СН інформації від усього обсягу винесеної на контроль.

Оцінювання результатів контролю СН можна виконувати в традиційний спосіб, виставляючи оцінку за чотирибальною або удосконаленою чотирибальною шкалою. Кінцевий результат такого оцінювання розраховують як середнє арифметичне отриманих оцінок, що для вузьких шкал не суперечить теорії, підтверджено результатами розрахунків та аналітичного моделювання.

Відповідна модель подання оцінних функцій викладача наведена на рис. 1.

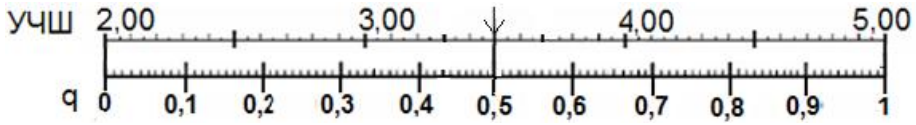


Рисунок 1 – Модель подання оцінних функцій викладача

Серед систем оцінювання знань найбільш розповсюджені у світі різні реалізації англо-саксонської літерної системи з оцінками від «A» до «F» у порядку спадання. Рейтингову стобальну шкалу укупі з літерною шкалою ECTS та чотирибальною шкалою (ЧШ) можна розглядати як Болонську модель оцінювання (рис. 2). Відмітимо характерну рису цієї моделі – нелінійність шкали ECTS і штучно «прив'язаної» до неї вербальної ЧШ.

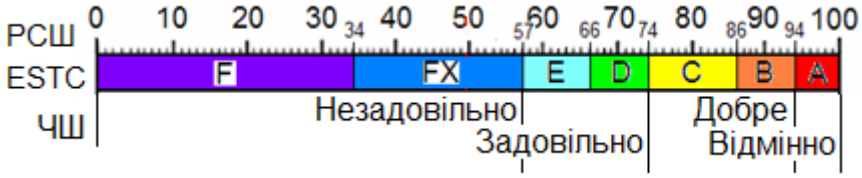


Рисунок 2 – Болонська модель подання оцінних функцій викладача

Подання результатів контролю стобального рейтингового оцінювання за болонською моделлю можливе за виразом

$$Q_{\text{РСШ}} = q \cdot 100. \qquad (2)$$

Відповідні оцінки Q_{ESTC} і $Q_{\text{ЧШ}}$ отримують за номограмою (рис. 2).

Імовірнісно-інформаційний підхід дозволив отримати вираз для розрахунку оцінок за логарифмічною чотирибальною шкалою (ЛЧШ) як функції від частки q повернутої об'єктом контролю інформації:

$$Q_{\text{ЛЧШ}} = 2 + log_2[-8/(7q - 8)]. \qquad (3)$$

Порівняння результатів розрахунку оцінок ЛЧШ з оцінкам ECTS-шкали дає змогу припустити, що в основу системи стобального рейтингового оцінювання покладена концепція імовірнісно-інформаційного підходу, і запропонувати гібридну модель подання оцінних функцій викладача, як показано на рис. 3.

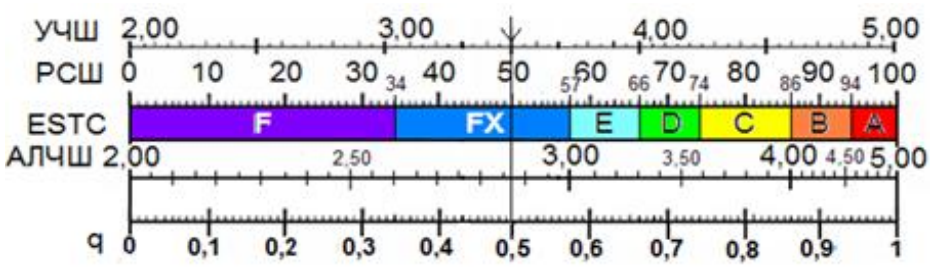


Рисунок 3 – Гібридна модель подання оцінних функцій викладача

На номограмі наведена апроксимована логарифмічна чотирибальна шкала (АЛЧШ), складена з трьох розбитих на рівні інтервали відрізків у діапазонах значень q 0…0,57; 0,57…0,86; 0,86…1, що не змінює її логарифмічний характер, а дозволяє усунути притаманний будь-якій логарифмічній шкалі суттєвий недолік – складність графічного відтворення. Така модель чітко прив'язує одну до одної оцінки за двобальною шкалою q, УЧШ, АЛЧШ, РСШ і ECTS шкалою: 0,5 → 3,50 →2,87 → 50 →FX відповідно.

Введена до розгляду модель дозволяє реалізувати метод оцінювання рівня вивченості суб'єкта навчання як послідовність таких кроків:

- оцінюють частку q повернутої СН інформації або розраховують усереднені оцінки в традиційній чотирибальній шкалі або в УЧШ для конкретних навчальної дисципліни, блоків змістових модулів, змістових модулів тощо, галузі знань як сукупності навчальних дисциплін навчального плану;
- виражають отримані оцінки у визначеній шкалі;
- розраховують (при необхідності) інтегральний показник (метрику) у вигляді модифікованого коефіцієнта конкордації або коефіцієнта відповідності для кожного з суб'єктів навчання з метою побудови їх ранжируваного списку, або ранжирують їх шляхом порівняння із взірцем типу «круглий відмінник»; усі три методи оброблення оцінок інваріантні [1].

Умовами застосування розглянутого методу мають бути:

- наявність специфікацій шкал – прийнятих за домовленістю документів, що містять визначення шкал вимірювань та/або опис правил і процедур їх відтворення та застосування;
- кваліфікація, неупередженість і відсутність змови експертів-викладачів;
- анонімність проміжних результатів.

Багаторічне практичне застосування методу показало його придатність для експертного оцінювання рівня підготовленості СН до визначеного типу діяльності і побудови їх рейтингових списків.

Список використаних джерел

1. Valentyn Kozlov, Yury Kozlov, Inna Moshchenko, Olena Novykova, Victor Olenchenko. Implementation information technology of competency assessment method of professional activity of the educational system employee. Сучасні інформаційні системи, Харків: НТУ «ХПІ»/ 2021. Т. 5, № 3. С. 142–150.

УДК [001.8/.816/.817] + 001.92 + [371.315.5/.315.6/.335] +655.52

Козубцова Л.М., Ліщина В.О., Бескровний О.І., Козубцов І.М., Саган Н.З.

РОЗВИТОК У КУРСАНТІВ SOFT SKILLS ЗА ДОПОМОГОЮ КОМАНДНОЇ ГРИ З ВИКОРИСТАННЯМ НАВЧАЛЬНО-ТРЕНУВАЛЬНОГО КІБЕРПОЛІГОНУ

Soft skills – це соціальні навички, завдяки яким людина може успішно взаємодіяти в команді під час розв'язання будь-яких робочих питань. На думку Ілона Маска, у час швидкого зростання технологій Soft skills мають стати надбанням чи не кожного здобувача освіти (в тому числі курсанті – прим. авторів) на будь-яку посаду у сфері цифрових технологій чи то інших високотехнологічних індустрій. Ще в 1959 р. військовослужбовці США почали розробляти науковий підхід для навчання офіцерів. В ході розробки якого вони зрозуміли важливість не лише професійних навичок (hard skills), але й універсальних якостей (soft skills), які не піддаються планомірному навчанню.

До зазначених характеристик належать наступні вміння:

– активне слухання (здатність уважно слухати, ставлячи допоміжні запитання, що

дозволяють опоненту ширше розкрити думку та зрозуміліше пояснити свою позицію);

– вміння вести перемовини;

– невербальні елементи комунікації (вміння не тільки висловлювати думку розумно та стисло, але й застосовувати жести, міміку, поставу на підтвердження слів, що робить спілкування більш виразним);

– вміння переконувати;

– вміння презентувати та виступати публічно;

– вміння розповідати;

– письмові навички (наприклад, вміння укладати звіти, вести бізнес-комунікацію).

Окремо слід акцентувати на вмінні курсантами критично мислити, а саме аналізувати ситуацію, що склалася, робити корисні висновки та змінювати поведінку відповідно до середовища. Важливою характеристикою сучасного працівника вважається емпатія, здатність відчувати, розуміти та аналізувати почуття та емоції інших людей.

Не на останньому місці емоційний інтелект, позитивне світосприйняття, бажання дізнатися нове, вміння розв'язувати проблеми творчо і нестандартно та прагнення до саморозвитку.

Отже, метою доповіді є вивчення досвіду розвитку у курсантів soft skills, на прикладі командної гри з використанням навчально-тренувального кіберполігону.

В процесі дослідження ми використовуємо поняття кіберполігон (КП), під яким будемо розуміти комплекс програмно-апаратних засобів для обробки інформації та забезпечення кібербезпеки, призначений для ознайомлення курсантів з сучасними засобами.

Функціонально-програмний склад системи КП складається з чотирьох кібепідсистем: захисту; розвідки; впливу; аналітики інформації які реалізовуються поверх удосконаленої онтології кібербезпеки [1].

Командну гра з використанням навчально-тренувального кіберполігону можна розглядати під кутом зору науково-педагогічних досліджень, як гейміфікацію. Тоді на підставі думки [2, с. 135] гейміфікацію можна вважати освітню технологією, яка стрімко розвивається та позитивно впливає на результативність навчального процесу. Крім того, результат позитивної апробації досвіду використання комп'ютерних ігор у технічних закладах вищої освіти можна вважати поштовхом до розгляду гейміфікації, як методу професійно-орієнтованого навчання [3].

Групова ділова гра за моделлю (рис. 1), як і будь-яка гра, має певні правила, що зобов'язують усіх учасників дотримуватися певної послідовностей, аналізу та вибір алгоритмів реагування в залежності від умов ігрової тактичної обстановки розгорнутої на віртуальному полі бою.

В дійсному дослідженні пропонується гру розглядати під кутом зору метода навчання. Тоді метод педагогічної гри набуде широкого застосування у розвитку мистецтва, а отже, сприятиме здобувачам у набутті професійної майстерності. Педагогічну командну гру можна охарактеризувати такими ознаками:

– дидактична мета ставиться здобувачам у формі ігрового завдання;

– навчальна діяльність підкоряється правилам гри;

– навчальний матеріал використовується в якості її засобу;

– у навчальну діяльність добувачів впроваджують елемент спортивного змагання, що перетворює дидактичне завдання в ігрове;

– успішне виконання дидактичного завдання пов'язується з ігровим результатом.

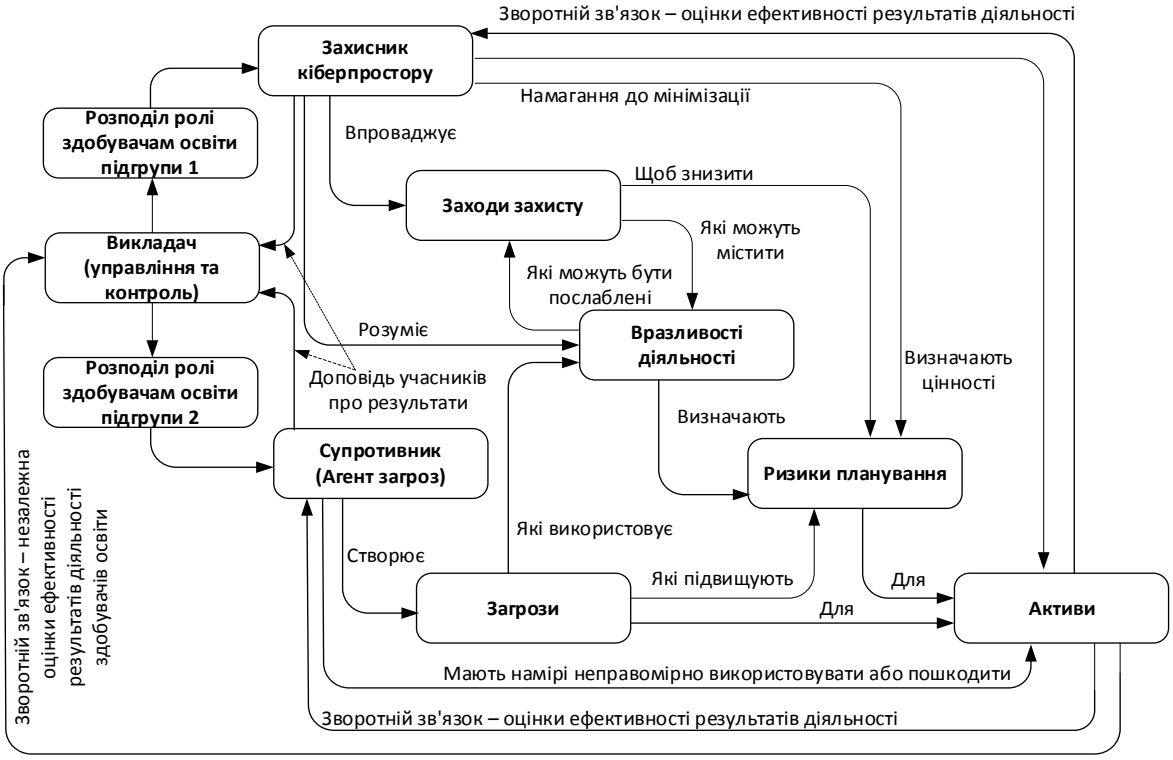


Рисунок 1 - Структурно-функціональна схема командної гри

На КП можуть проводитися різні навчання у сфері кібербезпеки інформаційних систем. Формат навчань у віртуальному кіберсередовищі невимушено, але стимулює до комунікації, набуттю як індивідуальних, так і командних навичок, творчо і ініціативна діяти в умовах навчальної інформаційної невизначеності.

Список використаних джерел

1. Козубцова Л.М. Удосконалення онтології кібербезпеки інформаційної системи. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2021. №44. С. 10–105.

2. Бугаєва В.Ю. Гейміфікація як спосіб формування активної професійної поведінки майбутніх фахівців ІТгалузі. *Педагогіка та психологія*. 2018. №56. С. 129–135.

3. Рибка Н.М. Граїзація та досвід використання комп'ютерних ігор у навчанні філософії у технічних закладах вищої освіти. *Інформаційні технології і засоби навчання*. 2018. Т. 67. № 5. С. 213–225.

УДК 355.433

Колеснік О. М., Барабаш С. С., Шелест О. О.

УДОСКОНАЛЕННЯ МЕТОДИКИ ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ РОЗВІДКИ ПОВІТРЯНОГО ПРОТИВНИКА

В доповіді, на основі аналізу наукових праць та досвіду проведення бойових дій під час відсічі широкомасштабної агресії російської федерації проти України розглянути існуючі показники та критерій ефективності вирішення завдань системи розвідки повітряного противника, як функціоналу від узагальнених показників якості виконання поставлених завдань.

Запропоновано удосконалення методики розрахунку узагальненого показника просторових бойових можливостей системи розвідки повітряного противника, а саме коефіцієнту реалізації потрібних рубежів видачі розвідувальної інформації підрозділам протиповітряної оборони (ППО) та винищувальної авіації. Удосконалення методики розрахунку просторового показника бойових можливостей системи розвідки повітряного противника запропоновано здійснювати шляхом врахування вкладу в можливості системи додаткових інформаційних систем, які працюють на не традиційних засобах, а саме на використанні акустичних та візуальних засобів виявлення повітряного противника. Врахування не традиційних систем виявлення повітряного противника, які працюють на інших фізичних принципах, дозволяє значно покращити можливості систем виявлення та оповіщення про повітряного противника на малих та гранично малих висотах.

В якості інтегрального показника просторових бойових можливостей угруповання ППО, на значення якого впливає ефективність системи розвідки повітряного противника, запропоновано використовувати коефіцієнт прикриття об’єкту визначеним складом угруповання ППО. Нормоване значення коефіцієнту прикриття об’єкту залежить від якості виконання завдань радіотехнічними підрозділами з радіолокаційного забезпечення підрозділів ППО і винищувальної авіації та від якості виявлення засобів повітряного нападу не традиційними акустичними та візуальними джерелами інформації.

Використання наведених вище показників та критерію дає можливість підвищити об’єктивність та інформативність результату порівняльної оцінки варіантів побудови бойового порядку угруповання радіотехнічних підрозділів та варіантів розміщення додаткових датчиків систем акустичного та візуального спостереження за повітряною обстановкою під час участі у відбитті ударів засобів повітряного нападу противника.

УДК 681.375

Коломійцев О.В., Комаров В.О., Львов А.С., Коломійцев В.О., Андрущенко В.М.

ПРИСТРІЙ ДЛЯ ПЕРЕДАЧІ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ЛАЗЕРНОГО ВИПРОМІНЮВАННЯ У ТЕХНОЛОГІЇ ОСТАННЯ МИЛЯ

В доповіді розглянуто особливості використання спектру одномодового багаточастотного з синхронізацією подовжніх мод лазерного випромінювання (ЛВ). Акцентовано увагу на те, що подовжні моди (несучі частоти) можливо використовувати для створення декілька каналів одночасної передачі інформації до споживачів як по закритих – волоконно-оптичних лініях зв’язку, так і по відкритих – атмосферних, за умови застосування лише одного лазера-передавача. Розкрито сутність створення багатоканальної передачі інформації. Приведено аналітичні та схемо-технічні рішення. Розроблені пропозиції щодо створення пристрою для передачі інформації за допомогою ЛВ у технології остання миля.

Сучасний розвиток корпоративних (приватних) мереж передачі інформації (мови та даних) потребує забезпечення як високої надійності ближнього зв'язку між головним офісом і розташованими неподалік підрозділами, так і – швидкості передачі інформації (пакетів даних та голосових повідомлень) загальним каналом зв'язку. Тому, при формуванні мереж передачі інформації, одним із важливих факторів – є витрати на придбання, монтаж та обслуговування такого мережевого обладнання.

Відомі рішення для організації ближнього зв'язку з використанням дротових (мідних) або волоконно-оптичних ліній, які знаходять широке застосування та добре відпрацьовані, не завжди зручні через великі витрати коштів і часу на прокладку нових ко-

мунікацій, а також через високу орендну плату за використання вже наявних комунікацій. При цьому, існуючи комунікації вже не справляються з постійно зростаючими потоками інформації через свою перевантаженість.

У зв’язку із цим, у сучасних містах, де висока щільність підземних і наземних комунікацій, а також у слабко освоєних районах із несприятливими умовами для ведення земляних робіт або низькою щільністю забудови, використовується бездротове радіо обладнання, яке дає змогу обійти зазначені вище труднощі (радіорелейні лінії та радіомодеми). Однак, такий бездротовий зв'язок має наступні основні недоліки: спотворення (втрата) сигналу через засміченість радіоефіру та великі витрати часу на отримання спеціального дозволу через паперову тяганину. Дані недоліки повністю не вирішуються за допомогою відомих технологій швидкого перескоку радіочастоти та цифрового кодування шляхом згортки сигналу з використанням псевдовипадкової шумової послідовності.

Існує бездротовий зв'язок – лазерний, який має явну перевагу над радіозв'язком, коли справа стосується організації бездротових мостів ("точка-точка") на дальність від сотні метрів до декілька кілометрів. Такий лазерний зв'язок, у порівнянні із радіозв'язком, має вищу пропускну здатність, більшу завадозахищеність та не вимагає отримання дозволу на користування радіочастотою, а також ціни на обладнання лазерного зв'язку порівнянні з цінами на радіо. При використанні лазерного обладнання (лазерних систем (ЛС)) не має необхідності у отриманні дозволу на прокладення комунікацій (використання радіочастоти) та пов'язаних із цим відповідних фінансових витрат. Застосування лазерів, у якості джерел випромінювання, відкрило можливість побудови широкосмугових систем оптичного зв'язку, які спроможні передавати не лише телефонні і телевізійні, але й комп'ютерні сигнали. Крім того, висока частота ЛВ забезпечує високу швидкість передачі інформації. До основних переваг лазерного зв'язку можливо віднести наступні: велика пропускна здатність, яка обумовлена високим значенням несучої частоти та, відповідно, можливістю передачі великих об’ємів інформації з великою швидкістю, а також – мала кутова розбіжність ЛВ, яка забезпечує просторову прихованість і високу енергетичну стійкість передачі інформації по оптичному каналу зв'язку при відносно малих габаритах приймально-передавальних пристроїв ЛС. Крім цього, ЛС сумісні із більшістю телекомунікаційного обладнання різного призначення (концентраторів, маршрутизаторів, повторювачів, мостів, мультиплексорів та автоматичних телефонних станцій).

ЛС здійснюють передачу будь-якого мережевого потоку, який доставляється їм за допомогою або дротового (мідного) кабелю або оптоволокна у прямому та зворотному напрямках. Передавач перетворює електричні сигнали у модульоване ЛВ у інфрачервоному діапазоні з довжиною хвилі 820 нм та потужністю до 40 мВт, яке передається через атмосферу до приймача, що має максимальну чутливість у діапазоні довжини хвилі випромінювання. Приймач здійснює перетворення ЛВ у сигнали використовуваного електричного або оптичного інтерфейсу. Таким чином здійснюється зв'язок за допомогою ЛС.

У доповіді розглянуто три відомі сімейства ЛС, що використовуються у США: LOO, OmniBeam 2000 та OmniBeam 4000. Акцентовано увагу на те, що LOO – є базовим та дає змогу здійснювати передачу даних і голосових повідомлень на відстань до 1000 м; OmniBeam 2000 – має аналогічні можливості, але діє на відстань до 1200 м та може передавати відеозображення та комбінацію даних і мови, а OmniBeam 4000 – може здійснювати високошвидкісну передачу даних: від 34 до 52 Мбіт/с на відстань до 1200 м та від 100 до 155 Мбіт/с – до 1000 м.

Доведено, що Alphabet у 2021 році запустила проект Taara для передачі даних повітрям із використанням лазерів. За прямої видимості передача даних у межах одного каналу можлива на відстані 20 км при швидкостіє до 100 Гбіт/с. У рамках тестування в Індії та Африці фахівцям проекту вдалося передати понад 700 ТБ даних на відстань у

5 км. При порівнянні, для досягнення такої ж ефективності на місці довелося б прокладати понад 400 км оптоволокна.

До основних переваг лазерного зв’язку можливо віднести: висока швидкість і великі об’єми передачі інформації, висока захищеність каналу зв’язку, залежність дальності від джерела випромінювання та невеликі фінансові витрати. До основних недоліків: залежність від природних умов та необхідність прямої видимості між передавачем і приймачем.

Розкрито особливості ЛВ та його спектру. Відмічено, що синхронізація подовжніх мод (mode-locking) ЛВ збільшує число мод, що генеруються за допомогою модуляційного процесу, який відбувається під дією зовнішньої сили (активної синхронізації подовжніх мод), що змушує. У результаті даного процесу різниці фаз між сусідніми модами залишаються постійними, тому й різниця фаз між довільними модами також залишається постійною. За такою умовою, отримуються окремі подовжні моди ЛВ, виділення яких дозволить їх використовувати у якості несучих частот для моделювання із інформаційними сигналами.

Отже, використання одномодового багаточастотного з синхронізацією подовжніх мод ЛВ дозволить розширити можливості передачі інформації на різних частотах до споживачів при застосуванні лише одного лазера, як джерела випромінювання. Таке багаточастотне розділення ЛВ дозволить значно збільшити об’єми інформації, що передаються при мінімальних фінансових витратах.

Проаналізовано сучасний стан атмосферної оптичної лінії зв'язку (АОЛЗ) (FSO – Free Space Optics). Дана технологія дозволяє створювати надійні канали зв'язку на відстанях від 100 до 7000 м в умовах атмосфери. За критерієм «ціна-якість» АОЛЗ – найкраще вирішення проблеми «останньої милі». Підключення нового кластера клієнтів до вузла доступу виділеною високошвидкісною лінією зв'язку протягом одного дня без отримання дозволу на радіочастоти і оренду ліній.

Обґрунтовано вибір лазера у якості джерела випромінювання для АОЛЗ. Розроблено і запропоновано пристрій для передачі інформації за допомогою ЛВ у технології остання миля. Пристрій містить у кожному з N каналів: оптичний поляризатор випромінювання, пасивну фазову пластинку $\lambda/4$, що повертає вектор E оптичного випромінювання на кут 45^0 за один прохід скрізь неї, вузькосмуговий інтерферометр Фабри-Перо, що настроєний на прохід визначеної моди (несучої частоти) та допоміжні дзеркала для каналізації ЛВ з каналу в канал. За необхідністю, конструкцію каналу можливо доповнити оптичним квантовим підсилювачем для підсилення вихідного випромінювання. Розкрито сутність роботи пристрою. Проведено оцінку втрат ЛВ у кожному з оптичних каналів, яка показала, що втрати у кожному з каналів можна не враховувати тому, що у його структурі використовуються сучасні оптичні елементи.

Таким чином, за допомогою ЛВ забезпечується передача інформації великих об’ємів через атмосферу з високою надійністю на відстанях в одиниць кілометрів у земних умовах та десятки тисяч кілометрів – у космічному просторі. Проте, методи та програмно-апаратні засоби передачі потребують суттєвого вдосконалення. Розроблено пристрій для передачі інформації за допомогою ЛВ у технології остання миля. Використання пристрою у АОЛЗ дозволить виділити із одномодового багаточастотного з синхронізацією подовжніх мод випромінювання єдиного лазера-передавача подовжні моди (несучі частоти) для подальшого формування N інформаційних каналів зв’язку зі споживачами, що істотно збільшить об’єм і підвищить швидкість інформації, що передається до споживачів.

Список використаних джерел

1. Патент України на корисну модель № 35477, Україна, H04 Q 1/453. Селектор подовжніх мод для багатоканальної передачі інформації. / О.В. Коломійцев, Г.В Альошин та ін. – № u200803492; заяв. 18.03.2008; опубл. 25.09.2008; Бюл. № 18. – 6 с.

2. Kolomiytsev A. V. Informatsionnyie tehnologii i sistemyi v upravlenii, obrazovanii, nauke //Information technologies and systems in management, education, science. – 2013.

3. Алешин, Г. В., & Коломийцев, А. В. (2015). Информационные технологии и защита информации в информационно-коммуникационных системах: коллективная монография; под ред. ВС Пономаренко. *Х.: [Щедра садиба плюс]*.

4. Aloshin G. V., Kolomiytsev A. V. Informatsionnyie tehnologii: problemyi i perspektivyi //Information technology: challenges and perspectives. – 2017.

5. Альошин Г. В. Ефективність лазерних інформаційно-вимірювальних систем / Г. В. Альошин, О. В. Коломійцев, В. В. Посохов, С. І. Клівець // Збірник наукових праць Харківського національного університету Повітряних Сил. - 2018. - № 2. - С. 59-65. - Режим доступу: http://nbuv.gov.ua/UJRN/ZKhUPS_2018_2_9.

6. Альошин, Г., Коломійцев, О., Третяк, В., Кулєшов, О., & Клівець, С. (2020). собливості оптимального вибору структури багатошкальних інформаційно-вимірювальних систем. *Збірник наукових праць ΛΟГОΣ*, 78-82. https://doi.org/10.36074/15.05.2020.v2.30.

7. Shmatko, O., Kolomiitsev, O., Rekova, N., Kuchuk, N., & Matvieiev , O. (2023). Designing and evaluating dl-model for vulnerability detection in smart contracts. *Advanced Information Systems*, *7*(4), 41–51. https://doi.org/10.20998/2522-9052.2023.4.05.

УДК 621.3

Коломійцев О.В., Третяк В.Ф., Катунін А.М., Рибальченко А.О., Любченко О.В., Кривчун В.І., Новикова О.О.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ БАЗ ДАНИХ У ПІДГОТОВЦІ ТА ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ

В доповіді розкрито особливості використання як баз даних (БД), так і реляційних і нереляційних БД у підготовці та діяльності сил охорони правопорядку. Розкрито які складні завдання можливо вирішувати за допомогою сучасних БД.

Використання БД у підготовці та діяльності сил охорони правопорядку є важливою складовою для забезпечення безпеки, стратегічного планування та прийняття якісних рішень [1-5]. До особливостей використання БД можливо віднести наступні:

– геопросторова інформація: БД зберігають геопросторову інформацію, таку як карти, координати об'єктів та географічні дані, що допомагають у військовому плануванні, розташуванні військ і об'єктів інфраструктури;

– розвідувальна інформація: БД містять розвідувальну інформацію, таку як дані про ворожі сили, їх рухи та збройні сили. Така інформація допомагає у визначенні стратегічних цілей та плануванні операцій;

– обробка сигналів та інформація з безпілотних літальних апаратів (дронів): дрони та інші датчики надсилають інформацію, яка обробляється і зберігається у БД для аналізу та прийняття рішень;

– управління запасами і обладнанням: БД використовуються для ведення обліку запасів, обладнання та боєприпасів, що дозволяє ефективно управляти ресурсами військових підрозділів;

– забезпечення зв'язку і комунікації: БД допомагають в управлінні зв'язком і комунікаціями, включаючи збереження та обробку даних із супутникових систем та комунікаційних мереж;

– аналіз даних: великі об’єми даних з БД аналізуються за допомогою спеціальних алгоритмів та програмного забезпечення для виявлення важливих залежностей та трен-

дів, що можуть бути корисними при прийнятті військових рішень;

– спільний доступ до інформації: забезпечення спільного доступу до даних між різними військовими підрозділами дозволяє підвищити координацію та співпрацю у рамках оборонної сфери.

Зважаючи на важливість і конфіденційність даних **у** підготовці та діяльності сил охорони правопорядку, забезпечення безпеки і захисту інформації є надзвичайно важливими аспектами у використанні БД.

Системи реляційних баз даних (РБД) базуються на моделі реляційних таблиць, яку вперше представив Едгар Кодд у 70-х роках минулого століття. До основних особливостей РБД можливо віднести наступні:

– таблична структура: дані у РБД зберігаються у вигляді таблиць (реляційних таблиць), де кожен рядок представляє запис, а кожна колонка – поле даних. Таблична структура дозволяє організовувати дані у логічну і структуровану форму;

– схема даних: вимагає визначення схеми даних перед створенням таблиць. Це означає, що для кожної таблиці потрібно визначити тип даних, обмеження, індекси тощо. Схема даних є строгою і не може бути змінена без перегляду та оновлення БД;

– цілісність даних: РБД підтримують цілісність даних завдяки можливості встановлювати обмеження на дані. Цілісність включає у себе обмеження унікальності, зовнішні ключі, перевірка правил та багато інших механізмів, які допомагають гарантувати, що дані відповідають певним правилам;

– можливість зв'язків: РБД дозволяють встановлювати зв'язки між таблицями за допомогою ключів, що дозволяє ефективно моделювати взаємозв'язки між даними;

– мова запитів SQL: для взаємодії з РБД використовується мова запитів SQL (Structured Query Language). SQL надає потужні можливості для операцій з вибіркою, вставкою, оновленням та видаленням даних;

– транзакції: РБД підтримують транзакції, які забезпечують атомарність, узгодженість, ізольованість та довговічність (ACID) для операцій з даними, що дозволяє забезпечити цілісність даних у разі виникнення помилок або відмов;

– підтримка індексів: РБД створюють індекси для прискорення операцій пошуку і фільтрації даних;

– запити зі з'єднаннями: запити до РБД включають операції з'єднання (JOIN), які дозволяють об'єднувати дані з різних таблиць на основі зв'язків.

Системи нереляційних баз даних (NoSQL) відрізняються від традиційних РБД із застосуванням різних підходів до зберігання та обробки даних. До основних особливостей систем NoSQL можливо віднести наступні:

– гнучкість схеми (Schema flexibility): відсутність фіксованої схеми дозволяє додавати нові поля до записів без змін вже існуючих;

– горизонтальне масштабування (Horizontal Scalability): системи NoSQL дозволяють легко масштабувати БД горизонтально, додаючи нові вузли або сервери для обробки додаткового обсягу даних;

– розподілена архітектура (Distributed Architecture): багато NoSQL БД побудовані на розподіленій архітектурі, що сприяє високій доступності та надійності даних;

– висока продуктивність для конкретних операцій: деякі NoSQL системи оптимізовані для конкретних типів операцій (наприклад, читання або запис), що може забезпечувати високу продуктивність для конкретних випадків використання;

– підтримка неструктурованих та напівструктурованих даних: NoSQL БД дозволяють зберігати та опрацьовувати різні типи даних, такі як JSON, XML, текстові файли тощо, не обмежуючи себе табличною структурою;

– відсутність мови SQL: багато NoSQL систем не використовують стандартні мови запитань, такі як SQL, вибірка та модифікація даних може відбуватися за допомогою інших інтерфейсів або мов програмування;

– різноманіття типів даних: NoSQL системи підтримують різні типи даних, такі як ключ-значення, стовпчасті, документні, графові та ін.;

– ефективність для великих обсягів даних: багато NoSQL БД спрямовані на оптимізацію роботи з великими обсягами даних та високою швидкістю операцій.

Таким чином, сучасні БД допомагають вирішувати складні завдання та сприяють наступному:

– зберіганню та обробці великих об’ємів даних: за ростом кількості та різноманітності даних з'явилися інструменти для зберігання та обробки великих об’ємів даних (Big Data). Сучасні БД можуть ефективно впоратися з великими даними та забезпечити їх аналіз;

– автоматизації бізнес-процесів: БД використовуються для автоматизації бізнес-процесів, що допомагає підвищити продуктивність, знизити ризики та забезпечити ефективне управління операціями;

– збільшенню інноваційності: дані, зібрані та збережені у БД, можуть бути використані для розробки нових продуктів, послуг та рішень, що сприяє інноваційному розвитку;

– забезпеченню бізнес-аналітики: БД надають дані для бізнес-аналізу та забезпечують компаніями можливість приймати обґрунтовані рішення на основі даних;

– оптимізації інфраструктури: сучасні БД можуть бути розгорнуті на хмарних платформах, що спрощує інфраструктуру та знижує витрати на обладнання і обслуговування;

– забезпеченню безпеки даних: з огляду на загрози кібербезпеки, сучасні БД включають різноманітні механізми захисту даних та використовують шифрування, аутентифікацію і інші види технологій для збереження конфіденційності та цілісності інформації;

– глобалізації та дистанційної роботи: БД здійснюють доступ до даних із різних точок світу, що сприяє глобалізації бізнесу та дистанційній роботі;

– інтернету речей (IoT): за розвитком IoT з'являється усе більше даних від різних пристроїв і датчиків та БД грають важливу роль у зберіганні і обробці цих даних.

Таким чином, сучасні БД відіграють ключову роль у різних аспектах підготовці та діяльності сил охорони правопорядку, надаючи інструменти для зберігання, обробки та аналізу даних.

Список використаних джерел

1. Аналіз напрямків розвитку військової техносфери країн НАТО / О. Коломійцев та ін. InterConf. 2023. № 37(171). С. 379–397. URL: https://doi.org/10.51582/interconf.19-20.09.2023.033 (дата звернення: 03.03.2024).

2. Аналіз сучасних систем управління базами даних / Третяк, В., Коломійцев, О., Євстрат, Д., Ворошилов, С., Чмир, В., Логвиненко, Є., Лисиця, А., & Місюра, В. InterConf. 2021. (78), С. 453-465. https://doi.org/10.51582/interconf.7-8.10.2021.050 (дата звернення: 03.03.2024).

3. Використання методів рангового підходу для рішення задачі оптимізації розміщення фрагментів реляційних баз даних у вузлах мережі хмарної структури / Коломійцев О.В, Голубничий Д.Ю., Третяк В.Ф., Осієвський С.В., Возний О.О., Крук Б.М., Полтавський Е.М., Добришкін Ю.М, Приходько С.М., Рибальченко А.О. // Society and Science: Interconnection: 2 між. наук.-практ. конф.: 6-8 травня 2023 р.: Порту, Португалія – С. 366–372.

4. Коломійцев О.В. Інформаційна технологія реплікації розподілених баз даних / Коломійцев О.В., Осієвський С.В., Третяк В.Ф., Крук Б.М., Борисенко М.В., Старцев В.В., Добришкін Ю.М., Приходько С.М., Рибальченко А.О., Любченко О.В. // Global and Regional Aspects of Sustainable Development: 8 між. наук.-практ. конф.: 26-28 берез-

ня 2023 р.: Копенгаген, Данія – С. 494–501.

5. Коломійцев, О., Третяк, В., Воронін, В., Старцев, В., Пустоваров, В., Осієвський, С., ... & Рудаков, І. (2023). Роль та застосування систем баз даних у військовому управлінні та плануванні: аналіз основних аспектів. Scientific Collection «InterConf», (176), 247-255.

6. Коломійцев, О., Рябуха, Ю., Карлов, Д., & Третяк, В. (2020). Особливості організації і класифікація сучасних технологій реплікації даних. *InterConf*, (14). вилучено із https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/2058.

7. Коломійцев, О., Третяк, В., Закіров, З., Кукобко, С., Калачова, В., & Мартовицький, В. (2020). Оптимізація завантаження файлів сховища даних в olap-файли на основі рангового підходу. *InterConf*, (25), 108-117. вилучено із https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/4300.

УДК 629.746

Kolomiitsev O.V., Kuleshov O.V., Tretiak V.F., Pustovarov V.V., Rudakov I.S., Biesova A.O.

PROPOSALS FOR IMPROVING FLIGHT SAFETY BY THE GROUP UNMANNED AERIAL VEHICLES IN URBAN AREAS

The report presents proposals for improving the safety of flights by a group of highly manoeuvrable unmanned aerial vehicles (UAVs) in urban areas based on the development of an intelligent system (algorithms and special software) for automated situational control. Nonlinear laws are used to form a group flight of UAVs and control them. The influence of changing weather conditions and the relative position of UAVs among themselves and nearby objects according to the traffic control laws of a UAV group are considered.

The use of a group of unmanned aerial vehicles (UAVs) is associated with solving a wide range of different challenges both in the military sphere (reconnaissance, defeating enemy air and ground targets, etc.) and in the national economy (climate control, digital mapping, monitoring urban infrastructure, etc.). The group use of UAVs is associated with their advantages - high probability and efficiency of flight missions (expansion of the information and control coverage area, which ensures a high value of the efficiency factor of UAV group use, organisation of joint information processing in the group, which increases information efficiency, etc.). The use of a group of UAVs in urban environment monitoring, as compared to single UAVs, has the following advantages: the ability to install different types of onboard equipment on separate UAVs, coverage of a larger area, the ability of the group to perform missions in case of failure of a part of the UAV, etc.

However, this usage also has disadvantages - insufficient safety of UAVs during intensive manoeuvring under the influence of weather conditions (atmospheric pressure, changes in wind directions and speeds, etc.), considering urban development. Such shortcomings are related to the organisation of UAV cooperation (the need to transmit control commands over long distances and self-organisation), as well as collisions, which can lead to the failure of a certain number of UAVs, making it difficult to perform the mission. Therefore, it is necessary to make constant adjustments (changes in the thrust of the power plant and the position of the steering surfaces) of flight parameters (speed, angular position and altitude), etc.

Overcoming these shortcomings is possible due to the high-quality organisation of the process of forming and managing the simultaneous use of a large amount of highly manoeuvrable UAVs in group flight. The term "group flight" itself describes the process of simultaneous, compatible, coordinated, synergistic (organisationally interconnected)

operation of several UAVs (with different flight characteristics, loads, equipment functional configuration, etc.) with a clearly defined target flight mission.

At present, the challenges of controlling the flight and orientation of individual UAVs are almost solved. However, an analysis of the experience of managing a group of highly manoeuvrable UAVs of different classes indicates that there is no universal approach to creating intelligent control systems for groups of UAVs in urban areas that would use mathematical models of control objects in real time.

Consequently, the use of a group of highly manoeuvrable UAVs can, on the one hand, provide a large amount of data for analysing and documenting the state of urban development, which allows to identify the actual state of construction, reduce the probability of emergencies (events) and save time and money compared to traditional methods, and on the other hand, requires solving the urgent scientific task of improving the safety of flights by such a group**.**

The report provides an analysis of the main tasks solved by a group of highly manoeuvrable UAVs for monitoring urban development, as well as the effectiveness of their use. The main advantages and significant disadvantages of their use are highlighted. The main directions for improving the forms and methods of forming a group flight of highly manoeuvrable UAVs and their management are outlined.

It is pointed out that some control methods have been developed for autonomous quadcopters and helicopters, and aircraft-type UAVs use approaches such as “master-slave” and “virtual structures”. There is also a meta-model of a multi-agent system for searching for and affecting a ground object by a group of UAVs. However, the disadvantage of these approaches is the lack of feedback from UAVs, as well as the high centralisation of the system.

There is also an approach based on the application of methods of optimal control theory. However, it has a high computational complexity.

In urban development, when managing a group of UAVs, intelligent systems should solve a number of key tasks, which may include the following.

Aggregation. The task of creating a compact group of UAVs is the basis for implementing other, more complex tasks, such as joint movement, geometric shape formation, etc.

Distribution. The task of distributing a group of UAVs in space while maintaining constant mutual communication.

Creating shapes. The task of creating (forming) certain geometric shapes by changing the location of individual UAVs in a group.

Coordinated movement. The task of coordinating the movement of individual UAVs and the entire group.

Task distribution. The mission to distribute roles or parts of a large task among individual group UAVs.

Search. Search tasks for individual UAVs and the entire group of buildings, ground objects, etc.

Group movement of objects. The task of moving objects of various loads over appropriate distances by individual UAVs and the entire group.

Group mapping. Mapping (video surveillance) tasks for individual UAVs and the entire group of urban buildings, etc.

Thus, according to the results of the analysis, the necessity of using a distributed intelligent system with elements of artificial intelligence to control a UAV group to ensure autonomous actions without the participation of operators at different stages of the flight task is substantiated. Proposals for the creation of this intelligent system (algorithms and special software) to improve the safety of UAV group flights have been developed and proposed.

References

1. Коломійцев, О., Альошин, Г., Пустоваров, В., Третяк, В., Никорчук, А., & Спори-шев, К. (2020). Підвищення точності сегментації міських будов на цифрових космічних

та аерофотознімках при автоматизованому моніторингу міського середовища. *Збірник наукових праць ΛОГОΣ,* 40-45. https://doi.org/10.36074/09.10.2020.v2.10.

2. Коломійцев О.В., Пустоваров В.В. Пропозиції щодо підвищення точності сегментації міських будов на цифрових космічних і аерофотознімках при автоматизованому моніторингу міського середовища. *Modern Information Technologies in the Sphere of Security and Defence* № 3(39)/2020. – Pp. 81-90. DOI: https://doi.org/10.33099/2311-7249/2020-39-3-81-90.

3. Theoretical foundations in research in Engineering. Collective monograph. / Коломійцев О.В., Голубничий Д.Ю., Третяк В.Ф., Пустоваров В.В.. – etc. – International Science Group. – Boston : Primedia eLaunch, 2022. – 181 p. Available at : DOI – 10.46299/ISG.2022.MONO.TECH.3.

УДК 355.5:004

Колос Р.Л.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У РОБОТІ САПЕРІВ

Розвиток сучасних інформаційних технологій активно змінюють способи застосування частин та підрозділів Сил підтримки Збройних Сил України, а особливо фахівців саперної справи завдяки застосуванню повітряних та наземних безпілотних систем, в основі керування яких лежать бездротові засоби передачі інформації. Військовослужбовці за їх допомогою успішно здійснюють заходи з мінування та розмінування місцевості, інженерну розвідку противника та об’єктів, влаштовують руйнування різноманітних споруд військового та господарського призначення, які використовуються противником.

Цивільні смартфони та планшети у поєднанні із сучасним програмним забезпеченням («Кропива», «Delta», «MilChat», «Hawk Map», «Saper Agent» тощо) надають можливість саперам значно зменшувати час на прийняття рішення та оперативного реагування на загрози, які виникають під час військово-професійної діяльності, вести спостереження в режимі реального часу за противником, який виконує інженерні заходи з фортифікаційного облаштування позицій, влаштування мінно-вибухових та не вибухових загороджень, подолання загороджень на всю глибину його оперативної побудови, прийом та передачу інформації про його місцезнаходження з похибкою до 5 метрів.

Надзвичайно цінним та життєдайним стало проведення практичних курсів підвищення кваліфікації виїзними групами, як у військових навчальних закладах, так і безпосередньо у військових частинах, на яких не зважаючи на звання та займані посади тих, хто навчається, відбувається на високому рівні вище перераховане програмне забезпечення.

У саперних підрозділах широкого розповсюдження з 2014 року отримала бойова система управління тактичної ланки «Кропива», яка являє собою програмне забезпечення для створення карт оперативної обстановки, на яких відображається інформація про динамічну мінну обстановку. В поєднанні з повітряними безпілотними літальними засобами та захищеними системами вона дозволяє здійснювати передачу інформації, а також проводити збір, аналіз та обробки даних для тих, хто здійснює мінування та розмінування місцевості протипіхотними вибуховими пристроями, протитанковими мінами, протидесантними мінами та мінами, що встановлюються дистанційними системами мінування. Дана система дозволяє саперам мати доступ до електронної карти місцевості з відображенням власної позиції за GPS без застосування мережі інтернету, проводити обмін інформацією як графічною, так і текстовими повідомленнями, з іншими колегами, які можуть знаходитись на значній відстані один від одного.

З лютого 2022 року система обміну інформацією «Delta», яка в режимі реального часу надає інформацію про тактичну та оперативну обстановку в районах ведення бойових дій,

почала активно застосовуватись командирами та начальниками саперних підрозділів. Завдяки тому, що програмне забезпечення взаємодіє з підрозділами повітряної розвідки, супутниками, безпілотними засобами, стаціонарними камерами дозволяє відстежувати положення військ противника та оперативно обліковувати виявлені інженерні споруди та об'єкти для їх подальшого врахування у плануванні застосування загальновійськових частин та підрозділів оперативного забезпечення.

Важливим напрямком практичного застосування інформаційних технологій стали пристрої для дистанційного виявлення мінно-вибухових засобів. Враховуючи всі небезпеки, з якими стикаються сапери при застосуванні ручних міношукачів (металодетекторів) при перевірці підозрілих ділянок місцевості застосування технологій розмінування дистанційними методами дають можливість уникати травмування саперів. Одним з напрямків стало впровадження методів і технологій виявлення мін та вибухонебезпечних предметів на основі автоматизованого аналізу матеріалів аерозйомки з пілотованих та непілотованих літальних апаратів. Починаючи з 2020 р. стали проводити інженерну розвідку місцевості з залученням технології автоматизованого виявлення мін на багатоспектральних зображеннях, які одержуються з безпілотних літальних апаратів. На квадрокоптер встановлюють апаратуру для зйомки місцевості: RGB-камера, ІЧ-камера, мультиспектральна камера. При застосуванні враховуються наступні принципи: в першій половині дня краще виявляються міни у не металевих корпусах, у другій — в металевих (з металевими складовими). Це пов'язано з накопиченням тепла впродовж світлового дня металевим корпусом міни, а під вечір, коли температура повітря починає знижуватися, він чіткіше виокремлюється на теплових зображеннях. Розвитком такої технології став аналіз конструкцій мостів, промислових споруд, будівель на виконання робіт щодо закладання зарядів вибухових речовин. Реалізація відбувається шляхом порівняння еталонного знімку та повторного. Періодичність перевірки та об'єкти сканування (фотографування) визначаються в залежності від тактичної обстановки. Ознаками втручання в конструкцію є: порушення кольорової гами зовнішньої поверхні, зміна форми окремих елементів, зміна щільності матеріалу споруди, розбіжності в теплопровідності матеріалів тощо.

Стрімкого розвитку отримали багаторазові наземні дрони, які застосовуються для мінування позицій противника, встановленні груп мін на шляхах руху, розмінування місцевості за допомогою подовжених зарядів вибухової речовини. Найбільшого розповсюдження отримали платформи з колісним та гусеничним рушієм.

Одним з напрямків застосування наземних дронів стало встановлення протитанкових мін на ґрунт. Керування проводиться по декільком радіоканалам. Дальність застосування складає до 8 км. При постановці противником радіоелектронних завад залучають повітряні дрони, які контролюють рух наземного. Прослідковується дві тенденції: дрони виступають носіями мін та у визначений час за командою оператора скидають боєприпаси з підривними, які переведені в бойове положення у потрібне місце, іншим напрямком стало те, що до корпусу прикріплений трос, на якому зафіксовані до десятка протитанкових мін, які по землі затягують на майбутнє мінне поле. Відчіплення тросу відбувається за командою оператора - дистанційно. Рух дрона може здійснюватись по завчасно визначеним координатам чи за командою по радіо. Швидкість руху досягає до 30 кілометрів за годину.

Для знищення техніки противника застосовують наземні дрони камікадзе, які за допомогою потужного заряду вибухової речовини виконують руйнування машин. При спорядженні їх готовими уламками вони уражають також живу силу противника при наближенні до позицій. Керування реалізовано через декілька радіоканалів, при цьому наземний дрон передає зображення з курсової камери. Також військовослужбовці паралельно здійснюють контроль над дроном камікадзе з квадрокоптера та ведуть відволікаючий вогонь.

За допомогою повітряних дронів успішно знищують одиночні протитанкові міни та групи мін, якщо вони розташовуються з кроком мінування менше 2 м. В якості підривного заряду переважно обирають ручні осколково-фугасні гранати, спеціально виготовлені підривні заряди вагою 400-600 гр. з механічним підривником типу МВ-5 або замикачем електри-

чного типу, який замикає електричне коло при контакті з твердою поверхнею. Система скидання активується за сигналом щодо увімкнення зовнішнього ліхтаря з пульта оператора.

Отже, робота фахівців саперної справи тісно пов'язана з застосуванням інформаційних технологій під час мінування та розмінування місцевості, ведення інженерної розвідки для виявлення інженерних заходів противника та вимагає залучення навчених фахівців з сформованими компетенціями по застосуванню методів, процесів використання обчислювальної техніки та систем зв'язку для збору, передачі, пошуку, обробленню та поширенню інформації з метою інженерної підтримки дій військ (сил).

УДК 621.3.006.357

Коляденко Ю.Ю.

КРИТЕРІЙ ЕНЕРГЕТИЧНОЇ ЕКВІВАЛЕНТНОСТІ ДЛЯ ОЦІНКИ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ ПРИ РЕФАРМІНГУ РАДІОЧАСТОТНОГО СПЕКТРУ

Критерій базується на еквівалентності енергетичних характеристик в мережі, що замінюється і новій мережі різних стандартів [1-3]. Використовуючи запропонований критерій, можна на етапі планування фрагмента мережі з новою технологією, визначити його склад за кількістю передавачів і допустимій потужності їх випромінювання.

Енергетична еквівалентність (ЕЕ) полягає в балансі енергетики, що випромінється каналами існуючої мережі LTE та мережі, яка планується 5G в смузі пропускання потенційно несумісного РЕЗ. ЕЕ [1] завад від мережі LTE і 5G в загальному має вигляд:

$$P_{T\sum 5G}(\Delta f_{РЭЗ}) \le P_{T\sum LTE}(\Delta f_{РЭЗ}), \quad (1)$$

де $P_{T\sum LTE}(\Delta f_{РЭЗ})$, $P_{T\sum 5G}(\Delta f_{РЭЗ})$ - сумарні потужності передавачів базових станцій (БС) LTE і 5G відповідно в смузі пропускання $\Delta f_{РЭЗ}$ потенційно несумісного РЕЗ.

Ступінь можливого збільшення потужності потенційної завади від 5G щодо діючої завади від LTE в смузі частот $\Delta f_{РЭЗ} = a \cdot m_f \Delta f_{LTE}$ описується співвідношенням [1]:

$$\eta = \frac{P_{T\sum 5G}(\Delta f_{РЭЗ})}{P_{T\sum LTE}(\Delta f_{РЭЗ})} = \frac{S_{\sum(\Delta f_{РЭЗ})5G} \cdot \Delta f_{5G}}{S_{ср(\Delta f_{РЭЗ})LTE} \cdot \Delta f_{LTE}} = \frac{P_{T5G}}{P_{TLTE}}(1-\beta_{5G})\alpha \frac{n_{T5G} N_{5G}}{\sum_{i=1}^{L_f}(1-\beta_{iLTE}) n_{LTE}(f_i)}, \quad (2)$$

де $S_{\sum(\Delta f_{РЭЗ})5G}$ – сумарна спектральна густина потужності випромінювання передавачів (СГПВП) БС 5G, близька до рівномірної в смузі $\Delta f_{РЭЗ}$; $S_{ср(\Delta f_{РЭЗ})LTE}$ – середня СГПВП БС LTE в смузі частот $\Delta f_{РЭЗ}$ (усереднена за смугою $\Delta f_{РЭС}$); Δf_{LTE}, Δf_{5G}, – смуги частот LTE і 5G відповідно; m_f - параметр, що характеризує кількість можливих частотних каналів LTE в смузі 5G, $1 \le m_f \le \left[\frac{\Delta f_{5G}}{\Delta f_{LTE}}\right]$, $[x]$ – ціла частина числа; $n_{TLTE}(f_i)$ – число передавачів LTE, що випромінюють на одній завадовій ("активній") частоті f_i); n_{T5G} – кількість передавачів на площадці 5G; N_{5G} – кількість площадок, на яких планується установка передавачів 5G; β_{LTE} – обмеження потужності БС LTE, $(0 < \beta_{LTE} < 1)$; β_{5G} – обмеження потужності передавачів 5G за умовами ЕМС $(0 < \beta_{5G} < 1)$; L_f – кількість "активних" частот, які не повторюються в смузі приймача РЕЗ; α – параметр, який показує, наскільки смуга РЕЗ більше (менше) смуги 5G:

$$\alpha = \begin{cases} \dfrac{\Delta f_{РЭЗ}}{\Delta f_{5G}}, & \Delta f_{5G} > \Delta f_{РЭС}, \\ 1, & \Delta f_{5G} \le \Delta f_{РЭС}. \end{cases} \quad (3)$$

Умовою збереження ЕМС за критерієм ЕЕ є співвідношення:

$$\eta = \frac{P_{T5G}}{P_{TLTE}}(1-\beta_{5G})\alpha \frac{n_{T5G}N_{5G}}{\sum\limits_{i=1}^{L_f}(1-\beta_{i\,LTE})n_{LTE}(f_i)} \le 1, \quad (4)$$

відповідно до якого сумарна потужність завади в смузі частот $\Delta f_{РЭЗ}$ від мережі 5G не перевищуватиме еквівалентну потужність завади, яка створювалась в цій смузі мережею LTE.

За умовами повторного використання радіочастот в мережі LTE кожен з цих передавачів знаходиться на одній з площадок, що входять до складу окремого кластера. Отже, число передавачів LTE з частотою f_i буде залежати від загальної кількості площадок LTE (N_{LTE}) і коефіцієнта повторного використання частот в мережі (K) (розмір кластера). За умов $N_{\text{LTE}} = N_{5G}$, маємо:

$$n_{TLTE}(f_i) = \frac{N_{LTE}}{K} = \frac{N_{5G}}{K}. \quad (5)$$

Кількість частот L_f:

$$L_f = K(l_1 + l_2 + l_3), \quad (6)$$

де l_1, l_2, l_3 – кількість передавачів в межах одного трисекторного стільника.

З урахуванням цього:

$$\eta = \frac{P_{T5G}}{P_{TLTE}}(1-\beta_{5G})\alpha \frac{n_{T5G}}{\sum\limits_{i=1}^{K(l_1+l_2+l_3)}\frac{(1-\beta_{iLTE})}{K_i}} \le 1. \quad (7)$$

Цей вираз дозволяє оцінити допустиму кількість передавачів 5G (n_{T5G}) на одній площадці, при якому не буде порушена ЕЕ:

$$n_{T5G} \le \frac{P_{TLTE}}{P_{T5G}} \frac{\sum\limits_{i=1}^{K(l_1+l_2+l_3)}\frac{(1-\beta_{iLTE})}{K_i}}{(1-\beta_{5G})} \frac{1}{\alpha}. \quad (8)$$

Вираз (8) дозволяє визначити умови збереження ЕЕ мережі LTE в смузі частот відповідної ширини для створення мережі 5G при рефармінгу.

Список використаних джерел

1. Коляденко Ю.Ю. Аналіз електромагнітної сумісності угрупувань радіоелектронних засобів в мережах мобільного зв'язку при рефармінгу радіочастотного спектру [Електронний ресурс] / Ю.Ю. Коляденко, Н.А. Чурсанов // Проблеми телекомунікацій. – 2019. – № 2 (25). – С. 56 - 66. – Режим доступу до журн.: http://pt.nure.ua/wp-content/uploads/2020/02/192_kolyadenko_chursanov.pdf.

2. Koliadenko, Y., Moskalets, M., Badieiev, V., Savchenko, R. (2023). Method Radio Resource Allocation in Cognitive Radio Network. In: Dovgyi, S., Trofymchuk, O., Ustimenko, V., Globa, L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. Pp. 102-115 https://doi.org/10.1007/978-3-031-46880-3_7

3. B. Muliar, Y. Koliadenko, M. Moskalets, V. Loshakov and D. Ageyev, "Interaction Model and Phase States at Frequency Resource Allocation in a Grouping of Radio-Electronic Equipment of 5G Mobile Communication Network," 2022 IEEE 9th International Conference

on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2022, pp. 495-501, doi: 10.1109/PICST57299.2022.10238581. https://ieeexplore.ieee.org/document/10238581

УДК 621.3.006.357

Коляденко Ю.Ю., Бадеєв В.О.

ТЕОРЕТИКО-ІГРОВА МОДЕЛЬ ВЗАЄМОДІЇ АТАК І ЗАХИСТУ

Мережа стільникового зв'язку характеризується величезною вартістю та великими термінами будівництва. Зміни у стандартах зв'язку відбуваються регулярно, але перехід до нового стандарту потребує нових вкладень та заміни обладнання, яке часто ще не виробило свій ресурс. Зараз для запуску мережі 5G все стає простіше завдяки технології програмних мереж, що конфігуруються. У мережах 5G основні функції комутаторів та маршрутизаторів перенесені на центральний мережевий контролер, що спрощує застосування мережевих політик, та моніторинг стану мережі. При такому підході передавальні пристрої відповідають лише за передачу даних, спираючись на таблицю потоків, яка будується централізованим мережевим контролером, що взаємодіє з передавальним пристроєм.

Взаємодія між мережним контролером і передавальними пристроями реалізується за допомогою програмного інтерфейсу, який використовується для прямого управління групами пристроїв. Архітектура комутатора базується на одній чи декількох таблицях правил, які визначають механізм обробки потоків мережного трафіку. Кожне правило є записом у таблиці комутатора. Запис зіставляється з певним потоком трафіку. Залежно від результату зіставлення, застосовується відповідна дія (блокування, передача, модифікація тощо) до пакетів з даного потоку.

Архітектура мережі, припускаючи істотно інший підхід до реалізації мережевої інфраструктури, не позбавлена потенційних вразливостей з погляду інформаційної безпеки. Необхідність поділу доступу мережевих додатків при роботі з контролером, питання аутентифікації та авторизації при роботі додатків з контролером – це лише мала частина аспектів безпеки, які доводиться брати до уваги при проектуванні мереж. Контролер як ключовий компонент в управлінні усією інфраструктурою мережі є найуразливішим елементом, атака на який може спричинити критичні для всієї інфраструктури наслідки.

Завдання безпеки стає особливо актуальним для мереж, де канал передачі часто розділяється між великою кількістю користувачів. У безпроводових мережах постає ще одна проблема — загальнодоступність каналу зв'язку.

Для забезпечення безпеки безпроводових міських мереж необхідно провести аналіз за тих чи інших ситуацій виникнення несанкціонованого доступу. З цією метою розробляються математичні моделі. Таким чином, розробка моделі взаємодії атак та захистів є актуальною науковою задачею.

Об'єктом дослідження є процес організації безпеки в безпроводових мережах зв'язку 5G.

Предмет дослідження становлять моделі взаємодії атак та захистів.

Метою даної роботи є розробка моделі взаємодії атак та захистів.

Аналіз взаємодії атак та захистів можна представити у вигляді теоретико-ігрової моделі [1-3]. Гра - це математична модель колективної поведінки: кілька учасників впливають на ситуацію, причому їх інтереси (виграші або втрати за різних можливих ситуацій) різні. При такому уявленні у взаємодії динамічних систем S_i, $i = \overline{1,n}$ можливі три

характерні стратегії поведінки. У загальному випадку ці стратегії можуть бути класифіковані таким чином:

1) антагоністична стратегія, коли учасники мають протилежні інтереси.

2) кооперативна стратегія, коли у всіх гравців є спільна мета та їх стратегії узгоджені;

3) стратегія байдужості або гра з природою, коли стратегія j гравця не залежить від стратегії гравця i.

Відомі й інші типи стратегій - чисті чи змішані [3]. Гра в чистих стратегіях передбачає детерміністський підхід, і як випливає з теорії, рідко коли призводить до рівноважних рішень. На відміну від цього, для ігор у змішаних стратегіях, при стохастичному підході коло рівноважних рішень значно розширюється. Очевидно, що процеси атак та захистів представляються антагоністичною стратегією або загалом – змішаною. При невеликих відхиленнях в інформації про апріорні дані поведінку такої системи можна представити моделлю взаємодій і фазових станів атак і захистів. Слід зазначити, що у відомих роботах відсутнє уявлення мережі як теоретико-ігровой моделі з антагоністичною стратегією поведінки.

Запропоновано теоретико-ігрову модель стану взаємодії атак та захистів у вигляді нелінійної системи Вольтерра:

$$\frac{dy_i(t)}{dt} = y_i(t)(\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(t) - \sum_{s=1}^{n}\sum_{j=1}^{n} \nu_{sj} y_s(t) y_j(t)), \quad (1)$$

де $y_i(t)$ - випадковий вплив атак, $i = \overline{1,n}$, $s = \overline{1,n}$, $j = \overline{1,n}$ n - число атак; ε_i - ефективність i-ї атаки; ν_s - параметр:

$$\nu_s = \frac{a_s y_s}{\sum_{s=1}^{n} a_s y_s}; \quad 0 \le \nu_s \le 1; \quad \sum_{s=1}^{n} \nu_s = 1. \quad (2)$$

a_s - нормативна кількість ресурсів s-го захисту.

Перетворимо цей диференціальний вираз до різницевого. Позначимо – t_k дискретний час.

$$\frac{dy_i(t_{k+1}) - dy_i(t_k)}{t_{k+1} - t_k} = y_i(t_k)(\varepsilon_i - \sum_{s=1}^{N} \nu_s y_s(t_k) - \sum_{s=1}^{N}\sum_{j=1}^{N} \nu_{sj} y_s(t_k) y_j(t_k)), \quad (3)$$

де $t_{k+1} - t_k = T_d$ - интервал дискретизации.

Позначивши дискретний час $t_k = k$ отримаємо різницеве рівняння:

$$y_i(k+1) = y_i(k) + T_d \times [y_i(k)(\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(k) - \sum_{s=1}^{n}\sum_{j=1}^{n} \nu_{sj} y_s(k) y_j(k))],$$

або

$$y_i(k+1) = y_i(k) \cdot (1 + T_d) \times (\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(k) - \sum_{s=1}^{n}\sum_{j=1}^{n} \nu_{sj} y_s(k) y_j(k)). \quad (4)$$

Дана модель дозволяє виконувати аналіз при різних конкретних параметрах та взаємодій атак та захистів.

Список використаних джерел

1. Коляденко Ю.Ю. Анализ взаимодействия и фазовые состояния группировки радиоэлектронных средств систем абонентского радиодоступа / Коляденко Ю.Ю. - Прикладная радиоэлектроника. Всеукр. Межвед. Научн.-техн. сб. - 2004. - Том.3, №3. - С. 37-42.

2. Коляденко Ю.Ю. Модель динамики неравновесных состояний при распределении ресурсов в сети абонентского радиодоступа /Коляденко Ю.Ю., Величко Т.В. - Радиотехника, Всеукр. Межвед. Научн.-Техн. сб. - 2005. - Вып. 142. - С. 34—39.

3. Лесик Р.А. Теоретико-игровая модель атак в городских беспроводных сетях/Лесик Р.А. - Материалы XVII Международного молодежного форума «Радиоэлектроника и молодежь в XXI веке» Харьков, 2013. - с. 103-104.

УДК 621.3.006.357

Коляденко Ю.Ю., Лютий А.О.

МОДЕЛЬ СИСТЕМ ЗВ'ЯЗКУ 6G ЗА УМОВ СПІЛЬНОГО ВИКОРИСТАННЯ МІЛІМЕТРОВИХ ТА СУБМІЛІМЕТРОВИХ РАДІОХВИЛЬ

Сучасні системи нового радіо (NR) міліметрового діапазону 5G [1], а також майбутні технології радіодоступу (RAT) терагерцового діапазону (ТГц) 6G [2,3] значною мірою покладатимуться на формування променя для боротьби з надмірними втратами на шляху проходження. Обидві технології радіодоступу націлені на подібний нееластичний трафік, що вимагає великої пропускної здатності, і на них впливають явища блокування.

Розглянемо стадію розгортання систем міліметрових хвиль (ММХ) NR і зосередимося на одній комірці ММХ базової станції (БС) круглої форми з радіусом R_M, (рис. 1), де R_M є таким, що блокування на краю комірки не призводить до відключення. Поряд з ММХ БС знаходиться ТГц БС, що характеризується радіусами покриття $R_{T,1}$ і $R_{T,2}$, де перший радіус такий, що жодні сеанси, які знаходяться всередині (0, $R_{T,1}$), не зазнають відключення у випадку блокування, в той час як сеанси з кільця ($R_{T,1}$, $R_{T,2}$) можуть зазнати відключення у випадку блокування. Висота БС однакова, h_A. Висота АС - h_U. Смуга пропускання БС ММХ і ТГц - B_M і B_T.

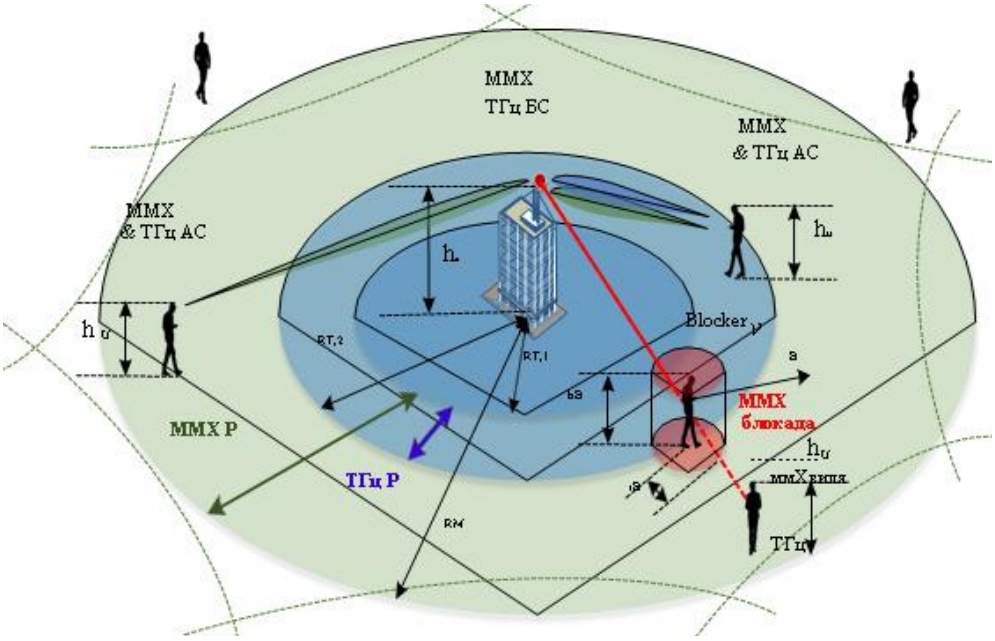
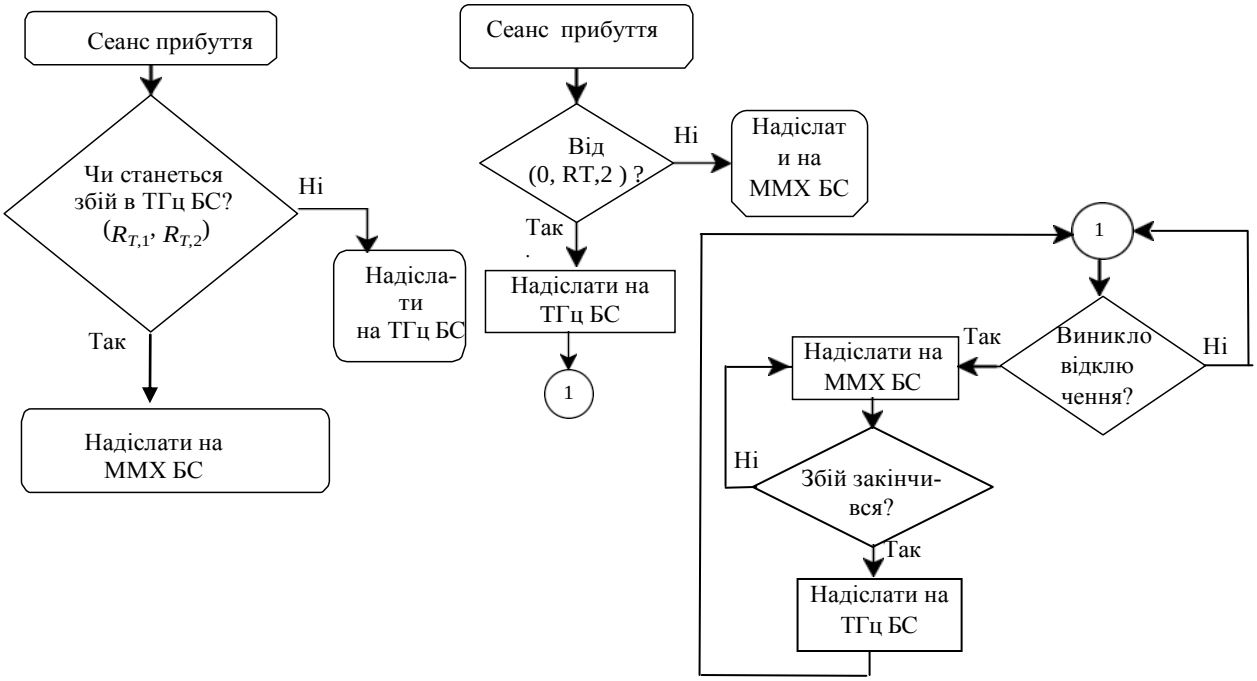


Рисунок 1 - Розгорнута система 6G зі спільним розміщенням БС ММХ/ТГц

Процес надходження сеансів є пуассонівським з інтенсивністю λ_A сес./с $м^2$. Вважається, що геометричні місця розташування сеансів рівномірно розподілені в зоні покриття ММХ. Час обслуговування сеансів розподілено за експоненціальним законом з параметрами μ. Кожен сеанс вимагає швидкість передачі даних R_b Мбіт/с.

Передбачається, що всі АС підтримують функцію мультизв'язності [3]. Оскільки основне погіршення продуктивності в розглянутих майбутніх щільних розгортаннях 6G ММХ/ТГц спричиняється динамічним блокуванням людського тіла, розглядаємо дві схеми об'єднання: ММХ (ММХ Р) і ТГц (ТГц Р), (рис. 2).

У першій схемі на ТГц БС приймаються лише ті сеанси, які не зазнають відключення через блокування. Це відповідає колу радіусом $R_{T,1}$ на рис. 1. Решта сеансів надходять до ММХ БС і залишаються там, доки їх обслуговування не буде завершено або сеанс не буде припинено. У схемі, якій надається перевага в ТГц, сеанси, що надходять з кола радіусом $R_{T,2}$, спочатку приймаються в ТГц БС. Ті сеанси, які зазнають відключення з ТГц БС в кільці ($R_{T,1}$, $R_{T,2}$) тимчасово перенаправляються на ММХ БС і повертаються назад, як тільки блокування з ТГц БС закінчується. У цій схемі більше трафіку спочатку спрямовується на ТГц БС, але частина сеансів може зазнати відключення в результаті блокування.



а) б)

Рисунок 2 - Схема об’єднання: (a) перевага надається ММХ, (b) перевага надається ТГц

Сесія, яка прийнята на обслуговування в ММХ БС, може бути втрачена в результаті переходу в стан блокування. Хоча в цьому випадку не відбувається відключення, кількість ресурсів, необхідних для обслуговування, збільшується через схему модуляції та кодування нижчого порядку. Якщо у ММХ БС немає достатньої кількості ресурсів, сеанс зв'язку обривається. Сеанси, які прийняті в ТГц БС в колі радіусом $R_{T,1}$, ніколи не втрачаються. Однак, у схемі, якій надається перевага в ТГц, сесія, що зазнає блокування на ТГц БС в кільці ($R_{T,1}$, $R_{T,2}$), може бути втрачена на ММХ БС, якщо немає достатньої кількості ресурсів, щоб тимчасово вивантажити її на ММХ БС.

Список використаних джерел

1. B. Muliar, Y. Koliadenko, M. Moskalets, V. Loshakov and D. Ageyev, "Interaction Model and Phase States at Frequency Resource Allocation in a Grouping of Radio-Electronic

Equipment of 5G Mobile Communication Network," 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2022, pp. 495-501, doi: 10.1109/PICST57299.2022.10238581.

2. Polese, M.; Jornet, J.M.; Melodia, T.; Zorzi, M. Toward end-to-end, full-stack 6G terahertz networks. IEEE Commun. Mag. 2020, 58, 48–54.

3. Moltchanov, D.; Samuylov, A.; Lisovskaya, E.; Kovalchukov, R.; Begishev, V.; Sopin, E.; Gaidamaka, Y.; Koucheryavy, Y. Performance Characterization and Traffic Protection in Street Multi-Band Millimeter-Wave and Microwave Deployments. IEEE Trans. Wir. Comm. 2022, 21, 163–178.

УДК 621.3.006.357

Коляденко Ю.Ю., Оголюк В.В.

МЕТОД ЦЕНТРАЛІЗОВАНОГО ЗОНДУВАННЯ СПЕКТРУ В КОГНІТИВНІЙ МЕРЕЖІ

Основною проблемою спектрального зондування є виявлення первинного користувача в зашумленому середовищі. Це складне завдання особливо при низьких значеннях відношення сигнал/шум (SNR) через загасання сигналу та затінення (рис.1) [1].

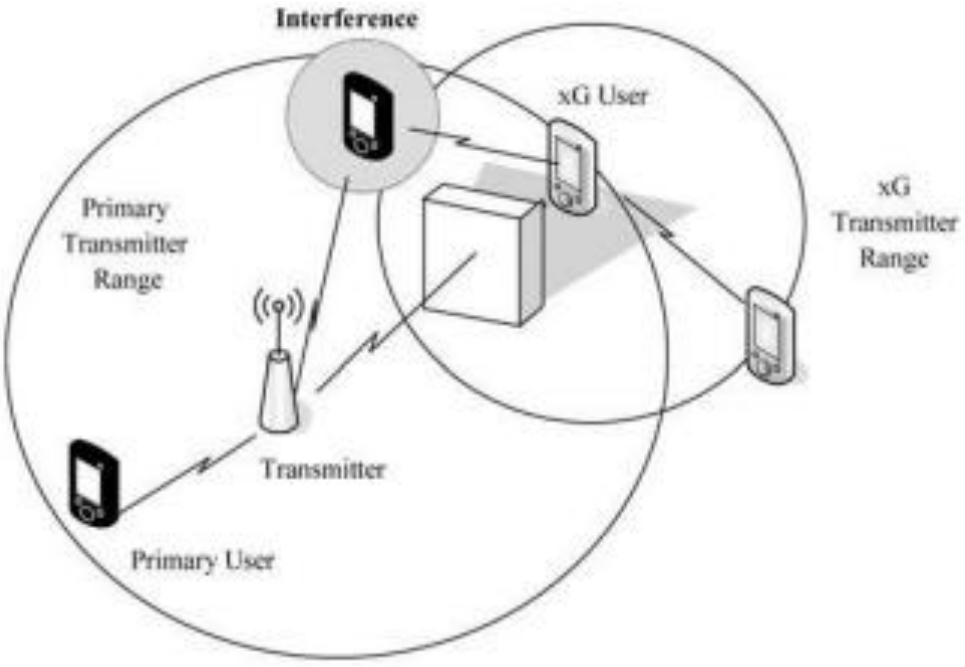


Рисунок 1 - Прихований термінал

Задачу зондування можна охарактеризувати як перевірку гіпотези [2,3]:

$H_0 : y(t) = n(t)$ - первинний користувач відсутній,

$H_1 : y(t) = h(t)s(t) + n(t)$ - первинний користувач працює зі спектром.

де $y(t)$ - прийнятий сигнал, $n(t)$ – шум в момент часу t з дисперсією δ, $s(t)$ - переданий сигнал, який є автокорельований $E\left[|s(t)|^2\right] \neq 0$, а $h(t)$ - коефіцієнт підсилення або затухання каналу. H_0 та H_1 - це гіпотези про наявність шуму та сигналу відповідно.

Класичні методи використовують виявлену енергію як індикатор присутності сигналу в каналі.

Процес прийняття рішення виглядає наступним чином [2]:

$$Рішення\begin{cases} E\left[\left|s(t)\right|^2\right] \le V_T & H_0, \\ E\left[\left|s(t)\right|^2\right] > V_T & H_1. \end{cases}$$

де V_T – потужність (дисперсія) шуму. Енергію часто оцінюють сумою, яка є неточною оцінкою особливо коли є невелика кількість відліків [2]:

$$E\left[\left|y(t)\right|^2\right] \approx \frac{1}{N}\sum_{k=1}^{N}\left|y(t)^2\right|.$$

Спільні підходи до спектрального зондування використовують інформацію, зібрану всіма приймачами, для визначення наявності сигналу в каналі. Така кооперативна стратегія дозволяє уникнути прихованої термінальної проблеми, в якій передавач когнітивного радіо не в змозі виявити первинного передавача через затінення або затухання, але його передача спричиняє завади для первинної користувацької передачі в первинному приймачеві. Такий сценарій зображено на рис. 2.

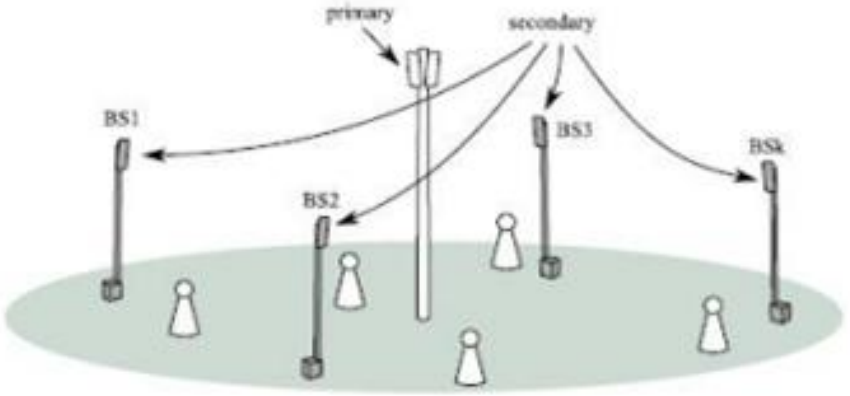


Рисунок 2 - Сценарій централізованого зондування

Оскільки завади виникають у приймачах, можна уникнути завад від основного приймача. Цей метод виявився практичним лише для телевізійних приймачів.

Спільне зондування спектра потребує декількох датчиків, розподілених на великій площі. Його точність залежить від щільності розміщення сенсорів на площі, оскільки низька щільність призводить до того, що дані, отримані сенсорами, є дуже некорельованими.

На продуктивність схеми прийняття рішень впливає також техніка злиття, що використовується для об’єднання інформації з багатьох джерел.

Припустимо, що:

- є K базових станцій зондування когнітивного радіо, які розподілені по місцевості випадковим чином, але їх точні просторові координати відомі. Припустимо, що ці базові станції можуть спілкуватися через проводову мережу і підтримка мережі управління не викликає проблем;

- усі вони здатні використовувати одну і ту ж ділянку спектру.

Визначимо S, матрицю зондування розмірністю $K \times N$, яка визначається N нещодавно зондованих зразків K базових станцій, $y_i(k)$ - k -й зразок, знятий i-ю антеною:

$$S = \begin{pmatrix} y_1(1) & y_1(2) & \dots \\ y_2(1) & y_2(2) & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{pmatrix}$$

У випадку H_0, коли присутній лише шум, внутрішній добуток всіх рядків буде оцінкою автокореляційної функції шуму. Оскільки припускається, що вибірки шуму є взаємно некорельованою, ця величина буде близькою до нуля.

У випадку H_1, внутрішній добуток рядів буде пропорційний автокореляції переданих сигналів. Визначимо постійний коефіцієнт підсилення каналу для періоду зондування. Оскільки шум є некорельованим з переданим сигналом, то матимемо:

$$S_m \cdot S_n = \sum_{i=1}^{N} y_m(i) \times y_n(i) = \sum_{i=1}^{N} \left(\left(h_m s(i) + N_m(i) \right) \times \left(h_n s(i) + N_n(i) \right) \right) \approx$$

$$\approx h_m h_n \times N \times E\left[|s(t)|^2 \right], \quad m \neq n.$$

Таким чином, використовуючи дану схему можливе спільне вимірювання спектру. В цій схемі використано просторову інформацію антен для знаходження спектральних дір в локальних регіонах.

Список використаних джерел

1. L. S. Cardoso, M. Debbah, P. Bianchi, J. Najim, Cooperative spectrum sensing using random matrix theory, IEEE ISWPC, pp. 334338, May 2008.

2. Поповский В.В. Метод обнаружения сигналов первичных пользователей в когнитивных радиосетях / В.В. Поповский, А.В. Коляденко // Радіоелектроніка, інформатика, управління. – 2017. – №2. – С. 7–15. DOI: 10.15588/1607-3274-2017-2-1.

3. Поповский В.В. Сравнительный анализ эффективности алгоритмов обнаружения сигналов при когнитивном распределении ресурсов в сетях мобильной связи / В.В. Поповский, А.В. Коляденко // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2017. – Т. 17, № 2. – С. 33 – 41. DOI: 10.14529/ctcr170203.

УДК 621.396.967

Komar O.

METHODS FOR EVALUATING THE IMPACT OF PROPERTIES OF SIGNALS ON THE RESILIENCE TO INTER-CHANNEL INTERFERENCE IN COGNITIVE RADIO SYSTEMS

The report discusses the methods of assessing the impact of energy and correlation characteristics of signals on resistance to inter-channel interference in intelligent radio systems. The development of new methods of signal generation aimed at optimizing the use of the spectrum and increasing the resistance of smart radio systems to interference was studied. The energy properties and correlation effects of signals are analyzed, based on which a mathematical apparatus, methods and approaches for automatic detection and compensation of disturbances are proposed. The need to take into account energy aspects and the influence of cross-channel interference for effective design and optimization of intelligent radio systems is substantiated. The report proves the importance of energy aspects and inter-channel interactions in the design of effective radio systems. The importance of improving productivity and reliability with the help of developed methods of countering interference, in

particular through improving the adaptability of systems to external interference, is emphasized. The importance of improving the productivity and reliability of communication systems by improving the methods of countering interference is substantiated. It is proven that the implementation of developed algorithms and mathematical tools allows to increase the adaptability of the system to external obstacles and improve the quality of telecommunications systems. Attention is focused on the key role of a multidisciplinary approach in the analysis and development of cognitive radio systems. The principles of creating flexible and adaptive systems that can independently adjust to changing environmental conditions, ensuring stable and efficient functioning, are highlighted. The role of innovation in strengthening the security and reliability of wireless communication is emphasized, pointing to the importance of developing the latest technologies to counter threats. The results of the study open up prospects for expanding the capabilities of cognitive radio systems, ensuring their effective integration into the complex information networks of today. The conclusions of the work emphasize the significance of the developed methods, approaches and algorithms for practical application in the field of telecommunications aimed at ensuring a high level of resistance of communication systems to various challenges in modern radio communication systems.

Копцов І.О., Бова Д.В., Першин О.В.

ДОСЛІДЖЕННЯ ПРОГРАМНИХ ЗАСОБІВ МОНІТОРИНГУ СТАНУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ

Ефективна передача інформації, розширення різноманітних потоків даних та забезпечення надійного зв'язку з зовнішніми джерелами інформації є неможливими без належної комунікаційної інфраструктури. Керування мережею передачі даних потребує комплексного підходу, включаючи організацію доступу до мережевих пристроїв, моніторинг, оперативну заміну комунікаційного обладнання та оновлення програмного забезпечення, створення резервних копій, а також документування мережевої інфраструктури.

З розвитком сучасних інформаційно-комунікаційних систем завдання управління мережами та їх моніторингу відіграють все більш важливу роль. У зв'язку з постійним зростанням складності інформаційно-комунікаційних систем, надійність цих систем та якість послуг, які вони надають, стають надзвичайно важливими.

Сучасна інформаційно-комунікаційна інфраструктура складається зі складної мережі, що включає в себе комунікаційне, серверне та програмне забезпечення різних виробників, працюючи на різних стандартах та під керівництвом різного програмного забезпечення.

Складність та розмір мережевої інфраструктури вимагають високого рівня автоматизованих засобів моніторингу та управління, які потребують розробки для забезпечення надійної роботи мережі. Для підтримки працездатності комунікаційних мереж необхідно постійно контролювати їхню роботу.

За допомогою моніторингу, забезпечується систематичний процес збору та обробки інформації про стан мережі, необхідний для прийняття управлінських рішень. Якщо для невеликих мереж часто достатньо власноруч контролювати файлів реєстрації чи протоколів, то для великих систем необхідно використовувати спеціалізовані засоби.

Для моніторингу великих мереж застосовують системи управління мережею, які збирають дані про стан вузлів і комутаційних пристроїв мережі, а також про трафік, що циркулює в мережі. Ці системи здійснюють управління мережею в автоматизованому режимі, інформація, зібрана ними, допомагає адміністраторам мережі приймати складні рішення щодо її управління/

УДК 623.1/.7: 621.396.931:007.5

Коркін О.Ю., Братченко Г.Д., Ковалішин С.С., Яструбенко О.В.

ШЛЯХИ ПІДВИЩЕННЯ ЗАВАДОЗАХИЩЕНОСТІ РАДІОКЕРОВАНОЇ БЕЗПІЛОТНОЇ НАЗЕМНОЇ СИСТЕМИ

В умовах активної фази українсько-російської війни з метою зниження втрат особового складу значно підвищується потреба у прийнятті на озброєння безпілотних наземних систем (БпНС) для виконання різноманітних завдань на лінії бойового зіткнення. В їх числі завдання вогневої підтримки, розвідувальні, логістичні, евакуація поранених та пошкоджених зразків озброєння, військової та спеціальної техніки з поля бою та інші [1, 2]. На сучасному етапі розвитку БпНС виконання ними поставлених завдань здебільшого здійснюється за участю оператора. Вони переважно є дистанційно керованими за допомогою телеметрії або напівавтономними з прийманням рішень оператором [2]. Команди дистанційного керування на мобільну платформу в БпНС передаються радіоканалом з пункту керування (ПК). Необхідна для вироблення команд керування інформація про поточний стан БпНС та зовнішнього середовища, в свою чергу, передається з платформи радіоканалом на ПК. Якість радіокерування може суттєво погіршитися в умовах радіоелектронної протидії противника. У найгіршому випадку мобільних платформ втрачає керованість. Для забезпечення стійкості функціонування БпНС в умовах радіопротидії противника система радіокерування має бути завадозахищеною.

Метою роботи є аналіз основних шляхів підвищення завадозахищеності радіокерованої БпНС з більш детальним обґрунтуванням можливостей просторової селекції корисних сигналів.

Для подавлення каналу радіокерування противник застосовує активні завади, які можуть бути прицільними або загороджувальними та мати різні види модуляції. Шляхом забезпечення завадозахищенності БпНС в складних умовах радіоелектронної обстановки може бути застосування методів частотно-часової селекції корисного сигналу. При цьому важливим є вибір виду модуляції сигналу. Широке застосування знаходить псевдовипадкове переналаштування робочої частоти (ППРЧ), застосування складних видів модуляції корисних сигналів. При цьому покращується якість частотно-часової селекції корисного сигналу і за рахунок широкосмуговості сигналу зменшується взаємний вплив засобів зв’язку та зростає відношення сигнал/шум на виходах приймачів корисних сигналів. Ефективність цих методів залежить від ступеня частотно-часового розділення корисного сигналу і завад, а за умов суттєвого перекриття та достатньо потужної завади ці методи можуть значно втрачати ефективність.

В переважній більшості практичних ситуацій напрямки з ПК на постановники завад не збігаються з напрямками на мобільні платформи БпНС. Ця відмінність може використовуватись для просторової селекції корисного сигналу та одночасно подавлення активної завади. Метод просторової селекції пропонується реалізувати із застосуванням адаптивних антенних решіток (ААР), які встановлюються як на ПК, так і на мобільних платформах БпНС. В процесі реалізації методу береться до уваги поточна інформація про взаємне розташування ПК та мобільних платформ. При цьому ураховується апріорна інформація про місцеположення ПК та заплановані маршрути руху платформ БпНС. Це дозволяє формувати діаграми спрямованості ААР на мобільних платформах таким чином, щоб головні пелюстки антен були постійно спрямовані на ПК в процесі їх переміщення заданим маршрутом. На ПК при цьому мають формуватись промені у напрямку на кожну з мобільних платформ. Завдяки такій орієнтації променів ААР суттєво зростає добуток коефіцієнтів підсилення антен і відповідно відношення сигнал/шум на виходах приймачів на ПК і на мобільних платформах. В той же час, завдяки спрямованості антен, зменшується рівень випромінювання у напрямку засобів радіорозвідки

противника. Відповідно має знижуватись розвідувальна доступність передавачів на ПК і на мобільних платформах.

За умови надходження корисного сигналу і завади з однакового кутового напрямку, якщо сигнали завад та корисні сигнали мають різні види поляризації, є можливість додатково реалізувати в ААР здатність поляризаційної селекції. Це дозволить в окремих ситуаціях покращити завадозахищеність приймачів ПК і мобільних платформ.

Для формування діаграми спрямованості ААР застосовуються два основних підходи – це прямі та градієнтні методи адаптивної обробки сигналів [3, 4]. Прямі методи засновані на оцінці кореляційної матриці спостереження та подальшому її обертанні. Обмеженнями при їх реалізації є великий обсяг обчислювальних витрат, висока точність арифметичних операцій і можлива втрата обчислювальної стійкості [5]. На відміну від прямих градієнтні методи засновані на оцінці градієнта критерію якості роботи ААР і послідовної корекції параметричного (вагового) вектору в напрямку, який визначається градієнтом критеріальної функції. Їх перевагою над прямими є простота практичної реалізації в реальному масштабі часу. При цьому градієнтним алгоритмам адаптації властиві деякі обмеження, головне з яких пов’язане із залежністю процесу їх збіжності і стійкості від сигнально-завадової обстановки.

Таким чином, кожен із розглянутих напрямів підвищення завадозахищеності радіокерованої БпНС має свої переваги та обмеження.

На наш погляд, метод просторової селекції є найбільш доцільним для реалізації в перспективних зразках БпНС. Важливим завданням подальших досліджень при проєктуванні ААР є обґрунтування вибору методу адаптивної обробки сигналів, що потребує розробки математичних моделей та імітаційного моделювання з урахуванням умов застосування БпНС.

Також представляє практичний інтерес подальше дослідження можливостей оптимального комплексування методів просторової, частотно-часової та поляризаційної селекції в системі радіокерування БпНС для забезпечення достатнього рівня її завадозахищеності в складних умовах радіоелектронної обстановки.

Список використаних джерел

1. Концепція розвитку та застосування наземних роботизованих комплексів (платформ) у підрозділах Сухопутних військ Збройних Сил України, ВКП 3-00(11).01. 2022. 21 с.

2. Доктрина “Застосування безпілотних систем у силах оборони України”, ОП 3-0(46), грудень 2023. 54 с.

3. Радиоэлектронные системы: основы построения и теория. Справочник / Ширман Я. Д., Лосев Ю. И., Минервин Н. Н., Москвитин С. В. Горшков С.А., Леховицкий Д. И., Левченко Л. С. / Под ред. Я. Д. Ширмана. М.: ЗАО “МАКВИС”, 1998. 539 с.

4. Адаптивная компенсація помех в каналах святи / Ю. И. Лосев. М.: Радио и связь, 1998. 208 с.

5. Skachkov, V. V., Chepkii, V. V., Yefymchykov, O. M., Korkin, O. Yu., Goncharuk, A. A. Solving the Problem of Forming Stable and Consistent Estimates of a Correlation Matrix of Observations Using the Method of Dynamic Regularization. Cybern Syst Anal 57, 82-90 (2021). URL: https://doi.org/10.1007/s10559-021-00331-3.

Корнієнко О.С., Бондар Р.В., Ликова І.В., Кравець Т.М.

ПОТОЧНИЙ ТИЖНЕВИЙ РЕЙТИНГ ФАКУЛЬТЕТУ РАКЕТНИХ ВІЙСЬК І АРТИЛЕРІЇ ТА ОТРИМАНІ РЕЗУЛЬТАТИ

Отримані результати за період використання – метою проведених спостережень та супроводження поточного тижневого рейтингу було визначити вплив рейтингу на навчальну діяльність та готовність курсантів до навчання. Протягом початкового етапу впровадження поточного тижневого рейтингу було зібрано значну кількість різноманітних показників навчання, які на даний момент проаналізовані та систематизовані. Дані дозволили виявляти фактори, які різноманітним чином впливають на процес навчання курсантів. Крім того, спостерігалися помітні позитивні ефекти, відображені у значному зростанні показників успішності, як для факультету в цілому, так і для окремих груп курсантів.

Оцінка впливу поточного тижневого рейтингу на рівень навченості курсантів факультету ракетних військ і артилерії, заснована на статистичних даних з 2021-2023 років, продемонструвала значні позитивні зрушення. За цей період часу факультет в цілому зазнав підвищення успішності на 8,59%. Зростання успішності у відповідних групах представлено таким чином: військовослужбовці чоловіки - 8,54%; військовослужбовці жінки - 5,56%; перший курс - 12,26%; другий курс - 12,13%; третій курс - 4,32%; четвертий курс - 10,86%; військовослужбовці контрактної служби - 11,26%; ліцеїсти - 7,96%; цивільна молодь - 8,46%; військовослужбовці зі званням солдат (курсант) - 9,06%; військовослужбовці зі званням старший солдат - 9,11%; військовослужбовці зі званням молодший сержант - 7,08%; військовослужбовці зі званням сержант - 10,45%; військовослужбовці зі званням старший сержант - 17,21%; курсанти з посадою головний сержант курсу - 7,28%; курсанти з посадою командир групи - 8,33%; курсанти з посадою командир першого відділення - 3,13%; курсанти з посадою командир другого відділення - 6,38%; курсанти з посадою командир третього відділення - 9,29%;курсанти з посадою курсант - 8,98%; спеціальність ракетні війська - 7,31%; спеціальність артилерійська розвідка - 5,72%; спеціальність артилерійська розвідка - 9,48%.

Показники успішності всіх груп підвищилися на 3–11%. Протягом трьох років ні один показник не зменшився, що свідчить про позитивний вплив поточного тижневого рейтингу на результати. Це підтверджується ще тим, що протягом 2022 року, коли поточний рейтинг не функціонував певний період, показники успішності значно знизилися через відсутність можливості для курсантів відстежувати свої результати. Лише після відновлення роботи рейтингу вони змогли повернутися до попереднього рівня успішності. Позитивний ріст результатів у всіх підгрупах вказує на те, що поточний тижневий рейтинг дозволяє відстежувати та впливати на успішність кожної підгрупи, що навчається на факультеті. Це сприяє підвищенню загальної успішності всього факультету. Не зважаючи на постійну зміну загальної чисельності факультету, надходження нових курсантів та випуск старих, факультет зміг значно покращити усереднені показники успішності курсантів.

Оцінка роботи поточного тижневого рейтингу на факультеті ракетних військ і артилерії свідчить про численні переваги цієї системи над традиційною системою: поточний тижневий рейтинг об'єктивніше оцінює знання курсантів; розподіляє їх за рівнем знань; усуває випадковість і суб'єктивність у підсумкових оцінках; підтримує мотивацію курсантів до навчання; акцентує значення поточного й підсумкового контролю, роблячи їх системними; визначає позицію кожного курсанта серед інших, груп та курсів; включає весь період навчання; сприяє здоровій конкуренції.

Оцінюючи рейтингову систему під час роботи на факультеті, керівництво факультету виявило, що вона відрізняється від традиційних підходів оцінювання. У поточному тижневому рейтингу враховуються не лише знання, вміння і навички, але й широкий

спектр діяльності курсанта: навчальна; методична; науково-дослідна; пошукова. Рейтинг оцінює не лише якість самостійної та аудиторної роботи, а й спрямованість курсанта – чи він працює систематично чи нерегулярно. Крім того, враховується особистісний стиль курсанта, активність у здобутті ним нових знань.

За результатами аналізу, отримані наступні висновки, що впровадження рейтингової системи навчання у військових вищих навчальних закладах покращує спосіб контролю та оцінювання, організацію самостійної роботи курсантів, і взаємини між курсантами та викладачами. Що є однією з ключових складових якісної підготовки фахівців. Застосування рейтингової технології дозволяє систематично контролювати прогрес, що стимулює підвищення академічної успішності. Таке навчання стає більш доступним, мотивуючим і цілеспрямованим, сприяючи формуванню довіри між всіма учасниками освітнього процесу, що слугує справжнім кроком у напрямку демократизації та гуманізації освіти.

Протягом трьох років поточний тижневий рейтинг став невід'ємною складовою системи підготовки факультету та широко використовується на всіх рівнях управління. Курсанти можуть відстежувати свою успішність в режимі онлайн та реагувати на зміни в результатах негайно. Командири груп та відділень здатні контролювати особовий склад, виявляти і допомагати слабким індивідам. Начальники курсів та курсові офіцери аналізують показники курсу та окремих курсантів, що сприяє підвищенню загальної успішності груп та курсу в цілому. Керівництво факультету має повний обсяг інформації про успішності кожного курсанта, дозволяючи відслідковувати як найуспішніших, так і тих, хто потребує додаткової уваги. Це дозволяє ефективно впроваджувати дисциплінарні заходи та покращувати середні показники успішності факультету в цілому. Ці переваги не повинні обмежуватися лише факультетом ракетних військ і артилерії, а мають бути впроваджені та реалізовані у всіх навчальних підрозділах Збройних Сил України з метою підвищення об'єктивності відбору та категоризації успішності навчаємих.

Існує сильна необхідність якомога швидше розробляти та впроваджувати автоматичні, автономні технології контролю оцінки якості навчання. Потрібно розуміти, що холодний автоматичний математичний аналіз який вільний від участі людини більш об'єктивний та має ряд значних переваг: спрощення процесу використання; зменшення затрат часу на експлуатацію; відсутність не об'єктивних критеріїв оцінювання; здатність виявляти не очевидні залежності; створювати відчуття здорової конкуренції; можливість курсанта аналізувати своє навчання самостійно.

Корнієнко О.С., Гера В.Я., Каляєв О.О., Кравець Т.М.

ДИСЦИПЛІНАРНІ ТА ІНШІ ЗАХОДИ ДЛЯ СУПРОВОДЖЕННЯ ЕФЕКТИВНОЇ РОБОТИ ПОТОЧНОГО ТИЖНЕВОГО РЕЙТИНГУ

Сутність дисциплінарної практики факультету полягає в тому, щоб кожен курсант розумів, що навчання - це відповідальність, а не лише обов'язок. Стимулювання курсантів до регулярної роботи, самоорганізації та постійного підвищення якості свого навчання. Для забезпечення високої якості навчання та ефективної роботи поточного тижневого рейтингу факультет застосовував різноманітні дисциплінарні заходи, які спрямовані на покращення освіти і створення сприятливого навчального середовища.

Поточний тижневий рейтинг і дисциплінарна практика взаємно доповнюють один одного, утворюючи одну закриту систему (рис.9), яка сприяє ефективному функціонуванню навчального процесу. Поточний тижневий рейтинг, в якому враховуються результати курсантів, прямо пов'язаний з дисциплінарною практикою, яка визначає норми, правила та структуру навчального процесу. Дисциплінарні заходи, в свою чергу,

підтримують якість та ефективність поточного тижневого рейтингу, створюючи умови для чіткого визначення критеріїв оцінки та спостереження за дотриманням навчальних правил і норм. Вони допомагають забезпечити, щоб навчання проходило належним чином і куранти виконували свої зобов'язання. З іншого боку, поточний тижневий рейтинг, враховуючи прогрес курсантів, народжує і підтримує нові дисциплінарні заходи, оскільки він надає викладачам та управлінню факультету інформацію про те, де можливо поліпшити дисциплінарну практику для забезпечення кращих результатів курсантів.

Заходи що застосовуються на факультетів в системі поточного тижневого рейтингу:

Планування і моніторинг навчальних програм: Визначення конкретних завдань та цілей навчання, формування змісту та послідовності навчальних програм, а також постійне оцінювання їх ефективності через використання поточного тижневого рейтингу - це важливий інструмент для кафедр та викладачів у процесі аналізу та вдосконалення навчального процесу. Поточний тижневий рейтинг надає можливість оцінити, які зміни відбуваються при впровадженні нових навчальних програм або методик. Рейтинг допомагає швидко та точно зрозуміти реакцію курсантів на різні навчальні зміни, що дозволяє адаптувати їх у процесі навчання. Головне, що рейтинг надає об'єктивну інформацію про рівень та спрямованість покращень у навчанні, співвідносячи їх з різними навчальними підходами;

Впровадження стандартів навчання: Встановлення чітких стандартів та критеріїв оцінювання сприяє створенню послідовного підходу до навчання і оцінки успішності курсантів. Система поточного тижневого рейтингу допомагає визначити якісні межі успішності курсантів факультету, замість використання суб'єктивного оцінювання. Рейтинг дозволяє курсантам точно оцінити свій рівень навчання. Відтепер, аналізуючи свій середній бал у порівнянні зі загальною групою або під групою курсантів, вони можуть зрозуміти, наскільки успішні вони насправді. Коефіцієнти оцінки кращих і гірших курсантів надають можливість зрозуміти, чи навчається курсант на низькому рівні порівняно з іншими, або чи є в нього потенціал для покращення;

Оцінка і звітність: Регулярне оцінювання знань курсантів є невід'ємною частиною навчання, включаючи формативну (під час навчання) та сумарну (після завершення якогось періоду) оцінку. Результати оцінки повинні бути доступні як для курсантів, так і для викладачів, щоб сприяти подальшому удосконаленню навчального процесу. Система електронних журналів та поточного рейтингу надає можливість постійно контролювати свій середній бал і отримані оцінки. Курсант може оперативно відстежувати зміни свого середнього балу та оцінок у контексті вжитих ним заходів для покращення навчання. Чим може обирати кращі та менш затратні підходи до покращення рівня навчання. Електронний журнал дозволяє аналізувати особисті результати успішності в реальному часі, а поточний тижневий рейтинг допомагає порівнювати їх з результатами інших груп та підгруп курсантів факультету. Зменшення часу між отриманням результатів та їх аналізом сприяє кращому розумінню впливу прийнятих заходів на успішність курсанта. Головною метою поточного тижневого рейтингу є забезпечення постійного контролю та звітування щодо рівня навченості як для викладачів, так і для курсантів;

Самооцінка і саморегулювання: Важливо навчати курсантів навичкам самооцінки та саморегуляції, що допоможе їм стати більш самостійними та відповідальними у процесі навчання. Майбутні офіцери мають розвивати самостійність та наполегливість, навчаючись самоаналізу та постійному вдосконаленню протягом навчання. Поточний тижневий рейтинг допомагає курсантам зрозуміти, наскільки ефективними є їх зусилля у покращенні свого рейтингу в порівнянні з іншими курсантами факультету протягом поточного місяця чи тижня. Електронний журнал дозволяє постійно аналізувати проблемні предмети та недоліки в знаннях, які потребують удосконалення. Рейтинг спонукає курсанта до самостійної роботи над собою та підтримує їхніх старших начальників, які

надають додатковий вплив та допомогу у мотивації для самовдосконалення. Цей процес сприяє розвитку культу самостійності та самоаналізу серед курсантів;

Створення відкритого та сприяючого середовища: Створення дружнього та підтримуючого клімату на факультеті чи в навчальній групі є важливою складовою для підвищення мотивації курсантів до навчання. Застосування поточного тижневого рейтингу та електронних журналів, в яких всі розрахунки автоматизовані та недоступні для втручання командирів на будь якому рівні, створює відчуття відкритості та справедливості серед курсантів. Кожен курсант розуміє, що вплив на результати рейтингу залежать виключно від його власних зусиль, що сприяє великому рівню довіри до представлених результатів. Постійне відстеження та нагляд за курсантами, які відстають у навчанні, допомагає командирам групи реагувати на цю ситуацію та надавати необхідну підтримку. На рівні навчального курсу та факультету - це дозволяє контролювати та розробляти додаткові заходи, такі як перездачі, додаткові заняття та консультації, щоб допомогти студентам наздогнати відставання у засвоєнні матеріалу;

Підтримка саморегуляції: Важливо навчати курсантів встановлювати конкретні цілі, розробляти плани навчання та визначати кроки для їх досягнення. Постійне самовдосконалення і рефлексія над власним навчанням, а також постійний аналіз результатів можуть служити сильним джерелом мотивації. Курсанти мають доступ до корисних інструментів, таких як електронні журнали та поточний тижневий рейтинг, які дозволяють їм встановлювати конкретні цілі і легко відстежувати їх виконання. Перебуваючи на певних місцях у рейтингу курсантів і вкладаючи значні зусилля у підвищення свого рейтингу, курсант розуміє, що його праця не марна. Курсант може ставити перед собою завдання, такі як підняття загального рейтингу, покращення середнього балу за конкретною дисципліною або зменшення кількості двійок, і з легкістю контролювати їх виконання завдяки наявним інструментам;

Визнання досягнень: Похвала та визнання досягнень курсантів можуть значно підвищити їхню мотивацію. Цю підтримку можна виражати через різні форми позитивного підкріплення, такі як нагороди, публічні висловлення подяки та інші способи. На факультеті розроблена система визнання досягнень та висловлення подяки курсантам. Кожні півроку факультет відзначає трьох найкращих курсантів факультету та по троє найкращих курсантів кожної спеціальності, поставляючи їх як приклад для інших. Щотижня також визначаються найкращі курсанти за покращення середнього балу, найуспішніший командир групи за тиждень та курсант, який перездав найбільше двійок. Крім цього, діє система заохочень, пов'язаних із наданням додаткових звільнень та відпусток для курсантів, які потрапляють до топ-100 на факультеті. Результати рейтингу використовуються при розподілі курсантів на стажування чи при випуску. Найкращі курсанти постійно висвітлюються на факультеті та в курсантських спільнотах;

Співпраця та групова робота: Застосування колективних завдань і цілей може сприяти співпраці та соціальній взаємодії, що може стимулювати мотивацію серед курсантів. Поточний тижневий рейтинг сприяє розвитку та керуванню роботою курсантів в колективі. Кожен курсант має змогу слідкувати не лише за своїми особистими результатами, але й за результатами своєї групи, навчального курсу чи спеціальності. Кожен курсант розуміє, що він — це не окрема ізольована одиниця, а частина великого механізму, який спрямований на досягнення спільної мети. Це спонукає до постійної співпраці між частинами організації для досягнення спільного успіху. Командири на різних рівнях зацікавлені в створенні здорового колективу, який має всі можливості досягнення спільної мети. Крім того, конкуренція на різних рівнях допомагає курсантам зрозуміти важливість комунікації та співпраці між частинами групи для досягнення якісного виконання завдань;

Впровадження конкуренції: Організація змагань і конкуренції може значно підвищити змагальний дух та бажання курсанта досягати кращих результатів у навчанні. Однією з ключових цілей поточного тижневого рейтингу є створення здорової конкуренції,

яка нагадуватиме процес гри. Кожен курсант постійно має можливість конкурувати в загальному рейтингу зі старшими та молодшими курсами, з одногрупниками або курсантами по спеціальності. Участь в цій "грі" дозволяє курсантам, зусиллями покращуючи свої знання, сягати вищого рівня, що відображається на їхньому місці у рейтингу. Такий асоціативний підхід спрощує конкуренцію, перетворюючи її на щось, схоже на таблицю лідерів у будь-якій онлайн-грі. Постійна конкуренція з кращими за себе стимулює курсантів до більшого зростання і розвитку, використовуючи нові методи та шляхи для досягнення бажаних результатів;

Зв'язок з майбутніми перспективами: Пояснення того, як висока якість навчання може вплинути на можливості та кар'єрні переваги, може бути великим стимулом для курсантів. Переваги курсантів з високим рейтингом постійно висвітлюються перед особовим складом факультету. Високий рейтинг курсанта має вплив на його можливості при обранні місця стажування, і найуспішні курсанти мають можливість обирати місця стажування на власний розсуд. Під час організації міжнародного співробітництва та відряджень за кордон, вибір кандидатів зазвичай базується на рівні володіння англійською мовою, але рейтинг факультету також враховується, як важливий показник. При прибутті представників різних служб, таких як Служба безпеки України, Головне управління розвідки та Національна гвардія України, які бажають прийняти випускників до свого складу, рейтинг також є важливим фактором в прийнятті рішення. При випуску, випускний рейтинг складається з урахуванням рейтингу факультету, надаючи можливість вибирати з більшого розмаїття частин і посад для випускників.

Корнієнко О.С., Сівак О.І., Ликова І.В., Кравець Т.М.

ПОТОЧНИЙ ТИЖНЕВИЙ РЕЙТИНГ ФАКУЛЬТЕТУ РАКЕТНИХ ВІЙСЬК І АРТИЛЕРІЇ ТА ОСОБЛИВОСТІ ЙОГО ФУНКЦІОНУВАННЯ

Поточний тижневий рейтинг факультету ракетних військ і артилерії – це система оцінки академічних та практичних досягнень курсантів протягом усього періоду їхнього навчання, що визначається та відображається щотижня. Цей рейтинг служить інструментом контролю, який акцентує увагу на щотижневому моніторингу та представленні результатів, охоплюючи різноманітні аспекти навчального процесу та військової підготовки курсантів. Рейтингова система дозволяє курсантам відображати свою щоденну роботу над предметами навчання у підсумковій оцінці в загальному тижневому рейтингу факультету. Використання рейтингового контролю стимулює у курсантів орієнтацію на цілі, мотивацію до вдосконалення, розуміння системи оберненого зв'язку, усвідомлення справедливості, сприйняття власного прогресу, стимулювання конкуренції, адаптацію до реальних вимог, розвиток самоорганізації, розуміння вагомості кожної частини навчання, підготовку до викликів.

Поточний тижневий рейтинг факультету ракетних військ і артилерії був розроблений та вперше застосований в січні 2021 року. Загалом термін використання поточного тижневого рейтингу становить 3 роки та 2 місяці з яких 2 роки використання та впровадження поточного тижневого рейтингу супроводжувалось виконанням науково-дослідної роботи .

Впровадження поточного тижневого рейтингу дозволило курсантам отримати чіткий зворотній зв'язок щодо їхніх досягнень. Курсанти стали більш свідомо відноситись до свого прогресу та слабких місць, що сприяє їхньому бажанню вдосконалювати знання. Такий підхід дозволив вчасно виявляти проблемні аспекти в навчанні, тим самим забезпечувати швидке реагування. Система вплинула на моральне становище курсантів, вони відчули більшу впевненість у своїх можливостях, оскільки отримували підтримку та визнання за вкладені зусилля. Зародилась здорова конкуренція, що стимулювало ку-

рсантів до покращення результатів. Система допомагає виявляти та підтримувати обдарованих курсантів. У великій мірі, впровадження поточного тижневого рейтингу на факультеті ракетних військ стало ключовим чинником у покращенні рівня навченості, підвищенні морального становища та мотивації курсантів. Впровадження системи поточного тижневого рейтингу навчальних досягнень на всіх рівнях має велике значення для управління якістю підготовки майбутніх офіцерів. Ця система надає об'єктивні та різноманітні критерії для оцінки якості навчальних досягнень, враховуючи як складність предметів, так і успішне засвоєння навчальної програми. Успішність кожного курсанта можна аналізувати й трактувати з різних позицій, оскільки враховується всі аспекти навчальної, наукової та методичної діяльності протягом усього періоду спостережень. Під час аналізу успіхів курсанта немає стандартизації кожен курсант сприймається, як індивід. Успішна робота поточного тижневого рейтингу вимагає систематичного та відкритого використання системи заохочень та покарань на всіх рівнях управління підрозділами факультету ракетних військ і артилерії. Впровадження рейтингової системи оцінювання підтвердило ефективність, впливу на усереднені показники навченості курсантів факультету.

Якісну роботи рейтингу забезпечують два основних документа (програми), електронний журнал та сам електронний рейтинг.

Основною метою електронного журналу є систематизація всіх поточних оцінок навчальної групи та їх розподіл за навчальними дисциплінами. Обчислення середніх балів для окремих військовослужбовців, оцінювання дисциплін та виявлення негативних оцінок взагалі. У електронному журналі відведено окремий розділ для систематичного обліку контрольних заходів, таких як диференційовані заліки та екзамени. Передбачений і розділ повної статистичної інформації за кожного військовослужбовця кількість його оцінок загалом, за кожну дисципліну по кожному критерію оцінювання у відсотковому співвідношенні та інше. В розділі повної статистичної інформації передбачено детальний аналіз для кожного військовослужбовця, включаючи загальну кількість отриманих оцінок, відображення результатів за кожною дисципліною відповідно до критеріїв оцінювання в процентному співвідношенні та інші важливі аспекти.

Метою електронного рейтингу є максимальна наочність та інформативність отриманих результатів, створення відчуття серед курсантів здорової конкуренції, відкритості та прозорості в навчальному процесі.

Перший аркуш електронного рейтингу забезпечує демонстрацію: трьох най успішніших курсантів; трьох най гірших курсантів; рейтинг успішності серед навчальних курсів (з зазначенням відсоткових змін); рейтинг успішності серед навчальних груп (з зазначенням на скільки змінилось їхнє загальне місце); статистичні дані успішності серед чоловіків та жінок; статистичні дані успішності серед строкової служби, контрактної служби, цивільної молоді та ліцеїстів; статистичні дані успішності серед спеціальностей ракетні війська, наземна артилерія, артилерійська розвідка; статистичні дані успішності серед військових звань; статистичні дані успішності серед посадовців командирів груп відділень; статистичні дані успішності серед років навчання; основний середній бал факультету на основі всіх показників.

Другий аркуш електронного рейтингу надає наступну інформацію: повний список курсантів, впорядкований за рейтингом на факультеті; середній бал успішності для всіх військовослужбовців; середній бал для кожної навчальної дисципліни кожного військовослужбовця; середній бал для іспитів та диференційованих заліків кожного військовослужбовця; кількість отриманих двійок для кожного військовослужбовця.

Третій аркуш електронного рейтингу надає таку інформацію: середній бал для кожної спеціальності; рейтинг успішності серед навчальних груп із розподілом по спеціальностям (з вказанням зміни місця відносно попереднього тижня та відсоткових змін успішності); двадцять найкращих військовослужбовців кожної спеціальності; десять найгірших військовослужбовців кожної спеціальності.

Четвертий аркуш електронного рейтингу надає наступну інформацію: середній бал для кожного року навчання; рейтинг успішності серед навчальних груп з розподілом по рокам навчання; графіки успішності кожного року навчання з вказівкою мінімальних, середніх та максимальних норм рівня успішності для навчальних груп; графік успішності для всіх років навчання з урахуванням мінімальних, середніх та максимальних норм рівня успішності для навчальних груп конкретного року.

П’ятий аркуш електронного рейтингу подає таку інформацію: кількість двійок для кожної спеціальності; рейтинг за кількістю двійок серед навчальних груп із розподілом за спеціальностями; висвітлення сорока одного військовослужбовця наземної артилерії, двадцяти восьми артилерійських розвідників та вісімнадцяти ракетників із найвищою кількістю двійок у відповідності до їхньої спеціальності; рейтинг кількості двійок серед навчальних курсів; рейтинг кількості двійок серед років навчання.

Шостий аркуш електронного рейтингу подає таку інформацію: повний список курсантів випускників певної спеціальності, впорядкований за рейтингом випускників на факультеті; середній бал успішності для всіх військовослужбовців; середній бал для кожної навчальної дисципліни кожного військовослужбовця; середній бал для іспитів та диференційованих заліків кожного військовослужбовця; кількість отриманих двійок для кожного військовослужбовця.

УДК 623.62

Корольов В.М., Заєць Я.Г.

АНАЛІЗ РОЗВИТКУ РОСІЙСЬКОЇ ТЕХНІКИ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ ТА ЗАХОДИ ЩОДО ПРОТИДІЇ

У перші дні широкомасштабного вторгнення в Україну експерти дивувались, наскільки погано працювали російські системи радіоелектронної боротьби (РЕБ). Але зараз вони створюють серйозні проблеми для українських Сил оборони.

За оцінками експертів, розроблені російською промисловістю нові засоби РЕБ дозволяють забезпечити можливість радіорозвідки та радіоподавлення інтегральних систем зв'язку та передачі даних колективного користування, збільшити вірогідність селекції об'єктів придушення та скоротити час реакції. Крім того, вони здатні забезпечити приховане, вибіркове за місцем та (або) системним адресом блокування абонентських терміналів стільникового зв'язку та збільшити розмір зони ефективної дії за рахунок застосування нетрадиційних способів інтелектуального блокування абонентських терміналів зв'язку. Більшість комплексів зроблено за одним принципом - постановка потужних шумових перешкод, що має як недоліки, так і переваги.

Як показав досвід бойових дій, засоби РЕБ при неправильному застосуванні однаково відчутно впливають як на противника, так і на власні війська. Однак, вирішити однозначно цю проблему, навіть за умови підвищення рівня селекції та точності нанесення радіоелектронних ударів, рф поки не вдається. Армія рф справді має певну перевагу над Силами оборони України в засобах РЕБ, особливо в централізованому РЕБ а також в плані інтенсивності застосування засобів РЕБ, за рахунок більшої кількості станцій для ведення радіоелектронної боротьби та широкої номенклатури об'єктів, на які здійснюється вплив.

Ворог постійно намагається вдосконалювати як самі засоби РЕБ так і прийоми та способи їх застосування.

Україна робить все, щоб вийти у паритет із російськими окупантами у засобах РЕБ.

При створенні оборонною промисловістю вітчизняної техніки РЕБ оперативно-тактичного та тактичного рівня, слід враховувати що вона повинна мати: можливість

реалізації гнучкої структури управління як комплексами, так і окремими зразками техніки, що функціонують автономно і в складі пов'язаних пар; здатність комплексної та ефективної дії на широку номенклатуру радіоелектронних та комп'ютерних систем та засобів; високу стійкість в умовах протидії засобам радіоелектронного ураження, а також надійність, ремонтопридатність та ергономічність.

Крім того, з метою мінімізації загрози бути знищеними після виявлення засобами радіоелектронної розвідки, основний акцент слід робити на їх мобільності, що дозволяє швидко вийти з-під удару, а також своєчасно вийти на вигідні позиції для нанесення чергової електромагнітної атаки.

Також, під час створення нових комплексів РЕБ слід враховувати той факт, що у районах ведення бойових дій працюють і цивільні радіоелектронні засоби - канали зв'язку, яких обслуговують "швидку допомогу", підрозділи Державної служби з надзвичайних ситуацій та поліції, які бувають безпосередньо задіяні в процесі організації забезпечення діяльності військ.

Одним із ефективних заходів щодо протидії російським засобам радіоелектронної боротьби є збільшення кількості засобів радіотехнічної розвідки (РТР) і РЕБ в Силах оборони України та оснащення їх сучасними зразками станцій РТР, які дозволяють виявляти ворожі станції РЕБ, а потім, за допомогою вогневих засобів знищувати їх, в тому числі з використанням високоточних керованих боєприпасів та ударних БПлА тощо.

УДК 623.4.05

Королюк Н.О., Дудко М.В., Забайрачна Є.В., Бабіч А.Г., Мананков Р.О.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ПРИНЦИПІВ ЦІЛЕСПРЯМОВАНОЇ ПРОТИДІЇ ПРИ ПОБУДОВІ МАРШРУТІВ ПОЛЬОТУ БЕЗПІЛОТНОГО АПАРАТУ

Застосування концепції рефлексії управління (РУ) при прийняті обґрунтованих рішень висвітлено у ряді робіт. У рамках даної концепції передбачається, що встановлюється ступінь обізнаності протиборчих систем про цілі і можливості одна одно. Іншими словами, приймаюча рішення система управління S_1 повинна враховувати знання про цілі і можливості системи управління протиборчої сторони (ПС) S_2, знання цих систем про свої цілі і можливості. Так, основні позиції S_1 перед початком бойових дій вважаються відомими S_2 з точністю до десятків метрів, достатньо точно визначені вогневі можливості і можливості щодо прикриття. Крім того, пункти управління, кількість та склад особового складу, озброєння та військова техніка, їх якісний склад, а також цілі противника можуть бути достовірно визначені на основі аналізу розвідувальної інформації.

Таким чином, врахування передбачуваних цілей і можливостей противника системою S_1 у процесі прийняття рішень дозволяє здійснювати рефлексію міркувань, відтворюваних в органах управління. Основні принципи РУ:

– силовий тиск, який передбачає демонстрацію сили, спрямовану на формування у противника непропорційних цілей;

– формування необхідної (хибної) оцінки вихідної обстановки у противника, що передбачає маскування, дезінформацію, імітацію діяльності;

– вплив на вибір моменту прийняття рішення ПС, який може бути реалізований раптовістю своїх дій, що змушує противника діяти в умовах гострого дефіциту часу.

У загальному випадку для планування маршрутів польоту БПЛА можна використовувати різні ранги рефлексії. Прийнято вважати, якщо система, яка приймає рішення,

повністю ігнорує цільові установки протиборчої сторони, то її ранг рефлексії дорівнює нулю.

Використання стратегії РУ другого рангу при плануванні маршрутів розвідувального польоту БПЛА зумовлює вирішення таких завдань: формування у ПС прагнення атакувати хибні БПЛА з метою розкриття системи ППО; побудова цілеспрямованого впливу на процес вибору і захоплення БПЛА на супровід радіолокаційною станцією зенітно-ракетних комплексів, прийняття рішення на обстріл БПЛА; порушення просторової і часової узгодженості дій ПС; створення у ПС наміру спотвореного уявлення про замисел дій противника.

У зоні відповідальності ПС засоби ППО можуть одночасно ефективно "обслуговувати" обмежену кількість цілей. Застосування хибних БПЛА, що імітують на екранах РЛС позначки, подібні оцінкам реальних цілей, значно ускладнює розпізнавання реальних цілей і перевантажує використовувану систему. При обмеженому часі радіолокаційного спостереження за цілями в зоні відповідальності ПС виділення реальних цілей серед хибних ускладняються. При цьому процес селекції хибних цілей займає більше часу. У результаті засоби ППО зможуть пропустити справжні цілі. Прагнення ПС управляти діями у бажаному для себе напрямку (реалізація стратегії РУ першого рангу) та необхідність реалізації системою S_1 більш високого рангу рефлексії вимагає використовувати при плануванні маршрутів та визначення доцільної стратегії запланованого розвідувального польоту БПЛА стратегії РУ другого рангу.

УДК 519.81

Королюк Н.О., Забайрачна Є.В., Бабіч А.Г., Мананков Р.О., Дудко М.В.

ДОСЛІДЖЕННЯ ПРОЦЕСУ ПРИЙНЯТТЯ РІШЕННЯ НА ПУНКТІ УПРАВЛІННЯ ПОВІТРЯНИХ СИЛ ПРИ ЗАСТОСУВАННІ КОМПЛЕКСУ ЗАСОБІВ АВТОМАТИЗАЦІЇ

Досвід війни на території України, локальних війн та конфліктів останнього десятиріччя свідчить, що угруповання сил та засобів повітряного нападу здатні виконувати як оперативно-тактичні, так і стратегічні завдання. Це обумовлює підвищення значення боротьби у повітряному просторі для досягнення успіху не лише в окремих операціях збройних сил, але й у війні в цілому. Зростання ролі авіації у воєнній сфері підтверджується об’єктивними закономірностями, в основі яких лежить зростання обсягу завдань авіаційних угруповань в сучасних операціях (бойових діях).

Саме тому авіації належить особлива роль при охороні державного кордону в повітряному просторі. Аналіз останніх досліджень і публікацій показав, що системи управління авіацією країн НАТО на теперішній автоматизована на 96-98%.

Забезпечення вимогам ефективності управління літаками досягається автоматизацією процесів прийняття рішень. Ефективне управління авіацією обґрунтовує доцільність модифікації спеціального програмного забезпечення АСУ на принципово нових основах. Зокрема, визначення параметрів запланованого впливу винищувачем по повітряних цілях обумовлюють автоматизацію цього процесу з урахуванням логіки процесу виробки рішення. Виробка єдиних правил визначення методу наведення та області можливих атак по повітряних цілях являється складною логіко-аналітичною задачею через: особливості реалізації методів наведення в конкретних умовах; необхідність забезпечення мінімального часу перехвату повітряної цілі; складності математичної формалізації задачі; неможливість встановлення точних кількісних залежностей між параметрами, що впливають на процес, що розглядається, та дослідження евристичного досвіду. Управління винищувачами характеризується впливом великої кількості факторів і

загальної тенденції до ускладнення обстановки, в якій приймаються рішення. Прийняття своєчасних і обгрунтованих рішень затрудняється великим об'ємом інформації, що обробляється. Таким чином, динамічна зміна обстановки, жорсткі часові обмеження, значні об'єми, невизначеності і протиріч інформації, що обробляється вимагає обґрунтованості і оперативності прийняття рішень по управлінню авіацією. Загальна проблема виробки і прийняття рішення з управління винищувальною авіацією в екстремальних ситуаціях свідчать про необхідність розробки нового формального апарату. Він повинен забезпечити представлення різної інформації для вирішення задачі управління винищувальною авіацією, узгодження в рамках єдиного формалізму. А механізм доступу до моделей повинен забезпечувати автоматизований пошук.

Список використаних джерел

1. Чернов В.Г. Аналіз помилкових дій офіцерів бойового управління під час наведення винищувачів на повітряні цілі / В.Г. Чернов, І.П. Мажара, В.М. Сургай, Б.А. Телятник // *Новітні технології для захисту повітряного простору*: зб. тез конф., 18-19 квіт. 2023 р. Харківського національного університету Повітряних Сил імені Івана Кожедуба. Харків: ХНУПС ім.І.Кожедуба, 2023. С. 61.

2. Королюк Н.О., Романюк А.О., Зенова Є.С., Сорожкін А.В. Формалізація знань для ефективного застосування безпілотних літальних апаратів під час повітряної розвідки. *Системи обробки інформації*. 2023. № 3 (174). С.44-51.

УДК 621.317

Коротій О.О., Шеховцова І.О.

ОСОБЛИВОСТІ КАЛІБРУВАННЯ РОБОЧИХ ЕТАЛОНІВ ПОТУЖНОСТІ ЕЛЕКТРОМАГНІТНИХ КОЛИВАНЬ У КОАКСІАЛЬНИХ ТРАКТАХ

Визначення справності конкретного зразка озброєння та військової техніки під час експлуатації здійснюється шляхом періодичного контролю технічних характеристик, які впливають на його працездатність. Однією із характеристик, що дозволяє робити висновок про працездатність зразка озброєння та військової техніки, є вихідна потужність для вимірювання якої використовуються вимірювачі потужності (ватметри). Для підтвердження стабільності метрологічних характеристик вимірювачів потужності проводиться їх періодичне калібрування.

Калібрування вимірювачів потужності електромагнітних коливань на високих частотах пов'язане зі значними труднощами. Під час передавання одиниці потужності від робочого еталону до робочих засобів вимірювань основною складовою сумарної похибки є похибка неузгодженості. Під час використання ідеально узгодженого навантаження (в даному випадку це і є вимірювач потужності) в лінії передавання відсутня відбита хвиля (коефіцієнт відбиття дорівнює нулю) і падаюча потужність дорівнює потужності, що проходить в навантаження. Але в реальних умовах коефіцієнт відбиття не дорівнює нулю, і в лінії передавання виникає відбита хвиля, яка і є причиною виникнення похибки неузгодженості. Отже, під час вимірювання вихідної потужності необхідно враховувати коефіцієнт відбиття, який пов'язаний з коефіцієнтом стоячої хвилі напруги (далі – КСХН), вимірювання якого і необхідно проводити з метою мінімізації похибки неузгодженості. Існуючі методи виключення похибки неузгодженості зводяться до створення максимально узгоджених вимірювачів потужності та до вимірювання і врахування фактичних значень коефіцієнтів відбиття з подальшим введенням поправок на похибку неузгодженості.

На даний час основними радіовимірювальними приладами для вимірювання параметрів ліній передавання, а отже і вимірювання КСХН, є вимірювальні коаксіальні лінії радянського виробництва, які перебувають в експлуатації понад 50 років, мають значне зношення покриття коаксіальних з'єднувачів та потребують великих затрат часу на проведення вимірювань, а тому потребують заміни сучасними засобами вимірювань.

У той же час у провідних країнах світу з метою проведення калібрування вимірювачів потужності вимірювання коефіцієнтів відбиття проводять за допомогою векторних аналізаторів ланцюгів. Увесь процес вимірювання є автоматизованим і виконується програмним способом. Вирішення проблеми зменшення похибки вимірювань, викликаної неузгодженістю, здійснюється за допомогою так званої гама корекції. Похибки неузгодженості можна розрахувати з достатньою точністю, якщо відомі комплексні коефіцієнти відбиття перетворювачів потужності та робочих еталонів вимірювання яких і проводиться за допомогою векторних аналізаторів ланцюгів. В подальшому ці дані враховуються при обробці результатів вимірювань, що дозволяє проводити калібрування вимірювачів потужності із значно меншими затратами часу та значно покращує точність вимірювань. За допомогою гама корекції похибка неузгодженості практично повністю виключається і, таким чином, сумарна похибка вимірювання буде приблизно дорівнювати похибці вимірювання перетворювача потужності.

Використання векторних аналізаторів ланцюгів замість вимірювальних ліній дозволить здійснювати калібрування вимірювачів потужності автоматизованим способом із значно меншими затратами часу на калібрування та досягнути найвищого рівня точності вимірювань.

УДК: 355.433

Косенко В.П., Бабенко О.І.

ПІДХОДИ ЩОДО РОЗВИТКУ ПІДГОТОВКИ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ ЗС УКРАЇНИ

Перспективним шляхом розвитку підготовки ОВУ ЗС України є автоматизація окремих форм навчання органів військового управління з поступовим їх поєднанням в єдину автоматизовану систему підготовки (АСП).

Автоматизована система підготовки ЗС України повинна базуватися на структурі органів управління ЗС України. Враховуючи реорганізацію структури ЗС України з метою приведення її до оптимальної та відповідної зовнішньополітичній обстановці, необхідно розглядати перспективну структуру ЗС України.

Основними елементами автоматизованої системи підготовки ЗС України повинні бути комплекси засобів автоматизації (КЗА) органів військового управління та частин, що виділяються за ознакою організаційної самостійності. Кожен із КЗА є програмно-технічним комплексом, що складається з АРМ, кількість і функціональність яких відповідатиме завданням, які вирішуються в процесі підготовки органів управління (частини). КЗА частини, у свою чергу, матиме у своєму складі підпорядковані КЗА підрозділу.

Функціональна структура АСП ЗС України повинна мати складові:

- автоматизована система управління підготовкою ЗС України;
- автоматизована система виконання заходів підготовки ЗС України;
- інформаційно-аналітична система.

Елементи (складові) функціональних підсистем повинні бути в складі всіх рівнів і ланок АСП ЗС України, забезпечуючи в своїй сукупності спільно із засобами зв'язку та обміну даними вирішення всіх завдань підготовки ЗС України.

Основні воєнно-технічні задачі розробки та впровадження автоматизованої системи підготовки ОВУ ЗС України.

1. Визначення складу, призначення та порядку взаємодії складових елементів АСП ЗС України. АСП ЗС України повинна відповідати організаційно-штатній структурі військ і прийнятим способам управління. Разом з тим, використання новітніх засобів автоматизації може, у свою чергу, суттєво вплинути на організаційно-штатну структуру військ, сприяти зміні співвідношення кількісного і якісного складу сил і засобів, змінити порядок підлеглості, привести до появи нових способів управління.

2. Визначення та раціональний розподіл функцій управління між посадовими особами й засобами автоматизації. Тенденція розвитку подібних АСУ (АСУВ) така, що все більша й більша кількість процесів, які здійснюються за допомогою людини, будуть повністю автоматизованими, а на людину (оператора, командира) будуть покладені винятково "творчі" функції. Ступінь автоматизації повинен бути техніко-економічно обґрунтований із урахуванням необхідності вивільнення персоналу органів управління від виконання дій, які повторюються й створення умов для більш ефективного використання творчих можливостей персоналу.

3. Визначення мети автоматизації базових процесів функціонування системи підготовки ЗС України. Автоматизація процесів отримання, обробки й передачі інформації в першу чергу повинна вирішити задачі збору, обробки, оформлення, розмноження й наочного відображення інформації; підготовки даних для оцінки обстановки й прийняття рішення командиром (начальником) у будь-який момент часу; проведення оперативних, технічних та інших розрахунків; передачі інформації у вищі, підлеглі та взаємодіючі штаби.

4. Визначення переліку задач, що підлягають автоматизації. Із загального комплексу задач базових процесів функціонування системи підготовки в першу чергу підлягають автоматизації завдання, які носять масовий характер, і потребують виконання великої кількості обчислювальних і логічних операцій за обмежений час.

5. Розробка математичних моделей, методів, алгоритмів і програм. При алгоритмізації задач, рішення яких покладається на КЗА, виникає необхідність розробки математичних моделей, методів, алгоритмів і програм, тобто системи формальних правил, що однозначно визначає поведінку АСП ЗС України й команди управління, які нею виробляються в будь-якій ситуації.

Костянець О.В., Гусар Р.В., Чудак М.М., Галаганюк А.А., Захарченко В.С.

ЗАСТОСУВАННЯ СУЧАСНИХ SDR ПРИЙМАЧІВ ДЛЯ ВИЯВЛЕННЯ БАРАЖУЮЧИХ БОЄПРИПАСІВ

Аналіз досвіду ведення російсько-української війни показує, що інтенсивне застосування авіаційної складової ураження, може значно вплинути на хід бойових дій. У взаємодії з розвідувальними безпілотними авіаційними комплексами (БпАК), окупаційні війська активно застосовують ударні безпілотних літальних апаратів (БпЛА) як іноземного так і власного виробництва з метою знищення вогневих засобів сил оборони України, елементів системи протиповітряної оборони (ППО), радіолокаційних станцій (РЛС), іншої бойової техніки.

У зв'язку із зростаючою кількістю різних типів БпЛА та їх можливостями, радіоелектронна протидія стала однією з найбільш важливих задач засобів радіоелектронної боротьби (РЕБ) сил оборони України.

Для успішної боротьби з ударним БпЛА необхідно вирішення наступних задач пов'язаних з виявлення їх радіолокаційними та радіотехнічними засобами та своєчасною постановкою перешкод каналам управління цих пристроїв.

Однак, радіолокаційна дальність виявлення БпЛА обмежується висотами їх застосування, малими габаритами та матеріалами з яких вони виготовляються. Тому виникає необхідність радіотехнічного моніторингу випромінювання сигналів управління даних БпЛА.

Для вирішення цієї задачі можливо використання недорогого програмно-апаратного комплексу у складі SDR приймача та персонального комп'ютера з відповідними програмним забезпеченням.

Практика використання ударних БпЛА показала, що на першому етапі проводиться розвідка цілей за допомогою розвідувальних БпЛА, а вже потім наноситься ураження по цілям. Тому застосування SDR приймача дозволяє своєчасно попереджувати про небезпеку.

В роботі проведено оцінку сигналів випромінювання телеметрії та відеозображення як розвідувальних так і ударних БпЛА. Частотний та часовий аналіз їх параметрів дозволяє створювати бібліотеки даних з наступним розпізнаванням конкретних зразків безпілотних апаратів, що може бути автоматизовано.

Матеріали даних досліджень можуть бути використані для створення засобів радіотехнічної розвідки груп прикриття важливих об'єктів.

Котова М.А.

МЕТОДИКА АВТОМАТИЗОВАНОЇ ПОВІРКИ БАГАТОЗНАЧНИХ МІР ЕЛЕКТРИЧНОГО ОПОРУ

Розглядається методика повірки багатозначних мір електричного опору, яка забезпечує автоматизацію процесу вимірювань і обробки результатів вимірювань.

На даний час у Збройних Силах (ЗС) України експлуатується великий парк багатозначних мір (магазинів) електричного опору класів точності 0,01, 0,02, 0,05 (типів Р327, Р4831, Р4834, МСР-60, МСР-63, тощо), які застосовуються в якості робочих еталонів при здійсненні повірки широкої номенклатури робочих засобів вимірювальної техніки (ЗВТ) таких, як комбіновані електровимірювальні прилади (тестери), універсальні аналогові та цифрові омметри, багатофункціональні цифрові мультиметри, вимірювачі опору заземлення, мікро - та міліомметри. Зазначені ЗВТ широко використовують для контролю параметрів різноманітних зразків озброєння та військової техніки (ОВТ) на всіх етапах їх життєвого циклу, а також при експлуатації військових електроустановок, силових кабелів та мереж живлення багатьох об'єктів військового призначення.

На даний час метрологічне підтвердження магазинів електричного опору класів точності 0,01, 0,02, 0,05 у діапазоні номінальних значень від $1 \cdot 10^{-2}$ до $1 \cdot 10^{5}$ Ом здійснюється за допомогою потенціометричних установок типу У309, які експлуатуються у регіональних метрологічних військових частинах (РМВЧ). Установки реалізують процес повірки магазинів компенсаційним методом, при якому за допомогою потенціометра установки здійснюється порівняння падіння напруги на еталонній однозначній мірі електричного опору (ОМЕО) та магазині опору при протіканні крізь них постійного струму високої стабільності. Процес повірки потребує застосування значної кількості ЗВТ і характеризується високою трудомісткістю, зумовленою технічно застарілою конструкцією установки, яка не дозволяє здійснити автоматизацію процесу вимірювань та обробки результатів вимірювань. Внаслідок довгочасної експлуатації, установки типу У309, які експлуатуються у РМВЧ, вичерпали свій технічний ресурс та знаходяться

у значній стадії фізичного зносу. Тому актуальною на даний час проблемою є пошук альтернативних методів повірки магазинів електричного опору з використанням сучасних ЗВТ, здатних забезпечити автоматизацію процесу вимірювань та зменшити їх трудомісткість.

У доповіді розглядається можливість здійснення повірки магазинів електричного опору за допомогою сучасного 8½ - розрядного цифрового мультиметра типу Keithley 2002, обладнаного двома вимірювальними входами. Аналіз метрологічних характеристик мультиметра показує можливість його застосування для здійснення повірки магазинів електричного опору класів точності 0,02 та 0,05 методом прямих вимірювань, що дозволяє значно зменшити їх трудомісткість. За допомогою мультиметра Keithley 2002 може бути також реалізований процес повірки магазинів електричного опору класу точності 0,01 методом заміщення з використанням еталонної ОМЕО 2-го розряду. Завдяки наявності у мультиметра дистанційного інтерфейсу IEE-488, стає можливим здійснення автоматизації процесу вимірювань, математичної обробки результатів вимірювань з урахуванням значення початкового опору магазина та реєстрації одержаних даних за допомогою спеціально розробленого програмного забезпечення.

Запропонована методика дозволяє скоротити кількість ЗВТ, потрібних для реалізації процесу повірки магазинів електричного опору, та зменшити його трудомісткість завдяки можливості автоматизації процесу вимірювань з використанням сучасних ЗВТ.

Кравець Т.М., Баранова Т.А., Корнієнко О.С., Сівак О.І.

WGS-84: ТОПОГРАФІЧНА ПІДГОТОВКА ЧЕРЕЗ LAND NAVIGATION TRAINING

Анімоване та інтерактивне програмне забезпечення LAND NAVIGATION TRAINING (Навчання орієнтуванню на місцевості (НОМ)) призначене для покращення навичок військовослужбовців у роботі з топографічною картою та орієнтуванні на місцевості. Це програмне забезпечення доступне для встановлення як на операційні системи Windows, так і на Android. І хоча версії програми для Windows і Android мають деякі відмінності у своєму інтерфейсі, їх завдання і ціль залишаються однаковими.

НОМ включає анімовані тривимірні моделі місцевості, графіку, навчальний матеріал, інтерактивні інструменти, такі як магнітний компас, відлік темпу руху, лінійка для вимірювання відстаней і протрактор. Крім того, воно містить різноманітні вправи, 40 тестових завдань з орієнтування на місцевості та приклади практичного застосування в різних умовах.

НОМ може використовуватися як для навчання курсантів, так і для підвищення та контролю навичок офіцерів, сержантів та солдат. Ця програма дозволяє швидко покращити навички персоналу у сфері орієнтування на різних типах місцевості.

Категорії навчання включають: Основну інформацію про карти. Умовні знаки об’єктів на місцевості. Визначення місцезнаходження за допомогою карти. Орієнтування на карті. Визначення прямокутних координат MGRS. Визначення абсолютної висоти. Визначення азимутів. Визначення власного місцезнаходження за допомогою прямих та обернених засічок. Виконання завдань з орієнтування на місцевості.

В сучасних умовах актуальність цього додатку викликана тим що ЗСУ перейшли на карти у форматі WGS-84, як електронні так і паперові, відповідно у багатьох військовослужбовців не достатні вміння користуватись протрактором, визначати кути у mils та координати у MGRS. Цей додаток дозволяє здобути необхідні навички

Тестування з орієнтування на місцевості включає в себе 40 питань, які охоплюють всі аспекти навчального курсу. Після завершення тестування слухачі можуть отримати роздруковані результати, що містять відсотки за кожною категорією, загальний відсо-

ток, назву та дату. Ці результати можуть легко використовуватися інструкторами для оцінки рівня розуміння та засвоєння навчального матеріалу.

Зміст тестів програми LNT в цілому відповідає вимогам щодо вмінь та навичок, необхідних для виконання завдань у контексті програми топографічної підготовки ЗС України та навчальної дисципліни "Військова топографія". Основні відмінності полягають у методах підрахунку відстані (не за парами кроків, а використовуючи бісер темпу руху для проходження 100-метрового відрізку місцевості), як уже вказувалось вимірювання на картах здійснюються за стандартами НАТО, зокрема: визначення прямокутних координат MGRS, кутових вимірів у mils, користування шкалою закладень, системою розграфлення та номенклатурою.

Існує достатня кількість відеооглядів на YouTube, які допомагають в освоєнні програмного забезпечення LNT, зокрема в категорії завдань з орієнтування на місцевості. Виконання цих завдань може стати цікавою грою для військовослужбовців, схожою на квест у комп'ютерній грі, що сприяє підготовці до реальних умов.

У контексті переходу на WGS-84 та використання координат MGRS, які є необхідними для роботи з топографічною інформацією та орієнтування на місцевості, саме використання LAND NAVIGATION TRAINING сприяє підвищенню ефективності навчального процесу, забезпечуючи військовослужбовця необхідними навичками для успішної роботи на місцевості в різних умовах.

Кравець Т.М., Корнієнко О.С., Бондар Р.В., Ликова І.В.

ІНТЕГРОВАНА ПЛАТФОРМА АСУ «ДЕЛЬТА»: ЗБІЛЬШЕННЯ ЕФЕКТИВНОСТІ ТА ТОЧНОСТІ УПРАВЛІННЯ ВОГНЕМ

Інтеграційна платформа АСУ "ДЕЛЬТА" відображає дані про розташування підрозділів у реальному часі, що дозволяє забезпечити оперативне планування артилерійської розвідки. Попередня оцінка важливості розвідувальних відомостей допомагає визначити пріоритетні об'єкти для ураження та вирішення нагальних ситуацій. Реєстрація та систематизація отриманих розвідувальних відомостей є важливим етапом для забезпечення доступу до необхідної інформації під час планування та проведення операцій.

Аналітична робота командирів та штабів з використанням інструментів АСУ "ДЕЛЬТА" спрямована на ефективне використання можливостей бойових засобів та правильне прогнозування обстановки на полі бою. Інтеграційна платформа "Дельта" є ключовим інструментом для забезпечення інформаційної взаємодії та сумісності між різноманітними інформаційними системами військового управління та частин Збройних Сил України. Метою створення цієї платформи є інтеграція різноманітних джерел інформації у єдиний інформаційний простір ЗСУ, що дозволяє ефективно обробляти та використовувати цю інформацію для прийняття стратегічних та тактичних рішень. ІП "Дельта" забезпечує доступ до єдиного інформаційного простору для посадових осіб органів військового управління та військових частин, дозволяючи їм отримувати необхідну інформацію у реальному часі. Завдяки цій платформі здійснюється обробка та видача інформації на автоматизовані робочі місця посадових осіб, що сприяє покращенню процесів загальновійськового планування та управління ними.

Встановлення платформи "Дельта" на кафедрі комплексів та приладів артилерійської розвідки факультету ракетних військ і артилерії свідчить про успішне впровадження та використання цієї системи у навчальному процесі для проведення тренувань з планування бойових дій, як в аудиторії так і на переносних пунктах під час польових виходів. Можливість використання карт різних місцевостей, включаючи зону бойових дій, підвищує реалістичність та ефективність навчальних занять та практичних вправ. Використання АСУ "ДЕЛЬТА" також дозволяє вивчати та оцінювати місцевість, а та-

кож планувати розгортання підрозділів артилерійської ракетної системи. Командир може аналізувати загальний характер місцевості, її вплив на дії свого підрозділу та противника, а також визначати густоту та напрямок доріг у смузі дій противника.

Додатково, за допомогою АСУ "ДЕЛЬТА" можливе відображення місцевості в тривимірному зображенні, що дозволяє значно спростити орієнтування на місцевості. Такі можливості допомагають командиру планувати розгортання своїх підрозділів, вибирати оптимальні позиції для спостереження та ведення вогню, а також вибирати оптимальні маршрути руху.

Використання інтегрованої платформи АСУ "ДЕЛЬТА" в артилерійській розвідці та управлінні вогнем є важливим кроком у підвищенні ефективності та точності бойових операцій. Ця платформа забезпечує можливість детального аналізу місцевості, ефективного ведення розвідки, та планування розгортання підрозділів, що дозволяє командирам артилерійських підрозділів приймати обгрунтовані рішення на основі точних даних. Крім того, за допомогою цієї платформи можливе швидке оброблення та аналіз інформації, що допомагає у вчасному реагуванні на зміни в обстановці та вирішенні нагальних завдань. Таким чином, використання інтегрованої платформи АСУ "ДЕЛЬТА" стає ключовим елементом в підвищенні бойової готовності та успішності операцій артилерійських підрозділів.

Кравець Т.М., Корнієнко О.С., Гера В.Я., Сівак О.І.

АСУВ “СЛАВУТИЧ” ЯК ПЕРСПЕКТИВНА ГІС У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Зараз, у зв'язку з модернізацією Збройних Сил України, функціонал ГІС значно розширився та удосконалився, враховуючи потреби різних військових частин та специфіку їх застосування. Згідно з наказом Головнокомандувача ЗС України від 30.12.2021 року № 422 “Про затвердження Інструкції з використання топографічних, спеціальних, цифрових (електронних) карт геопросторових даних у Збройних Силах України”, ГІС ArcGIS стала невід'ємною частиною усіх систем управління та контролю над ресурсами та діяльністю Збройних Сил. Ця технологія також є основою систем управління в інших країнах-членах НАТО. Важливе значення мають хмарні сервіси ArcGIS OnLine, які є основою автоматизованих систем управління "Славутич" та "Дельта". Підсистема введення та відображення інформації про розташування, стан та дії військ "Славутич" розроблена для оперативного нанесення змін у ситуації на мапі та зберігання цих даних у цифровому вигляді. У результаті досліджень були створені електронні карти, які відображають оперативно-тактичну ситуацію з масштабами 1:50 000 та 1:200 000.

У результаті випробувань використання системи управління засобами "Славутич" було встановлено, що вона дозволяє відмовитися від ручного ведення оперативно-тактичної обстановки на паперових картах, що значно економить час на підготовку такої інформації. Також, за допомогою цієї системи можна швидко встановлювати точки на карті за плоскими прямокутними координатами або переводити їх до іншої системи координат. Зокрема, спеціалісти можуть точно визначати координати об'єктів на місцевості та їх висоту, а також швидко змінювати обстановку за потреби.

Однією з переваг системи є можливість відображення рельєфу обраної території в кольорі, що дозволяє краще координувати дії військових командирів у плануванні маршрутів, розташуванні загороджень та інших важливих об'єктів. Додатково, система дозволяє зберігати всю інформацію про обстановку в електронному вигляді та надійно захищати її за допомогою різних носіїв даних.

Наявність спеціалізованого довідника з тактико-технічними характеристиками обладнання військ, противника та союзників, а також можливість пошуку цих даних, робить

систему "Славутич" незамінною для військового планування та прийняття стратегічних рішень.

Кіберджура - це нова ініціатива, яка активно розвивається на базі АСУВ "Славутич". Основна мета Кіберджури - створення мережі комп'ютерних класів з використанням АСУВ "Славутич-Кіберджура" у Національному університеті оборони України імені Івана Черняховського. Наразі функціонує три таких класи, які з'єднані через центральний сервер Кіберджури в університеті. Згідно з планом, школи, які мають доступ до хмарних технологій ArcGIS Online, формують опорно-штурмові команди кіборгів, тоді як інші школи та міжнародні проекти створюють мережеві команди кіборгів. У деяких ліцеях та позашкільних закладах, які мають підвищену військову підготовку, створюються Класи Кіберджури, що сприяє професійній орієнтації на тактичному рівні під час підготовки до Кіберджури.

Отже, АСУВ "Славутич" надає можливості для: Ведення та відображення положення, стану та дій військ на електронній карті місцевості, формування карт операцій та передачі та отримання даних обстановки. Аналізу та вивчення даних обстановки. Забезпечення топогеодезичного та навігаційного забезпечення. Надання службовим особам різноманітної довідкової інформації за допомогою інформаційно-довідкової системи, включаючи тематичні довідники у різних форматах.

Кравець Т.М., Поляков А.Ю., Гера В.Я., Бондар Р.В.

ЗАСТОСУВАННЯ ARCGIS ДЛЯ ПІДВИЩЕННЯ ПРОФЕСІЙНОЇ МАЙСТЕРНОСТІ ВІЙСЬКОВИХ ФАХІВЦІВ ЗСУ

Геоінформаційні системи (ГІС) знаходять своє застосування у різних галузях життя, у тому числі й у військовій справі. ГІС, спрямовані на військові потреби, використовуються для оптимізації управління військами та зброєю. Головне призначення таких систем полягає у забезпеченні ефективного керівництва військами, збереженні та відображенні інформації, обробці даних та підтримці у процесі прийняття стратегічних рішень на різних рівнях командного складу, від підрозділів і частин до високого командування. ГІС для військових застосувань забезпечують можливість автоматизованого розв'язання завдань управління військами та зброєю, враховуючи місцеві умови. Вирішення таких завдань з використанням геоінформаційного забезпечення, зокрема у контексті повномасштабної війни, є актуальною проблемою для ефективного керівництва підрозділами та частинами Збройних Сил України.

Розвиток передових інформаційних засобів для ведення війни на території Донецької, Луганської, Запорізької областей, таких як супутникові навігаційні системи, радіолокаційні станції AN/TPQ, безпілотні авіаційні комплекси, автоматизовані комплекси розвідки, метеорологічні засоби тощо, вимагає перегляду традиційних підходів до аналізу інформації про дії військ. Для ефективного розв'язання таких завдань потрібно використовувати технології, які поєднують простір та час з обширними наборами даних, такими як атрибутивна інформація про об'єкти, дані розвідки, кліматичні умови тощо. У цьому контексті геоінформаційний продукт ArcGIS є оптимальним рішенням.

Основні переваги використання ГІС у військовому навчально-виховному процесі включають автоматизацію збору, зберігання та використання інформації про місцевість у електронному вигляді, аналіз місцевості та об'єктів, можливість розрахунків та моделювання ситуацій на електронній карті, створення тривимірних моделей, а також обмін інформацією та зменшення використання паперових карт.

Для кращого розуміння території та її особливостей, корисно створювати тривимірні моделі. Це дозволяє краще оцінити рельєф, визначити переваги та недоліки. Для цього використовується модуль ArcScene в рамках програмного забезпечення ArcGIS. Споча-

тку шар рельєфу копіюється з ArcMap до ArcScene, що створює зображення в двомірному форматі та чорно-білий колір. Проте після визначення градації та вибору потрібної палітри кольорів створюється тривимірна модель, де вказується розташування шару з рельєфом та його масштабування для кращого візуального сприйняття. Створення файлової бази геоданих дуже спрощує роботу курсантів при нанесенні тактичної обстановки. Такі бази дозволяють легко змінювати, переміщувати та змінювати тактичні умовні знаки, що значно полегшує планування бойових дій.

Сучасні умови війни вимагають від армії використання передових засобів, таких як геоінформаційні системи. Це дозволяє поєднати топографічну та навігаційну інформацію з сучасними технологіями, що підвищує ефективність управління військами та забезпечує оперативний аналіз та оновлення інформації про місцевість.

Використання геоінформаційних систем у військовому навчанні та практичній діяльності є надзвичайно важливим етапом у модернізації та підвищенні ефективності збройних сил. Впровадження тривимірних моделей місцевості, файлових баз геоданих та інших сучасних технологій дозволяє не лише краще зрозуміти та аналізувати територію, але й значно полегшує процес планування бойових дій та управління військами.

Красинський С.В., Ніколенко В.В.

ІНФОРМАЦІЙНИЙ ФОНД ЗАБЕЗПЕЧЕННЯ ЄДНОСТІ ВИМІРЮВАНЬ У СФЕРІ ОБОРОНИ: СТАН І НАПРЯМКИ РОЗВИТКУ

Законом України «Про метрологію та метрологічну діяльність» (далі – Закон) передбачено ведення науковими метрологічними центрами інформаційних фондів щодо забезпечення єдності вимірювань за напрямами своєї діяльності у сфері законодавчо регульованої метрології.

Створення, розвиток та вдосконалення інформаційного фонду забезпечення єдності вимірювань у сфері оборони передбачає розробку військових нормативних документів з питань метрологічного забезпечення, у тому числі на методи та засоби калібрування засобів вимірювальної техніки (далі – ЗВТ), метрологічного обслуговування зразків озброєння та військової техніки (далі – ОВТ), метрологічні норми, правила і методики виконання вимірювань, а також тактико-технічні, техніко-економічні, оперативно-технічні вимоги до створення, закупівлі та експлуатації ОВТ та ЗВТ.

За результатами узагальнення раніше проведених досліджень та з урахуванням завдань забезпечення єдності вимірювань у сфері оборони, здійснена перевірка наявності, достатності та актуальності діючих національних та військових нормативних документів за напрямками та видами метрологічної діяльності у сфері оборони.

Аналізування діючих національних та військових нормативних документів має на меті визначення їх здатності задовільнити потреби щодо: досягнення необхідної точності і достовірності результатів вимірювань параметрів (характеристик) зразків ОВТ, які забезпечують ефективність їх використання, безпеку і безаварійність; достовірність результатів вимірювань під час бойового застосування ОВТ та виконання ремонтно-відновлювальних робіт; метрологічне підтверджування придатності ЗВТ до використання в реальних умовах експлуатації ОВТ.

На стратегічному рівні управління метрологічною діяльністю у сфері оборони визначаються: концепція, загальні напрямки військово-технічної політики в галузі метрологічного забезпечення та здійснюється загальне управління метрологічним забезпеченням.

Правовою основою стратегічного управління метрологічною діяльністю є законодавство України, яке складається з: Закону; Постанови КМ України «Про особливості забезпечення єдності вимірювань у сфері оборони України» (далі – Постанова); Постанови КМ України «Про затвердження Порядку логістичного забезпечення сил оборони

під час виконання завдань з оборони, захисту її суверенітету, територіальної цілісності та недоторканності»; Доктрини застосування сил логістики; наказу Міністерства оборони України «Про затвердження Порядку координації роботи метрологічних служб у сфері оборони».

Закон відокремлює сферу законодавчо регульованої метрології та визначає види метрологічної діяльності, щодо яких здійснюється державне регулювання стосовно вимірювань, одиниць вимірювання та засобів вимірювальної техніки.

Управління системою забезпечення єдності вимірювань, метрологічною діяльністю сил оборони здійснюється в єдиній системі логістичного забезпечення. Механізм планування та організації логістичного забезпечення Збройних Сил України, а також інших утворених відповідно до законів військових формувань (Національної гвардії, Держспецтрансслужби), інших складових сил безпеки, які залучаються до виконання завдань з оборони держави визначаються Постановою КМ України «Про затвердження Порядку логістичного забезпечення сил оборони під час виконання завдань з оборони держави, захисту її суверенітету, територіальної цілісності та недоторканності» та «Доктриною застосування сил логістики». Аналіз цих документів показує, що вони створюють необхідну нормативну основу для розробки концептуальних основ розвитку системи забезпечення єдності вимірювань у сфері оборони, напрямів військово-технічної політики у галузі метрологічного забезпечення військ (сил).

На теперішний час офіційної концепції забезпечення єдності вимірювань у сфері оборони України не існує. Концепція повинна передбачати розвиток засад забезпечення єдності вимірювань з урахуванням прийняття на озброєння новітніх видів ОВТ та економічних взаємовідносин з постачальниками ОВТ та ЗВТ, необхідність удосконалення нормативно-правової бази метрологічної діяльності за стандартами НАТО.

На оперативному рівні управління метрологічною діяльністю у сфері оборони вирішуються завдання щодо планування та організації МлЗ військ під час проведення заходів бойової підготовки, оперативного розгортання, підготовки та ведення операцій (бойових дій), відновлення боєздатності військ (сил). Нормативна основа оперативного рівня управління метрологічною діяльністю складається з відомчих керівних документів, які затверджені та введені в дію відомчими наказами та директивами, а також національними нормативними документами.

В цілому діючи нормативні документи на оперативному рівні управління метрологічною діяльністю дозволяють забезпечити стале функціонування системи метрологічного забезпечення у сфері оборони. Більшість документів розроблено протягом останніх 5 років та є такими, що відповідають національному законодавству, сучасній міжнародній практиці нормативного забезпечення метрологічної діяльності (стандартам НАТО), але потребують часткового перегляду та подальшого розвитку.

В цілому інформаційний фонд нормативних документів дозволяє забезпечити функціонування системи метрологічного забезпечення у сфері оборони України.

Нормативно-правова основа забезпечення єдності вимірювань забезпечення єдності вимірювань у сфері оборони сформована, але не в повній мірі враховує особливості метрологічної діяльності в реальних умовах функціонування сил оборони. Постанова КМ України «Про особливості забезпечення єдності вимірювань у сфері оборони України» не охоплює всі види метрологічної діяльності, особливості забезпечення єдності вимірювань у сфері оборони України, не створює передумов розвитку нормативної основи забезпечення єдності вимірювань у сфері оборони України.

Подальша розбудова інформаційного фонду нормативних документів повинна здійснюватися з урахуванням нової Концепції забезпечення єдності вимірювань у сфері оборони, необхідності гармонізації зі стандартами НАТО на єдиній термінологічної основі та бути спрямована на вирішення актуальних проблем, які пов’язані з організаційними, економічними, міжнародними відносинами, сучасними метрологічними вимогами до ОВТ.

УДК 621.327:681.5

Kryvonos V., Tupitsya I.

TECHNOLOGY OF AUTOMATED AERIAL RECONNAISSANCE DATA PROCESSING FOR UNMANNED AVIATION SYSTEMS

Problematic aspects of the process of air reconnaissance data processing are studied, taking into account the experience of combat operations on the territory of Ukraine. The technology of automated aerial reconnaissance data processing for unmanned aircraft systems is proposed, the distinctive feature of which is the use of a synthesis of computer vision technologies and deep machine learning based on artificial neural networks to automate the process of detecting aerial reconnaissance objects. The use of the specified technology allows to increase the efficiency of air reconnaissance data processing.

The experience of hostilities on the territory of Ukraine shows the active use of unmanned aerial systems (UAS) both by units of the defense forces and by the enemy. At the same time, it should be noted that both domestically produced anti-aircraft missiles and those provided from the first days of the war by partner countries are used for reconnaissance and strike purposes. Thus, the experience of using reconnaissance UAS by units of the security and defense sector shows the dependence of the efficiency of decryption of air reconnaissance data (ARD) and the reliability of the decryption results on the professional abilities of the operator of the target load and the physiological abilities of the human visual system. This is due to the lack of means (tools) for automating the processes of processing and deciphering ARD both on board unmanned aerial vehicles and at ground command and control stations.

In turn, a characteristic feature of the enemy in the field of anti-missile defense is the dynamic implementation of modern progressive technologies and testing their effectiveness in combat conditions. Thus, among the enemy's innovations, it should be noted the use of computer vision technologies, which make it possible to provide conditions for increasing the level of efficiency of processing intelligence information and the reliability of ARD. At the same time, it should be noted that this trend is observed for UAS of all classes, i.e. from FPV drones (actively used on the battle lines) to UAS of the operational-tactical class. Thus, to date, the advantage of the enemy in the digitalization of the intelligence and information space is observed, which leads to the need to find new approaches and transform the process of processing and deciphering air reconnaissance data.

In turn, the automation of the video image processing process today is closely related to the use of OpenCV computer vision libraries, which have a fairly large functionality for processing and evaluating video data. So today, the synthesis of computer vision technologies and deep machine learning based on artificial neural networks has made it possible to implement the process of automating the detection, segmentation and classification of objects of interest [1-4].

Analysis of the latest scientific research shows that the above-mentioned technologies are actively used in the following areas:

- automated tracking of vehicle traffic on busy road sections, vehicle parking lots and other city infrastructure facilities;
- detection and recognition of license plates of vehicles and faces of violators in the system of situational centers of law enforcement agencies for prompt response to offenses.

In this regard, in order to increase the level of processing efficiency and reliability of air reconnaissance data, it is proposed to investigate the possibility of automating the process of detection and recognition of aerial reconnaissance objects based on computer vision technologies, deep machine learning, and artificial neural networks.

To solve the above-mentioned scientific problem, algorithms of the YOLO family were studied, which are quite actively developing (dynamic transformation from the first to the eighth versions) [3]. These algorithms are used in many directions (detection, recognition, segmentation, classification, posture determination) due to the possibility of balancing between efficiency and accuracy indicators [4].

The analysis of the conducted studies shows that today the YOLOv8 algorithms have an advantage compared to their predecessors according to the following indicators:

- accuracy of detection of objects of interest;
- algorithmic complexity;
- efficiency of data processing.

Therefore, it is proposed to use YOLOv8 algorithms for the further development of technology for automated processing of air reconnaissance data for unmanned aircraft systems.

To develop this technology, the concept proposed in [5, 6] was used, which provides for the formation of a data set according to the requirements of the air reconnaissance system for model training. The results of the evaluation of the effectiveness of the developed technology of automated processing of air reconnaissance data indicate that the use of the developed technology allows to increase the efficiency of video data processing.

References

1. Object Detection in 2024: The Definitive Guide. Viso: web site. URL: https://viso.ai/deep-learning/object-detection. (Accessed 12 January 2024).

2. Shi Z. Object Detection Models and Research Directions. 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China. 2021. P. 546-550. DOI: https://doi.org/10.1109/ICCECE51280.2021.9342049.

3. Enhanced Object Detection: How to Effectively Implement YOLOv8. Towardsdatascience: web site. URL: https://towardsdatascience.com/enhanced-object-detection-how-to-effectively-implement-yolov8-afd1bf6132ae. (Accessed 7 January 2024).

4. Algorithm Principles and Implementation with Yolov8. Mmyolo.readthedocs.io: web site. URL: https://mmyolo.readthedocs.io/en/latest/recommended_topics/algorithm_descriptions/ yolov8_ description.html. (Accessed 7 January 2024).

5. Tupitsya I., Kryvonos V., Kibitkin S., Ivashchuk L., Bielivtsov A. The Conceptual Model of the Automation of Deciphering Aerial Reconnaissance Data Using Artificial Intelligence System Technologies. Systems of Arms and Military Equipment. 2023. № 1 (73). C. 75-81. DOI: https://doi.org/10.30748/soivt.2023.73.09.

6. Tupitsya I., Deinezhenko I., Kryzhanivskyi Ye., Parkhomenko M., Volkov Yu., Eidelstein G. Method of Automating the Process of Object Detection to Increase the Efficiency of Deciphering Aerial Reconnaissance Data. Information Processing Systems. 2023. № 2 (173). C. 63-73. DOI: https://doi.org/10.30748/soi.2023.173.08.

Кубявка М.Б., Пирогов К.О., Черних Ю.О.

ІНФОРМАЦІЙНА ПІДГОТОВКА ЯК СПОСІБ ФОРМУВАННЯ ФУНДАМЕНТУ ІНФОРМАЦІЙНОЇ КУЛЬТУРИ ОФІЦЕРА ЗБРОЙНИХ СИЛ УКРАЇНИ

Аналіз професійних вимог до офіцерських кадрів Збройних Сил (далі – ЗС) України показує наявність як єдиних загальних складових до підготовки фахівців з вищою освітою, так і специфічних особливих вимог, характерних тільки для військових фахівців. Іншими словами, вимоги до офіцерського складу ЗС України мають відповідати як

державним вимогам до рівня підготовки дипломованих фахівців, так і особливим умовам військової служби та діяльності офіцерського складу.

Розглядаючи розвиток системи військової освіти, не можна залишити поза увагою зміни у структурі особистості, що відбуваються під впливом сучасного інформаційного середовища. Очевидно, що ці зміни мають впливати на всі складові підготовки сучасного військового фахівця. Насамперед це стосується такого елементу підготовки, як готовність до професійної діяльності. При цьому зміст готовності офіцера до службової (бойової) діяльності має такі складові:

– мотиваційна готовність, тобто співвідношення зовнішніх спонукань та внутрішньої потреби до набуття професійних якостей;

– емоційно-вольова готовність, тобто націленість на діяльність із придбання професії;

– когнітивна готовність або необхідний рівень розвитку сприйняття, мислення, пам'яті;

– операційна готовність тобто здатність до виконання професійних завдань, володіння навичками застосування певних зразків озброєння та експлуатації військової техніки;

– інформаційна готовність тобто наявність вмінь користувача у сфері нових інформаційних технологій, певний рівень інформаційної культури.

Включення інформаційної компоненти у зміст готовності до професійної діяльності майбутнього офіцера ЗС України нині відповідає потребам інформаційного суспільства та має стати предметом пильного вивчення та пошуку шляхів її реалізації у навчальному процесі вищих військових навчальних закладів (далі – ВВНЗ).

Професійна діяльність офіцера виступає найважливішою стороною його військової праці. Для успішної військово-професійної діяльності офіцеру необхідно сформувати знання, навички, уміння, особистісну позицію, психологічні та інші якості. Офіцер повинен бути в змозі усвідомити цілі та завдання військової служби, вивчити обстановку та прийняти рішення, спланувати роботи з реалізації рішення та організувати його виконання, провести аналіз результатів та корекцію військово-професійної діяльності. Іншими словами, необхідно забезпечити підготовку офіцерських кадрів, здатних кваліфіковано управляти підлеглими військовими підрозділами та частинами як у процесі повсякденної професійної діяльності, так й у бойової обстановці, домагаючись ефективного вирішення поставлених завдань.

Серед чинників, які впливають на якість управління, можна назвати: знання загальних методів управління; вміння використовувати технічні засоби для збирання та обробки інформації; знання цільових функцій об'єкта управління.

Виходячи з перерахованих факторів можна сформулювати основні вимоги до військово-професійної підготовки офіцерів, а саме: глибокі знання у предметній області; вміння творчо мислити та приймати обґрунтовані рішення; знання сучасних методів управління, уміння використовувати технічні засоби збирання, обробки та доведення інформації (інформаційні технології). Виділені вище формулювання вимог до сучасних офіцерів вказують на необхідність формування інформаційної культури сучасного офіцера для ЗС України, оскільки інформатизація всіх сторін професійної діяльності сучасної армії посилюється з кожним днем.

Найсуттєвішою закономірністю сучасного етапу військово-технічного прогресу стала інформатизація військової справи загалом, тобто. розвиток систем управління, зв'язку, навігації, розвідки, засобів радіоелектронної боротьби тощо. Необхідність інформатизації обумовлена об'єктивними потребами воєнної практики. Ефективність військової діяльності, бойова ефективність зброї тепер у найбільшої мірі визначаються інформаційним забезпеченням. Це обумовлено різким зростанням масштабності і складності завдань, розв'язуваних у сучасному бою, його швидкоплинністю, участю в ньому різ-

норідних сил і засобів, що призвело до багаторазового збільшення одержуваної командиром інформації з одночасним скороченням часу на її обробку та прийняття рішень.

Проведений у ВВНЗ аналіз стану справ, пов'язаних із оснащенням, застосуванням обчислювальних засобів, виявив загальні проблеми, без вирішення яких неможливо очікувати відчутних результатів. До найважливіших з них, на наш погляд, слід віднести відсутність єдиної методології впровадження нових інформаційних технологій, недостатнє опрацювання психолого-педагогічних завдань інформатизації військової освіти, слабку координацію та кооперацію ВВНЗ при розробці програмного та методичного забезпечення навчального процесу, недостатню підготовку керівного та викладацького складу щодо впровадження сучасних інформаційних технологій, різнотипність. Наголошується і на необхідності вирішення низки проблемних питань, пов'язаних з організацією управління процесом інформатизації системи військової освіти.

Перехід сучасного суспільства до інформаційної епохи свого розвитку висуває як одне з основних завдань, що стоять перед системою військової освіти, завдання формування основ інформаційної культури майбутнього офіцера. Потреба ЗС України у кваліфікованих офіцерських кадрів, які володіють повним арсеналом засобів та методів інформатики, перетворюється на провідний фактор освітньої політики у ВВНЗ.

Цілісна реалізація цієї потреби неможлива без включення інформаційної компоненти до системи підготовки майбутніх офіцерських кадрів. У сучасних умовах потрібно підготувати офіцера до швидкого сприйняття та обробки інформації, що надходить. Стає недостатнім вміти самостійно освоювати та накопичувати інформацію, оскільки з'являється залежність від інформації, набутої іншими людьми, а також істотного збільшення її обсягу. Для того, щоб вільно орієнтуватися в інформаційному потоці, сучасному військовому фахівцю необхідно володіти також інформаційною культурою як однією зі складових культури загалом.

Отже, у службової (бойової) діяльності офіцерських кадрів ЗС України можна виділити інформаційну компоненту, тобто. діяльність з накопичення та використання інформації за допомогою інформаційних технологій. До неї можна віднести: збирання та реєстрацію інформації; передачу інформації; формалізацію, кодування та зберігання інформації; пошук інформації; обробку інформації; прийняття рішень; доведення рішень до виконавців. На перший погляд, всі ці компоненти цілком можуть бути реалізовані і без використання інформаційних технологій, за допомогою традиційних способів прийняття рішення, як це й робилося протягом тривалого часу. Але використання інформаційних технологій дозволяє підвищити один із основних показників ефективності управління у військово-технічних системах – оперативність управління, а також забезпечити підвищення якості прийнятих рішень. Особливої ролі при цьому набуває діяльність людини-оператора сучасної АСУ військами та зброєю.

Як було зазначено вище, діяльність багатьох офіцерів на первинних офіцерських посадах пов'язана з виконанням операторських функцій в автоматизованих системах управління (далі – АСУ) військами, зброєю та повсякденною діяльністю. Роль цього виду службової (бойової) діяльності офіцерів надалі зростатиме. Тому доцільно розглянути концептуально-формальну модель діяльності оператора АСУ.

Роль людини в АСУ, її місце та функції визначаються ступенем автоматизації, під якою розуміється обсяг функцій управління переданих апаратно-програмному комплексу АСУ. Для АСУ військового призначення характерною є реалізація функцій автоматизації збору інформації про об'єкт (об'єкти) управління та пред'явлення її оператору.

Дані про об'єкт, його поточний стан подаються у вигляді інформаційної моделі на відповідних засобах відображення. Необхідність таких засобів виникає за багатьма обставинами, зокрема віддаленістю об'єкта управління, неможливістю сприйняття оператором тих чи інших характеристик об'єкта, небажаністю присутності людини поблизу об'єкта тощо. На основі інформаційної моделі у свідомості оператора формується концептуальна модель об'єкта, за допомогою якої він оцінює ситуацію, що склалася на

об'єкті управління, і на основі знань та професійного досвіду виробляє керуючий вплив, передаючи його через командний пульт управління на виконавчі органи, тим самим втручаючись у процес функціонування системи.

Розглянемо докладніше засоби інформатики та інформаційних технологій, знання яких необхідні підвищення ефективності діяльності офіцерських кадрів ЗС України. Випускники ВВНЗ на первинних офіцерських посадах, тобто. на нижньому щаблі системи управління, можуть використовувати у своїй професійній діяльності такі види інформаційних технологій: інформаційні технології обробки даних; інформаційні технології управління; інформаційні технології організації та підтримки комунікаційних процесів у штабній роботі; інформаційні технології підтримки прийняття рішень; інформаційні технології експертних систем.

Для роботи з переліченими вище видами інформаційних технологій випускники ВВНЗ відповідно до вимог відповідного професійного стандарту за військово-обліковою спеціальністю повинні мати наступну систему умінь, знань та навичок у галузі інформатики та інформаційних технологій:

бути ознайомленими:

- з предметом інформатики, завданнями та вимогами до обсягу знань, умінь та навичок з навчальної дисципліни, що вивчається;
- з тенденціями розвитку інформатики за сучасних умов;

мати уявлення:

- про інформацію, методи її зберігання, обробки та передачі;
- про математичне моделювання;

знати та вміти використовувати:

- математичні моделі систем та процесів у природознавстві та техніці;

мати досвід:

- програмування та використання можливостей обчислювальної техніки та програмного забезпечення;
- використання засобів комп'ютерної графіки.

Перелічені вище формалізовані цілі інформаційної підготовки були отримані як в результаті аналізу діяльності офіцерських кадрів на первинних офіцерських посадах, так і виділення варіантної складової у вимогах стандарту вищої освіти для інженерних спеціальностей та освітніх програм, за якими здійснюється підготовка військових фахівців у ВВНЗ ЗС України.

УДК 623.462.22

Кудряшов В.Є., Коломійцев О.В., Кулєшов О.В., Клівець С.І., Бердочник А.Д., Беспалько О.В.

МЕТОДИКА ЧИСЛОВОГО МОДЕЛЮВАННЯ ВИЗНАЧЕННЯ ПОКАЗНИКА ЕФЕКТИВНОСТІ СТРІЛЬБИ РАКЕТОЮ БОЙОВОЮ МАШИНОЮ ПО РІЗНИХ ЗА ТИПАМИ ПОВІТРЯНИХ ЦІЛЯХ ПРИ ЗМІНІ ВИПАДКОВИХ ЗНАЧЕНЬ ЇЇ ПРОМАХУ

В доповіді проведено аналіз існуючих методів стрільби ракетами по різним за типами повітряних цілей (ПЦ). Запропоновано методику числового моделювання визначення показника ефективності стрільби ракетою бойовою машиною (БМ) зенітного ракетного комплексу (ЗРК) по різних ПЦ при зміні випадкових значень її промаху у вигляді значень умовної ймовірності їх ураження. В методиці враховані конструктивні і технічні характеристики станцій та систем БМ ЗРК малої дальності та ракети.

Представлено результати розрахунків похилої дальності пуску ракет та похідні дальності до дальньої межі і середньої зон ураження ЗРК у різних умовах стрільби. Обґрунтований підхід щодо використання результатів запропонованої методики до використання командирам БМ ЗРК та батарей при плануванні бойових дій.

Відомо, що проблема моделювання бойових дій військ є однією з ключових у теорії і практиці управління військами. Загальний показник ефективності стрільби БМ ЗРК – є ймовірність виконання вогневого завдання, яку можливо визначити на основі технічних характеристик та параметрів систем комплексу. При цьому, необхідно враховувати ефективну площу розповсюдження (ЕПР) ПЦ та протидію противника.

Протидія противника у вигляді постановки завад по системам (станціям виявлення (СВЦ) і супроводження (ССЦ) цілей тощо) ЗРК та маневрування ПЦ і вогнева дія – знижують ефективність стрільби, яку необхідно оцінювати.

Значення показника ефективності стрільби, а саме – значення умовних ймовірностей ураження ПЦ при стрільбі одною ракетою необхідні при розгляді похибок наведення ракет та похибок системи підриву бойової частини ракети.

Однак, досі відсутній чисельний метод, який дозволяє розрахувати ймовірність виконання вогневого завдання з врахуванням технічних характеристик та параметрів систем БМ ЗРК і ракети, а також протидію противника стрільбі.

Таким чином, задача визначення ймовірності виконання вогневого завдання у різних умовах застосування БМ ЗРК є актуальною науковою задачею. Тому, необхідно розробити методику числового моделювання визначення показника ефективності стрільби ракетою БМ по різних ПЦ при зміні випадкових значень її промаху.

Представлені результати розрахунків похилі дальності до дальньої межі зони ураження (ДМЗУ) комплексу. Визначені значення першого роду похибок стрільби ракетами у якості ймовірностей проходження ракети у ”трубці” заданого радіусу. Надані значення другого роду похибок стрільби, у вигляді величин умовних ймовірностей спрацювання радіозривника (РЗ) ракети у різноманітних умовах.

Показано, що зміна значень ефективної площі розповсюдження ПЦ та рівня завад по радіолокаційним каналам станції супроводження цілей і РЗ, а також швидкості їх польоту і перевантажень – надають значення показника ефективності стрільби з визначенням ДМЗУ комплексу.

Отже, за вхідними даними технічних характеристик і параметрів станцій та систем ЗРК знайдено відношення сигнал/шум у радіолокаційній станції (РЛС) розвідки БМ і ССЦ.

Визначено ймовірності правильного виявлення та ймовірності пуску ракет по ПЦ з різними ЕПР в умовах завад та можливого їх маневрування.

Розраховано дальності пуску ракет та похідні дальності до ДМЗУ ЗРК у різних умовах стрільби.

Відмічено деякі обмеження в енергетичному потенціалі РЛС розвідки БМ та завадостійкості ССЦ БМ.

При відсутності протидії стрільбі величина умовної ймовірності ураження ТЦ: $R_{1\,i}$~0,93 та у завадах сильної щільності ~0,64, а ще і з маневром цілі (~4g) ~ 0,47 у середині зоні ураження ЗРК.

На ДМЗУ відповідно отримано: $R_{1\,i}$~0,8; ~0,24 та ~0,19, що свідчить про високу ефективність бойового застосування ЗРК.

Внаслідок необхідності врахування у $P_{B3\,i}$ показників надійності станцій, систем та ракет ЗРК, а також вогневої протидії противника отримано не значні значення загального показника ефективності стрільбі.

Для середньої зони ураження ЗРК та роботі по ТЦ (у тому числі по безпілотному літальному апараті) отримано ~ 0,14 (~0,13), а в умовах у сих видів протидії стрільбі ~ 0,07 (~10^{-6}). Хоча, підтримка достатньої експлуатаційної надійності ЗРК, застосування

способів зниження вогневої протидії противника та кваліфікований особового складу БМ під час стрільби у змозі підвищити величину $P_{ВЗ\ i}$.

Таким чином, результати даної методики можливо використовувати командирам БМ та батарей при плануванні бойових дій.

Список використаних джерел

1. Коломійцев О. В., Кудряшов В. Є., Адамовскій О. О., Коротя А. А. Умовна імовірність ураження цілі з врахуванням надійності роботи елементів комплексу і протидії стрільби ракетами. *Збірник наукових праць Харківського університету Повітряних Сил*. 2014. №. 1(38). С. 3-9.

2. Коломійцев О. В., Кудряшов В. Є., Машталір В. В., Опенько П. В., Олійник Р. М. Модель протиповітряного бою як елемент системи управління вогнем підрозділами військ ППО Сухопутних військ. *Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки.* 2019. № 1(1). С. 94-101.

3. Кудряшов В. Є., Артеменко А. А., Коломійцев О. В., Олійник Р. М., Живець Ю. М., Шумигай О. В. Часткова модель показника завадостійкості станції супроводження цілі зенітного ракетного комплексу малої дальності. Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. 2020. № 3(1). С. 56–66. https://doi.org/10.37701/dndivsovt.3.2020.08.

4. Кулєшов О. В., Коломійцев О. В., Єрмошин М. О., Клівець С. І. Методичний підхід щодо оцінки ефективності системи радіолокаційної розвідки повітряного противника військ протиповітряної оборони сухопутних військ та шляхи її підвищення. *Наука і техніка Повітряних Сил Збройних Сил України*. 2023. № 1 (50). С. 82-87. https://doi.org/10.30748/nitps.2023.50.09.

5. Коломійцев О. В., Кудряшов В. Є., Воїнов В. В., Кулєшов О. В., Клівець С. І. Моделювання значень загального показника ефективності стрільби ракетою бойової машини. *Системи озброєння і військова техніка*. 2023. № 1 (73). С. 61-67. https://doi.org/10.30748/soivt.2023.73.07.

УДК 629.7.051

Кузьміч О.Є., Аркушенко П.Л., Флорін О.П.

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ОСНОВА КОМПЛЕКСУ БОРТОВОГО ОБЛАДНАННЯ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ

Робота сучасного високотехнологічного виробу військової техніки характеризується великою кількістю та об’ємами різноманітної інформації. Так від первинних перетворювачів (сенсорів) до бортових систем повітряного судна надходять сигнали, що потребують обробки та прийняття миттєвих управлінських рішень. Одним із варіантів вирішення цього завдання є використання штучного інтелекту на базі бортових інтелектуальних систем.

Основними особливостями бортових систем повітряних суден нового покоління, в які впровадженні суттєві технологічні інновації, перш за все розвинута архітектура, інтелект, що забезпечує високу інформаційну підтримку виконання завдання на політ, а насамперед високий рівень автоматизації управління судном від зльоту до посадки.

Результати досліджень доводять, що в якості ефективних моделей організації бортових інформаційних систем (БІС) можуть застосовуватися мультиагентні системи, які є найбільш перспективним напрямком розвитку комп’ютерних систем з високим рівнем

штучного інтелекту та БІС на основі штучного інтелекту математичної моделі нейрону людини.

В даній роботі проводиться аналіз цих напрямків розвитку та можливості створення новітнього комплексу бортового обладнання для підтримки прийняття управлінських рішень.

Доцільно зазначити, що тільки вдосконалення бортових розрахунків, вимірювальних та виконавчих пристроїв повітряного судна забезпечить можливість розробки та реалізації у комплексі бортового обладнання алгоритмів та систем нового типу, які здатні сумісно з екіпажом вирішувати як загальні так і спеціальні завдання.

Впровадження результатів фундаментальних досліджень та нових технологій повинно забезпечити створення комплексу бортового обладнання повітряних суден, що забезпечить високу ефективність їх застосування, ефективного обміну інформацією між літаками та іншими платформами.

УДК 355

Кулєшов О.В., Коломійцев О.В., Комаров В.О., Клівець С.І., Кулєшова Т.В., Бордунова К.І.

ПРОПОЗИЦІЇ ЩОДО ФОРМУВАННЯ ЗАГАЛЬНИХ ВИМОГ ДО ПЕРСПЕКТИВНОГО КОМПЛЕКСУ ПРОТИДІЇ СУЧАСНИМ БЕЗПІЛОТНИМ АВІАЦІЙНИМ КОМПЛЕКСАМ ПРОТИВНИКА

В доповіді проведено аналіз основних тактико-технічних характеристик безпілотних літальних апаратів, що використовуються з боку російської федерації проти України. Розроблено пропозиції щодо формування вимог до перспективного комплексу протидії сучасним безпілотним авіаційним комплексам противника. Надані практичні рекомендації.

Аналіз досвіду застосування противником безпілотних літальних апаратів (БпЛА) різних класів та типів у ході повномасштабної збройної агресії з боку російської федерації проти України підтверджує високу ефективність даного виду озброєння. Так, БпЛА використовуються для здійснення повітряної розвідки, коригування вогню артилерії тощо, а також для виявлення та ураження об’єктів інфраструктури держави та Збройних Сил України. При цьому, БпЛА мають можливість діяти у автономному режимі. Робота бортових навігаційних систем БпЛА забезпечується корекцією за допомогою приймачів систем глобального позиціювання.

Застосування противником високоманеврених підрозділів, які на основі наданої розвідувальної інформації (координати об’єктів тощо) за допомогою БпЛА мають можливості у короткий проміжок часу нанести вогневе ураження по підрозділам, які знаходяться у першому та другому ешелонах, у районах вогневих позицій, а також по резервам, складам з матеріально-технічними засобами тощо. Тому, боротьба з БпЛА є одним із пріоритетних завдань протидії системам розвідки, управління та бойового застосування противника.

Сучасні безпілотні авіаційні комплекси (БпАК) відносяться до найскладніших повітряних цілей. Боротьба з ними потребує обґрунтування вимог до відповідних засобів виявлення, вогневого та невогневого ураження БпЛА, системи управління цим комплексом протидії БпАК, а також прийняття допоміжних організаційно-технічних заходів при його створенні.

Перспективний комплекс протидії БпАК противника призначений для прикриття військ в районах зосередження, на марші та у бою, а також – важливих воєнних і дер-

жавних об’єктів від БпЛА, гарантованого їх знищення або блокування роботи їх систем в умовах застосування противником пасивних та активних завад, вдень і вночі, у складних метеорологічних умовах та в усіх кліматичних зонах на території України.

При цьому, комплекс повинен забезпечувати:

– виявлення БпЛА противника у повітряному просторі, мереж (каналів) управління (телеметрії) та передачі інформації від (на) БпЛА на пункти управління (ПУ);

– вогневе ураження БпЛА противника;

– невогневу протидію БпЛА шляхом радіоелектронного подавлення (блокування) каналів обміну інформацією, управління (телеметрії) між БпЛА та ПУ, бортових приймачів сигналів супутникової навігації, бортових оптико-електронних засобів розвідки з метою зриву виконання ним завдання, а також шляхом введення похибки у канали управління;

– стійке та безперервне управління, ефективне застосування усіх засобів, які входять до складу комплексу під час підготовки та у ході виконання бойових завдань;

– тренування і навчання бойових обслуг за допомогою вбудованих навчальних програм із імітацією процесів застосування вогневих та невогневих засобів ураження тощо.

Таким чином, перспективний комплекс протидії БпАК противника повинен забезпечувати виконання наступних бойових завдань:

– своєчасне оповіщення про виявлення роботи БпАК, виявлення та видачу точної інформації (координат) про місцезнаходження БпЛА;

– прикриття частин та підрозділів у пунктах дислокації, розгорнутих у бойові порядки, на маршрутах руху, ПУ військ, переправ, воєнних та державних об’єктів;

– ефективне управління вогневими засобами ураження і радіоелектронної боротьби (РЕБ) та управління діями інших сил і засобів, які залучаються до протидії БпЛА;

– ураження БпЛА вогневими засобами;

– ефективне застосування засобів РЕБ для радіоелектронного впливу на канали управління (телеметрії), передачі інформації на ПУ, бортових приймачів сигналів супутникової навігації;

– підсилення угруповань протиповітряної оборони на малих і гранично малих висотах з урахуванням впливу рельєфу місцевості (долини рік, передгір’я, ущелини гір тощо), прикриття ділянок, що знаходяться у зонах недосяжності зенітно-ракетних комплексів;

– оперативне відновлення порушеної системи зенітного (зенітно-ракетного) вогню тощо.

Список використаних джерел

1. Кулєшов О. В., Коломійцев О. В., Єрмошин М. О., Клівець С. І. Методичний підхід щодо оцінки ефективності системи радіолокаційної розвідки повітряного противника військ протиповітряної оборони Сухопутних військ та шляхи її підвищення. *Наука і техніка Повітряних Сил Збройних Сил України*. 2023. № 1 (50). С. 82-87. https://doi.org/10.30748/nitps.2023.50.09.

2. Кулєшов, О., Коломійцев, О., Гордієнко, А., Болюбаш, О., Батурін, О., Клівець, С., & Третяк, В. (2022). Методичний підхід щодо моделювання оцінки ефективності системи вогню угруповання військ протиповітряної оборони Сухопутних військ. *Scientific Collection «InterConf+»,* (19(99), 930–946. https://doi.org/10.51582/interconf.19-20.02.2022.102.

3. Коломійцев О. В. Умовна ймовірність ураження цілі з врахуванням надійності роботи елементів комплексу і протидії стрільби ракетами / О. В. Коломійцев, В. Є. Кудряшов, О. О. Адамовский, А. А. Коротя // Збірник наукових праць Харківського університету Повітряних сил. – 2014. – Вип. 1. – С. 3-9. – Режим доступу: http://nbuv.gov.ua/UJRN/ZKhUPS_2014_1_3.

4. Коваленко, С. П., Коломійцев, О. В., Обрядін, В. В., & Хударковський, К. І. (2007). Метод ефективного розподілу цілей при управлінні вогнем підрозділу. *Системи обробки інформації*, (3), 41-43.

5. ВП 7-00(03).01. Методичні рекомендації "Боротьба з безпілотними літальними апаратами" (за досвідом проведення ООС (раніше АТО). Березень 2019. Обмеження розповсюдження: обмежень для розповсюдження немає. Центр оперативних стандартів і методики підготовки Збройних Сил України спільно з головним управлінням підготовки Збройних Сил України. – Режим доступу: https://sprotyvg7.com.ua/wp-content/uploads/2022/04/%D0%92%D0%9F-7-0003.01-%D0%91%D0%BE%D1%80%D0%BE%D1%82%D1%8C%D0%B1%D0%B0-%D0%B7-%D0%91%D0%9F%D0%9B%D0%90.pdf.

UDC 681.396

Kut V., Veretenikov I., Logvinenko O.

IMPROVEMENT OF THE VIBRATION DIAGNOSTIC SYSTEM OF GAS TURBINE ENGINES

The basic element of the power plant of weapons samples (aircraft, some samples of armored vehicles) is a gas turbine engine. Such an engine contains a multi-stage vane machine, which includes a set of rotating (nozzle) devices of a compressor and a turbine. The technical condition of the turbocharger rotor determines the resource and reliability of the power plant of weapons samples, therefore, affects safety [1, 2]. Thus, control of the technical condition of the gas turbine engine by vibration parameters is an important direction in the general system of technical diagnostics of weapons samples [3].

The development of effective systems of nondestructive control of parameters of the technical condition of elements of weapons samples is an urgent task [4, 5].

Compared to other diagnostic methods, vibration analysis has a number of characteristic features. This is due to the fact that the latter usually record the results of the force load, and with the help of vibration methods, direct control of the most dynamic force effect is carried out. From this follows the fundamental possibility of earlier, compared to other methods, detection, and even prevention of a malfunction [1, 6].

The application of vibration analysis methods is limited by the lack of systems for collecting and analyzing information from vibroacoustic signals that are fairly easy to use and maintain [3, 4]. The paper proposes a system for collecting, inputting and processing analog signals, which is intended for measurement and digital processing of vibroacoustic signals during vibrodiagnostics of gas turbine units in turbine construction. The developed system has the necessary characteristics for timely and reliable detection of possible failures during the control of the technical condition of the gas turbine engine of weapons samples.

Carrying out technical diagnostics of gas turbine engines of weapons samples in real time allows to move from the operation of engines by time to the operation of engines by technical condition [2]. One of the main elements of technical diagnostics is vibration diagnostics [4, 5].

Vibrations, that is, mechanical oscillations, are usually defined as the system's response to the action of disturbing forces. Exasperating loads acting on the elements of the gas turbine engine are determined by the principle of operation and features of the turbocompressor, which is a bladed rotary machine and forms the basis of a modern gas turbine engine, as well as the operating conditions of the power plant. Internal and external disturbing forces are mainly of mechanical and gas-dynamic (aero-mechanical) origin. When used in ground

installations, there are additional external influences from the electric generator of the compressor.

The main source of vibration of the gas turbine engine is the rotating rotor of the turbocharger. Statistical and dynamic imbalances of the rotor lead to the emergence of forces and moments that cause vibration of both the rotor itself and the entire turbomachine as a whole.

Rotor aeromechanical vibration is caused by gas-dynamic non-stationary loads. Its main source is the surrounding non-uniformity of the gas (air) flow flowing through the moving and stationary grates of the blade apparatus.

Vibration caused by acoustic noise created by the compressor and turbine, and also occurs during the operation of the inlet device, jet nozzle and combustion chamber.

Vibration generated by toothed connections found in engine gears and drive systems.

Vibration generated by bearings. It is caused by geometric errors that occur during their manufacture and installation.

There are two classes of devices for measuring these parameters: analog devices and digital systems, special methods of digital signal processing. Analog systems make it possible to obtain values of measured parameters in real time - (real-time systems). Signal filtering is the basis of these systems. But this class has a significant drawback - the minimum error in determining the amplitude is 10%. It should be noted that the registration of analog signals is complicated. Therefore, in the last (10–15) years, digital methods have become widely used. Vibration diagnostics is performed with the help of information and measurement systems. Currently, it is digital methods that have become widely used in vibration diagnostics of gas turbine engines. They are based (if the power spectral density estimate is calculated) on the use of Fourier transformation, autoregression estimation methods - special calculation algorithms that allow working in quasi-real time.

In connection with the above, it is possible to outline a general list of tasks that should be solved by the development module for inputting measurement information: removing parameters; analog-digital conversion; accumulation of information; digital processing.

Thus, there is a problem of developing equipment for measuring vibration parameters. The sensors must monitor the rotational harmonics of the engine. But this is not enough, it is necessary to know the amplitude-frequency characteristic of the engine in order to predict its condition, that is, the accumulation of information with subsequent processing is necessary. The main requirement is to maintain a stable frequency or discretization of the channel sampling period during the entire operation. The possibility for the module to work at a variable sampling frequency of the input signal should be implemented.

References

1. S. Yevseiev, O. Kuznietsov, S. Herasimov and etc. **Development of an optimization method for measuring the Doppler frequency of a packet taking into account the fluctuations of the initial phases of its radio pulses**. *Eastern-European Journal of Enterprise Technologies*, 2021, 2 (9) (110), p.p. 6-15, https://doi.org/10.15587/1729-4061.2021.229221.

2. O. Brytov, D. Bieliaiev, S. Kukobko and etc. **Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects**, *Proceedings of the 3rd International Scientific and Practical Conference* "*Scientific Trends and Trends in The Context of Globalization*", UMEÅ, SWEDEN, 21-22.12.2021, p.p. 431-434, https://doi.org/10.51582/interconf.21-22.12.2021.050.

3. V. Dzhus, Y. Roshchupkin, S. Kukobko and etc. **Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction Method**, *Information Processing Systems*, 2021, Issue 4 (167), p.p. 19-26, https://doi.org/10.30748/soi.2021.167.02.

4. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.

5. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of airspace radio engineering monitoring systems**, *International scientific and practical conference* "*Application of information technologies in the preparation and operation of law enforcement forces"*, March 15, 2022, p.p. 31-32.

6. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (ISMSIT), 2022, p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.

UDC 681.396

Kutsenko V., Lutsenko A.

APPLICATION METHOD INERTIAL NAVIGATION SYSTEMS TO ENHANCE THE SAFETY OF AIRCRAFT NAVIGATION

Inertial navigation systems are the basis of navigation complexes of modern moving objects [1, 2]. This is due to the fact that they provide complete information about the navigational parameters of the movement - course, trim, roll angles; acceleration, speed of movement and coordinates of the location of the object [3, 4]. At the same time, they are completely autonomous, that is, they do not require any information from the outside. Due to the ability to determine the angular position of the object with high accuracy in any range of angles and with a high frequency of information output, inertial navigation systems have no alternative, especially in the absence of their own satellite network [5, 6].

Practical implementation of inertial navigation methods is associated with significant difficulties caused by the need to ensure high accuracy and reliability of operation of all devices at given weights and dimensions [1, 3].

Increasing the accuracy of navigation of moving objects is associated with the improvement of both measuring equipment and mathematical support for solving information processing problems [2, 5].

The use of inertial methods under the influence of the Earth's anomalous gravitational field in promising aircraft navigation systems requires a deeper study of the possibilities of stochastic models of the anomalous gravitational field, which coherently describe the anomalies of gravity, geoid height, and temple deviation [4]. The choice of which models should be based not only on the requirements of adequacy to the real field, but also on the convenience of their use in information processing tasks [1, 6].

In connection with this, an urgent scientific task arises in the field of aircraft navigation: the synthesis of methods of using inertial navigation systems in flight conditions.

The complex structure of errors of navigation systems as functions of time, the uniqueness of their implementations, is caused by the influence of a number of unaccounted factors that require the use of models of random functions for their description.

At the same time, the navigation system errors contain components that do not have ergodic properties and have, for example, the form of known functions of time with parameters that change from one system launch to another. It should be noted that the question of the meaningful introduction of the probability space is not only methodological in nature, which ensures the mathematical correctness of the analysis, but also reveals the meaning of the averaged accuracy characteristics that should be used in the tasks of analysis and synthesis of navigation systems.

At the heart of modern approaches to information processing and management tasks are processes that are the solution of linear differential equations with random initial conditions and the right-hand side containing random functions of the white noise type and represent a special class of random processes that are solved using stochastic differential equations.

The transition from one differential equation of higher order to a system of stochastic differential equations of the first order, written, for example, in the normal form, completes the task of describing the errors of the navigation system in this case.

Each of the navigation system errors in aircraft flight conditions is characterized by the fact that they are dependent on several parameters. We will call the generalized concept of a random process, which is a function of several arguments, a random field.

The need to use a pulsating filter is caused by the desire to reduce computational costs when filtering a navigation signal with a possible change of the model number from step to step of discrete time.

The interpretation of the unknown parameters of the signal model as random variables is, as a rule, conditional; the considered approach is no more than one of the evaluation methods, which reduces the problem of adaptive processing to the problem of optimal filtering. Moreover, the effectiveness of the adaptive procedure built on this basis turns out to be significantly dependent on the degree of influence of the species and density parameters on the result of the estimation of the vector of navigation parameters. It is clear that the estimation of navigation parameters will be practically satisfactory only if the influence of density on it is weakened due to the use of measurements. It is easy to see that the extended state vector of the flight parameters satisfies the stochastic finite-difference equation, which makes it possible to use the recurrence relation for the posterior density of the vector of navigation parameters to solve the problem.

The considered adaptive algorithm, based on the discretization of the vector of uncertain parameters, is easily generalized to the case when the a priori uncertainty consists in assuming the possibility of describing the signals to be processed using one of the models that differ not only in the numerical values of the parameters, but also in their structure. Indeed, understanding the number of one of the alternative hypotheses about the signal belonging to the corresponding model, we come to the solution of the problem of optimal estimation of the vector of navigation parameters, which is of interest to us in the conditions of uncertainty of the corresponding model number.

References

1. S. Yevseiev, O. Kuznietsov, S. Herasimov and etc. **Development of an optimization method for measuring the Doppler frequency of a packet taking into account the fluctuations of the initial phases of its radio pulses**. *Eastern-European Journal of Enterprise Technologies*, 2021, 2 (9) (110), p.p. 6-15, https://doi.org/10.15587/1729-4061.2021.229221.

2. O. Brytov, D. Bieliaiev, S. Kukobko and etc. **Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects**, *Proceedings of the 3rd International Scientific and Practical Conference* "*Scientific Trends and Trends in The Context of Globalization*", UMEÅ, SWEDEN, 21-22.12.2021, p.p. 431-434, https://doi.org/10.51582/interconf.21-22.12.2021.050.

3. V. Dzhus, Y. Roshchupkin, S. Kukobko and etc. **Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction Method**, *Information Processing Systems*, 2021, Issue 4 (167), p.p. 19-26, https://doi.org/10.30748/soi.2021.167.02.

4. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.

5. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (ISMSIT), 2022, p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.

6. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of airspace radio engineering monitoring systems**, *International scientific and practical conference "Application of information technologies in the preparation and operation of law enforcement forces"*, March 15, 2022, p.p. 31-32.

Лавренченко М.В., Вакуленко І.В., Мазур В.В.

АНАЛІЗ ЗАСТОСУВАННЯ НОВІТНІХ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ В ХОДІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Радіоелектронна боротьба (РЕБ) являє собою сукупність узгоджених за метою, завданнями, місцем і часом заходів і дій з виявлення та радіоелектронного придушення систем і засобів управління військами та зброєю противника, а також з радіоелектронного захисту своїх систем і засобів управління військами та зброєю.

Згідно діючої "Настанови з радіоелектронної боротьби у Збройних Силах України" вона включає радіоелектронне придушення радіоелектронних об'єктів (засобів) противника, радіоелектронний захист своїх систем і засобів управління військами та зброєю, електронну підтримку РЕБ. Стосовно останньої складової, то це комплекс технічних заходів щодо пошуку й перехоплення радіосигналів і визначення місць знаходження радіоелектронних засобів на місцевості за їх радіовипромінюванням.

У широкому розумінні РЕБ – це протиборство (сукупність заходів і дій військ), у якому противники вирішують свої бойові завдання з використанням електромагнітних хвиль. Тобто, основною відзнакою радіоелектронної боротьби, яка обмежує галузь її застосування, є використання у збройній боротьбі електромагнітних хвиль.

В ході російсько-української війни широке застосування мають засоби РЕБ різного типу та базування.

Росія протягом багатьох років приділяла величезну увагу використанню свого військово-промислового комплексу щодо виробництва і розвитку величезного спектру засобів РЕБ для протидії високо розгалуженим мережевим системам НАТО. Засоби РЕБ російського виробництва, що використовуються в ході воєнних дій, та їх технічні характеристики відомі. До найбільш розповсюджених засобів належать: "Леєр", "Красуха", "Москва", "Житель", "Мандат", "Борисоглебськ", "Поле-21" та інші.

Серед багатьох російських систем РЕБ відносно новою та сучасною є встановлена на вантажівці система "Шиповник-Аеро", що є особливо смертоносною для українських безпілотників.

Водночас Україна на початку війни мала на озброєнні переважно системи РЕБ радянських часів.

Для ефективної протидії крилатим ракетам (КР) і ударним безпілотним літальним апаратам (БЛА) противника важливо не лише наявність достатньої кількості систем протиповітряної оборони різних типів і класів, а й засобів, які можуть протидіяти їх застосуванню.

В Україні останнім часом розгортається загальнонаціональна система "Покрова". Вона має бути високоефективною проти "шахедів", але менш ефективною проти крилатих ракет, тому що КР російського виробництва типу Х-101 мають більш точну інерціальну навігацію, а також використовують високотехнологічні системи наведення DSMAC (Digital Scene Matching Area Correlation) і TERCOM (Terrain Contour Matching).

Для виявлення та придушення роботи БЛА противника в Збройних Силах України використовується відносно новий комплекс РЕБ “Буковель-AD”.

Крім того, вже пройшла польові випробування система Piranha AVD 360, яка показала високу ефективність протидії атакам російських безпілотників. Також в Україні розроблена легка переносна система AD Counter FPV, що блокує радіочастоти для російських FPV-дронів.

Отже, війна все більше перетворюється у протистояння високих технологій і вміння сторін протиставити противнику свої більш якісні засоби протидії сучасному озброєнню.

УДК 004.9+005.2

Лаврут О.О., Лаврут Т.В., Колесник В.О.

КІБЕРЗБРОЯ: ТЕНДЕНЦІЇ, МОЖЛИВІСТЬ, ПЕРСПЕКТИВА

Аналіз характеру ведення сучасних війн, збройних конфліктів і протистоянь свідчить, що поняття “поле бою” давно трансформувалося в поняття “бойовий простір”, складовою частиною якого є “кіберпростір” [1-5]. Указом Президента України №447/2021 було введено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України”. В цьому документі йдеться про сучасні виклики у сфері кібербезпеки, а саме: активне використання кіберзасобів у міжнародній конкуренції; змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо; мілітаризацію кіберпростору та розвиток кіберзброї; упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки.

Виходячи з цього сьогодні потребують розробки наступні питання [1, 4]:

- визначення особливостей, потенційних можливостей та тенденцій розвитку кіберзброї;
- класифікація кіберзброї;
- обґрунтування співвідношення понять кіберзброя та кібервплив;
- визначення потенційних об’єктів кібервпливу та їх “слабких місць” тощо.

Враховуючи стрімкий розвиток автоматизації всіх процесів управління у військовій сфері провідних країн світу, системи управління військами та зброєю на тактичному рівні є одними з основних об’єктів застосуванні перспективних зразків кіберзброї. Потенційними об’єктами кібервпливу можуть бути:

1) АСУ військами - автоматизовані системи управління окремими підрозділами;
2) АСУ окремими зразками озброєння і військової техніки;
3) Система зв’язку - окремі засоби зв’язку;
4) Комунікаційні системи - телекомунікаційні системи; бази даних тощо.

Це, в свою чергу, вимагає розробки низки заходів та нових видів кіберозброєння для вдосконалення боротьби з ворогом.

Список використаних джерел

1. Lavrut T., Kolesnyk V., Kolesnyk H., Bohutskyi S., Polishchuk L. Cyber defense is a modern component of Ukraine’s security. *III International Scientific And Practical Conference “Information Security And Information Technologies”*, September 13–19, 2021, Odesa, Ukraine. PP. 169-174. URL: http://ceur-ws.org/Vol-3200/paper23.pdf.

2. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) Modeling of security systems for critical infrastructure facilities. Modeling of security systems for critical

infrastructure facilities. 2022. Kharkiv: PC TECHNOLOGY CENTER, 196 p. DOI: http://doi.org/10.15587/978-617-7319-57-2.

3. Іохов О., Лаврут О., Лаврут Т., Флорін О. Сучасні засоби зв'язку та інфокомунікаційні технології у Збройних Силах України та Національній гвардії України: сьогодення та перспективи застосування. *Честь і закон*. 4 (83). С. 111-119.

4. Лаврут О.О. Вибір критерію оцінювання якості управління потоками інформації у телекомунікаційній мережі мобільного компоненту перспективної системи зв'язку ЗС України. *Наука і техніка Повітряних сил Збройних Сил України*. 2014. Вип. 3 (16). С. 113-115.

5. Лаврут О.О., Лаврут Т.В. Модель та метод управління трафіком в мережах зв'язку критичного призначення. *Prospects and priorities of research in science and technology: Collective monograph.* Vol. 2. Riga, Latvia: "Baltija Publishing", 2020. P. 36-60. DOI https://doi.org/10.30525/978-9934-26-008-7.2-3.

УДК 621.396

Лаврут О.О., Лаврут Т.В., Обиход Л.П.

ОСОБЛИВОСТІ ТА ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМИ ЗВ'ЯЗКУ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ З УРАХУВАННЯМ СТАНДАРТІВ НАТО

Російська агресія проти України прискорила оборонну реформу, спрямовану на досягнення цілей євроатлантичної інтеграції. Війна показала, що особливу роль у військових протистояннях відіграє саме система управління, основу якої складають автоматизовані системи управління та розгалужена система зв'язку.

В сучасних війнах в умовах критичного зростання ролі просторо-часового фактора на усіх рівнях прийняття рішення на застосування зброї набирає актуальності скорочення часу реакції на загрози, що виникають. Забезпечення військ найкращими системами озброєння та військової техніки ще не є гарантією перемоги в бою. Навіть за умови рівних бойових потенціалів перемогу здобуде сторона, краще обізнана з поточною обстановкою. Отже, логічним виходом є протиставлення грубій силі противника асиметричної відповіді, складовими якої є на порядок глибша автоматизація у військах.

Метою доповіді є дослідження особливостей та тенденцій розвитку закордонних систем зв'язку, а також новітніх систем зв'язку в Україні, їх можливостей, застосування для розробки рекомендацій щодо створення універсальної системи зв'язку тактичної ланки управління Збройних Сил України з урахуванням стандартів НАТО [1-5].

Для досягнення мети нашого дослідження було вирішено наступні задачі:

1. Проаналізовано загальні світові тенденції розвитку зв'язку та управління армій провідних країн.

2. Проаналізовано стан сучасної системи управління військами і зброєю в США та інших країнах НАТО.

3. Проаналізовано та узагальнено тенденції розвитку сучасної системи управління військами і зброєю в росії.

4. Розроблено пропозиції щодо подальшого розвитку системи зв'язку та управління у Збройних Силах України з урахуванням сучасних світових тенденцій.

Результати наукових досліджень авторів можуть бути використанні для побудови як для перспективних систем управління, так і для розробки окремих засобів зв'язку та телекомунікацій.

Список використаних джерел

1. Lavrut O. Promising approaches and technologies for building control systems of force structures agencies. «Findings of modern engineering research and developments»: *Scientific monograph.* Riga, Latvia: "Baltija Publishing", 2022. P. 233-264. DOI https://doi.org/10.30525/978-9934-26-207-4-9.
2. Іохов О., Лаврут О., Лаврут Т., Флорін О. Сучасні засоби зв'язку та інфокомунікаційні технології у Збройних Силах України та Національній гвардії України: сьогодення та перспективи застосування. *Честь і закон*. 4 (83). С. 111-119.
3. Лаврут О.О. Вибір критерію оцінювання якості управління потоками інформації у телекомунікаційній мережі мобільного компоненту перспективної системи зв'язку ЗС України. *Наука і техніка Повітряних сил Збройних Сил України*. 2014. Вип. 3 (16). С. 113-115.
4. Лаврут О.О., Лаврут Т.В. Модель та метод управління трафіком в мережах зв'язку критичного призначення. *Prospects and priorities of research in science and technology: Collective monograph.* Vol. 2. Riga, Latvia: "Baltija Publishing", 2020. P. 36-60. DOI https://doi.org/10.30525/978-9934-26-008-7.2-3
5. Настанова "Тактичний зв'язок" ВКДП 6-110(03).01. Київ. 2020. 54 с.

Лагунов В.Є., Шевченко А.О., Першин О.В.

ДОСЛІДЖЕННЯ VPN-ПРОТОКОЛІВ ДЛЯ ОРГАНІЗАЦІЇ ЗАХИЩЕННИХ КАНАЛІВ ЗВ'ЯЗКУ У КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Безпека інформаційної взаємодії різних користувачів у сфері оборони країни (засоби інформатизації та автоматизації систем управління) через відносно слабо захищені від атак виділені комунікаційні мережі мультисервісних мереж зв'язку спеціального призначення (ММЗ СП), зокрема через багатопротокольну транспортну мережу ММЗ СП, яка здійснює базову послугу перенесення інформації на основі широкосмугових технологій, вимагає ефективного вирішення наступних завдань:

- захисту підключених до каналів та трактів транспортної мережі ММЗ СП обладнання мереж доступу комплексів технічних засобів адміністративного управління (засобів інформатизації та автоматизації) від широкого спектра несанкціонованих дій з боку порушників;
- захисту інформації користувачів органів військового управління в процесі її передачі по слабо захищеному середовищу ММЗ СП, що здійснює транспортування (прозоре перенесення) інформації.

Вирішення першої задачі зазвичай здійснюється за рахунок застосування в комплексах технічних засобів адміністративного управління міжмережевих екранів, що підтримують безпеку інформаційного обміну за рахунок фільтрації двосторонніх потоків інформації, а також виконання функцій санкціонованого посередництва при обміні інформацією транспортної мережі ММЗ СП.

Вирішення другого завдання, тобто забезпечення захисту інформації при її передачі по слабко захищених каналах і трактах транспортної мережі ММЗ СП, засноване на виконанні наступних функцій:

- автентифікації мережевих користувачів (коштів мереж доступу) транспортних послуг;
- криптографічне закриття інформації, що транспортується;
- підтвердження справжності та цілісності доставленої до мереж доступу інформації та ін.

Загалом наведені заходи пов'язані один з одним, а їх реалізація базується як на традиційному криптографічному захисті даних, що передаються, так і на більш гнучких

сучасних рішеннях, пов'язаних з об'єднанням різних виділених мереж доступу комплексів технічних засобів адміністративного управління через слабо захищене зовнішнє середовище передачі (транспортування) інформації в єдину віртуальну приватну або VPN-мережу, що забезпечує безпеку даних, що циркулюють (так звана захищена VPN-мережа).

Використання VPN-протоколів, що використовуються для розгортання VPN мереж, забезпечує безпеку та конфіденційність даних, що передаються по транспортній мережі МСЗ СП. За допомогою шифрування та автентифікації VPN-протоколи забезпечують захист від перехоплення та зміни інформації незаконними користувачами.

Але не всі VPN-протоколи створені рівнозначними. Кожен з них має свої переваги та недоліки, а також відмінності у пропускній спроможності, швидкості, безпеці та інших характеристиках. Тому проведення дослідження VPN-протоколів стає важливим кроком для забезпечення надійного та ефективного захисту даних в мережі ММЗ СП.

Вибір оптимального VPN-протоколу для конкретної задачі є критичним завданням. Недоцільний вибір може призвести до недостатнього рівня захисту даних або зайвих витрат на утримання мережі. Тому дослідження VPN-протоколів допомагає зрозуміти їхні можливості та переваги, щоб зробити інформований вибір.

УДК 681. 323

Лазарев В.Д.

КІБЕРБЕЗПЕКА ЯК ЗАПОРУКА УСПІХУ В БОЙОВОМУ ЗАСТОСУВАННІ СИСТЕМИ ЗВЯЗКУ НГ УКРАЇНИ

Розглянутий сучасний стан та завдання забезпечення кібербезпеки під час використання інтернет ресурсів при веденні бойових дій.

З розвитком інформаційних технологій та впровадженням їх у всі сфери життя суспільства одним з найбільш пріоритетних напрямків наукових досліджень у галузі забезпечення інформаційної та кібернетичної безпеки на вузлах зв'язку пунктів управління Національної гвардії України є створення нових та дієвих методів, засобів виявлення кібератак для захисту комп’ютерних систем та мереж. Оскільки кількість різних типів і способів організації несанкціонованих проникнень в чужі мережі за останні роки значно збільшилася, системи виявлення вторгнень і кібератак стали необхідним компонентом інфраструктури безпеки інформаційних систем та мереж.

Особливу увагу інформаційні ресурси набувають в сучасних умовах швидкої глобалізації інформаційних процесів і прагнення розвинених країн досягти інформаційного домінування заради власних національних інтересів, завдань і так далі. Саме тому стає необхідним дослідження проблем забезпечення кібербезпеки в сучасному глобалізованому світі, країні та конкретно в інформаційних системах НГУ.

Кібербезпека розглядається як глобальна проблема захисту інформації, захисту інформаційного простору та інформаційного суверенітету. Практичне розв’язання проблем кібербезпеки, притягнення до відповідальності за порушення або загрозу інформаційній безпеці у частинах і підрозділах НГУ здійснюється у порядку, передбаченому нормами внутрішнього законодавства України.

Основними напрямками забезпечення безпеки інформаційного простору електронних комунікаційних мереж Національної гвардії є:

- захист інформації та інформаційних ресурсів;
- організаційно-технічне забезпечення інформаційної безпеки;

- проведення робіт з захисту інформації, які передбачені технічними умовами та керівними документами;
- введення територіальних, частотних, енергетичних, просторових і часових обмежень в режимах використання технічних засобів, що підлягають захисту;
- перевірка адекватності та надійності функціонування застосованих технічних засобів рівню потенційних загроз;
- встановлення категорійності приміщень, у яких може циркулювати таємна інформація.

Кібератаки із використанням сучасних методів надзвичайно небезпечні, оскільки ефективно приховують як факт проведення самої кібератаки, так і канал виведення інформації з системи. Таке приховання даних дозволяє успішно пройти сигнатурні системи виявлення вторгнень та деяке антивірусне програмне забезпечення. Особлива небезпека таких кібератак полягає, в першу чергу, у прихованні каналу, яким здійснюється кібератака. Практична потреба в механізмах захисту від таких кібератак полягає в їх специфічному характері, а саме використанні професійних методів, які класично розглядаються у якості засобів захисту, а не навпаки.

Для досягнення очікуємого результату в забезпеченні кібербезпеки телекомунікаційних систем НГУ необхідно впроваджувати в життя певних організаційних та технічних заходів.

Організаційні заходи що повинні проводитися на вузлах зв'язку включають в себе: формування системи забезпечення кібербезпеки; створення кіберпідрозділів; створення системи підготовки висококваліфікованих фахівців у сфері кібербезпеки; організаційне, законодавче та технічне забезпечення дій кіберпідрозділів; науковий супровід, розробку та впровадження новітніх технологічних розробок; посилення контролю за кіберпростором, збільшення чисельності кіберпідрозділів.

Технічні заходи включають проведення кібернавчань; участь у дослідженнях і розробці нових видів наступальної, оборонної і розвідувальної кіберзброї.

Левкович П.В., Сівак О.І., Фіщук І.М., Поліщук А.М.

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ МАЛОГАБАРИТНИХ РАДІОЛОКАЦІЙНИХ СТАНЦІЙ В ІНТЕРЕСАХ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РЕЖИМНИХ ОБ'ЄКТІВ

Охорона режимних об'єктів - це комплекс заходів, спрямованих на забезпечення безпеки, недопущення несанкціонованого доступу та збереження конфіденційності важливих об'єктів, таких як важливі установи, державні заклади, об'єкти інфраструктури та інші об'єкти, які потребують особливого захисту. Цими об'єктами в рамках обговорення можуть бути польові склади, райони зосередження підрозділів, польові командні пункти тощо.

Зазвичай забезпечення безпеки включає в себе встановлення фізичних бар'єрів (таких як огорожі, бар'єри), систем безпеки (включаючи відеоспостереження, сигналізацію), а також впровадження процедур контролю доступу та режиму роботи персоналу. Крім того, можуть бути використані спеціалізовані служби охорони з високою кваліфікацією та досвідом у захисті об'єктів від потенційних загроз. Метою такої охорони є запобігання несанкціонованому доступу, втратам та пошкодженням майна, а також захист від можливих терористичних актів.

Виявлення спроб наближення до об'єкту може відбуватися через організацію системи відеоспостереження, яка ефективно відіграє свою роль лише на відстані 15 метрів. В умах ускладненої видимості (дощ, сніг, туман) важко прослідковувати за підступами до об'єкту. Проаналізувавши дані обставини, виявлення на відстані неможливе, тобто електронна система безпеки у вище описаних випадках не буде ефективною.

Підрозділам, що задіяні в охороні, важливо знати щодо проникнення умовного безпекового периметру для прийняття рішення. Забезпечити виявлення рухомих об’єктів здатні малогабаритні радіолокаційні станції розвідки рухомих наземних, надводних та повітряних цілей. Для прикладу, яскравими представниками даних радіолокаційних станцій є Ground Observer 12 та Squire виробництва компанії Thales Group, що спеціалізується на оборонній промисловості.

Ці легкі компактні радари імпульсно-доплерівської системи Ku-діапазону підходять для широкого спектра застосувань, включно зі спостереженням за підступами до об'єкту, державним кордоном, узбережжям тощо.

Радари забезпечують високими можливостями виявлення до 26 кілометрів в режимі кругового огляду наступні об’єкти:

– рухомі наземні, надводні- людина, група осіб, автомобіль, вантажний автомобіль, важко-броньована техніка, катер, корабль;

– аеродинамічні об’єкти – безпілотний літальний апарат мультироторного типу, фіксованого крила.

При виявлені одну із вище перелічених небезпек, оператор володітиме координатами різних систем, щодо місцезнаходження об’єкту, його напрям та швидкість руху.

Прилади є надзвичайно компактними. Безпосередня вага антенного прийомопередавача не перевищує 16 кілограм. Радари можна експлуатувати, встановивши на штатив чи транспортний засіб будь-якого типу. Завдяки невеликій вазі GO12 можна легко прикріпити і на телескопічну щоглу для стаціонарного розміщення.

Застосування малогабаритних радіолокаційних станцій розвідки рухомих наземних, надводних та аеродинамічних цілей забезпечить цілодобово, в зоні дії прямої радіолокаційної видимості, за будь-яких погодних умов в режимі реального часу спостереження за підступами до режимного об’єкту, державного кордону, узбережжя, що значно підвищить їх систему безпеки.

УДК 004.852

Літвін С.Г.

МЕТОД ЛОГІЧНИХ МЕРЕЖ ДЛЯ РОЗПОДІЛЕНИХ СИСТЕМ ДИСТАНЦІЙНОГО ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

В наш час повномасштабної агресії, що триває, важливим трендом розробки навчального розподіленого середовища є підтримка дидактичних систем підвищення кваліфікації та перепідготовки військовослужбовців та співробітників силових структур в дистанційному форматі.

Метою дослідження є вирішення низки завдань, що відносяться до питань взаємозв'язку між теорією категорій і алгеброю предикатів, як математичних засобів технології штучного інтелекту при розробці розподіленого віртуального навчального середовища. Категорні моделі логічних мереж розглядаються як об'єкт досліджень. Методом обрано математичні моделі формалізації та представлення інформації на основі предикатних та модифікованих категорій [1]. Проведено формалізацію досліджуваних моделей декларативною мовою, створеною в процесі дослідження, що дозволяє дослідити моделі за допомогою загальної універсальної моделі логічної мережі.

На прикладі обробки навчально-методичної інформації штучним інтелектом можна розглянути загальну класифікацію завдань, що виникають у процесі роботи з первинною неформалізованою інформацією:

– аналіз (наприклад, розпізнавання – одержання з неформалізованої інформації конкретних параметрів, необхідних для застосування деякого формалізму);

– нормалізація – приведення інформації до деякої еталонної форми, що актуально в завданнях пошуку інформації;

– синтез – подання внутрішнього представлення інформації, збереженої відповідно до формальних вимог у вигляді, що адаптований для сприйняття людиною;

– змішані завдання.

Іншою перевагою логічних мереж є широке розпаралелювання обчислень, що за умови правильної побудови моделі завдання дає гарантію високої ефективності. На сьогоднішній день розпаралелювання широко застосовується в окремих завданнях штучного інтелекту, зокрема в системах віртуального навчання [2], є методом розкриття прихованої інформації з великих наборів даних. Цей процес включає аналіз підмножин даних для виявлення повторюваних моделей поведінки чи встановлення прогнозованих моделей на основі обробленої інформації.

Оскільки логічні мережі є графічним вираженням алгебро-логічного опису об'єкта, то з практичної точки зору вигідніше розглядати модифіковану предикатну категорію зі визначеною операцією множення, що базується на використанні властивостей алгебри предикатів. Для того щоб практично використовувати поняття предикатної модифікованої категорії, спочатку потрібно отримати загальну модифіковану категорію, окремим випадком якої вона є. Тому слід абстрагуватися від поняття модифікованої предикатної категорії і сформувати як альтернативу загальному поняттю класичної категорії, загальне поняття модифікованої категорії.

Відмінність між теорією категорій і алгеброю предикатів полягає лише в тому, що перша здійснює рух зверху вниз, націлена на пізнання вищих логічних механізмів і тому використовує в якості відправних поняття рекордного рівня спільності. Друга ж, відправляючись від потреб інформатизації, рухається у вивченні тієї ж логіки мислення знизу нагору. Якщо б удалося дати переконливу інтерпретацію понять, формованих теорією категорій, і методів, розроблювальних нею, у термінах алгебри предикатів, тобто, конкретизуючи, наблизити їх до інформатизації, це суттєво збагатило б інструментарій алгебри предикатів. Саме алгебру предикатів використовуємо в ролі такої проміжної області знання [3].

Логічна мережа копіює дії людини, але з тією лише різницею, що людина діє послідовно, а мережа – паралельно. Мережа працює по тактах. У першому півтакті *i*-го такту мережа для кожного зі своїх рівнянь виду ДО(x, y)=1 (ДО – відношення, задане таким рівнянням) відшукує: 1) по відомим знанню $P_i(x)$ про значення змінної x на початку i-го такту знання $Q_i(y)$ про значення змінної в наприкінці i-го такту; 2) по відомому знанню $Q_i(y)$ про значення змінної *y* на початку *i*-го такту, визначається знання $P_i(x)$ про значення змінної *x* наприкінці *i*-го такту. Математично ці дві операції виражаються формулами:

$$\exists_{x\in} A(K(x, y)P_i(x))=Q_i(y); \quad (1)$$

$$\exists_{x\in} B(K(x, y)Q_i(y))=P_i(x) \quad (2)$$

де A и B– області зміни змінних *x* и *y*.

У другому півтакті кожного такту мережа відшукує загальну частину $P_{i+1}(x)$ усіх знань $P'_{i1}(x)$, $P'_{i2}(x)$,…, $P'_{il}(x)$ про значення кожної зі своїх предметних змінних x сторін, що надходять по галузях мережі із усіх, до полюса x. Виражається ця операція в такий спосіб:

$$P'_{i1}(x) \wedge P'_{i2}(x) \wedge \ \ldots \wedge P'_{il}(x)=Pi_{+1}(x) \quad (3)$$

Отримане знання $P_{i+1}(x)$ потім використовується в ролі стану полюса x у початковий момент *i+1*-го такту. Символ *l* позначає число галузей, що підходять до полюса x. До початку *i+1*-го такту в кожному полюсі формується знання про множину $P_{i+1}(x)$, яка завжди виявляється включеним у знання о множині $P_i(x)$, що втримувалася в тому ж полюсі на початку *i*-го такту. Таким чином, єдиним результатом роботи логічної мережі є уточнення знань, що втримуються у всіх її полюсах відповідно до вихідних даних.

При впровадженні теорії категорій поряд зі звичайним поняттям категорії зустрілося і більш загальне поняття безоб'єктної категорії.

У процесі конкретизації раніше введене поняття обростає додатковими властивостями. На додаток до морфізмів категорії *K* уводимо об'єкти категорії *K*. Множина усіх об'єктів категорії *K* записується у вигляді Ob в *K* або Obk. Об'єкти позначаємо буквами *A, B, C*,…. Якщо $A \in$ Obk, то говорять, що *A* є *K*-об'єктом. Говорять, що *f* є морфізм із об'єкта *A* в об'єкт *B*, і пишуть $f: A \to B$ або $A \xrightarrow{f} B$. Об'єкт *A* називається початком морфізма *f*, а об'єкт *B* – його кінцем. Замість терміну «морфізм» також використовується слово форма. Кожній парі (*A, B*) об'єктів $A, B \in$ Obk ставиться у відповідність якесь, можливо й порожнє, множина *HK*(*A, B*) морфізмів категорії *K*. Можливий випадок, коли багатьом різним морфізмам, наприклад, *f, g, h*, поставлена у відповідність та сама пара об'єктів (*A, B*), тобто $f, g, h: A \to B$. Такі морфізми називаються паралельними. А для якоїсь іншої пари об'єктів (*C, D*) у категорії *K* взагалі може не знайтися жодного морфізма *f*, такого що $f: C \to D$. Замість запису *HK*(*A, B*) також використовуються позначення Hom(*A, B*), Mork(*A, B*), *K*(*A, B*), а якщо це не приводить до двозначності, – те й більш лаконічні записи *H*(*A, B*), Hom(*A, B*), Mor(*A, B*). Замість запису $f \in HK(A, B)$ інакше пишуть $f: A \to B$ або $A \xrightarrow{f} B$; *A* = domf (початок морфізма, у прийнятій нами інтерпретації – його область визначення), *B*=*codf* (кінець морфізма, у нашій інтерпретації – його область значень).

Категорія з об'єктами K складається з множини морфізмів Mork і множини об'єктів Obk. Передбачається, що множини Mork і Obk не перетинаються. Категорія *K* характеризується наступними п'ятьма властивостями:

– кожній парі *K*-об'єктів *A, B* відповідає множина *HK*(*A, B*) морфізмів (можливо, порожнє), включене в Mork;

– для кожного морфізма $f \in$ Mork існує єдина пара *A, B K-об'єктів*, така що $f \in HK(A, B)$;

– у множині Mork визначена, загалом кажучи часткова, двомісна операція – множення морфізмів; добуток *fg* морфізмів $f: A \to B$ і $g: C \to D$ визначене лише в тих випадках, коли *B*=*C*, тобто коли кінець морфізма *f* збігається з початком морфізма *g*. У цьому випадку добуток *fg* є *K*-морфізм із об'єкта *A* в об'єкт *D*. У цьому випадку говорять, що для об'єктів $A, B, C \in K$ визначене відображення

$$H_K(A,B) \times H_K(B,C) \to H_K(A,C) \tag{4}$$

Знак × у цьому випадку позначає декартовий добуток множин морфізмів. Морфізми *f, g* категорії *K* виду $f: A \to B$ і $g: B \to C$ називаються послідовними, а виду $f: A \to B$ і $g: A \to B$ – паралельними.

Будь-яка категорна діаграма утворюється з об'єктів і стрілок (морфізмів), вона являє собою орієнтований граф з розфарбованими вершинами й дугами. У ролі вершин графа в категорної діаграмі виступають об'єкти категорії, а в ролі дуг її морфізми. Такого виду діаграми широко використовуються в теорії категорій. Вони – головний засіб наочної вистави внутрішньої будови й властивостей математичних структур, зв'язків між ними.

Діаграма, що виражає категорний закон асоціативності, характеризує зв'язки між будь-якими об'єктами *A, B, C, D* і морфізмами *f, g, h*. Ці зв'язки виражають суть закону асоціативності. В даному випадку ми висловили один із законів теорії категорій.

Категорні діаграми поділяються на замкнуті і розімкнуті. Замкнені діаграми називаються інакше комутативними. Така назва походить від того, що комутативність діаграми характеризуються тим, що результат дії морфізму при їх послідовному виконанні, зазначеному на діаграмі, виходить однаковим під час руху різними шляхами діаграми, якщо ми вирушаємо від однієї і тієї ж точки діаграми і приходимо знову до однієї і тієї ж точки іншої діаграми.

Оскільки логічні мережі є графічним вираженням алгебро-логічного опису об'єкта, то з практичної точки зору вигідніше розглядати модифіковану предикатну категорію зі визначеною операцією множення, що базується на використанні властивостей алгебри предикатів. Для того щоб практично використовувати поняття предикатної модифікованої категорії, спочатку потрібно отримати загальну модифіковану категорію, окремим випадком якої вона є. Тому слід абстрагуватися від поняття модифікованої предикатної категорії і сформувати як альтернативу загальному поняттю класичної категорії, загальне поняття модифікованої категорії.

Видобування даних займається пошуком та виявленням прихованих знань у необроблених даних за допомогою машинних алгоритмів та інструментів штучного інтелекту, виявляючи невідомі раніше, нетривіальні та практично значущі інформації, які можуть бути інтерпретовані людиною. Його потенціал дозволив розширити застосування до освітньої сфери.

Список використаних джерел

1. Kozyriev A., Shubin I. Method for solving quantifier linear equations for formation of optimal queries to databases. CEUR workshop proceedings. 2023. Vol. 3396, P. 449-459.

2. Kyrychenko, I., Malikin, D. Research of Methods for Practical Educational Tasks Generation Based on Various Difficulty Levels, 6th International Conference COLINS-2022, CEUR Workshop Proceedings 3171, Volume I: Main, P. 1030-1042. available at: https://ceur-ws.org/Vol-3171/paper74.pdf

3. Shubin, I. Development of conjunctive decomposition tools. CEUR Workshop Proceedings, 2870, 2021. P. 890–900. Available at: https://ceur-ws.org/Vol-2870/

УДК 623.4.017

Ліщук М. Є., Соломоненко Ю. С.

АНАЛІЗ ТАКТИКО-ТЕХНІЧНИХ ХАРАКТЕРИСТИК РЛС КРАЇН-ПАРТНЕРІВ (КРАЇН НАТО)

Від 24 лютого 2022 року російська федерація розпочала повномасштабне вторгнення в Україну. Під час повномасштабного вторгнення було знищено багато українських радіолокаційних станцій (РЛС), що призвело до погіршення показників радіолокаційного поля угруповання радіотехнічних військ (РТВ), насамперед маловисотного.

Слід зазначити, що противник широко застосовує тактику використання безпілотних засобів різного призначення, які переважно діють на малих висотах. Такі повітряні цілі як об'єкт радіолокації, відносяться до класу малорозмірних та малошвидкісних, їх виявлення суттєво ускладняється дією пасивних завад, що обумовлені відбиттям від підстеляючої поверхні.

Радіолокаційне виявлення й супроводження безпілотних літальних апаратів (БпЛА) стратегічного та оперативного рівня застосування проблем не викликає, оскільки вони, як об’єкти радіолокації, за своїми характеристиками майже не відрізняються від пілотованих літаків тактичної авіації. Щодо можливостей виявлення та супроводження БпЛА стратегічного застосування, то вони визначаються формулярними даними оглядових РЛС, які визначають параметри зон виявлення саме літаків тактичної авіації. Для виявлення та супроводження БпЛА оперативно-тактичного рівня застосування характерним є суттєве стискання зон виявлення цілей оглядовими РЛС майже вдвічі.

Розрахунки показують, що сучасні РЛС, які знаходяться на озброєнні частин та підрозділів РТВ, можуть забезпечити виявлення БПЛА типу “Орлан-10” на висотах від

100 м – на дальностях 15…30 км, на висотах більше 500 м – на дальностях 50…60 км, та на висотах більших 1000 м – на дальностях 70…90 км.

З метою покращення спроможностей угруповання РТВ щодо виявлення цілей такого класу країнами-партнерами були надані РЛС Ground Master 200, TRML-4D, AN/TPQ-64.

Вказані РЛС відносяться до класу багатофункціональних радіолокаційних систем повітряного спостереження. Вони здатні виявляти, супроводжувати та класифікувати різні типи повітряних цілей. Велика увага приділяється режимам виявлення малорозмірних, швидкісних крилатих ракетах, маневруючих літаків та вертольотів, що діють на малих та граничномалих висотах. Корисним є режим контрбатарейної боротьби та виявлення балистичних цілей, що дозволяє розширити сферу застосування РЛС.

Аналіз показав, що розглянуті РЛС відносяться до класу маловисотних та забезпечують просторові показники зони виявлення близькі до РЛС вітчизняного виробництва, але показники завадозахищеності, можливості з спряження та мобільності на кращому рівні.

Слід відзначити високі експлуатаційні характеристики (час напрацювання на відмову як правило перебільшує 2500 годин), розширену підтримку життєвого циклу, простоту операцій технічного обслуговування та сервісну підтримку виробником.

Широко використовується резервування на рівні підсистем, що у поєднані із розвиненою вбудованою системою безперервної діагностики забезпечує можливість:

- виявити та локалізувати відмову;
- виконати компенсацію відмови та забезпечити працездатність РЛС до початку ремонту.

Суттєвим недоліком є їх висока вартість порівняно з вітчизняними РЛС подібного призначення та відсутність ремонтних підприємств на території України. Також загальною проблемою, що потребує вирішення є відсутність вбудованого запитувача системи державного впізнавання "Пароль".

Любішин Б.В., Удніков О.М., Лейба В.О.

ВИКОРИСТАННЯ МУЛЬТИМЕТРІВ ДЛЯ АВТОМАТИЗАЦІЇ ПРОЦЕСУ КАЛІБРУВАННЯ ВИМІРЮВАЛЬНИХ ПЕРЕТВОРЮВАЧІВ ХВИЛЕВОДНИХ ТИПУ М5

Вимірювальні перетворювачі хвилеводні типу М5 входять до комплекту вимірювачів потужності НВЧ-сигналів М3-22 та М3-22А, які призначені для вимірювання середнього значення потужності безперервних та імпульсно-модульованих НВЧ-сигналів у коаксіальних і хвилеводних трактах та широко використовуються при обслуговуванні радіолокаційних станцій, радіонавігаційного обладнання, систем зв'язку, керованої, в тому числі високоточної, зброї та інших зразків озброєння, з метою контролю їх параметрів. Ефективність їх використання значною мірою залежить від точності визначення метрологічних характеристик вимірювальних перетворювачів типу М5, які визначаються при їх калібруванні. Калібрування вимірювальних перетворювачів хвилеводних типу М5 здійснюється за допомогою вихідного еталону ЗС України одиниці потужності в хвилеводних трактах в діапазоні частот від 5,64 ГГц до 37,5 ГГц.

Проведення метрологічного підтвердження вимірювальних перетворювачів хвилеводних супроводжується низкою негативних факторів, а саме: нестабільністю рівня потужності вихідного сигналу генераторів, дрейфом еталонних ватметрів, складною процедурою визначення результатів повірки (калібрування) і, як наслідок, високою трудомісткістю. Зменшення впливу випадкових факторів та підвищення точності про-

ведення вимірювань можливе при проведенні багаторазових вимірювань, що в свою чергу значно підвищить час проведення калібрування.

Одним із шляхів вирішення цієї проблеми є автоматизація процесу отримання, перетворення та обробки вимірювальної інформації під час визначення метрологічних характеристик вимірювальних перетворювачів, а саме КСВН (коефіцієнта стоячої хвилі) та $К_{еф}$ (коефіцієнта ефективності) вимірювальних перетворювачів. Однак до складу вихідного еталону входять вимірювальні прилади, які не мають функцію дистанційного керування вимірювальною інформацією, а в якості еталонних вимірювачів потужності використовуються два вимірювачі потужності НВЧ-сигналів М3-22А. Замінити дане обладнання сучасними засобами вимірювання закордонного виробництва недоцільно через суттєві технічні проблеми, а саме: використання сучасних перехідників, які для сумісності з існуючими зразками вимірювальних перетворювачів хвилеводних типу М5 потребують наявності переходів, які необхідно атестувати, що призведе до збільшення загальної похибки.

Отже, в якості засобів для спостереження за результатами вимірювань пропонується використовувати сучасні мультиметри. Значення потужності еталонного ватметра можливо визначати шляхом вимірювання мультиметром напруги на контрольних виходах вимірювального блоку М3-22А, та наступного перерахунку у значення потужності за допомогою відповідних коефіцієнтів. Відведену потужність вимірювального перетворювача хвилеводного типу М5, що калібрується, визначаємо на вході іншого М3-22А. Так, як М3-22А по своїй суті є мостом, до плечей якого підключені опорний та робочий терморезистор вимірювального перетворювача, його еквівалентне значення потужності визначається як різницю квадратів падіння напруг на робочому та опорному терморезисторі.

Таким чином, введення до вимірювальної схеми сучасних мультиметрів, з відповідним програмним забезпеченням, дозволить автоматизувати процес отримання та обробки інформації, що в свою чергу підвищить точність вимірювань та зменшить час на проведення калібрування.

УДК 621.396

Майборода І.М.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ПОРТАТИВНОЇ АНТЕНИ СУПУТНИКОВОГО ЗВ’ЯЗКУ В СИСТЕМІ MUOS

Досвід бойових дій з російськими окупантами наочно показав як збільшення бойової потужності угруповання різнорідних сил, перш за все, досягається за рахунок створення єдиного інтегрованого інформаційно-комунікаційного простору, що забезпечує доведення до учасників операцій достовірної та повної інформації про обстановку практично в реальному масштабі часу. А це завдання може вирішити тільки сучасна система радіозв’язку, яка передбачає розгортання багаторівневої транспортної мережі на базі електрокомунікаційних платформ, з інтелектуалізацією процесу управління мережами радіозв’язку, застосуванням широкосмугових сигналів, спеціальних смарт антен та використанням сучасних технологій, таких як MIMO, SDR, TDMA, MANET, FANET та ін.

Так, з метою надання гарантованих послуг зв’язку мобільним розосередженим підрозділам у глобальному масштабі була розроблена вузькосмугова тактична супутникова система зв’язку нового покоління MUOS (Mobile User Objective System). MUOS працює як "розумний телефон у небі", підтримуючи зв'язок між абонентами на дуже великих відстанях в УКХ діапазоні. MUOS надає військовим більше можливостей зв’язку

ніж існуючи системи, у тому числі з одночасною передачею голосу, відео та даних. Крім того, система дозволяє підтримувати зв'язок між абонентами по радіоканалам навіть тоді, коли будь-який канал припиняє задовольняти певним вимогам, тобто мережа автоматично встановлює зв'язок з абонентами системи MUOS, забезпечуючи його безперервність.

Однією з антен, що забезпечує максимальну ефективність супутникового зв'язку в системі MUOS є портативна антена RF-3080-AT001. Її поперечна Yagi конструкція в частково зібраному вигляді забезпечує швидке розгортання і високий коефіцієнт підсилення (11 dB). Частотний діапазон антени - від 240 до 400 МГц. Унікальна складна конструкція дає змогу антені вписуватися в легку, невелику за обсягом сумку для перенесення. В упакованому вигляді антена має розміри (470 х 152 х 152 мм) і легко може транспортуватися.

Антена RF-3080-AT001 містить систему живлення з рефлектором, два комплекти директорів, штатив, два коаксіальні кабелі та сумку для транспортування. Кругова поляризація з вузькою шириною основного променя випромінювання досягається завдяки внутрішній схемі узгодження, яка живить два плоских дипольних елементи. Рефлектор, розміщений позаду дипольних елементів, має вісім радіальних гілок, що відбивають енергію від збуджуваних елементів. Шість директорних елементів, зібраних у три зібрані пари, забезпечують фокусування у вузький промінь діаграми спрямованості та підвищують підсилення антени. Антена може працювати з комплектом директорних елементів або без них, збільшуючи смугу робочих частот при зменшеному значенні коефіцієнта підсилення.

Антена забезпечує високоякісний та безперервний зв'язок разом у комплекті з радіостанціями УКХ діапазону виробництва компанії HARRIS RF-7850M-HH, RF-7800M-MP, які є основою транспортної мережі системи радіозв'язку Національної гвардії України. Завдяки змінним роз’ємам коаксіальних кабелів з комплекту антени забезпечується легке підключення до роз’ємів типу BNC радіостанцій для роботи у супутниковому діапазоні. Антена RF-3080-AT001 схрещеного типу Yagi нового покоління забезпечує як повнодуплексний зв'язок MUOS, так і застарілий UHF SATCOM.

УДК 623.55.02

Малюк В.Г.

КОМП’ЮТЕРНЕ МОДЕЛЮВАННЯ АКТИВНОГО РАДІОМАСКУВАННЯ КАНАЛУ ЗВ’ЯЗКУ VHF/UHF ДІАПАЗОНУ ІЗ ВРАХУВАННЯМ ДАЛЬНОСТІ РОБОТИ РАДІОЗАСОБІВ

Розглядається необхідність створення активного захисту каналу мобільного радіозв'язку в діапазоні UHF/VHF від радіорозвідки противника за допомогою генератора радіоперешкод із врахуванням дальності роботи радіозасобів. Сформульовано завдання та запропоновано алгоритм визначення меж області розміщення спрямованого генератора радіоперешкод, у кожній точці якої забезпечується активний захист радіоканалу. Проведені практичні розрахунки доводять ефективність комп’ютерного моделювання розвідзахищеної роботи на тактичному рівні каналу мобільного радіозв'язку в умовах роботи розвідувального радіоприймача противника.

При тактичних розрахунках умов розвідзахищеної роботи каналів радіозв'язку UHF/VHF діапазону формувань сил охорони правопорядку відстані між радіозасобами збільшуються до кількох кілометрів. Це робить актуальною проблему врахування да-

льності роботи радіозасобів у задачах протидії засобам радіорозвідки противника шляхом застосування активних та пасивних засобів радіомаскування.

Одним із пасивних способів зниження ефективності радіорозвідки є розрахунок зони електромагнітної доступності (ЕМД) систем мобільного радіозв'язку [1], поза якою потужність сигналу передавачів є недостатньою для прийому розвідувальним радіоприймачем супротивника. Якщо такий приймач перебуває всередині зони ЕМД, можна застосувати активне придушення корисного радіосигналу у тракті прийому розвідувального радіоприймача противника шляхом постановки джерела навмисних радіоперешкод за умови електромагнітної сумісності (ЕМС) зі своїми засобами радіообміну [2,3].

Запропоновано простий та ефективний метод визначення меж області можливого розміщення генератора радіоперешкод для захисту мобільних засобів радіозв'язку в діапазоні UHF/VHF від прослуховування наземним розвідувальним радіоприймачем супротивника. Метод враховує наявність зон ЕМД систем мобільного радіозв'язку та дальність дії генератора радіоперешкод.

Показано, що застосування генератора активних радіоперешкод є доцільним, якщо забезпечена працездатність каналу мобільного радіозв'язку, і розвідувальний радіоприймач противника має можливість прослуховування каналу мобільного радіозв'язку. У кожній точці зони розміщення генератора радіоперешкод шляхом орієнтації його антенного пристрою азимуту забезпечується придушення корисного радіосигналу на вході розвідувального радіоприймача противника з одночасним виконанням умов ЕМС з радіозасобами каналу зв'язку. Завдання орієнтації антенного пристрою генератора радіоперешкод вирішується з використанням удосконаленої моделі каналу мобільного радіозв'язку UHF/VHF діапазону, яка дозволяє обчислити відношення сигнал/перешкода з урахуванням просторового розташування та ЕМД взаємодіючих радіозасобів.

Для визначення меж області розміщення генератора радіоперешкод використана процедура повного перебору точок ROI (Region of Interest), що включає повністю або частково область рішення. Більш швидкий хвильовий алгоритм [4], використаний раніше, у розглянутій задачі не може бути застосований, оскільки область рішення у багатьох випадках складається з кількох несуміжних фрагментів.

Проведені практичні розрахунки доводять ефективність врахування зон ЕМД джерел радіовипромінювання у задачі оцінювання розвідзахищеної роботи каналу радіозв'язку на відстанях до 10 км і більше, що може бути корисним при тактичних розрахунках.

Найбільш переважний варіант організації роботи радіоканалу, який відкриває широкі можливості для його активного захисту за допомогою генератора радіоперешкод, – це наявність спрямованих антенних пристроїв в обох радіозасобів каналу мобільного зв'язку, взаємно орієнтованих один на одного. У цьому випадку площа області розміщення генератора радіоперешкод є найбільшою порівняно з іншими комбінаціями типів ДС антенних пристроїв радіозасобів каналу зв'язку.

Список використаних джерел

1. V. Maliuk, O. Iohov, S. Horielyshev, V. Olenchenko,A. Oleschenko, E. Novikova, K. Tkachenko. Bounds Calculation Method Of Electromagnetic Availability Zone Of Radio Emission Source. *Advances in Military Technology* Vol. 17, No. 2, 2022, pp. 341-356. DOI 10.3849/aimt.01739

2. Ткаченко К. М., Іохов О. Ю., Малюк В. Г.. Математична модель радіообміну при застосуванні активного радіомаскування. *Системи управління, навігації та зв'язку.* 2016. Вип. 1. С. 129-132. URL: http://nbuv.gov.ua/UJRN/suntz_2016_1_34 (дата звернення: 26.02.2024).

3. Іохов О.Ю., Малюк В.Г., Горбов О.М. Імітаційне моделювання захищених радіоканалів військового призначення. *Наука і техніка Повітряних Сил Збройних сил Украї-*

ни, 2015, №1(18). С. 92-96. URL: http://nbuv.gov.ua/UJRN/Nitps_2015_1_22 (дата звернення: 26.02.2024).

4. Iohov O., Maliuk V., Horielyshev S., Tkachenko K., Herasimov S. Development of a Method for Boundary Determination of the Noise-resistant Area of the UHF/VHF Band. Advances in Military Technology, 2020, vol. 15, no. 2. pp. 231-246. DOI 10.3849/aimt.01376

Мартинюк В.В., Паламарчук С.А., Чередниченко О.Ю, Овсянніков В.В., Мальцева І.Р.

ЗАСТОСУВАННЯ МЕТОДІВ БЕЗДРОТОВОГО ПЕРЕДАВАННЯ ЕНЕРГІЇ ДЛЯ ЕНЕРГОЗАБЕЗПЕЧЕННЯ МУЛЬТИРОТОРНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Застосування безпілотних літальних апаратів (далі – БпЛА) в сучасних війнах дозволяє вести розвідку, коригувати вогонь артилерії, скидати вибухівку на ворожі об’єкти, розташовувати на борту ретранслятори радіозв’язку, встановлювати обладнання робототехнічних комплексів для розмінування і т.д. Під час виконання завдань БпЛА повинен мати характеристики, які визначають його мобільність, такі як: тривалість польоту, швидкість руху, можливість зависання над певними об’єктами (компенсація дії вітру), швидкість підйому, висота польоту та інші. Ці характеристики залежать від джерела електроенергії на борту БпЛА. Крім силової установки, споживачами електроенергії на борту БпЛА є суміжні бортові системи: система управління, широка номенклатура корисного спорядження: датчики збору розвідувальної інформації, система скидання, підвісне озброєння. Відповідно, енергоспоживання БпЛА збільшується завдяки розширеним функціям.

Існує два варіанти заряджання акумуляторної батареї БпЛА. Перший – шляхом заміни розрядженої батареї на заряджену. Для цього БпЛА необхідно повернутися в район запуску де оператор здійснить заміну батареї. Другий варіант – заряджати батарею від зовнішнього джерела електроенергії, використовуючи методи дротового і бездротового передавання енергії. З використанням методу передавання електроенергії через дроти БпЛА може підтримувати необмежену автономність, але кабелі важкі, їх здуває вітром разом із самим БпЛА, при цьому відсутня мобільність.

Бездротові методи передавання електроенергії (WPT – Wireless Power Transfer) [1] забезпечують більшу свободу пересування. Вони розділяються на методи з випромінюванням енергії ближнього поля (NFR – Near Field Radiation) і методи з випромінюванням енергії дальнього поля (FFR – Far Field Radiation) (рис.1). Методи FFR все ще знаходяться на стадії досліджень. Методи NFR вже застосовуються у сфері побутової електроніки для заряджання гаджетів.

Процес WPT складається з двох послідовних кроків: перетворення енергії в альтернативний вид зручний для передавання (електричне або магнітне поле), подальше передавання перетвореної енергії до споживачів шляхом використання електростатичних явищ, магнітної індукції або електромагнітного випромінювання. Кожен метод WPT включає три основні частини, такі як: передавач, приймач і сполучні пристрої. Передавач безпосередньо підключається до джерела енергії, яка перетворюється в змінне у часі електромагнітне поле та випромінюється через пристрій сполучення. З іншого боку приймач використовує свій сполучний пристрій, щоб отримати випромінювану потужність і перетворити її назад у постійний (DC) або змінний струм (AC), який використовується навантаженням.

Запропоновано використання методів бездротового передавання енергії (WPT) для автоматичного заряджання акумуляторних батарей БпЛА. На основі аналізу було зроб-

лено висновок, що на даний час більш практичними є методи ємнісно-резонансного (RCCWPT) та індуктивно-резонансного (RICWPT) бездротового передавання енергії, тому що їх застосування не вимагає посадки БпЛА на станцію заряджання з точністю до міліметра, що може додатково зменшити складність керування для автономної посадки.

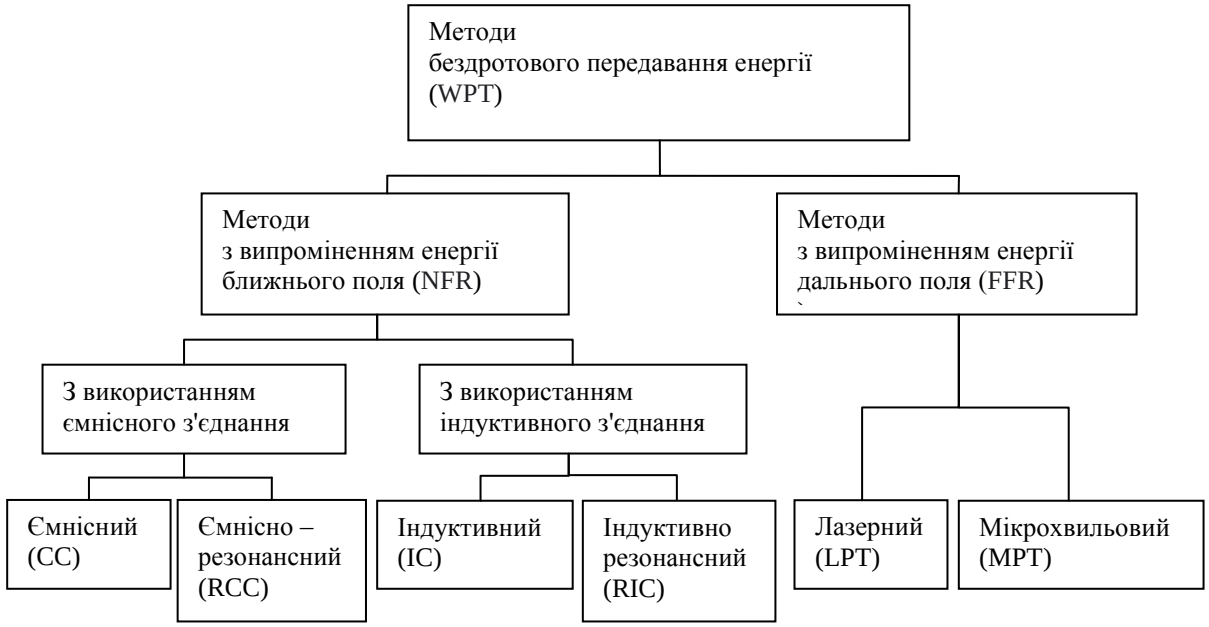


Рисунок 1.

Використання зарядних станцій БпЛА, які працюють в автоматичному режимі, дозволить звільнити оператора від ручного перезаряджання батарей та виключити перебування на території де здійснюється розмінування [2], тим самим унеможливити його поранення або загибель. Для цього пропонується використовувати зарядні станції які розгорнуті на місцевості неподалік від району проведення розмінування, де є можливість підключення до промислового джерела живлення або військової електроустановки. Таким же чином зарядна станція, що працює в автоматичному режимі, доцільна під час використання БпЛА для спостереження за ділянкою місцевості. Це дозволяє здійснювати цілодобове і безперервне проведення вказаних робіт, у разі використання декількох БпЛА, у черговому режимі (один працює, інший заряджається). При розряджанні акумуляторної батареї першого БпЛА в автоматичному режимі здійснюється зліт іншого БпЛА який продовжує виконання завдання та посадка на звільнену зарядну станцію першого. Цей процес контролюється оператором з віддаленого робочого місця.

Подальші дослідження будуть присвячені зарядним станціям які використовують методи WPTNFR з параметрами, що дозволяють ефективно і за мінімальний час здійснювати заряджання акумуляторних батарей БпЛА і датчикам, які будуть використовуватися БпЛА для визначення місцезнаходження та точного приземлення на бездротову зарядну станцію.

Список використаних джерел:

1. Mostafa, T.M.; Muharam, A.; Hattori, R. Wireless battery charging system for drones via capacitive power transfer. In Proceedings of the 2017 IEEE PELS Workshop on Emerging Technologies: Wireless Power Transfer (WoW), Chongqing, China, 20–22 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.

2.Чередниченко О.Ю., Паламарчук Н.А., Шемендюк О.В., Мартинюк В.В. Синтез системи виявлення вибухонебезпечних предметів на базі безпілотного літального апарата. Системи і технології зв'язку, інформатизації та кібербезпеки. ВІТІ № 3 – 2023р.

УДК 621.39:623.1/.7

Марченко Б.С., Джус В.В., Титаренко Р.В.

УДОСКОНАЛЕННЯ СИСТЕМИ СИНХРОНІЗАЦІЇ БАГАТОКАНАЛЬНОЇ СТАНЦІЇ НАВЕДЕННЯ РАКЕТ ЗЕНІТНОГО РАКЕТНОГО КОМПЛЕКСУ С-300В1 В РЕЖИМАХ ВИЯВЛЕННЯ ТА СУПРОВОДЖЕННЯ ПОВІТРЯНИХ ЦІЛЕЙ

Виконання завдань за призначенням радіотехнічного засобу можливо лише при справності всіх його систем [1-15]. В ході проведеного дослідження з'ясовано, що при веденні сучасного протиповітряного бою багатоканальної станції наведення ракет **(**БСНР) буде використовувати різні типи сигналів та різні режими роботи, постійно здійснювати переходи між ними, що потребує удосконалення такої системи станції, що забезпечить покращення її роботи в усіх режимах та з усіма типами сигналів.

За результатами аналізу системи синхронізації встановлено, що вона відіграє важливу роль у виконанні завдань за призначенням БСНР у будь-якому режимі та **п**ризначена для організації синхронної роботи всіх систем станції.

При переході з одного режиму в другий система синхронізації забезпечує автоматичну зміну часового розміщення всіх імпульсів та стробів. Імпульси, сформовані системою синхронізації, за призначенням поділяються на групи, які змінюють часове розміщення в залежності від режиму роботи станції. Для кожного режиму набор імпульсів та їх часове розміщення зумовлено програмою, закладеною в апаратурі синхронізатора.

Нестабільності видачі імпульсів (стробів) та флуктуації їх рівнів пов'язані з застарілою елементною базою, в загальному випадку приводить до збільшення часу встановлення потрібних режимів роботи станції і, як наслідок, збільшення робітного часу ЗРК при роботі по повітряних цілях, що не завжди дозволяє виконати завдання за призначенням с заданими показниками якості. Запропоновано удосконалити систему синхронізації БСНР 9С32, основним недоліком якої є застарілість елементної бази, що не задовольняє сучасним вимогам.

За результатами аналізу сучасної матеріальної бази запропоновано використовувати мікроконтролери на заміну блоків, з яких складається система синхронізації БСНР 9С32.

Реалізація запропонованих рішень дозволить суттєво підвищити точність формування стробів та імпульсів при роботі систем БСНР 9С32 у різних режимах та з різними типами сигналів, у зв'язку з чим мета роботи досягнута.

Список використаних джерел

1. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2005). Организация когерентной обработки на промежуточной частоте при приеме широкополосных сигналов крупноапертурными антенными решетками и многопозиционными системами. Прикладная радиоэлектроника, (Т.4, №4,) 437-440.

2. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2006). Алгоритмы когерентной обработки широкополосных сигналов на промежуточной частоте с использованием схем фазонастраивающих контуров с управляемыми дисперсионными линиями задержки в крупноапертурных антенных решетках и многопозиционных системах. Прикладная радиоэлектроника, (Т.5, №2), с. 250-254.

3. Туринский, А.В., Певцов, Г.В., Крючков, Д.Н., & Рощупкин, Е.С. (2020). Методы повышения достоверности и эффективности контроля технического состояния радиотехнических систем подвижных объектов. Azərbaycan dövlət dəniz akademiyasının elmi əsərləri (ISSN 2220-1025), 1, 176–182. https://doi.org/10.5281/zenodo.5035847

4. Седишев П.Ю. Однозначне оцінювання дальності рухомої цілі при її супроводженні по швидкості й кутових координатах радіолокатором з використанням когерентних сигналів з високою частотою повторення імпульсів / П.Ю. Седишев, А.О. Подорожняк, Є.С. Рощупкін // Наука і техніка Повітряних Сил Збройних Сил України. – 2009. – № 1(1). – С. 71-74. http://nbuv.gov.ua/UJRN/Nitps_2009_1_20

5. Рощупкин Е.С. Оценка прямоугольных координат цели при объединении результатов независимых первичных измерений в активной многопозиционной системе радиолокации / Е.С. Рощупкин // Зб. наук. пр. ОНДІ ЗС. – Х.: ОНДІ ЗС, 2006. – Вип. 2(4). – С. 156-162.

6. Рощупкин, Е.С. (2003). Уточненный алгоритм измерения координат источника излучения при обработке пространственной фазовой структуры принимаемого разнесенной корреляционно-базовой системой сигнала. Sistemi obrobki ìnformacìï, 2(24), 90–95. https://doi.org/10.5281/zenodo.5035861

7. Рощупкин, Е.С. (2007). Ошибки определения прямоугольных координат источника излучения в пассивных гиперболических измерительных системах. Збірник наукових праць Об'єднаного науково-дослідного інституту Збройних Сил, 2 (7), 156–161. https://doi.org/10.5281/zenodo.5088597

8. S. Herasimov, M. Pavlenko, E. Roshchupkin, M. Lytvynenko, O. Pukhovyi, and A. Salii, Aircraft flight route search method with the use of cellular automata, International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, is. 4, 2020, p.p. 5077-5082, https://doi.org/10.30534/ijatcse/2020/129942020

9. Герасимов С.В. Теоретические основы оценки ошибок значений сигналов с гармонически меняющимися параметрами / С.В. Герасимов, Е.С. Рощупкин // Озброєння та військова техніка. – 2018. – № 2. – С. 43-49. http://nbuv.gov.ua/UJRN/ovt_2018_2_9

10. S. Herasimov, Y. Kozhushko, E. Roshchupkin, V. Dekadin, V. Djus and Y. Melenti, Evaluation of surface profile of holographic diffraction reflective coatings on scattering chart using in laser alarm systems, International Journal of Emerging Trends in Engineering Research, vol.8, is. 8, 2020, p.p. 4502-4507, https://doi.org/10.30534/ijeter/2020/74882020

11. Tymchenko, S., Kaplun, Y., Roshchupkin, E., Kukobko, S. (2023). Substantiation of Time Distribution Law for Modeling the Activity of Automated Control System Operator. In: Shkarlet, S., et al. Mathematical Modeling and Simulation of Systems. MODS 2022. Lecture Notes in Networks and Systems, vol 667. Springer, Cham. https://doi.org/10.1007/978-3-031-30251-0_9

12. Yaroslav Kozhushko, Evgeniy Roshchupkin, Vadym Yevsieiev, Sergey Pavlenko, Sergii Starodubtsev, Roman Honcha and Yevgen Melenti, Assessment of the influence of the manufacturing quality of a reflective coating on the angular distribution function of the reflected radiation intensity of laser signaling systems, International Journal of Emerging Trends in Engineering Research, vol.8, is. 10, 2020, p.p. 6696-6701, https://doi.org/10.30534/ijeter/2020/128102020

13. Кукобко С.В., Місценко Р.В., Британов Д.М., Рощупкін Є.С., & Гайбадулов Б.В. (2023). Пропозиції щодо автоматизації процесу прийняття рішення при класифікації ситуацій у повітряному просторі. Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку", Харків

14. Кукобко С.В., Рощупкін Є.С. (2022). Моделювання системи технічного обслуговування безпілотних літальних апаратів. Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2022): тези доповідей XII Міжнародної науково-практичної конференції, Чернігів

15. Herasimov, S., Borysenko, M., Roshchupkin, E. et al. Spectrum Analyzer Based on a Dynamic Filter. J Electron Test 37, 357–368 (2021), https://doi.org/10.1007/s10836-021-05954-0

Марченко О.С., Нікора І.В., Рябоконова Д.М.

ДОСЛІДЖЕННЯ БАГАТОШЛЯХОВОЇ МАРШРУТИЗАЦІЇ БЕЗДРОТОВИХ MESH-МЕРЕЖ

MESH-мережі мають широке застосування у військовій сфері оскільки використовуються для з'єднання військових баз, великих складів, також такі мережі дозволяють наземному персоналу отримувати доступ до відео з високою роздільною здатністю в реальному часі під час польоту беспілотних літальних апаратів.

MESH являє собою бездротову систему, що складається з кількох пристроїв, об'єднаних мережею. Кожен пристрій у мережі посилає власні сигнали та передає інформацію з інших пристроїв. Всі вузли в мережі з'єднуються через виділене з'єднання. Це дозволяє інформації переміщатися від вузла до вузла без затримок або збоїв. Дані мережі можуть організовуватись самостійно, оскільки новий вузол автоматично включається в існуючу мережу.

Більшість протоколів маршрутизації, запропонованих для сітчастих і спеціальних мереж, тобто для передачі між джерелом і вузлом призначення використовується лише один маршрут.

Мета даної маршрутизації — дозволити використовувати кілька шляхів для досягнення пунктів призначення, а не лише найкращого шляху.

Наявність кількох шляхів між джерелом і одержувачем зазвичай має наступні переваги:

- відмовостійкість: забезпечення резервних маршрутів, які будуть використовуватись у разі збою, є формами впровадження відмовостійкості на рівні маршрутизації в сітчастих мережах, для цієї ж мети можуть бути застосовані деякі методи, як-от збереження пакетів, що полягає у зміні маршруту пакета, якщо фактичний маршрут пошкоджено;

– підвищення пропускної здатності: маршрутизація вздовж одного шляху може не забезпечити достатньої пропускної здатності для з'єднання отже, використання одночасно кількох шляхів для маршрутизації даних може бути хорошим підходом для задоволення вимог щодо пропускної здатності деяких програм, а саме завдяки цьому досягається менша наскрізна затримка та покращується якість обслуговування;

– балансування навантаження: розподіл трафіку за кількома маршрутами може зменшити перевантаження в деяких ланках і вузьких місцях;

– стійкість до помилок: багатошляхові протоколи можна використовувати для забезпечення стійкості до помилок шляхом розподілу трафіку за кількома шляхами;

– безпека: через протоколи маршрутизації з одним шляхом зловмиснику легко запускати атаки маршрутизації, але багатошляховий доступ забезпечує стійкість до атак.

Типові протоколи маршрутизації в бездротових мережах використовуються для пошуку та підтримки маршрутів між джерелом і вузли призначення, тому що добре працюють в бездротових MESH – мережах, протокол маршрутизації має бути налаштований відповідно до заданих характеристик мережі.

Було розглянуто різноманітні протоколи маршрутизації, які використовуються в бездротових сітчастих мережах, і визначенню продуктивності цих протоколів маршрутизації для оптимального способу конструювання трафіку. Продуктивність визначається з урахуванням балансування навантаження, коефіцієнта доставки пакетів, перевантаження, накладних витрат на мережу, пропускної здатності та мобільності вузлів.

Порівнюючи протоколи багатошляхової маршрутизації з протоколами одношляхової маршрутизації, по-перше, можна помітити, що вони додають складності та додаткових витрат. Крім того, обслуговування таблиць маршрутизації в проміжних вузлах призводить до збільшення таблиць маршрутизації. У маршрутизації також є додатковий етап, який є необхідним у протоколах, а саме розподілом трафіку, що призводить до збільшення часу, необхідного для встановлення маршрутів. На підставі представленого аналізу дослідження, можна зробити висновок що добре розроблений протокол маршрутизації повинен враховувати такі аспекти: кілька шляхів, низькі накладні витрати, хороша продуктивність, низький ступінь сполучення маршрутів.

УДК 681.5.015

Медовкін В.В., Дядюн С.В.

РОЗРОБКА ТА РЕАЛІЗАЦІЯ ВЕБ-ДОДАТКУ ДЛЯ УПРАВЛІННЯ ФІНАНСОВИМИ РЕСУРСАМИ З ВИКОРИСТАННЯМ СУЧАСНИХ МЕТОДІВ ТА ТЕХНОЛОГІЙ ВЕБ-РОЗРОБКИ

У сучасному світі, де інформаційні технології стають все більш важливими в усіх сферах життя, управління фінансовими ресурсами набуває нового рівня значущості. Традиційно, для цього використовувалися різні ручні методи, такі як записи в блокноті або ведення таблиць у Excel. Проте, такі методи можуть бути громіздкими, схильними до помилок і не дають чіткого уявлення про загальний стан фінансів.

Веб-додатки для управління фінансовими ресурсами стають все більш популярними, завдяки своїй зручності, доступності та гнучкості. Такі додатки дозволяють користувачам відстежувати свої доходи і витрати, створювати бюджети, ставити фінансові цілі та отримувати аналітику своїх фінансів.

Дана робота починалася з глибокого аналізу вимог до системи управління фінансами, який включав у себе як технічні, так і функціональні аспекти. Було проведено дослідження потреб цільової аудиторії, визначено основні функції та можливості, які мали бути доступними для користувачів.

Сучасні Методи та Технології Веб-Розробки:

Фронтенд та Інтерфейс: Для створення дружнього та зручного інтерфейсу було використано одну з найпопулярніших JavaScript бібліотек - React.js. Вона дозволила побудувати інтерактивні компоненти інтерфейсу, що забезпечують користувачам зручний спосіб взаємодії з додатком. Дизайн інтерфейсу був створений з використанням фреймворку Bootstrap, що спростило процес розробки і забезпечило зручний та сучасний вигляд додатку.

Бекенд та Логіка: Для реалізації серверної частини додатку було використано Python з фреймворком Django. Django забезпечує швидку розробку та зручний синтаксис, що дозволило ефективно реалізувати бекендову логіку додатку. У якості бази даних було обрано PostgreSQL, що є потужною та надійною реляційною базою даних. Django також має вбудовану систему аутентифікації та авторизації, що дозволяє забезпечити безпеку даних користувачів.

Безпека: Забезпечення безпеки даних користувачів було пріоритетом під час розробки додатку. Django має вбудовані засоби для захисту від різноманітних атак, таких як CSRF та SQL ін’єкції. Також було використано SSL-шифрування для захисту даних під час передачі між клієнтом та сервером.

Розгортання та Масштабування: Для розгортання додатку було використано Docker та Kubernetes, що дозволило легко розгортати та масштабувати додаток в залежності від потреб користувачів.

Визуалізація Інтерфейсу: Нижче представлені деякі візуальні елементи розробленого додатку:

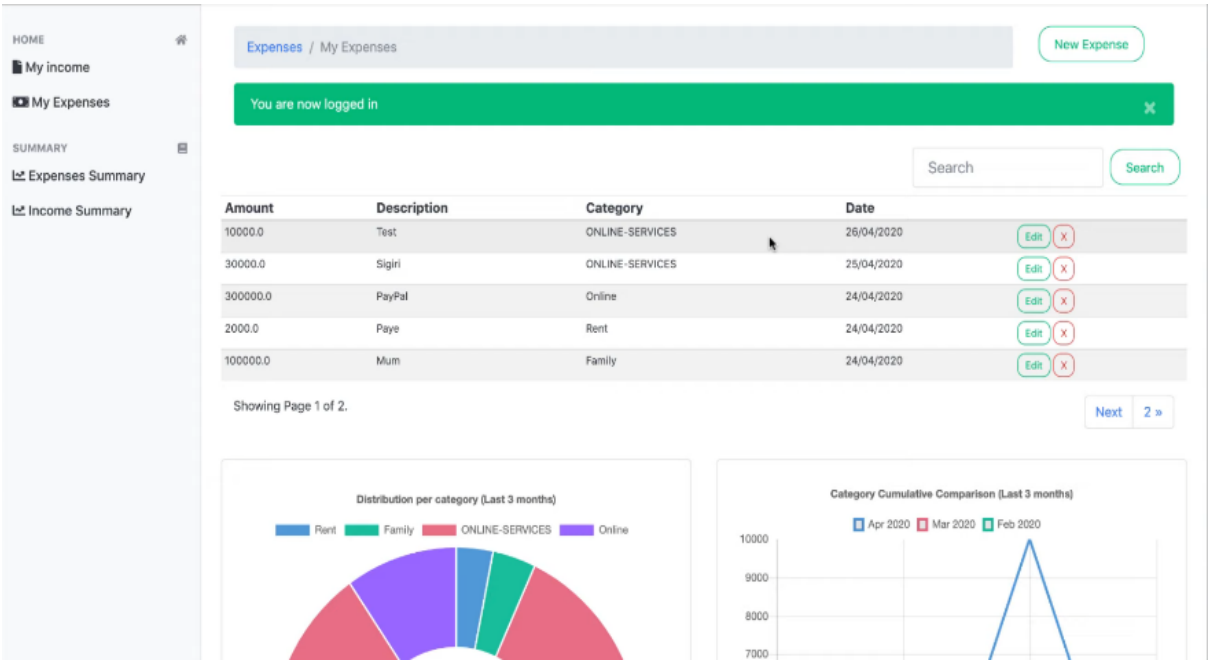


Рисунок 1 – Головна сторінка додатку

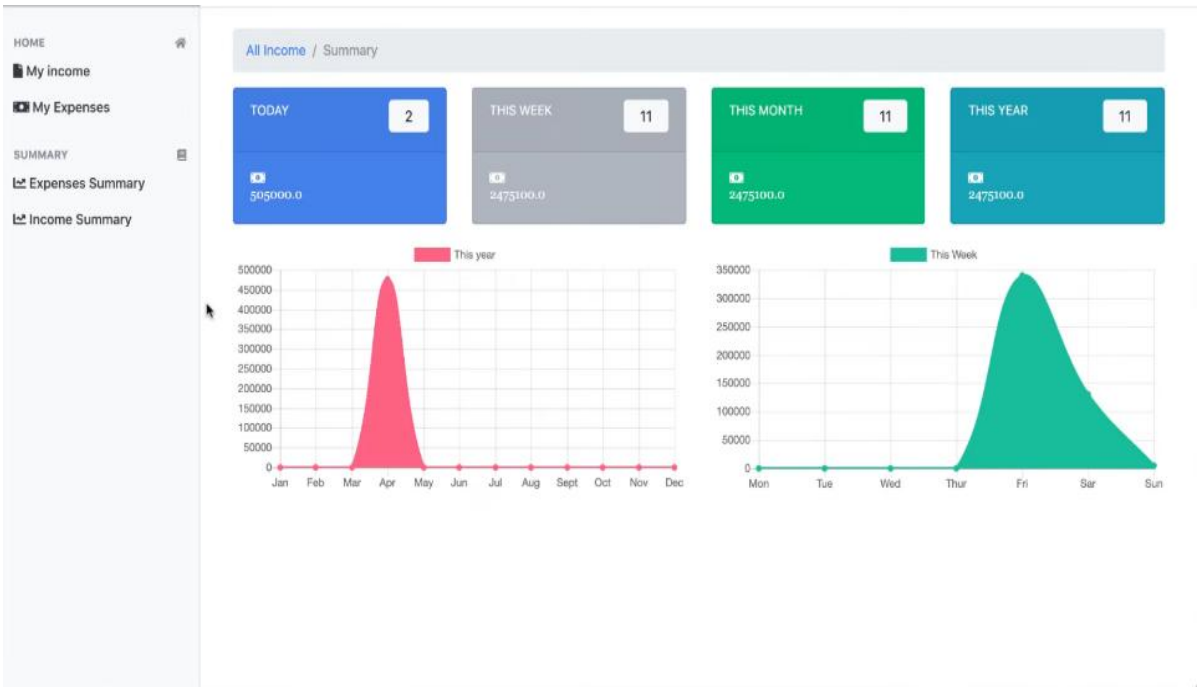


Рисунок 2 – Сторінка статистики та звітів

У результаті проведеної роботи отримано веб-додаток, який є не лише інструментом для управління фінансами, але й справжнім помічником у фінансовому плануванні та аналізі. Користувачі мають можливість легко створювати та відстежувати свої бюджети, ведучи детальні списки витрат і доходів. Вони можуть аналізувати свої фінансові потоки та отримувати звіти і статистику про свої фінансові дії.

Додаток має зручний та інтуїтивно зрозумілий інтерфейс, що дозволяє користувачам легко навігувати і використовувати всі його функції. При цьому забезпечується висо-

кий рівень безпеки даних з використанням найсучасніших методів шифрування та захисту від потенційних загроз.

Крім того, додаток готовий до масштабування та розгортання на різних хмарних платформах, що дозволяє йому легко пристосовуватися до зростання обсягів користувачів та забезпечувати стабільну і надійну роботу незалежно від обставин.

У цілому, додаток є не лише інструментом для вирішення конкретних фінансових завдань, але й партнером, який допоможе користувачам досягати фінансової стабільності і успіху у їхній особистій та професійній сферах життя.

Меркулов О.А.

АНАЛІЗ СУЧАСНОГО СТАНУ ТА ПЕРСПЕКТИВ РОЗВИТКУ ВИМІРЮВАЛЬНОЇ ТЕХНІКИ У ГАЛУЗІ ВИМІРЮВАННЯ ПАРАМЕТРІВ ІМПЕДАНСУ (ЕЛЕКТРИЧНОЇ ЄМНОСТІ ТА ІНДУКТИВНОСТІ) В УКРАЇНІ ТА ЗБРОЙНИХ СИЛАХ УКРАЇНИ

У колах змінного струму необхідно вимірювати, крім електричного опору, ще й такі фізичні величини, як індуктивність, ємність, реактивний, активний та повний опори, добротність, кути втрат, тощо. Ці величини ще називають параметрами імпедансу, імітансу або комплексного опору.

Основні досягнення науки і техніки в галузі вимірювання параметрів імпедансу у світі приходяться на початок та кінець XX сторіччя, а стосовно автоматизації (комп'ютеризації) вимірювань – на початок XXI сторіччя. На прикладі всесвітньовідомої та ведучої компанії за цим напрямком - IETLABS, INC (США) можливо виділити такі основні віхи у розвитку галузі вимірювання електричної ємності та індуктивності:

- 1915 р. – розпочато серійне виробництво конденсаторів;
- 1918 р. – розроблено десятичний міст;
- 1920 р. – виготовлено змінний повітряний конденсатор;
- 1930 р. – створено конденсатор "десятиріччя";
- 1933 р. – розроблено міст для вимірювання показників імпедансу;
- 1935 р. – виготовлено стандарт змінної індуктивності;
- 1976 р. – створено сучасний вимірювач LCR "Digibridge";
- 2002 р. – розроблена серія стандартів індуктивності 1482;
- 2004 р. - розроблена серія стандартів електричної ємності 1409.

Засоби вимірювання (ЗВ) електричної ємності та індуктивності, за звичай, поділяються на:

- засоби зберігання (відтворення) одиниць електричної ємності та індуктивності;
- засоби вимірювання електричної ємності та індуктивності (вимірювачі імпедансу, RLC-метри,LCR-метри).

У якості засобів зберігання (відтворення) одиниць електричної ємності та індуктивності використовуються однозначні або багатозначні міри.

Однозначні міри (котушки, стандарти, еталони, тощо) електричної ємності, як правило, представляють собою конденсатори з посрібленою слюдою і фольгою для використання у схемах з дво- або три контактним під'єднанням.

Однозначні міри індуктивності, як правило, представляють собою котушки (обмотки) дроту, які виконані на діелектричному сердечнику, що мінімізує захват від зовнішніх електромагнітних полів та не створює зовнішнього магнітного поля.

Багатозначні міри електричної ємності та індуктивності (магазини) представляють собою набори елементів - конденсаторів (котушок індуктивності), які поєднані між собою електричними ланцюгами та конструктивно об'єднані в одному корпусі. Значення

електричної ємності (індуктивності) задається шляхом підключення відповідної комбінації окремих елементів магазину. Переключання може бути як механічним, так і за допомогою спеціальних реле.

У якості засобів зберігання (відтворення) одиниць електричної ємності та індуктивності до складу вихідних еталонів Збройних Сил України одиниці електричної ємності ВЕЗСУ 08-06-05-09 та одиниці індуктивності ВЕЗСУ 08-00-06-09 входять два комплекти однозначних мір, а саме:

– комплект мір ємності Р597/1-19 класу точності 0,05/0,2;
– міри індуктивності Р5101 – Р5115 класу точності0,02/2,0.

Вимірювання параметрів комплексного опору здійснюється, як правило, методом порівняння, при якому вимірюваний параметр порівнюється зі зразковою мірою (зразковим резистором, конденсатором, котушкою індуктивності), чи резонансним методом. При вимірюванні на низьких частотах найбільше поширення одержав мостовий метод вимірювання. Прилади, що використовують мостовий метод, називаються мостами постійного і змінного струму – у залежності від характеру напруги живлення. Структура моста змінного струму аналогічна структурі моста постійного струму. На відміну від моста постійного струму у мості змінного струму слід враховувати під час врівноваження мосту не тільки амплітудні, а й фазові співвідношення, що значно ускладнює процес урівноважування. Вимірювальні мости змінного струму призначені для вимірювання ємності, тангенса кута втрат, індуктивності, добротності, взаємної індуктивності, частоти і неелектричних величин (при наявності відповідного параметричного перетворювача).

Сучасні мости змінного струму - це складні вимірювальні комплекси, до складу яких входить мікропроцесор. Це дає змогу автоматизувати процес врівноважування, вибирати автоматично оптимальну схему заміщення і діапазон вимірювання та виконувати інші сервісні функції.

Найбільш сучасними ЗВ параметрів імпедансу є різноманітні RLC-метри та LCR-метри. В основі принципу дії RLC-метру лежить аналіз одержуваних тестових сигналів. Серед основних способів, які використовуються для отримання необхідних параметрів, виділяють мостові методи, а також ті, які пов'язані з визначенням співвідношень по закону Ома.

Мостові вимірювачі RLC працюють з використанням вимірювального моста, який врівноважується за допомогою наборів зразкових реактивних (ємнісних) і активних опорів. Подібні прилади сприймають тільки фіксовані частоти.

До 2010 року у якості засобу порівняння мір ємності та індуктивності у складі вихідних еталонів Збройних Сил України одиниці електричної ємності ВЕЗСУ 08-06-05-09 та одиниці індуктивності ВЕЗСУ 08-00-06-09 використовувався міст змінного струму Р5083, похибка якого при виконанні вимірювань методом заміщення або перестановки становила від 0,005 до 0,03 %. У 2011 році на заміну мосту змінного струму Р5083 був закуплений вимірювач RLC МНС 1100 вітчизняного виробництва вартістю (на той час) близько 82 тис. грн (10 тис. $).

Вимірювач RLC МНС-1100 класу точності 0,01/0,001 виробництва ТОВ “КПФ “ПРОМІКС” (м. Київ) є одним із найсучасніших зразків вимірювальної техніки українського виробництва, який за критерієм “ціна-якість” переважає багатьох відомих аналогів іноземного виробництва.

Українську національну еталонну базу вимірювань ємності та індуктивності очолюють відповідно Державний первинний еталон одиниць електричної ємності та фактору втрат (ДЕТУ 08-06-01) і Державний первинний еталон одиниць індуктивності та тангенса кута втрат (ДЕТУ 08-09-09), які зберігаються в ДП “Укрметртестстандарт” (м. Київ). Передача одиниць ємності та індуктивності відбувається за державними повірочними схемами відповідно за ДСТУ 4064:2001 та ДСТУ 7161:2010. Щорічно із застосуванням зазначених державних еталонів одиниць ємності та індуктивності повіряється і

калібрується відповідно від 40 до 70 робочих еталонів (мір) ємності та від 20 до 50 робочих еталонів (мір) індуктивності.

Еталон складається з комплексу засобів вимірювальної техніки:

– комплекту термостатованих еталонних мір електричної ємності Andeen-Hagerling типу AH11A номіналом 10 пФ (4 од.);

– комплекту термостатованих еталонних мір електричної ємності Andeen-Hagerling типу AH11A номіналом 100 пФ (4 од.);

– комплекту еталонних перехідних мір електричної ємності номіналом від 1 пФ до 1 мкФ (6 од.);

– комплекту еталонних мір активного електричного опору номіналом від 0,1 Ом до 1 МОм (8 од.);

– еталонного компаратора з ПЕОМ;

– стандарту частоти та часу СЧВ-74;

– електронно-лічильного частотоміра Ч3-54.

Державний еталон забезпечує відтворення одиниць вимірювань на частоті 1000 Гц. Еталонний компаратор зі складу ДЕТУ 08-06-01 дозволяє здійснювати передачу розмірів одиниць параметрів імпедансу в діапазоні значень, що визначається набором мір активного опору та електричної ємності. Термостатовані еталонні міри електричної ємності Andeen-Hagerling типу AH11A утворюють групову двономінальну міру.

Еталонні міри, зі складу групової, безперервно досліджуються понад 15 років. Завдяки дослідженням, проведеним в національних метрологічних інститутах провідних країн світу (PTB, Німеччина; NIST, США; NPL, Великобританія, тощо), а також дослідженням, проведеним в ДП «Укрметртестстандарт», значення електричної ємності еталонних мір AH11A відомо з розширеною невизначеністю U_p=1,0 10^{-6} пФ при коефіцієнті охоплення k=2. Постійні дослідження зазначених мір дозволяють оцінити та врахувати дрейф їх основних характеристик.

Міри, що входять до складу еталона, завжди ввімкнені і підключенні до електричної мережі. До складу національного еталона входять:

– міра індуктивності термостатована номінальним значенням 1 Гн;

– міра індуктивності термостатована номінальним значенням 10 мГн;

– комплекс з трьох мір індуктивності термостатованих з номінальними значеннями по 100 мГн, які складають групову міру індуктивності номінальним значенням 100 мГн;

– магазин термостатованих еталонних мір СА-5200;

– компаратор індуктивності СА-2100;

– система стабілізації температури.

Діапазон значень індуктивності, у якому відтворюється та передається одиниця вимірювання, становить від 1мкГн до 10 Гн, тангенса кута втрат від 1 10^{-5} до 1.Робоча частота - 1кГц.

Розширена невизначеність відтворення одиниці індуктивності становить U_p=4 10^{-5} з коефіцієнтом охоплення k=2 за довірчої ймовірності 0,95.

Основний засіб вимірювання, який входить до складу обох вихідних еталонів ВЕЗСУ 08-06-05-09 та ВЕЗСУ 08-00-06-09 - прецизійний вимірювач RLC типу МНС-1100 (2-го розряду) щорічно проходить калібрування на Державних первинних еталонах ДЕТУ 08-06-01 та ДЕТУ 08-09-09.

Таким чином, підводячи підсумки проведених досліджень, визначено наступне.

Основні досягнення науки і техніки в галузі вимірювання параметрів імпедансу у світі здійснені на початку та в кінці XX сторіччя, а стосовно автоматизації (комп'ютеризації) вимірювань – на початку XXI сторіччя.

Найбільш сучасними ЗВ параметрів імпедансу є RLC-метри та LCR-метри.

Як Державний первинний еталон одиниць електричної ємності та фактору втрат (ДЕТУ 08-06-01), Державний первинний еталон одиниць індуктивності та тангенса кута втрат (ДЕТУ 08-09-09), так і вихідні еталони Збройних Сил України одиниці електричної ємності ВЕЗСУ 08-06-05-09 та одиниці індуктивності ВЕЗСУ 08-00-06-09 використовують практично усі сучасні досягнення світової науки і техніки у галузі вимірювання електричної ємності та індуктивності.

Мироненко О.В., Мострянський А.П.

ФОРМУВАННЯ НАБОРУ ДІАГНОСТИЧНИХ ОЗНАК ТА ЇХ ОПТИМІЗАЦІЯ ПРИ ПРОВЕДЕННІ ОЦІНКИ ТЕХНІЧНОГО СТАНУ МАНОМЕТРІВ ЗРАЗКОВИХ АБСОЛЮТНОГО ТИСКУ ТИПУ МПА-15

Визначений комплекс технічних характеристик і параметрів, які можуть бути використані в якості діагностичних параметрів, що дозволяють достовірно оцінити технічний стан манометрів зразкових абсолютного тиску типу МПА-15.

Підтримка високого рівня бойової готовності складних зразків ОВТ в умовах повномасштабного вторгнення російської федерації та обмежених матеріально – технічних ресурсах можливо лише шляхом підвищення ефективності всіх видів технічного обслуговування даних зразків. У зв’язку з цим постає завдання з підтримки в справному стані парку приладів, необхідних для технічного обслуговування зразків ОВТ. Рішення даного завдання в значній мірі залежить від можливості проведення діагностування цих приладів з метою визначення їх технічного стану. Відповідно до військової метрологічної схеми абсолютного тиску в діапазоні від $2{,}7\times10^{2}$ до 4×10^{5} Па, в якості робочого еталона використовується манометр зразковий абсолютного тиску типу МПА-15.

Аналіз останніх досліджень показав, що загальна проблема полягає в тому, що в процесі експлуатації манометра зразкового абсолютного тиску типу МПА-15 виникають ситуації (під час довготривалого зберігання, після транспортування, або якщо в поршневу пару потрапили мікро-частини бруду) коли у оператора можуть з’явитися сумніви в правильності показань приладу. Оскільки операції з підготовки до застосування манометра дуже трудомісткі, алгоритм опрацювання результатів вимірювань складний, а також відсутній самоконтроль роботи манометра, швидко визначити його технічний стан дуже важко. Це пов’язано з тим, що конструктивно МПА-15 має складну поршневу систему. Виходячи з цього виникає завдання з розробки діагностичного пристрою, який дозволить швидко визначити технічний стан приладу.

При створені діагностичного пристрою одним із основних питань є визначення ряду якісних технічних параметрів, які необхідно контролювати в процесі проведення діагностики МПА-15, та на їх основі сформувати набір діагностичних параметрів з їх подальшою оптимізацією.

Виходячи із конструктивних особливостей МПА-15, а також вимог, які пред’являються до проведення його метрологічного підтвердження до числа якісних параметрів манометра можна віднести такі показники:

- неповернення поршнів системи в нульове положення;
- чутливість манометра;
- жорсткість врівноважувального механізму;
- герметичність порівняльної і вимірювальної камер;
- вертикальність вісі поршневої системи;
- швидкість опускання поршня.

На основі обраних технічних параметрів манометра, проводилось формування діагностичних параметрів серед яких необхідно виділити дві групи ознак контролю:

- параметри, що будуть контролюватися безпосередньо діагностичним пристроєм;
- параметри, що контролюються без застосування діагностичного пристрою.

Виходячи з технічних вимог, які пред'являються до манометра зразкового абсолютного тиску типу МПА-15, в першу групу ознак були обрані такі діагностичні параметри:

- неповернення поршнів системи в нульове положення;
- неповернення поршнів в нульове положення;
- чутливість манометра;
- жорсткість врівноважувального механізму.

Параметри першої групи задаються безпосередньо в програмі, яка проводить опрацювання і аналіз динамічних процесів манометра.

У другу групу ознак були обрані параметри, які контролюються безпосередньо оператором, проводить діагностику манометра, а саме:

- герметичність порівняльної і вимірювальної камер;
- вертикальність вісі поршневої системи;
- швидкість опускання поршня.

По всім переліченим показникам, у цілому, можна зробити висновок про технічний стан манометра зразкового абсолютного тиску типу МПА-15.

Роблячи висновки можна сказати, що в разі впровадження діагностичного пристрою, за допомогою якого можна оцінити технічний стан манометра зразкового абсолютного тиску типу МПА-15 збільшиться достовірність передачі одиниці абсолютного тиску, що в свою чергу дозволить більш якісно проводити метрологічне підтвердження парку приладів, необхідних для технічного обслуговування зразків ОВТ. Перспективи подальшого розвитку даної тематики полягають в розробці та створенні автоматизованого пристрою, який по своїм технічним та метрологічним показникам зможе проводити метрологічне підтвердження манометра зразкового абсолютного тиску типу МПА-15.

Музика О.О., Бєляков В.Ф., Ринський І.М., Микитин В.Ф., Ніколаєва Л.Я.

ДО ПИТАННЯ ІНФОРМАЦІЙНО-МЕТОДИЧНОГО УЗГОДЖЕННЯ МОДЕЛЕЙ ВОЄННИХ ДІЙ, ДО ЯКИХ ЗАЛУЧАЮТЬСЯ СТРУКТУРИ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ ДЕРЖАВИ

Одним з основних інструментів логіко-аналітичної діяльності, що має значний інтелектуальний зміст і до певної міри адекватно відображає військову предметну область, є математичні моделі військових (спеціальних) дій різного масштабу. Багатократне моделювання за різними сценаріями бойових (спеціальних) дій дозволяє посадовим особам здійснювати порівняльну оцінку варіантів рішень і планів застосування сил і засобів та вибирати найбільш раціональний з них. Щоб забезпечити єдність системи управління військами (силами) по рівнях ієрархії і по підсистемах, математичні моделі військових (спеціальних) дій повинні відповідати вимозі інформаційно-методичної узгодженості. Так, при моделюванні в інтересах обґрунтування рішень і планування військових (спеціальних) дій в різних інстанціях його результати, незважаючи на їх відмінності по рівню узагальненості, мають бути погодженими в часі і просторі. Іншими словами, рішення вищої інстанції, яке обґрунтоване за допомогою моделювання і директивно передане в нижчу інстанцію, має бути підтверджене результатами подальшого детального моделювання в даній інстанції. Якщо на одному ієрархічному рівні управління планується застосування різнорідних (різновідомчих) сил та засобів, то результати моделю-

вання мають бути погоджені з «вихідними даними», які отримують при плануванні бойових (спеціальних) дій окремих родів військ (сил) або різновідомчих структур.

Виходячи із вищезазначеної вимоги інформаційно-методичної узгодженості моделей на різних рівнях ієрархії управління і видах модельованих процесів в загальному випадку доцільно об'єднати в три взаємозв'язані групи: перша – узгодженість оперативно-тактичної інформації, включаючи початкову інформацію для моделювання; друга – узгодженість застосованих математичних методів, розрахункових методик і алгоритмів; третя – узгодженість критеріїв і вихідних розрахункових показників моделей.

Зазначені вимоги входять в протиріччя з необхідністю відповідності ступеню деталізації опису модельованих процесів ієрархічному рівню органу управління, який застосовує певну модель. Особливо гостро це проявляється в органах управління вищої ланки і полягає в протиріччі між високим рівнем агрегації (узагальнення і укрупнення) оперативно-тактичної інформації та необхідністю адекватного відтворення в моделі бойових (спеціальних) дій з урахуванням усіх тактичних чинників, які істотно впливають на хід і результат бойових (спеціальних) дій.

Вирішення цього протиріччя може бути ґрунтуватися на методах агрегування і декомпозиції моделей. Завдання агрегування моделі в загальному вигляді полягає в наступному: маючи математичну модель процесу, потрібно отримати як деяку її похідну (точну або наближену), так звану агреговану модель, яка зв'язує не вихідні (початкові) змінні, а деякі їх функції або функціонали. Кількість цих величин повинна бути меншою, ніж початкових, а зв'язки між ними в якомусь сенсі простіші.

Вирішення проблеми узгодженості застосованих математичних методів, розрахункових методик і алгоритмів може ґрунтуватися на методах декомпозиції і агрегування опису процесу бойових (спеціальних) дій, зокрема на методі стратифікації, що припускає побудову загальної моделі у вигляді структурованої сукупності погоджених моделей процесів, що відрізняються один від одного рівнем абстрагування. Іншими словами, побудована на основі такого підходу модель повинна відтворювати процес бойових (спеціальних) дій за етапами у поєднанні з більш детальними методиками відтворення дій сторін одна на іншу з урахуванням усіх існуючих чинників.

Як варіант може бути розглянута трирівнева схема відтворення в моделі процесу бойових (спеціальних) дій.

На першому рівні моделюється управління елементами бойового порядку створеного угрупування і будується процес бойових дій в цілому, у вигляді послідовності етапів. Послідовність і умови початку етапів визначаються на цьому рівні на основі деталізованих початкових даних, а також результатів завершених попередніх етапів.

На другому рівні відтворюються етапи бойових (спеціальних) дій. Кожен з них представляється як послідовність дій сторін одна на одну з певним часовим інтервалом, що має назву крок моделювання. При цьому на основі відповідних нормативів моделюються: управління діями підрозділів, їх всебічного забезпечення, а також перевіряються умови завершення етапу в цілому або припинення певного дії (наприклад, при витраті вогневого ресурсу).

На третьому рівні відтворюються способи впливу сторін один на одного в межах кроку моделювання. Спосіб впливу тієї або іншої дії описується аналітичними залежностями, що враховують усі істотні тактичні чинники і забезпечують розрахунок найбільш вірогідних або усереднених результатів дії.

Важливим елементом даної узагальненої моделі є блок агрегування результатів моделювання бойових дій до рівня показників ефективності, що відповідають завданням, які вирішуються в штабах, зокрема міжвідомчих. Функціональний зміст цього блоку пов'язаний із забезпеченням узгодженості критеріїв і вихідних розрахункових показників моделей.

УДК 004.056

Мул Д.А., Прокопенко Є.В.

СИСТЕМА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНІЙ МЕРЕЖІ ДПСУ

В умовах постійної цифрової трансформації та зростання кількості кіберзлочинів система управління інцидентами інформаційної безпеки (ІБ) стає ключовою складовою для забезпечення безпеки та стабільності сучасних корпоративних інформаційно-комунікаційних систем (ІКС). Визначення моделі системи управління інцидентами в інформаційній безпеці (УІІБ) являє собою важливий етап в забезпеченні цілісності, конфіденційності та доступності даних, які циркулюють в корпоративній мережі Державної прикордонної служби України (ДПСУ).

Управління інцидентами інформаційної безпеки є важливим процесом, який забезпечує організацію можливістю своєчасного виявлення інциденту та якомога швидшого реагування на нього за допомогою коректно обраних засобів підтримки.

Поняття інциденту та події інформаційної безпеки визначено у міжнародному стандарті ISO/IEC TR 18044. Термін інцидент інформаційної безпеки (information security incident, ІІБ) трактується як одинична подія або ряд небажаних і непередбачених подій інформаційної безпеки, через які існує ймовірність компрометації службової інформації і загрози інформаційній безпеці. Подія інформаційної безпеки (information security event, ПІБ) розглядається як ідентифікований випадок стану системи або мережі, що вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідома ситуація, яка може бути істотною для безпеки.

Інциденти інформаційної безпеки є окремим підкласом кризових і надзвичайних ситуацій, що можуть відбутися в інформаційній інфраструктурі прикордонного відомства, і, як окремий випадок, в організаційно-технічних системах (ОТС) та інформаційно-комунікаційних мережах (ІКМ), впливаючи на стан корпоративних інформаційних ресурсів.

Система управління інцидентами ІБ - це комплексний набір процедур, інструментів та політик, спрямованих на виявлення, реагування та відновлення від інцидентів, що стосуються безпеки інформації. Головна мета такої системи - забезпечити безперебійну роботу інформаційних систем та захист від потенційних загроз.

Серед основних функцій системи управління інцидентами ІБ можна виділити наступні:

– виявлення інцидентів. Ця функція передбачає впровадження механізмів моніторингу та аналізу інформаційних потоків з метою виявлення підозрілих або аномальних активностей;

– аналіз інцидентів. Після виявлення інциденту має проводитись детальний аналіз, включаючи визначення його характеристик, потенційних наслідків та джерела загрози;

– реагування на інциденти. Ця функція повинна передбачати прийняття заходів для зупинення атаки, локалізації пошкоджень та запобігання подальшим загрозам;

– відновлення після інциденту. Після припинення загрози важливо відновити нормальну роботу інформаційно-комунікаційної системи та здійснити аналіз події з метою вдосконалення заходів безпеки.

Серед методів впровадження системи управління інцидентами ІБ в процес функціонування корпоративної мережі слід відзначити:

створення політик безпеки. Визначення правил та процедур, які регулюють виявлення, реагування та відновлення після інцидентів;

впровадження інформаційних технологій. Використання спеціалізованих програмних засобів для автоматизації процесів виявлення та аналізу інцидентів;

підготовка персоналу. Проведення тренінгів та навчання персоналу щодо процедур реагування на інциденти та використання інструментів безпеки.

Для опису процедури управління інцидентами безпеки може бути використана типова модель безперервного покращення процесів PDCA (плануй, Plan – виконуй, Do – перевіряй, Check – дій, Act), яка отримала назву від циклу Шухарта-Демінга.

Відповідно до стандарту ISO 27001 модель PDCA розглядається як основа функціонування всіх процесів системи управління інформаційною безпекою в корпоративній мережі. Ця модель об'єднує чотири взаємозв'язані процеси: розробка, впровадження, моніторинг і розвиток.

Система управління інцидентами інформаційної безпеки повинна будуватись відповідно до вимог циклу PDCA. Відповідно до цього, процес функціонування системи управління інцидентами інформаційної безпеки буде визначатись наступними етапами:

– планування і підготовка. На цій стадії здійснюється розробка схеми управління інцидентами, розробка і затвердження ряду організаційно-регламентуючих документів, виділення людських і матеріальних ресурсів, проведення необхідного навчання та апробація обраної схеми управління;

– експлуатація. На даному етапі здійснюється виявлення інциденту ІБ, ідентифікація інциденту ІБ, реагування, розслідування й аналіз;

– аналіз. На даному етапі здійснюється аналіз системи управління інцидентами інформаційної безпеки, виявляються ділянки щодо поліпшення та міри з поліпшення;

– покращення. На даному етапі реалізуються рекомендації, розроблені на етапі аналізу.

Недооцінка важливості вчасного реагування на загрози може призвести до серйозних наслідків, включаючи втрату конфіденційної інформації, порушення законодавства та збитки в грошовому виразі. Швидке та ефективне реагування дозволяє мінімізувати ризики та зберегти інформаційну безпеку.

Система управління інцидентами інформаційної безпеки відіграє критичну роль у забезпеченні безпеки та стабільності функціонування інформаційно-комунікаційної інфраструктури Державної прикордонної служби України (ДПСУ). Її впровадження та ефективна робота дозволяють вчасно виявляти, реагувати та відновлювати після інцидентів, забезпечуючи надійний захист інформації та оптимальне функціонування корпоративних інформаційних систем.

УДК 621.762:621.396.96

Невмержицький І.М., Цуприков Р.Ю., Романов С.О., Седлецький В.П.

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АДАПТИВНИХ АЛГОРИТМІВ ЗАХИСТУ РЛС РАДІОТЕХНІЧНИХ ВІЙСЬК ВІД АКТИВНИХ ШУМОВИХ ПЕРЕШКОД ЗА ДОПОМОГОЮ ВІЗУАЛЬНО-ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ В СЕРЕДОВИЩІ MATLAB/SIMULINK

Сьогодні неможливо уявити собі процес проєктування, дослідження та аналізу алгоритмів роботи складних технічних систем озброєння РТВ без використання обчислювальної техніки та сучасного математичного програмного забезпечення [1]. Особливої уваги серед інженерів і науковців займає програмне забезпечення MATLAB. Це високопродуктивна мова для технічних розрахунків, яка містить обчислення, візуалізацію і програмування в зручному середовищі, де завдання виражаються у формі, близькій до математичної [1].

Дослідження ефективності адаптивних алгоритмів захисту РЛС радіотехнічних військ від активних шумових перешкод проводилась з використанням раніше розроб-

леної в [1] візуально-імітаційної моделі, яка імітує алгоритми компенсації активних шумових перешкод з кореляційним зворотнім зв'язком та прямим розрахунком вагових коефіцієнтів. Візуально-імітаційна модель створена завдяки використанню пакета Simulink системи MATLAB. Цей засіб призначений для візуально-імітаційного моделювання та аналізу динамічних систем. Візуально-імітаційні моделі, які створені завдяки Simulink, найбільш повно реалізують класичну технологію імітаційного експерименту, включаючи його планування, проведення та обробку результатів. Детальний опис засобу Simulink наведено в [2].

При проведенні дослідження ефективності адаптивних алгоритмів захисту РЛС радіотехнічних військ від активних шумових перешкод, у якості критерія ефективності, було обрано кількість хибних перевищень порогу виявлення нескомпенсованими сигналами перешкоди на виході схем компенсації, за визначений період часу. Для проведення експерименту, щодо оцінки ефективності вказаних вище алгоритмів компенсації, на вхід Simulink-моделі подавалися імітовані значення активних шумових перешкод, власних шумів основного та додаткового каналів прийому та ехосигнали цілі. Тривалість дії активної шумової перешкоди імітувалась випадковим чином за певний визначений час моделювання.

Результати оцінки ефективності адаптивних алгоритмів захисту РЛС радіотехнічних військ від активних шумових перешкод подані за допомогою осцилограм пакета Simulink та графіків. Також надані рекомендації щодо використання створеної візуально-імітаційної Simulink-моделі в освітньому процесі вищого військового навчального закладу.

Список використаних джерел

1. Невмержицький І., Гризо А., Дідковський А. Проєктування візуально-імітаційного Simulink-додатка для моделювання адаптивних алгоритмів захисту радіолокаційних станцій радіотехнічних військ від активних шумових завад. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. Т. 46, № 1. С. 56–62. URL: https://doi.org/10.33099/2311-7249/2023-46-1-56-62 (дата звернення: 28.02.2024).

2. Dabney J. B., Harman T. L. Mastering Simulink. Prentice Hall, 2003. 464 p.

Нюкін М.В., Толстов О.С.

ІДЕНТИФІКАЦІЯ КОСМІЧНИХ АПАРАТІВ ПІД ЧАС ВИКОРИСТАННЯ ЛІНІЙНОЇ ТА КРУГЛОЇ АНТЕНИ

Для вирішення завдання ідентифікації космічних апаратів (КА) радіотехнічним комплексом (РТК) особливий інтерес викликає функціонування антенних облаштувань цих комплексів. При цьому антени з круглою апертурою, яка використовується в радіотехнічних системах при ідентифікації КА, мінімізується потужність бічного випромінювання при заданому дозволі двох точкових когерентних об'єктів за критерієм Спароу (КС). Рішення задачі мінімізації отримане у вигляді аналітичних формул. Серед оптимальних осесиметричних діаграм спрямованості (ДС) виявлені енергетично ефективні з максимальним пригніченням першої бічної пелюстки (БКЛ). Споріднені завдання раніше вивчалися в оптиці .

Також розглядається можливість виявлення, ідентифікації і контролю космічних апаратів по паразитного випромінювання і використання амплітудних розподілів для вирішення когерентних джерел постійно функціонуючих блоків бортової апаратури (БА) за допомогою наземних радіотехнічних комплексів.

В умовах розпаду системи контролю космічного простору колишнього СРСР і зростанням кількості зарубіжних орбітальних угруповань космічних апаратів (КА) для

України стає актуальним завдання створення системи ідентифікації КА, що знаходяться в зоні видимості національних засобів.

Для створення бортових комплексів ідентифікації потрібно порівняно великі технічко-економічні витрати, зумовлені перш за все необхідністю виведення декількох десятків КА різного орбітального побудови. Тому дані комплекси можуть залучатися лише для вирішення вкрай обмеженого обсягу завдань.

Перевагою лазерних і оптичних комплексів є забезпечення великої дальності дії, високої роздільної здатності та точності вимірювання координат зі скритністю в роботі і практичній несхильності різного виду організованих перешкод. У той же час залежність від метеоумов роботи і часу доби не дозволяє забезпечувати постійний контроль космічного простору і ідентифікувати КА.

Існуючі національні спеціалізовані комплекси противокосмічної оборони забезпечують порівняно низьку скритність і оперативність обробки отриманої інформації, обслуговують фіксовані зони території держави, що призводить до появи "дірок" в поле контролю. При цьому ці комплекси дорогі у виготовленні і експлуатації.

Активні і пасивні радіолокаційні комплекси обмежено застосовні до завдань ідентифікації КА. Ці комплекси можуть бути застосовані тільки для виявлення космічних об'єктів.

Ідентифікація активних КА, тобто КА з працюючими передавальними пристроями під час прольоту в зоні радіовидимості національних радіотехнічних комплексів (РТК), не є складним завданням. Однак, для більшості космічних систем оборонного призначення особливою характеристикою їх функціонування є скритність. Що насамперед обумовлює відключення бортових передавальних пристроїв КА поза зоною радіовидимості своїх РТК. Ця обставина значно ускладнює ідентифікацію цих КА над територією інших держав. Розглядається можливість застосування лінійних антен для ідентифікації космічних апаратів. Отримані аналітичні вирази для діаграми спрямованості і амплітудного розподілу, що реалізовують мінімум потужності бічних пелюсток.

УДК 004.715

Оленченко В.Т.

СИМУЛЯТОРИ ТА ЕМУЛЯТОРИ У ПРОЦЕСІ ПІДГОТОВКИ ФАХІВЦІВ ЗВ’ЯЗКУ

Досвід наших партнерів з НАТО щодо використання емуляторів і віртуалізації проведення занять у системі підготовки фахівців у вищих військових навчальних закладах особливо яскраво відображений у доповіді Британського цивільного співробітника НАТО пана Пола Туркетла на 5-й Міжнародній науково-практичній конференції 2022 року “Проблеми впровадження дистанційного навчання в освітньому процесі вищих військових навчальних закладів та можливі шляхи їх вирішення”. Продемонстровано тренажери від компанії SATCOM, які дозволили віртуалізувати процеси підготовки фахівців різних напрямків – зв’язківців, спецназівців.

Кафедрою військового зв’язку та інформатизації використовуються різноманітні емулятори для отримання базових знань і початкових навичок налаштування мережевого обладнання електронних комунікаційних мереж, розрахунку і перевірки роботи електрообладнання, розрахунку радіоліній, підготовки радіотелеграфістів, підготовки файлів прошивки і програмування КХ та УКХ радіостанцій. Отримані знання і навички потім успішно реалізуються на практичних заняттях як у аудиторіях, так і під час проведення польових занять.

Яскравим прикладом симулятора для отримання навичок щодо проектування та адміністрування електронних комунікаційних мереж є додаток Cisco Packet Tracer. Він дозволяє будувати мережі з різноманітними фізичними топологіями, отримати уяву як щодо фізичних характеристик використовуваного обладнання, так і його фактичного розміщення у будівлях, кімнатах, стійках. У режимі моделювання можна візуалізувати процес обміну пакетами між пристроями у створеній мережі та дослідити використовувані протоколи і рівні моделі OSI, на яких вони реалізуються. Рижим Multiuser дозволяє здійснювати дослідження мережі (працювати над одним проектом) користувачам, що працюють на комп'ютерах розміщених як в локальній, так і віддалених мережах. Вбудовані засоби Activity Wizard, дозволяють створювати різні навчальні сценарії (проекти) мереж з метою подальшого конфігурування, виконання визначених викладачем завдань, а також автоматичне оцінювання виконаної роботи.

Можна створити необхідну мережу, виконати відповідне налаштування обладнання, протестувати мережу на працездатність, а потім зберегти файли конфігурацій обладнання і втілити їх в реальне обладнання. Це дозволяє уникнути істотних проблем при створенні локальної обчислювальної мережі організації.

Разом з тим, однією з вад симулятора Cisco Packet Tracer є те, що він працює лише з обладнанням одного вендора – Cisco.

Варіантом рішення цієї проблеми є емулятор EVE-NG (Emulated Virtual Environment - Next Generation) - емульоване віртуальне середовище наступного покоління. Він дозволяє створити мережі з обладнанням і програмним забезпеченням від провідних світових вендорів, що дозволяє отримати навички роботи з цим обладнання у здобувачів освіти. Крім того, що емулятор має вже готові образи певного обладнання існує можливість додавання інших образів пристроїв.

Ще одним рішенням є симулятор GNS3 (Graphical Network Simulator 3) – графічний мережевий симулятор, що дозволяє здійснювати конфігурацію і дослідження мережевих систем з різними пристроями на різних операційних системах. Однак цей симулятор висуває суттєві вимоги до розміру оперативної пам'яті і потужності процесора.

Підсумовуючи викладене: функціонування електронних комунікаційних мереж вимагає від персоналу, що здійснює їх обслуговування та експлуатацію, чіткої орієнтації у програмному забезпеченні та функціоналі мережевого обладнання різних вендорів. Отримати досвід (навички) роботи з таким обладнанням дозволяють чисельні симулятори та емулятори.

Олійник С.Е., Опалинський В.Б.

ЗАХИСТ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА

Глобальна інформатизація сьогодні активно впливає на існування і життєдіяльність держав світової спільноти, інформаційні технології застосовуються у вирішенні завдань забезпечення національної, військової, економічної безпеки тощо. Разом із тим одним із фундаментальних наслідків глобальної інформатизації державних і військових структур стало виникнення принципово нового середовища протиборства конкуруючих держав – кіберпростору, яке не є географічним у загальноприйнятому сенсі цього слова, але, тим не менш, у повній мірі є міжнародним. І якщо сьогодні між провідними у військовому та економічному відношенні світовими державами склався в тій чи іншій мірі певний паритет у галузі застосування звичайних озброєнь і зброї масового ураження, а в міжнародному праві зафіксовані основні принципи взаємовідносин цих держав у межах таких просторів, як наземне, морське, повітряне, космічне, то питання про міждержавний паритет і взаємини в кіберпросторі натепер продовжують залишатися відкритим.

Кібервпливи все частіше стають ефективним інструментом для досягнення мети щодо несилового контролю та управління, як об’єктами з критичною інформаційною інфраструктурою держави, що може піддатися такому впливу, так і окремо взятими громадянами, їх об’єднаннями. Вони відкривають можливості досягнення політичних цілей, змін легітимних урядів, а також здійснення деструктивних змін в усіх сферах життєдіяльності суспільства і держави (економічній, енергетичній, духовній тощо), взяття під контроль і навіть поневолення цілих народів і країн практично без застосування військової сили в класичному її розумінні.

Істотно підвищився рівень інформаційного негативного впливу на процеси збереження та розповсюдження інформації, зросла чисельність нових загроз інформаційній безпеці, таких як нові форми кібератак. Особливо це проявилося з початком активної фази вторгнення в Україну військ російської федерації 24 лютого 2022 року, яка намагалася шляхом проведення кібератак на державні структури управління, силові відомства та пдприємства критичної інфраструктури.

Одним із пріоритетних напрямів забезпечення національної безпеки є інформаційна безпека, оскільки сьогодні важливим стратегічним пріоритетом України є розвиток інформаційного суспільства та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільства.

Оскільки в комп’ютерних системах зберігаються і обробляються великі обсяги облікової інформації, будь-який збій може привести до надмірних витрат, недостатніх доходів, втрати активів, санкцій, унеможливення керування зброєю тощо. Тому головним пріоритетом захисту облікової інформації є розроблення заходів, спрямованих на збереження інформації, що міститься у комп’ютерних базах.

Кібербезпека включає в себе захист інформації, але не обмежується лише нею. Це захист від вірусів, хакерських атак, підробки даних, які можуть не тільки видалити або вкрасти дані, але і вплинути на роботу і продуктивність співробітників, використовувати інформацію проти людини або структури, а також зупинити виробництво.

Кібербезпека – це вже новий виток інформаційної безпеки, який спрямований саме на діджитал середовище. В якій власне ми і знаходимося з вами. Кібербезпека має на увазі не тільки сам по собі захист інформації, а й захист всієї системи в інформаційному полі, в ІТ-полі (поле комп’ютерних технологій) в цілому.

Важливим елементом забезпечення цілісності конфіденційної інформації є захист від несанкціонованого доступу до ресурсів інформаційних систем, що викликає необхідність створення надійних і зручних систем контролю доступу. Ці процедури виконуються кожний раз, коли користувач вводить пароль для доступу до інформаційної системи, мережі, бази даних або при запуску прикладної програми. В результаті їх виконання користувач або отримує доступ до певних ресурсів інформаційної системи, або не отримує.

Ідентифікація – процедура розпізнавання користувача в системі за допомогою наперед визначеного імені (ідентифікатора) або іншої інформації про нього, яка сприймається системою. Вона є початковою процедурою надання доступу до системи, після неї здійснюється автентифікація та авторизація.

Автентифікація – це процедура перевірки належності ідентифікатора об'єкту, тобто встановлення чи підтвердження дійсності, і перевірка чи є об'єкт або суб'єкт, що перевіряється, справді тим, за кого він себе видає.

В інформаційних технологіях використовуються такі види автентифікації: –однобічна автентифікація, коли клієнт системи для доступу до інформації доводить свою автентичність; –двобічна – коли, крім клієнта, свою автентичність повинна підтверджувати і система; –трибічна – коли використовується, так звана, нотаріальна служба автентифікації для підтвердження достовірності кожного з партнерів при обміні інформацією. Методи автентифікації умовно можна поділити на однофакторні (слабкі, з точки зору безпеки) та багатофакторні (сильні).

Коли захист інформації стосується забезпечення безпеки інформаційних баз даних, а також різних програм, що входять у комп'ютерні мережі, виникає необхідність визначити співвідношення між захистом інформації та кібербезпекою. Сутність кібербезпеки означає наступальні дії, тобто кібербезпека відрізняється від традиційної інформаційної безпеки тим, що вона включає застосування практичних дій і засобів для атаки супротивників. Під час розмежування понять «кібербезпека» та «захист інформації» загрози кібербезпеці визначаються в уразливості об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, а також у фізичній і моральній застарілості системи охорони державної таємниці та інших видів інформації з обмеженим доступом. На відміну від інформаційної безпеки мова йде не про інформацію взагалі, а про ту інформацію, яка циркулює в кіберпросторі і становить важливу частину її змісту. Зрозуміло, що втрата інформації, яка зберігається в окремому комп'ютері і є важливою для користувача цього комп'ютера, не може розглядатися як загроза кібербезпеці. Привабливою може бути інформація з обмеженим доступом, управлінського обліку, яка містить комерційну таємницю.

Кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача. Відповідно кібербезпека – це стан системи, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах.

Кіберзлочинність постійно вдосконалюється і йде в ногу з технологіями. Це ускладнює виявлення та протидію зазначеним протиправним діям. Тому варто усвідомити, що проблема кібербезпеки – це проблема не лише загально-державного рівня, а кожного окремо взятого користувача. Очевидно, що об'єктом зацікавленості злочинців була і завжди буде інформація, витоки якої здійснюють під час використання соціальних мереж через такі канали, як персональні комп'ютери, ноутбуки, смартфони, тому користувачавам необхідно прописувати правила користування цією інформацією і стежити за безумовним їх виконанням, особливо в умовах воєнного стану.

Кібербезпека захищає обладнання та програми підприємств і держструктур від хакерських атак**.** Її завдання – не допустити витоку даних. Подібні загрози – це сценарій не лише для установ. Під прицілом може опинитися ваш комп'ютер або вебсайт. Потреба в особистій кібербезпеці буде все зростати, тому що чим далі, тим більше ми "зростаємось" з нашими гаджетами. Кібербезпека відповідає за захист конфіденційної інформації та взаємодію з нею при користуванні будь-яким пристроєм. Люди настільки інтегровані з телефоном і комп'ютером, що навіть не усвідомлюють цього. Коли ми забуваємо десь стільниковий телефон, то здається, ніби втратили «частину тіла». І так воно і є. Ми вже повністю пов'язані з нашими телефонами, без яких ми нікуди не можемо вийти і не мислимо життя без них. Наш телефон – це погода, переміщення, карти, розпорядок роботи, планування особистих заходів дня, їжа, сон, стан здоров'я. Цей список можна доповнювати ще безліччю можливостей, з якими ми живемо день у день. Це поняття з'явилося в еру інформаційних технологій.

Існує два основні підходи до захисту від загроз, що виходять із глобального інформаційного простору – кібербезпека та інформаційна безпека. Ці підходи не є взаємовиключними. Проте вони відображають соціально-культурні, економічні та політичні особливості держав і спрямовані на реалізацію відповідних національних інтересів. Інформаційна безпека ширше кібербезпеки і крім питань, пов'язаних з технічним забезпеченням безпеки інфраструктури та безпеки інформації, розглядає проблеми захисту особистості й суспільства від деструктивного інформаційного впливу.

Особливої уваги заслуговують системи протидії кіберзлочинам на рівні окремих держав. Наприклад, у США поряд з уже функціонуючим Центром національної кібербезпеки (National Cyber Security Center) у складі Збройних сил сформовано Об'єднане

кібернетичне командування (Unified US Cyber Command), яке в глобальному масштабі має координувати зусилля всіх структур Пентагону в ході ведення бойових дій, надавати відповідну підтримку цивільним федеральним установам, а також взаємодіяти з аналогічними за завданнями відомствами інших країн. У Великобританії реалізуються програми зі створення кіберзброї, які забезпечать здатність влади протистояти зростаючим загрозам з кіберпростору. В Австралії створено групу координації безпеки електронної пошти (ESCG). Основним завданням цієї групи є створення безпечного і надійного електронного оперативного простору як для суспільного, так і для приватного секторів

Підводячи підсумки, можно сказати, що кібербезпека була частиною інформаційної безпеки. Зараз же – це еволюція інформаційної безпеки. Зараз саме від захисту процесів, інформації та діяльності в кіберпросторі залежить дуже багато ніж просто втрата інформації.

У числі рекомендацій для політики України у сфері забезпечення інформаційної безпеки та кібербезпеки на національному та міжнародному рівні необхідно продовжити і розширити діяльність зі створення умов для формування системи міжнародної інформаційної безпеки на основі загальновизнаних принципів і норм міжнародного права. Важливо розвивати співробітництво в цій сфері і створити необхідні умови для дотримання режиму експертного контролю та налагодження каналів формального та неформального обміну інформацією стосовно загроз комп'ютерної злочинності та кібертероризму з країнами – партнерами України..

Таким чином, серед можливих шляхів підвищення ефективності заходів кібернетичного захисту в умовах воєнного стану можуть бути:

- налагодження ефективної системи кіберзахисту об'єктів;
- підвищення ефективності інформаційно-аналітичної роботи суб'єктів інформаційної безпеки;
- створення та постійне оновлення бази кіберзлочинців;
- створення системи раннього виявлення інформаційних небезпек.

УДК 004.42

Олійник О.В., Широкопетлєва М.С.

ДЕЦЕНТРАЛІЗОВАНА СИСТЕМА ГОЛОСУВАНЬ ТА ОПИТУВАНЬ "YOUR VOTE" ДЛЯ ЗБОРУ СОЦІОЛОГІЧНИХ ДАНИХ

В сучасному світі, де технологічні інновації революціонізують кожен аспект нашого життя, виникає необхідність перегляду традиційних підходів до прийняття суспільночутливих рішень та управління великими державними або комерційними структурами. Децентралізовані системи голосувань та опитувань, які засновані на технології Blockchain, набувають великого значення як ефективний інструмент для забезпечення прозорості, відкритості та легітимності в процесах прийняття рішень. У цьому контексті, робота присвячена вивченню можливостей використання децентралізованої системи голосувань та опитувань як інноваційного механізму для збору даних та формування об'єктивної картини щодо настроїв та думок у суспільстві та колективі, а також для оптимізації взаємодії між громадянами та державними органами. В даній роботі розглядаються ключові аспекти цього підходу та визначаються перспективи впровадження відокремлених систем голосувань та опитувань у сучасних демократичних процесах та механізмах управління. У роботах [1–3] досліджено можливості використання технології Blockchain для створення розподілених додатків (DApps) та гібридних додатків (ви-

користовують блокчейн з централізованими базами даних), для проведення голосувань.

На підставі проведеного аналізу виникає необхідність створення розподіленого застосунку для проведення різного роду голосувань та опитувань з використанням технолгії блокчейн.

Децентралізовані застосунки, часто відомі як DApps (Decentralized Applications), представляють собою програми, які операційно працюють на децентралізованих мережах, таких як блокчейн. Ці застосунки використовують технології блокчейну для забезпечення розподіленого зберігання та обробки даних, уникнення централізованого управління. Також вони часто використовують смарт-контракти що сприяє автоматизації процесів та уникненню посередництва. Важливим аспектом є відкритий код, який дозволяє розробникам перевіряти безпеку та функціональність застосунків, а також вносити свої внески в розвиток платформи.

Блокчейн це розподілений реєстр (distributed ledger) зі зростаючими списками записів (блоків), які надійно пов'язані разом за допомогою криптографічних хешів [4]. Кожен блок містить набір транзакцій і хеш-код попереднього блоку, створюючи послідовний ланцюг. Розподілені копії блокчейну зберігаються на вузлах мережі, що гарантує децентралізованість та надійність системи. Принцип роботи блокчейну базується на концепції консенсусу. Коли учасники мережі вносять нову транзакцію, вона перевіряється і групується в новий блок. Після цього мережа використовує алгоритм консенсусу, наприклад, Ethereum використовує алгоритм Proof-of-Stake для прийняття рішення про те який блок додається до ланцюга. Кожен блок унікально ідентифікується своїм хеш-кодом, який враховує вміст блоку і хеш попереднього блоку. Це робить маніпулювання історією транзакцій вкрай складним, оскільки будь-яка зміна в одному блоку вимагає змін у всіх наступних блоках. Цей підхід робить блокчейн прийнятним для створення децентралізованих систем, таких як системи електронного голосування та опитувань.

Смарт-контракт – це програмний код, що розміщено на блокчейні, який виконується за визначеними умовами автоматично та забезпечує безпеку та невідмінність даних [5]. Ця технологія дозволяє безпосередньо взаємодіяти між сторонами угоди з використанням автоматизації та спрощення процесу виконання угод, що дозволяє їх використати в системах проведення голосувань та опитувань.

DApp-система проведення голосувань та опитувань «Your Vote», представлена в даній роботі, забезпечує прозорість голосування та неможливість підробки результатів. Ця система складається з декількох компонентів, а саме веб-частини, розробленої за допомогою JavaScript-фреймворку React; Mobile-частини, розробленої за допомогою React Native. Для розробки серверної частини було обрано ASP.NET Core та бібліотеку Nethereum для використання можливостей Web 3.0 та безпосередньо Ethereum. Для уточнення потрібно зазначити, що запропонована система не є повністю децентралізованою, а гібридною, що поєднує використання блокчейну з використанням централізованого сховища. Блокчейн використовується саме для зберігання інформації про вибір кожного учасника та про саме голосування, але для зберігання інформації про користувачів системи використовується класична централізована база даних. Обраною базою даних є SQL Server, управління якою буде реалізовано за допомогою SQL Server Management Studio 19. В програмах-клієнтах для запровадження функціоналу локалізації використовується бібліотека i18n. В централізованому сховищі зберігається інформація про профіль користувача та про його персональні налаштування в системі. Для забезпечення конфіденційності даних використовується захищене з'єднання SSL/TLS з SQL Server. Усі паролі при створенні хешуються, та зберігаються в сховищі тільки у виді хеш-значень. На діаграмі компонентів стисло показано архітектуру системи (рис 1).

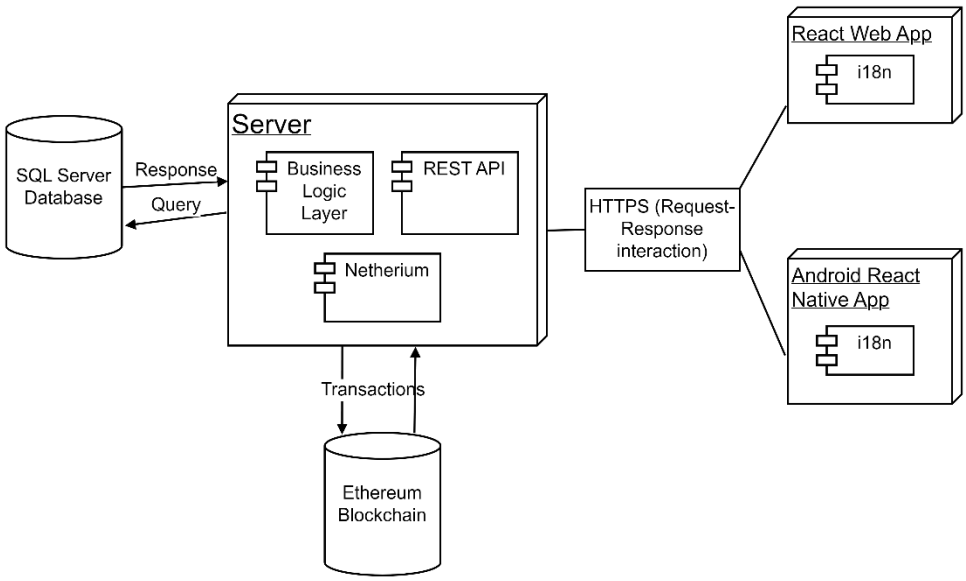


Рисунок 1 – Діаграма компонентів додатку

Впровадження даної системи значним чином ускладнить підробку голосів громадян та фальсифікацію голосувань та опитувань. За допомогою впровадження системи біометричної ідентифікації можна майже повністю вирішити проблему ідентифікації громадянина. Це допоможе в критичні моменти доволі чітко та прозоро уникати підробок голосувань та об'єктивно визначати переважні інтереси громадян при різного роду соціологічних опитуваннях та голосуваннях. Окрім цього, функціонал системи може бути розширено значним чином, визначаючи коло людей, що голосує, а також визначаючи, чи є голосування таємним або відкритим. Наприклад, при прийнятті рішень можна запровадити відкрите голосування та зафіксувати рішення з визначених питань. Система ідентифікації забезпечить неможливість голосування кожної особи більше ніж дозволено. Таким чином, використання запропонованої системи голосувань створить не лише ефективний інструмент для попередження шахрайства та забезпечення прозорості опитувань, але й сприятиме активній участі громадян у формуванні ключових рішень для розвитку держави та ще більш буде заохочувати людей цікавитись суспільними проблемами і наблизить наше суспільство до стандартів прямої демократії.

Список використаних джерел

1. Shukla A., Mishra D.P., Pattnaik A., Salkuti S.R. Analysis and design on acceptance of blockchain based e-voting system. *Indonesian Journal of Electrical Engineering and Computer Science*. 2024. Vol.33. No.3. P.1793-1801. DOI:https://doi.org/10.11591/ijeecs.v33.i3.pp1793-1801. (дата звернення: 03.02.2024).

2. Vikkurty S., Hegde N.P., Kumar S.V., Punna S.T., Poluri H. E-Voting Using Block Chain Technology and OTP Generation. *Lecture Notes in Electrical Engineering*. 2024. P.481-487. DOI:https://doi.org/10.1007/978-981-99-7137-4_47. (дата звернення: 03.02.2024).

3. Patil P.R., Rout D., Mohite S.S. A Survey of Decentralized Digital Voting System Using Blockchain Technology. *Lecture Notes in Networks and Systems.* 2024. P.27-44. DOI:https://doi.org/10.1007/978-981-99-7817-5_3. (дата звернення: 03.02.2024).

4. Zheng Z., Xie S., Dai H., Chen X., Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017.* 2017. P.557-564. DOI:https://doi.org/10.1109/BigDataCongress.2017.85. (дата звернення: 03.02.2024).

5. Christidis K., Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*. 2016. Vol.4. P.2292-2303. DOI:https://doi.org/10.1109/ACCESS.2016.2566339. (дата звернення: 03.02.2024).

Опалинський В.Б., Олійник С.Е.

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА

Ми живемо в епоху інформаційного суспільства, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини та держави. Сьогодні ми все більше й більше використовуємо їх у своїй діяльності. Не є винятком і сили охорони правопорядку. Рада національної безпеки і оборони визнає важливість кіберпростору та його вразливість до зовнішнього впливу. Вона підкреслює особливе значення кібербезпеки для військової і цивільної сфери, де використання сучасних інформаційних технологій суттєво зросло внаслідок війни з російською федерацією. Також існує точка зору, що об'єкти критичної інфраструктури (КІ) можуть бути цілями кібертероризму і часто стають об'єктом кібератак та кіберзлочинів.

Вразливість інформаційної та кібербезпеки – одна з основних проблем, яка сьогодні викликає занепокоєння. На об'єктах КІ, до яких відносяться автоматизовані системи управління підготовки та діяльності ЗС України і правоохоронних органів, такі вразливості перетворюються на кіберзагрози через: неадекватність електронно-комунікаційної інфраструктури, її розвитку та захисту у порівнянні з сучасними вимогами; недостатній та непослідовний захист КІ; розвиток організаційно-технічної інфраструктури, який недостатній для забезпечення кібербезпеки та кіберзахисту КІ, а також державних електронно-інформаційних ресурсів; недостатня спроможність суб'єктів сектору безпеки та оборони протидіяти кіберзагрозам кримінального, терористичного та воєнного характеру; брак координації, співробітництва та обміну інформацією між агенціями з кібербезпеки.

Стратегія інформаційної та кібербезпеки України визначає основні пріоритети щодо розвиту технології захисту інформації та кібербезпеки, а саме: розробка безпечного, стійкого та надійного кіберпростору; безпека урядових інформаційних ресурсів; безпека КІ; розбудова кібербезпекових спроможностей в оборонному секторі; боротьба з кіберзлочинами. Саме тому стратегічним завданням державної політики має стати формування комплексної системи інформаційної і кібернетичної безпеки, в основу якої покладено науково обґрунтовані політичні, соціальні й економічні критерії та світовий досвід щодо правових і організаційних аспектів функціонування. Для досягнення вище зазначених пріоритетів в доповіді автором пропонується визначити три головні ризики, для стратегічних цілей України, які мають бути подолані:

– виклики щодо вироблення операційної стійкості, достатньої для протидії постійним кіберзагрозам, у тому числі пов'язаним з російською агресією;

– бюджетні рамки, що обмежують здатність уряду платити конкурентоспроможні зарплати для залучення та утримання потрібних фахівців з питань кібербезпеки;

– структура політики та управління, що потребує більшої координації всередині уряду для вироблення узгоджених зі стратегічними пріоритетами підходів, що ґрунтуються на консенсусному управлінні ризиками і ресурсному забезпеченні, для вироблення стратегічної та операційної стійкості.

Усе вище викладене, як і щоденна життєва практика, переконливо доводить: забезпечення інформаційної і кібернетичної безпеки – процес безперервний, надзвичайно складний і багатогранний, причому успіх у його реалізації надасть можливість забезпечити належний стан інформаційної та кібербезпеки

автоматизованих систем в ході підготовки та діяльності ЗС України і правоохоронних органів.

УДК 004.942.001.57: 681.513.66

Орлов В.В., Наумов О.І.

ЗАСОБИ ЗВУКОМЕТРИЧНОЇ РОЗВІДКИ У СКЛАДІ БОРТОВИХ СИСТЕМ БЕЗПІЛОТНОГО ТРАНСПОРТУ

Ефективність висвітлення бойової обстановки за допомогою радіолокаційних та оптичних засобів, що розміщуються на транспортних засобах військової розвідки, суттєво ускладнена в умовах застосування противником засобів радіоелектронної боротьби, димових та аерозольних завіс.

Мобільна система звукової локації може бути встановлена на безпілотних транспортних засобах (наземних або повітряних) та призначена для доповнення можливостей існуючих засобів розвідки підчас виконання завдань щодо виявлення, розпізнавання й визначення координат позицій вогневих засобів противника: пострілів снайперів и артилерії; гусеничної и колісної наземної техніки; аеродинамічних об'єктів: літаків, гелікоптерів, БпЛА [1,2]. Звукова розвідка проводиться по всій смузі оборони (охорони) механізованого батальйону на глибину від 1 до 3 км при інтенсивному веденні вогню в масштабі реального часу.

Звуколокаційна система складається з 8 датчиків, що просторово рознесені на борту транспортного засобу, бортового комп'ютера, дисплея, блока сполучення між датчиками та бортовим комп'ютером, з'єднувальних кабелів. Блок сполучення між решіткою датчиків та бортовим комп'ютером має 8 входів для підключення датчиків, вхід живлення постійного струму від бортової мережі і USB-вихід для підключення до бортового комп'ютера. Дисплей відображає обстановку в горизонтальній площині (режим екрану РЛС кругового огляду), в вертикальній площині (режим екрану висотоміра РЛС) із застосуванням позначок для класів розпізнаних цілей.

Основним вузлом системи є спеціалізоване програмне рішення, котре здійснює цифрову фільтрацію сигналів, що надходять з акустичних датчиків, нівелює вітрові звукові завади та обробляє тільки інформацію, що стосується коротких сигналів от пострілів та безперервних сигналів від транспорту, що рухається [3]. Після обчислення параметрів акустичної хвилі проводяться розрахунки координат та розпізнавання калібру пострілу і класів транспорту.

Проведені дослідження показали, що сучасні методи цифрової обробки сигналів із застосуванням елементів штучного інтелекту забезпечує наступні тактичні характеристики.

Звуколокаційна система має функцію розпізнавання об'єктів:

– калібр зброї, що розпізнається – від 5,45 до 14,5 мм; артилерії, мінометів і ракет; гусеничного и колісного транспорту; літаків, гелікоптерів и БпЛА;

– сектор ведення розвідки – 360°;

– кількість цілей, що визначаються одночасно – до 10;

– час визначення цілі – не більше 2 с;

– максимальна дальність розпізнання та визначення координат вогневих позицій стрілецької зброї: калібру 5,45-7,62 мм – до 600 м; калібру 12,7-14,5 мм – до 1500 м;

– похибка визначення координат вогневих позицій по дальності на дистанціях до 600 м – не більше 5%, на дистанціях до 1500 м – не більше 10%.

Звуки стрілецької зброї при слабких завадах або їхньої відсутності можуть бути виявлені на відстані більше 8 км, а при сильних шумах за рахунок вітру або дощу визначаються на відстані від 6 до 7 км, а при поганих метеоумовах дальність може знижуватися до 3 км.

Постріли артилерії визначаються на відстані від 10 до 15 км, а при поганих метеоумовах дальність може знижуватися до 5 км.

Повітряні об'єкти: літаки, гелікоптери и БпЛА, навіть ті, що летять на малих висотах до 50 м, можуть визначатися на відстані більше 8 км. Під час завад вітру, низькій температурі й вологості дальність зменшується до 5 км. При значних завадах вітру, дощу й граді дальність може істотно знижуватися до 1 км.

Малорозмірні БпЛА з електродвигуном і вагою 0,5 кг виявляються на дистанції до 700 метрів, а вагою 2,5 кг – до 3000 метрів. У нічний час доби дальність вірогідної локації збільшується в кілька разів.

Об'єкти наземної техніки при відсутності завад можуть визначатися на відстані від 4 до 6 км, при сильному вітрі і дощу – на відстані менее 0,5 км.

Точність визначення координат за азимутом напряму залежить від конфігурації розташування датчиків на борту транспортного засобу, а також від максимальної відстані між датчиками. Акустичні датчики можуть розташовуватись в одній з трьох конфігурацій: компактного встановлення на телескопічній вежі; розподілення по бортах транспортного засобу; розташування по землі на стаціонарній позиції.

Помилка по азимуту не перевищує:

– 10°, за умов компактного розташування на борту транспортного засобу із відстанню між мікрофонами 0,5 м;

– 2°, за умов розподіленого розташування по кутах периметру транспортного засобу із відстанню між мікрофонами до 4 м;

– 0,1°, за умов розподіленого розташування на землі на стаціонарній позиції із відстанню між 4 парами датчиків до 50 м.

Такої точності достатньо для подальшого супроводу цілей засобами відеомоніторингу.

Подальше збільшення точності визначення координат може забезпечуватися за рахунок комплексування даних від декількох транспортних засобів, що розташовані в зоні чутності. Далі, за командою оператора, спостерігачам передаються координати розпізнаної цілі для супроводу оптичними засобами спостереження та застосування засобів протидії.

Система може бути використана в якості підсистеми в загальній схемі розвідки механізованого батальйону для формування єдиного інформаційного поля в зоні відповідальності. Це забезпечить єдине розуміння бойової обстановки на усіх рівнях управління механізованого батальйону та умови для прийняття обґрунтованих рішень по вогневому ураженню противника.

Список використаних джерел

1. Артилерійська звукова розвідка: Підручник / О.Красюк, Р. Сергієнко, С. Сокольский та ін. – Львів: НАСВ, 2020. – 346 с.

2. Adrien Dagallier, Sylvain Cheinet, Matthias Cosnefroy, Winfried Rickert, Thomas Weßling, Pierre Wey, and Daniel Juvé. Long-range acoustic localization of artillery shots using distributed synchronous acoustic sensors. *The Journal of the Acoustical Society of America*. 2019. № 6. P. 4860-4872. DOI: 10.1121/1.5138927.

3. K. Liu and G. Mattyus. Fast multiclass vehicle detection on aerial images. *Geoscience and Remote Sensing Letters, IEEE*. 2015. P(99):1–5. DOI: 10.1109/LGRS.2015.2439517

УДК 623.4.017

Очередько В.О., Худов Г.В.

АНАЛІЗ ДОСВІДУ ЗАСТОСУВАННЯ БПЛА ТИПУ «SHAHED» В РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ

Починаючи з початку вересня 2022 року, підрозділи Сил оборони України стикнулися з фактами ураження бойової та іншої техніки невідомими боєприпасами. Водночас кількома тижнями раніше з'явилась інформація, що армія російської федерації (рф) отримала іранські безпілотні літальні апарати (БпЛА) "Shahed" та почала активно застосовувати їх у війні проти України. Повідомляється про неодноразові випадки ураження озброєння та військової техніки з характерними ознаками застосування дронів типу камікадзе. Через невеликий розмір та відносно високу швидкість апарати доволі складно виявити і збити. 13 вересня 2022 року України вперше вдалося знищити іранський БпЛА "Shahed" поблизу Куп'янська на Харківщині. Нанесене на них маркування свідчить, що армія рф, видає їх за ударні БпЛА власної розробки типу "Герань" та використовує їх під цією назвою.

Для ураження цілей противник застосовував "Shahed" переважно парами з різницею у декілька секунд. При цьому пріоритет надавався одиночним об'єктам (танки, бойові броньовані машини, артилерійські системи, автомобілі). Ураження розвіданих раніше цілей відбувалось з практично 100-відсотковою ймовірністю. Для здійснення інформаційно-психологічного тиску на військовослужбовців ЗС України противник також активно поширює у мережі "Інтернет" відеозаписи успішного знищення озброєння, військової техніки та особового складу. Перш ніж вирішувати, як краще і дешевше знищити БпЛА, його треба спочатку виявити і ідентифікувати. Як і всякий матеріальний об'єкт, БпЛА несе в собі демаскуючі ознаки, які видають його в навколишньому просторі, роблячи помітним для спостереження. Ступінь помітності визначається величиною його сигнатур в радіочастотному, інфрачервоному і видимому діапазонах, а також сигнатури акустичної. Сучасні легкі безпілотники мають сигнатури невеликої величини: БпЛА роблять з композитних матеріалів, пластика зі спеціальним фарбуванням і з особливою комбінацією шарів, їх невеликі бензинові і тим більше електричні двигуни мало випромінюють тепла і працюють майже безшумно. БпЛА типу камікадзе "Shahed" призначений для ураження наземних нерухомих об'єктів шляхом наведення та контактного підриву бойової частини БпЛА. Виробник – "Shahed Aviation Industries Research Center". Для запуску "Shahed" використовується наземна платформа.

Велика дальність польоту дронів-камікадзе "Shahed" дозволяє його застосовувати для ураження нерухомих цілей у глибині території України, а також можливість здійснення підготовки до пуску у польових умовах за рахунок завантаження польотного завдання за допомогою портативного комп'ютеру (ноутбук, планшет).

З проведеного аналізу часу застосування дронів-камікадзе "Shahed" зс рф встановлено, що з початку збройної агресії зазначені БпЛА застосовувались впродовж доби, але найбільш часто та найбільш ефективним є їх застосування в темну пору доби у період з 23:00 по 06:00 з метою ускладнення візуального їх виявлення, визначення їх кількості та зниження ефективності застосування засобів безпосереднього прикриття об'єктів.

Тому напрямком подальших досліджень є прогноз польотів БпЛА типу "Shahed" для розрахунків зон радіолокаційної інформації радіотехнічних підрозділів.

УДК 621.39:623.1/.7

Панько М.О., Кущ П.С., Крючков Д.М., Чміль Ю.О.

ОБҐРУНТУВАННЯ ПОТРІБНОЇ ДЛЯ ЗЕНІТНОЇ РАКЕТНОЇ БАТАРЕЇ С-300В1 НОМЕНКЛАТУРИ ТА КІЛЬКОСТІ ЗАСОБІВ ЗВ'ЯЗКУ, РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ПОБУДОВИ ПРИСТРОЇВ СПРЯЖЕННЯ ТА АЛГОРИТМІВ ЇХ РОБОТИ

Особливостями ведення бойових дій є швидка зміна позиції ЗРК для підвищення їх живучості. За результатами аналізу встановлено, що один з шляхів успішного виконання поставлених завдань є використання перешкодозахищенних, з широким діапазоном зміни робочих частот, засобів радіозв'язку [1-18].

Для з'ясування відповідності сучасним вимогам, що висуваються для засобів зв'язку, був проведений аналіз системи телекодового зв'язку, що використовується в зенітній ракетній батареї, озброєної ЗРК С-300В1.

Встановлено, що існуючі засоби володіють низькою швидкістю передачі даних, малим діапазоном перестройки частоти, низькою перешкодостійкістю та великими габаритними розмірами.

В доповіді розглянуті сучасні тенденції та принципи, що забезпечують перешкодостійкість обміну інформації. Наведені результати аналізу сучасних засобів, що відповідають сьогоденним вимогам, забезпечують можливість роботи в потрібних режимах, та можуть бути використані на заміну штатних засобів.

Встановлено, що існуюча система телекодового зв'язку забезпечує обмін інформацією між цифровими обчислювальними пристроями (ЦОП) бойових засобів, що викликає потребу в розробці пристрою спряження між засобами зв'язку, що пропонуються, та ЦОП, та алгоритмів роботи пристроїв спряження. Наведені пропозиції щодо розв'язання цього питання.

Список використаних джерел

1. Застосування онтології задачі вибору для опису процесів взаємодії суб'єктів управління О. Ю. Іохов / [та ін.] // Сучасні інформаційні системи. – 2021. – Т. 5, № 1. – С. 54-62

2. Іохов О. Ю. Захист радіомереж підрозділів Національної гвардії України від радіотехнічної розвідки : монографія. Харків : НА НГУ, 2017. 214 с.

3. Белокурський Ю. П., Іохов О. Ю., Козлов В. Є., Щербіна О. О. Антени для захисту каналів радіозв'язку підрозділів Національної гвардії України. Збірник наукових праць Національної академії Національної гвардії України. Харків : НА НГУ, 2015. Вип. 2 (26). С. 65–69.

4. Іохов О. Ю. Оцінювання завадостійкості каналу радіозв'язку тактичної ланки управління підрозділів внутрішніх військ методом імітаційного моделювання / О. Ю. Іохов, І. В. Кузьминич, В. Г. Малюк, О. В. Сєвєрінов // Системи управління, навігації та зв'язку. - 2013. - Вип. 3. - С. 179-185. - Режим доступу: http://nbuv.gov.ua/UJRN/suntz_2013_3_35.

5. Белокурський Ю. П. Шляхи удосконалення характеристик імпровізованих антен каналів зв'язку підрозділів сил охорони правопорядку / Ю. П. Белокурський, О. М. Горбов, О. Ю. Іохов, В. Є. Козлов, О. О. Щербина // Збірник наукових праць Національної академії Національної гвардії України. - 2014. - Вип. 2. - С. 15-17. - Режим доступу: http://nbuv.gov.ua/UJRN/znpavs_2014_2_5.

6. Сєвєрінов О. В. Аналіз методів побудови кодів автентифікації повідомлень / О. В. Сєвєрінов, О. Ю. Іохов, О. С. Жученко, В. П. Лисечко // Системи обробки інформації. - 2006. - Вип. 4. - С. 156-. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2006_4_25.

7. Белокурський Ю. П. Організація захисту каналів радіозв'язку підрозділів охорони правопорядку України / Ю. П. Белокурський, О. Ю. Іохов, В. Є. Козлов, О. О. Щербина // Збірник наукових праць Академії внутрішніх військ МВС України. - 2014. - Вип. 1. - С. 46-49. - Режим доступу: http://nbuv.gov.ua/UJRN/znpavs_2014_1_11.

8. Колачов С. П. Стан та перспективи розвитку телекомунікаційних мереж спеціального призначення / С. П. Колачов, Д. О. Люлін, Ю. А. Мазниченко, О. Ю. Подольський, О. Ю. Іохов // Збірник наукових праць Академії внутрішніх військ МВС України. - 2014. - Вип. 1. - С. 43-45. - Режим доступу: http://nbuv.gov.ua/UJRN/znpavs_2014_1_10

9. Іохов О. Ю. Визначення шляхів побудови перспективної системи мобільного радіозв'язку внутрішніх військ МВС України / О. Ю. Іохов // Системи обробки інформації. - 2011. - Вип. 4. - С. 196-198. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2011_4_46.

10. Малюк В. Г. Метод визначення меж зони стійкого радіообміну підрозділів внутрішніх військ в умовах радіопридушення / В. Г. Малюк, О. М. Іохов, І. В. Кузьминич // Системи озброєння і військова техніка. - 2014. - № 1. - С. 56-61. - Режим доступу: http://nbuv.gov.ua/UJRN/soivt_2014_1_14.

11. Пузиренко О. Г. Методика кількісно-якісного аналізу та визначення рівня інформаційної безпеки / О. Г. Пузиренко, О. Ю. Іохов, О. М. Горбов, І. В. Кузьминич // Системи озброєння і військова техніка. - 2013. - № 1. - С. 123-128. - Режим доступу: http://nbuv.gov.ua/UJRN/soivt_2013_1_32.

12. Крючков, Д. М., Рощупкін, Є. С., Калита, О. В., & Дранник, П. А. (2023). Пропозиції щодо підвищення ефективності відновлення сукупності різнотипних радіоелектронних засобів спеціального призначення при їх використанні в різних умовах. XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023), Kharkiv. https://doi.org/10.5281/zenodo.10257044

13. Бєляєв, Д.М. Застосування векторних аналізаторів сигналів для забезпечення електромагнітної сумісності радіоапаратури / Д.М. Бєляєв, С.В. Герасимов, С.В. Кукобко [та ін.] // Збірник наукових праць ЦНДІ ОВТ ЗС України, - 2016. №3(62), -с. 77-84.

14. Tymchenko, S., Kaplun, Y., Roshchupkin, E., Kukobko, S. (2023). Substantiation of Time Distribution Law for Modeling the Activity of Automated Control System Operator. In: Shkarlet, S., et al. Mathematical Modeling and Simulation of Systems. MODS 2022. Lecture Notes in Networks and Systems, vol 667. Springer, Cham. https://doi.org/10.1007/978-3-031-30251-0_9

15. Рощупкін Є.С. Великоапертурна (рознесена) радіолокаційна система: пат. 148518 Україна : G01S7/42, H01Q21/00 / Є.С. Рощупкін, С.В. Герасимов, С.В. Кукобко, М.В. Борисенко, Ю.О. Крихтін, О.Ф. Галицький, Б.В. Гайбадулов, В.В. Джус, І.В. Помогаєв, В.В. Борисов, Ю.О. Чміль, А.Ю. Задорожна. – u 202100336; заявл. 29.01.2021; опубл. 18.08.2021, бюл. № 33/2021, – 7 с.

16. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2005). Организация когерентной обработки на промежуточной частоте при приеме широкополосных сигналов крупноапертурными антенными решетками и многопозиционными системами. Прикладная радиоэлектроника, (Т.4, №4), 437-440.

17. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2006). Алгоритмы когерентной обработки широкополосных сигналов на промежуточной частоте с использованием схем фазонастраивающих контуров с управляемыми дисперсионными линиями задержки в крупноапертурных антенных решетках и многопозиционных системах. Прикладная радиоэлектроника, (Т.5, №2), 250-254.

18. Herasimov, S., Borysenko, M., Roshchupkin, E. et al. Spectrum Analyzer Based on a Dynamic Filter. J Electron Test 37, 357–368 (2021), https://doi.org/10.1007/s10836-021-05954-0

УДК 057.087.1:621.391.26

Пастушенко М.О., Пастушенко М.С., Романюк В.А.

МЕТОДИКА ОЦІНКИ ФОРМАНТНОЇ ІНФОРМАЦІЇ ГОЛОСОВОГО СИГНАЛУ СИСТЕМИ АВТЕНТИФІКАЦІЇ

Забезпечення безпеки держави нині пов'язані з широким застосуванням різноманітних інформаційних систем. Однак, поряд із широкими можливостями інформаційних систем, з'являється і низка складних проблем. Кількість цих проблем значно розширюється, якщо інформаційні системи підключені до мережі Інтернет. Одним із шляхів вирішення цих проблем – удосконалення систем ідентифікації та автентифікації користувачів [1].

Останнім часом у цих системах використовують біометричні ознаки користувачів. При цьому у багатьох випадках перевага надається голосовим системам, які мають кращі характеристики за критерієм ефективність/вартість [2, 3]. При функціонуванні голосових систем використовується низка ознак мовного сигналу користувача. Серед ознак мовного сигналу користувача можна відзначити формантну інформацію, кепстральні та мел-частотні коефіцієнти та ін. Серед цих ознак особливе місце займає формантна інформація, яка дозволяє встановити частоту і кількість формант, ширину спектра кожної форманти, а також огинаючу спектра.

На жаль, спектральні методи оцінки формантної інформації не дозволяють якісно отримувати зазначені дані, особливо в умовах обробки корисного сигналу та шуму.

У даній методиці пропонується використовувати властивості автокореляційної функції, а як матеріали обробки використовувати зашумлений голосовий сигнал. У цьому випадку, за рахунок властивостей кореляції збільшуватиметься відношення сигнал/шум. Особливістю методики є й те, що розрахунок проводитися ітераційно, тобто, на наступному циклі оцінки автокореляційної функції використовують матеріали попереднього циклу обробки. Відношення сигнал/шум підвищуватиметься на кожному циклі обробки. Обмежитися можна п'ятьма циклами обробки.

Як показали результати експериментальної цифрової обробки голосового сигналу користувача, зазначена методика оцінки формантної інформації дозволяє:

- на третину збільшити кількість формант, що виділяються;
- на порядок підвищити точність визначення формантних частот;
- суттєво підвищити точність визначення ширини та огинаючої спектру формантних частот.

Поряд з перевагами є й недоліки аналізованої методики, які зводяться до наступного. Істотно збільшується кількість обчислювальних процедур. Наприклад, кожен цикл обробки включає обчислювальні операції, які пропорційні величині $n \cdot n!$. Тут n – кількість елементів в масиві голосового сигналу, що обробляється. На кожному наступному етапі обробки масив аналізованих даних збільшується приблизно в три рази.

Розглянуті процедури оцінки формантної інформації можна використовувати у процедурах автентифікації користувача, а й під час вирішення завдань розпізнавання мови та ідентифікації диктора.

Список використаних джерел

1. Pastushenko, M., Pastushenko, V., Pastushenko, O. (2019), "Specifics of Receiving and Processing Phase Information in Voice Authentication Systems", International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kyiv, Ukraine, 2019, pp. 621-624. DOI: 10.1109/PICST47496.2019.9061260

2. Pastushenko, M., Krasnozheniuk, Ya., Lemeshko, O. (2020), Analysis of voice signal phase data informativity of authentication system // Zaporizhzhia, Ukraine, April 27-May 1, 2020. Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020). PP 1040-1053.URI: http://openarchive.nure.ua/handle/document/11843

3. Pastushenko, M., Krasnozheniuk, Ya., Zaika, M. (2020), "Investigation of Informativeness and Stability of Mel-Frequency Cepstral Coefficients Estimates based on Voice Signal Phase Data of Authentication System User," International Conference "Problems of Infocommunications. Science and Technology" (PIC S&T′2020), pp. 1-5. DOI: 10.1109/PICST51311.2020.9468083

УДК 057.087.1:621.391.26

Пастушенко М.С., Петраченко М.О.

ПОПЕРЕДНЯ ОБРОБКА ГОЛОСОВОГО СИГНАЛУ В СИСТЕМАХ АВТЕНТИФІКАЦІЇ

У сучасному світі, де кібербезпека та ідентифікація стають все важливішими термінами, методи автентифікації на основі біометричних даних, зокрема голосу, набувають широкого застосування. Проте, для ефективної роботи систем автентифікації необхідна попередня обробка голосового сигналу для визначення його характеристик та властивостей. У даній роботі проводиться аналіз фазової інформації голосового сигналу та розробка методів попередньої обробки для систем автентифікації.

Для початку дослідження використано метод аналізу фазової інформації, що є одним із ключових методів у сфері аудіо-технологій. Фазова інформація відіграє важливу роль у відтворенні та аналізі звукових сигналів, оскільки містить значну кількість деталей про часову структуру сигналу, такі як періодичність коливань та фазові зміщення [1].

Під час аналізу одночастотного голосового сигналу використовувалося програмне забезпечення Matlab з метою докладного вивчення його параметрів. Проведені вимірювання амплітуди та частоти сигналу вказали на лінійний характер даного сигналу. Для подальшого аналізу були використані спеціальні алгоритми обробки сигналу з метою встановлення його відповідності лінійній апроксимації. Цей етап аналізу є критичним у забезпеченні точності та адекватності моделювання [2].

Після встановлення відповідності сигналу лінійній апроксимації, був застосований критерій хі-квадрат для оцінки правильності цієї апроксимації. Цей критерій є одним із стандартних методів, що дозволяє числово оцінити, наскільки добре модель відтворює спостережувані дані. Результати підтвердили високу точність моделювання, що підтримує відповідність між теоретичною апроксимацією та експериментальними даними [3, 4].

Другий етап дослідження передбачав більш складний аналіз двохчастотного голосового сигналу, оскільки він характеризується наявністю двох різних частот, які можуть змінюватися з часом. У порівнянні з одночастотним сигналом, який має лише одну основну частоту, аналіз двохчастотного сигналу вимагає більш складних методів обробки та аналізу. На даному етапі застосовувався аналогічний підхід, що й для одночастотного сигналу, але для апроксимації використовувався поліном четвертого ступеня. Такий вибір поліномів дозволив зберегти більше деталей у графіку та точніше відобразити зміни частот з плином часу. Поліном четвертого ступеня є досить гнучким і може ефективно апроксимувати складніші форми сигналів, що характерно для двохчастотних сигналів.

Останній етап дослідження був спрямований на вивчення ефективності використання поліномів для апроксимації голосових сигналів з метою покращення систем автентифікації голосу. Шляхом обчислення параметрів полінома четвертого ступеня для апроксимації двохчастотного сигналу було визначено оптимальний спосіб представлення цього типу сигналу. Відповідно, аналіз результатів порівняння показав значне покращення точності апроксимації в порівнянні з іншими методами. Це підтверджує високу ефективність використання поліномів для апроксимації голосових сигналів, зокрема двохчастотних, що є важливим кроком у розвитку алгоритмів обробки та аналізу аудіосигналів.

Застосування даного підходу має прямий практичний вигляд у підвищенні надійності та ефективності систем автентифікації голосу. Збільшення точності апроксимації голосових сигналів сприяє підвищенню рівня впізнаваності та аутентичності в системах біометричної ідентифікації. Це особливо важливо у сферах, де забезпечення безпеки та автентифікація користувачів мають критичне значення, таких як фінансові установи, мережеві системи та інші області.

Дослідження не лише підтвердило ефективність використання поліномів для апроксимації голосових сигналів, але й вказало на його потенційні переваги у сфері біометричної ідентифікації та безпеки. Додаткові дослідження в цьому напрямку можуть сприяти подальшому розвитку технологій автентифікації голосу та забезпеченню більшої захищеності інформаційних систем.

Список використаних джерел

1. Pastushenko, M., Pastushenko, V., Pastushenko, O. (2019), "Specifics of Receiving and Processing Phase Information in Voice Authentication Systems", International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kyiv, Ukraine, 2019, pp. 621-624. **DOI:** 10.1109/PICST47496.2019.9061260

2. Pastushenko, M., Krasnozheniuk, Ya., Lemeshko, O. (2020), Analysis of voice signal phase data informativity of authentication system // Zaporizhzhia, Ukraine, April 27-May 1, 2020. Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020). PP 1040-1053.URI: http://openarchive.nure.ua/handle/document/11843

3. Pastushenko, M., Krasnozheniuk, Ya., Zaika, M. (2020), "Investigation of Informativeness and Stability of Mel-Frequency Cepstral Coefficients Estimates based on Voice Signal Phase Data of Authentication System User," International Conference "Problems of Infocommunications. Science and Technology" (PIC S&T′2020), pp. 1-5. **DOI:** 10.1109/PICST51311.2020.9468083

4. Проакіс Дж. Г., Манолакіс Д. Г. Цифрова обробка сигналів: принципи, алгоритми та застосування. Видавництво Пірсона, 2018.

УДК 681.5.015

Пачков М.К., Дядюн С.В.

ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ПІДБОРУ ЯКІСНОГО ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА ЗА ВИМОГАМИ КОРИСТУВАЧА

В доповіді розглядається розробка веб-додатку для підбору якісного персонального комп'ютеру за вимогами користувача. В результаті розробки інформаційної системи користувачі зможуть конструювати персональні комп'ютери за своїми вимогами або обирати самостійно усі комплектуючі, отримуючи ефективність збірки.

Об’єкт дослідження - розробка інформаційної системи для підбору якісного персонального комп'ютера за вимогами користувача, яка побудована на мікросервісній архітектурі. У цій системі кожен мікросервіс повинен виконувати свою певну функцію.

Предмет дослідження - розробка інформаційної системи для побудови якісного ПК, яка базується на мікросервісній архітектурі, де кожен мікросервіс буде виконувати свою певну функцію, тобто мати свою область функціональності зі своїми границями. Кожен мікросервіс може працювати незалежно та має власну базу даних, що повинно дозволити забезпечувати гнучкість, масштабованість та гарний захист системи.

Метою даної роботи були проектування та розробка інформаційної системи для підбору якісного персонального комп’ютера за вимогами користувача, яка повинна базуватися на мікросервісній архітектурі.

Завданнями виконаної роботи були опис предметного середовища, аналіз предметної області та об’єктів управління, огляд та оцінка наявних аналогів, вивчення мікросервісної архітектури, опис функціональної моделі, постановка задачі, аналіз предметної області, проектування бази даних, побудова об’єктно-орієнтованої моделі, розробка програмного забезпечення. Основною задачею системи було забезпечення швидкого і точного підбору комплектуючих, та отримання показників ефективності обраної користувачем збірки. Користувач інформаційної системи, окрім показників ефективності, повинен отримувати рекомендації щодо покращення своєї обраної збірки з отриманням порівнянь результатів. Також повинна бути можливість порівняти отриману збірку з запропонованою збіркою середнього класу та найкращою збіркою.

Система повинна забезпечувати ефективний та точний підбір комп’ютерної техніки, що відповідає вимогам та потребам користувача. Окрім цього, користувач може сам обирати збірку за певними компонентами та отримувати результати роботи цієї збірки у певних додатках та комп’ютерних іграх, при цьому результати роботи для додатків повинні відображатися у середній оцінці метрик. У свою чергу, для ігор результати повинні відображатися у FPS. Можна також виділити ще і додаткову мету даного дослідження, а саме вивчення та аналіз різних підходів до розробки мікросервісної архітектури, та реалізацію інформаційної системи на цій архітектурі.

З швидким розвитком сучасних технологій, почалося зростання популярності комп’ютерів. Вони є майже у кожній домівці. Комп’ютер є основним інструментом для роботи та розваг для багатьох людей. Це пов’язано з професійною діяльністю людей та зі зростанням популярності відеоігор.

Популярність збірки персонального комп’ютера збільшилася декілька років назад. Це пов’язано з декількома факторами: гнучкість та індивідуальність, продуктивність та оновлюваність, економічний аспект.

Багато людей, особливо ті, хто не розбирається в комп’ютерах чи їхніх комплектуючих, зіштовхуються з проблемою вибору комп’ютера, оскільки вони не розуміють усіх технічних характеристик комп’ютера. Крім того, придбати комп’ютер, який вже зібраний, буде у декілька разів дорожче, ніж купити комплектуюче та зібрати його самому. Кожен користувач має свої унікальні потреби та вимоги до персонального комп’ютера. Розробка інформаційної системи, яка допомагає користувачам вибрати оптимальний ПК, з отриманням результатів як у відеоіграх, так і в популярних додатках, які потрібні людини для роботи, є необхідністю – також вона спростить весь процес вибору.

З ростом популярності почали з’являтися деякі сервіси, які допомагають користувачу зібрати особистий персональний комп’ютер.

Серед існуючих рішень немає повністю аналогічного проекту і точного конкретного аналогу розробленої системи, але деякі рішення є схожими на деякі компоненти системи, що пропонується. Тим не менш, прямих аналогів системи не існує. Більшість інших інформаційних систем представляють собою або конфігуратор ПК, або інформацію про роботу комплектації у певних іграх. До проектів, які мають схожі компоненти, можна віднести Technical City [1], що містить великий обсяг інформації та вивід результатів

формування збірки для ігор, Telemart [2], що має можливість конфігурації персонального комп'ютера, та PCPARTPICKER [3]. Проведено аналіз необхідних комплектуючих для побудови персонального комп'ютера, вимоги користувачів, сумісність та конфігурацію компонентів ПК, досліджені системи „Telemart", „Technical City" та „PCPARTPICKER", після дослідження для кожної системи визначено їх переваги та недоліки.

На основі даних про вибір компонентів для конструювання та аналіз результатів збірок і потреб користувачів було сформовано загальний функціонал системи, після чого була спроектована та реалізована інформаційна система для підбору якісного ПК з використанням мікросервісів. Для цього було розглянуто системні архітектури, спроектовано бази даних, визначено основну мову програмування і всі необхідні фреймворки, побудовано UML діаграми, розглянуто програмні забезпечення для автоматизації розгортання та управління додатками у середовищах з підтримкою контейнеризації.

Було реалізовано багато важливих елементів для покращення роботи додатку, а саме кожний логічний блок, розбитий на свій мікросервіс, був розміщений на Docker, тому навантаження йде на окремі компоненти, а не на весь додаток, при чому якщо вийде з ладу один із мікросервісів, додаток усе одно буде працювати, але з меншим функціоналом. Було використано новий фреймворк Blazor, який замінює JavaSript та дозволяє створювати динамічні сторінки, з використанням його компонентів, якщо один з компонентів сторінки виходить з ладу, то сторінка також буде продовжувати роботу, працювати не буде лише один з її компонентів. Для реалізації авторизації користувача було застосовано JWT токен, для безпечної передачі інформації між сторонами у вигляді JSON-об'єктів.

Реалізація усіх цих елементів у розробленій інформаційній системі покращить роботу додатку та зробить його більш швидким та безпечним.

Одною з ідей подальшого розвитку цієї роботи є додавання мікросервісу з новинами, де будуть публікуватися новини ринку комплектуючих у світі та надавання можливості користувачеві писати новини і надавати адміністрації сайту їх на перевірку для подальшої публікації, що дозволить значно збільшити аудиторію. Також можна додати форму для спілкування користувачів одного з іншим для обговорення збірок комплектуючих або інших важливих питань. Можна покращити профіль користувача додаючи туди можливість завантажувати аватар та змінювати персональні дані. Надати можливість користувачам формувати url сторінки для поширення власних зборок та надати можливість залишати коментарі для кожної збірки. Використати новітню технологію Identity від компанії Microsoft, яка дозволяє авторизуватися у системі завдяки іншим обліковим записам, що полегшить процес реєстрації для нових користувачів, наприклад зробити вхід через Google або Facebook.

Кожен проект повинен мати свою сторону заробітку, тому можна підключати більшу кількість сайтів для переходу на сторінки інших магазинів, та домовлятися з магазинами мати доступ напряму до їх API, а не використовувати web scraping.

Висновки. У результаті виконання роботи було розроблено інформаційну систему для підбору якісного персонального комп`ютера за вимогами користувача, яка вже готова для використання.

Новизною проекту є створення додатку, завдяки якому кожен зможе швидко зібрати собі персональний комп'ютер за своїми вимогами. У роботі використано мікросервісну архітектуру для даної інформаційної системи, яка повинна покращити масштабованість та гнучкість, забезпечити її технічну незалежність. Багато сучасних великих компаній переходять на такий дизайн, тому в майбутньому багато додатків будуть працювати саме з такою архітектурою.

Даний проект можна продовжити розвивати далі, вважаючи, що для реалізації нового функціоналу не потрібно переробляти код, а достатньо створити новий мікросервіс, який розмістити на докері та налаштувати подальшу взаємодію.

Проект має достатню кількість розробленого матеріалу для того, щоб ним можна було користуватися, але є немало речей, які можна додати, щоб ще покращити роботу системи.

Сервіс, який дозволяє конструювати персональний комп'ютер за вимогами користувача, може вплинути позитивно на різні сфери життя. Людина, яка знаходиться в певній робочій сфері, може вільно підібрати необхідний персональний комп'ютер, що може значно покращити її продуктивність в роботі.

Список використаних джерел

1. About Technical City // Technical City. URL: https://technical.city/en/about.
2. Інструкція зі створення конфігурації // Telemart. URL: https://telemart.ua/ua/assembly-start.html.
3. About PCPartPicker // PCPartPicker. URL: https://pcpartpicker.com/about.

УДК 004.056.55

Першин О.О., Шило С.Г.

ОБГРУНТУВАННЯ ВИБОРУ СТЕГАНОГРАФІЧНОГО МЕТОДУ ПРОСТОРОВОЇ ОБЛАСТІ ДЛЯ ПРИХОВАНОЇ ПЕРЕДАЧІ КОНФІДЕНЦІЙНИХ ДАНИХ

На сьогоднішній день Україна зазнала надзвичайно великої кількості кібератак у зв'язку з повномасштабною російською агресією проти нашої держави. Протидія навалі агресора в кіберпросторі реалізується за рахунок використання криптографічних механізмів, що реалізовані програмними, апаратними та програмно-апаратними засобами. Але впровадження ефективних методів боротьби з кіберзагрозами пов’язане з необхідністю витрати значних обсягів обчислювальних та інформаційних ресурсів, що створює проблему можливості їх практичного використання на всіх рівнях управління.

В зв’язку з цим актуальним є питання пошуку альтернативних методів захисту інформації, які можуть забезпечити цілісність даних від зловмисників, за умови допустимої витрати ресурсів на їх реалізацію.

На теперішній час конфіденційні дані впроваджуються в повідомлення за допомогою методів стенографії, найбільш широке розповсюдження з яких, отримали заміна найменш значущого біту (LSB), дискретне косинусне перетворення (DCT), дискретне вейвлет-перетворення (DWT).

Результати аналізу ефективності методів стеганографії свідчать, що кожному типу стеганоконтейнера притаманна тільки для нього область приховування інформації зі службовим доступом.

До найбільш суттєвих переваг та недоліків зазначених методів слід віднести наступні.

Метод LSB має високе корисне навантаження, але вразливий до атак, спрямованих на виявлення прихованої інформації.

Метод DCT має високу ефективність стиснення, але втрата даних при стиснені та обмеження простору для вбудовування робить його більш вразливим від модифікації стеганоконтейнера.

Метод DWT подібний до методу з дискретно-косинусним перетворенням, обидва методи можуть ефективно використовуватися для стиснення даних, що дозволяє реалізувати їх з обмеженими ресурсами для зберігання та передачі.

Відмінність між методами DCT та DWT полягає в просторових і частотних розмірах: DCT зазвичай забезпечує більшу компактність в частотному домені, тоді як DWT може

забезпечити кращу локалізацію у просторовому домені. Тому методи DWT є найбільш ефективними для виявлення локальних змін у зображеннях.

Також до недоліків методів DWT та DWT слід віднести значні обчислювальні витрати, особливо для обробки великих зображень або даних великої розрядності, що унеможливлює їх використання на високих рівнях управління.

Враховуючи простоту реалізації і незначну обчислювальну складність, порівняно з іншими методами, доцільно обрати модифікацію методу найменшого значущого біту для підвищення стійкості до атак, які спрямовані на виявлення інформації.

УДК 355.421

Петлюк І.В., Щерба А.А., Кострица В.О.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ІННОВАЦІЇ ПІД ЧАС НАВЧАННЯ МЕХАНІКІВ-ВОДІЇВ ТА ВОДІЇВ АВТОМОБІЛЬНОЇ ТЕХНІКИ

Специфіка підготовки і роботи механіків-водіїв та водіїв автомобільної техніки, котрі проходять службу у військових формуваннях, кардинально відрізняється від підготовки таких же фахівців у цивільних транспортних компаніях. Військові фахівці працюють в дуже важких та складних умовах, як фізичних так і психологічних. Переважно напружений спосіб життя, швидке та здебільшого неправильне харчування, постійне недосипання – обов'язково призводять до проблем пов'язаних із здоров'ям, мають підвищений ризик виникнення депресії. Тому, важливим чинником при відборі потрібних кадрів є врахування морально-ділових якостей кандидатів, їх здатність вміло діяти в небезпечних ситуаціях, які часто пов'язані з ризиком для життя, адже від успішних, своєчасних та вмілих їх дій зачасту буде залежати успіх виконання завдання підрозділом в цілому.

Саме тому при відборі механіків-водіїв та водіїв автомобільної техніки для потреб військових формувань потрібно проводити додаткову роботу, щодо виявлення категорії осіб, які потенційно зможуть правильно діяти в умовах небезпеки. Скориставшись інформаційними технологіями, а саме, проведенням сучасних психологічних тестувань, які стануть надійним, об'єктивним і дієвим інструментом для визначення придатності до керування механічним засобом та до дій в небезпечних ситуаціях. Психологічні тестування можуть бути одним із засобів попередження нещасних випадків на індивідуальному рівні.

Науково-технологічні процеси постійно змінюють умови праці механіків-водіїв і водіїв автомобільної техніки та їх діяльності загалом. Змінюється потреба в тих знаннях і навичках, що їх вони повинні мати, а це в свою чергу змінює зміст та технологію підготовки їх відповідно. Для вирішення цієї проблеми, зокрема, потрібно застосовувати сучасні інноваційні підходи. Адже інноваційний підхід якраз орієнтований на формування готовності навчаємого до динамічних змін за рахунок розвитку різноманітних форм логічного та творчого мислення. При цьому завданням викладача є створення ситуацій, в яких навчаємі, використовуючи різні джерела інформації та міжпредметні зв'язки, самостійно повинні їх аналізувати. Створюючи такі ситуації викладач використовує всі можливі способи інформаційно-комп'ютерних технологій та пам'ятає, що завдання яке він ставить перед навчаємим, повинно відповідати його інтелектуальним можливостям, тобто має бути досить складним, але водночас можливим для виконання, завдяки сформованим навичкам мислення.

Очікуваним результатом практичних занять з водіння для навчаємих є набуття навичок правильної роботи з органами керування і доведенні їх до автоматизму. Тому при проведенні таких занять також доцільно використовувати інформаційно-комп'ютерні

технології, зокрема комп’ютерні тренажерні комплекси. Однією з переваг використання таких тренажерних комплексів є істотне збереження моторесурсу озброєння та військової техніки та економія пального, що в свою чергу робить таке навчання значно дешевшим.

Отже, використання сучасних інноваційних підходів та інформаційних технологій при відборі на навчання механіків-водіїв і водіїв автомобільної техніки та під час його проведення дозволяє ефективно застосовувати сучасні методи навчання для активізації пізнавальної діяльності навчаємих, покращує ефективність управління їх навчальною діяльністю та забезпечує підрозділи надійними кадрами і сприяє успішному виконанню ними поставлених завдань.

УДК 004.932.4

Площик А.С.

ВИКОРИСТАННЯ ФУНКЦІЇ КОРЕЛЯЦІЇ ДЛЯ РОЗПІЗНАВАННЯ, АВТОМАТИЧНОЇ ОБРОБКИ ЗОБРАЖЕНЬ ТА ВИЯВЛЕННЯ РУХОМИХ ОБ’ЄКТІВ

Виявлення та відстеження рухомих об'єктів у різних типах візуальних медіа є критично важливим аспектом численних застосувань, таких як відеоспостереження, інтелектуальне управління дорожнім рухом та цифрової міської інфраструктури. Способи реалізації цих завдань представляються камерами відеоспостереження (closed-circuit televisions – CCTV), літаками та безпілотними літальними апаратами (БПЛА). Навіть здатність до транспортування наночастинок у ґрунті задля захисту навколишнього середовища.

Виявлення об'єктів в межах одного кадру або зображення передбачає ідентифікацію цього об'єкта, тоді як відстеження об'єктів, із врахуванням його початкового розташування, фокусується на прогнозуванні положення об'єкта у певній відеопослідовності. Ці можливості мають масштабне застосування у великій кількості завдань в межах комп'ютерного зору, включаючи спостереження, виявлення об’єкта з фону, автономну навігацію для транспортних засобів та робототехніки тощо.

Саме відстеження об'єктів в переважній більшості відбувається в розрізі двох методик. Виявлення та відстеження одного конкретного об'єкта (Single object tracking – SOT) зосереджене на цій одній цілі протягом усього періоду часу відео, в той час як відстеження кількох різних об'єктів (Multiple object tracking – MOT) або відстеження одночасно декількох цілей (Multiple target tracking – MTT) передбачає спостереження певної кількості об'єктів одночасно.

В умовах сьогодення забезпечення відслідковування та виявлення об’єктів військовими може здійснюватися для патрулювання кордонів в межах спостереження та виявлення рухомих об’єктів, так і для вдосконалення навігаційних систем.

Ще одним важливим способом застосування є виявлення і відслідковування об'єктів на інфрачервоних (ІЧ) зображеннях, де є можливість зміни цілі за розміром або фіксується наближення з різною швидкістю.

В залежності від деталізації інформації існує залежність завдання, які пов'язані з виявленням і відстеженням. Саме відстеження може бути здійснене досить складно через масу різноманітних факторів.

Основна проблематика полягає саме у виявлення об’єктів, що здійснюють динамічний рух, які зазнають оклюзії або стають невидимими. Складність виявлення зберігається і при виникненні шуму, виготовлення досліджуваних об’єктів з різних матеріалів, обертання об’єктів, зміни масштабу та руху камер. Враховуючи значний прогрес, ця

проблематика залишається, особливо при здійсненні відстеження малих об'єктів на фоні великих.

Вивчення цих об’єктів є найбільш актуальним і поширеним у таких галузях, як БПЛА та дистанційне зондування (ДЗ). Ці об’єкти можуть маскувати зовнішні ознаки, їх важко відстежити та виявити через їхній розмір.

Через невеликий розмір ці об’єкти часто приймають за шум, що негативно впливає на точність відстеження. Термін «малий об'єкт» зазвичай визначається в двох значеннях. По-перше, це може стосуватися об’єктів, фізично малих у реальному світі. Крім того, згідно з оцінкою метрики MS-COCO, малий об’єкт — це об’єкт із площею від 32 до 32 пікселів або менше, що є загальноприйнятим порогом для наборів даних, що містять звичайні об’єкти. Таким чином, виявлення та відстеження малих об'єктів є особливим аспектом виявлення та відстеження об'єктів, який потребує спеціальних методів обробки цифрових зображень та відеоматеріалів. Наприклад, при аерофотозйомці природа малих об'єктів часто вимагає вдосконалення методів .

В цілому, прикладне завдання функції кореляції та кореляційної обробки зображення полягає у порівнянні об’єктів. Один із способів виявлення об’єктів полягає у здійсненні порівнянні отриманого досліджуваного зображення із стандартом. Пошук об'єктів на зображенні шляхом зіставлення отриманого зображення із стандартом

При цьому еталон порівнюється з усіма об'єктами, що знаходяться на зображенні, шляхом послідовного переміщення зображення, зазвичай фіксується зчитування зліва направо та зверху вниз. Як оцінювальна величина використовується взаємна кореляція між вхідним та еталонним зображеннями.

Визначення наявності об’єкта на зображенні кореляційним способом полягає в поелементному порівнянні двох зображень одного і того ж об'єкта, отриманого або різними датчиками або одним датчиком з проміжком в часі. При цьому здійснюється формування величини, що здійснює вимір кореляції між двома зображеннями, і знаходить положення максимуму функції кореляції.

Таким чином, розглянуті задачі обробки зображень, у загальному випадку, передбачають обчислення взаємної кореляції між двома порівнюваними зображеннями та подальшого порівняння її з пороговим значенням.

Щодо порогового значення, то в ході обрахунків самостійно встановлюється порогове значення, яке визначає результативність якісного виявлення об’єкта.

Слід зазначити, що кореляційна обробка передбачає роботу із зображеннями, представленими у растровому вигляді.

Растрове зображення – це двовимірна матриця, яке з великого числа просторово упорядкованих дискретних елементів, пікселів, кожен із яких може мати, при однакових розмірах, відмінне від інших елементів значення оптичних характеристик, таких як колір, насиченість та інші характеристики. Для бінарних зображень растрова матриця містить всього два види пікселів: 0 і 1.

Растрове представлення є досить зручним для його використання, оскільки має ряд істотних переваг у порівнянні з векторним поданням:

- об’єкти розпізнаються без втрати інформації;
- швидке та просте обчислення певних параметрів зображень;
- автоматично зникає необхідність в здійсненні растр-векторних перетворень, що забирають частину часу, що відведено на обробку зображення.

Актуальним є саме кореляційний аналіз зображень ґрунтується на тому, що пари значень яскравості з однієї і тієї ж географічної області (наприклад, об'єкта) між різночасовими наборами зображень мають тенденцію до високої кореляції, коли відбуваються незначні зміни, і некорельовані, коли зміни відбуваються.

В загальному, основний недолік кореляційних методів оброблення полягає саме в тому, що потрібні громіздкі обчислювальні, а отже, і тимчасові витрати під час розв'язання практичних задач. Але в силу того, що постійно зростає потужність сучасних

обчислювальних машин та досить швидко розвиваються математичні засоби, і створюються спецпроцесори, орієнтовані саме на обробку растрових зображень, можна вважати, що кореляційна обробка є перспективною для практичного застосування.

УДК 004.94

Поліщук Л.І., Богуцький С.М., Лаврут Т.В.

ОСНОВНІ ВИМОГИ І ПРОПОЗИЦІЇ ДЛЯ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

В доповіді розглядаються питання вимог до інформаційно-довідкової системи з порядку прийняття рішень на ведення бойових дій як підсистеми АСУ СВ ЗС України, а також можливі напрями їх реалізації.

Світовий досвід розвитку засобів управління свідчить, що найбільш перспективним є шлях перебудови управління військами і засобами ураження на якісно новій технологічній основі, головним чином – за рахунок автоматизації та роботизації найбільш трудомістких та важливих процесів.

Управління військами здійснюється на підставі рішення командира на ведення бойових дій. Військові командири на сьогоднішній день дотримуються однієї з двох процедур прийняття рішень за стандартами ЗС США:

- процедура військового керівництва (ПВК - TLP) – процедура призначена вирішувати тактичні питання;
- процес військового прийняття рішення (ПВПР - MDMP) - використовують командири батальйонів та вищого рівня.

При відпрацюванні та прийнятті в АСУ рішень, які відповідають обстановці, що склалася, головну роль відіграє інформація і дані, які повинні задовольнити вимоги з їх повноти, адекватності та несуперечливості.

За таких умов основними вимогами до інформаційно-довідкової системи (ІДС) з порядку прийняття рішень на ведення бойових дій можуть бути:

- постійна готовність;
- відповідність ІДС структурі ланки управління бойовими діями;
- створення інтегрованого банку даних;
- застосування баз даних в процесі прийняття рішень;
- створення єдиного інформаційного простору (ЄІП);
- безпека даних та розмежування доступу до інформації;
- стандартизація (уніфікація).

Все вищенаведене може бути реалізовано за рахунок:

- забезпеченості швидкодіючими технічними засобами обробки інформації;
- значної кількості джерел постачання інформації та їх надійності;
- поєднання індивідуальної роботи окремих виконавців з колективним процесом роботи на етапі прийняття рішення;
- забезпечення своєчасності постановки завдань підлеглим, організації та здійснення постійного контролю за їх виконанням.

Науковий центр Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного у своїх науково-дослідних роботах послідовно відпрацював цілу низку питань зі створення системи підтримки прийняття рішень на планування і управління бойовими діями як підсистеми АСУ СВ ЗС України.

УДК 004.62

Полурєзов Д.С.

ОБРОБКА BIG DATA НА МОБІЛЬНИХ ПРИСТРОЯХ

На сьогодні в сфері розробки мобільних додатків спостерігається зростаючий інтерес до проблем обробки великих об'ємів даних за допомогою мобільних пристроїв. Вимоги користувачів до сучасних мобільних застосунків містять потребу в отриманні доступу до важливої інформації у будь-який момент часу та в будь-якому місці. Це означає, що сучасні застосунки повинні бути орієнтовані на обробку великих об'ємів даних та забезпечувати швидку і ефективну реакцію на запити користувачів. У більшості випадках користувачі очікують, що дані будуть оновлюватися в режимі реального часу, надаючи їм актуальну інформацію.

Однією з основних стратегій для покращення продуктивності та забезпечення швидкої реакції на запити користувачів є використання методів паралельної обробки даних. Це означає, що додаток може виконувати кілька операцій одночасно, розділяючи завдання на менші частини і оброблюючи їх паралельно на різних обчислювальних ядрах пристрою. Паралельна обробка дозволяє зменшити час обчислень і підвищити загальну продуктивність, що є важливим фактором для багатьох мобільних застосунків.

Поширення методів паралельної обробки великих об'ємів даних на платформі iOS серед користувачів персональних мобільних пристроїв має безпосереднє значення для різних сфер, включаючи медицину, військову справу, правоохоронну діяльність. Ці методи базуються на підвищенні продуктивності iOS-додатків за рахунок впровадження методів розпаралелювання, заснованих на GCD, NSLock та OperationQueue для формування та обробки запитів до розподілених БД.

Основним елементом будь-якої БД слід вважати ключ. Носієм даних в моделі NoSQL БД є кортеж:

$$KV = \{\langle f, e\rangle\},$$

де $\boldsymbol{f}$ – ключ, який приймає унікальне значення для кожної пари; $\boldsymbol{e}$ – значення, яке йому відповідає.

Сигнатура моделі має наступний вигляд:

$$O = \langle \pi, \sigma\rangle,$$

де $\boldsymbol{\pi}$ – операція проекції за атрибутами (ключ або значення), $\boldsymbol{\sigma}$ – селекції атрибутів (вибір значення за ключем, ключів за значеннями, наслідування ключів). Ці операції відносяться до категорії читання [1].

Одним з варіантів реалізації розподіленого зберігання великих обсягів даних є система BigTable від компанії Google [2], яка має наступні властивості:

– неповна реляційна модель даних;
– підтримка динамічного контролю над розміщенням даних.

Основу моделі збереження даних в BigTable складають рядки, стовпці та тимчасові мітки:

$$\text{BigTable} = \{< r, c, t >\}.$$

Якщо в декількох стовпцях зберігаються дані, що відносяться до одного типу, то такі стовпці, згідно з моделлю Bigtable, утворюють сімейство:

$$\text{col } F = \{ c_i, c_j \mid \text{dom } (c_i) \in T \wedge \text{dom } (c_j) \in T\}.$$

Використовувати сімейство стовпців досить зручно хоча б з того міркування, що це дозволяє стиснути однорідні дані, тим самим зменшивши їх обсяг. Саме сімейства стовпців складає одиницю доступу до даних.

Вміст інформації, що супроводжує будь-який динамічний об'єкт, що перебуває під наглядом, постійно змінюється. Щоб врахувати ці зміни, кожна з копій даних, які зберігаються в стовпці, отримують тимчасову мітка (timestamp). В BigTable в якості тимча-

сової мітки використовується 64-розрядне число, яким можна кодувати час і дату таким чином, як це потрібно клієнтським програмам. Шляхом використання тимчасові мітки додатки можуть забезпечувати в BigTable пошук, наприклад, тільки щодо найновіших копій даних [3].

Отже, для будь-якої предметної області в сервісі Google можна створити власну карту даних Bigtable, що містить задану кількість рядків і унікальний для цієї предметної області набір сімейств стовпців. Повтори даних у стовпцях для таких даних упорядковуються за значеннями тимчасових міток. Головною перевагою цього підходу є те, що таку базу неважко поділити на незалежні елементи та розподілити по множині серверів. Відсортовані за алфавітом рядки діляться на діапазони, що мають назву tablet. Оскільки рядки в кожному таблеті відсортовані за ключовим іменем, то клієнтським додаткам достатньо просто знайти потрібний таблет, а в ньому – необхідний рядок.

Для синхронізації таблетів призначений сервіс Chubby. Для кожного таблет-сервера Chubby створює спеціальний chubby-файл, за рахунок чого файл Bigtable може визначити, які із серверів є працездатними. Ще один chubby-файл містить посилання на розташування кореневого таблета (Root-tablet) з даними про розташування усіх інших. Цей файл повідомляє майстру, який з серверів якими таблетами керує.

Використання сервісу Chubby в середовищі Bigtable дозволяє забезпечити підтримку несуперечності даних у розподіленому середовищі з безліччю реплік. Подальші дослідження будуть спрямовані на визначення метрик для порівняння методів розпаралелювання та проведення експериментів з метою визначення найбільш продуктивного метода формування та обробки запитів до БД за допомогою мобільного додатку у середовищі iOS.

Список використаних джерел

1. Zhou Feng, W. Hsu, Mong Li Lee. Efficient pattern discovery for semistructured data // 17th IEEE International Conference on Tools with Artificial Intelligence (ICTAI-05). – 2005. – P. 301–309.

2. Cloud Bigtable (назва з екрану) / URL: https://cloud.google.com/bigtable (дата звернення: 16.02.2024).

3. Chang, Fay; Dean, Jeffrey; Ghemawat, Sanjay; Hsieh, Wilson C; Wallach, Deborah A; Burrows, Michael ‘Mike’; Chandra, Tushar; Fikes, Andrew; Gruber, Robert E (2006), "Bigtable: A Distributed Storage System for Structured Data", Research (PDF), Google.

УДК 007.2+ 004.942 + 004.05 +004.056.5

Пономарьов О.А., Нестеров О.М., Козубцов І.М., Ольшанський В.В, Філіпов В.В.

ПІДГОТОВКА ФАХІВЦІВ ЗВ’ЯЗКУ ТА КІБЕРБЕЗПЕКИ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ НА ЗАСАДАХ ЛІДЕРСЬКОЇ ПРОФЕСІЙНО-ДІЛОВОЇ ГРИ

В даний час триває пошук рішень щодо підвищення мотивації засвоєння навчального матеріалу курсантами вищих військових навчальних закладах (ВВНЗ). Впровадження інтерактивних форм навчання є одним з найважливіших напрямків вдосконалення навчального процесу у ВВНЗ. Першою інтерактивною формою навчання був навчальний комплекс системи бойової підготовки військових спеціалістів танкових військ. Для цього І. Руснак та В. Шевченко використали сучасні комп'ютерні технології, які дозволяють взаємодіяти з безліччю речей, в яких курсант може взяти певну участь. Відновлення та реалізація наукових досліджень обумовлені зміною підходу в системі бойової підготовки військових фахівців підрозділів зв'язку та кібербезпеки.

Основним двигуном процесу освоєння знань є їхнє практичне застосування. Нерідко курсанти відчувають серйозні труднощі в практичному застосуванні знань. Важливо курсантів навчити застосувати знання на практиці, сформувати в них прийоми поєднання розумових і практичних дій. Для цього потрібно створити умови, щоб курсанти в процесі занять на фаховому курсі тактичного рівня професійної військової освіти (L-1B), наприклад, з дисципліни «Бойового застосування систем та комплексів військового зв'язку» переконалися, що теоретичні знання одержані на технічних кафедрах стали основою їхньої практичної діяльності. Включення курсантів в навчальну діяльність слід за ідеєю роботи на основі методики викладання ділової професійної гри «виконання курсантами обов'язків за відповідною офіцерською посадою». Що стосується реформи бойової підготовки, заснованої на засадах лідерства, то сьогодні це можна вважати інноваційним рішенням.

Нині виділяються три основні напрями концепцій лідерства [1]:

- концепції, у яких обґрунтовується перевага фактору рис особистості;
- концепції, у яких вирішальним фактором вважається ситуація;
- концепції, у яких поєднуються особистісні і ситуаційні фактори.

Незважаючи на зазначену тему дослідження, слід визнати, що в розглянутих публікаціях питання якості підготовки військових фахівців не знайшло відображення в підготовці військових фахівців для підрозділів зв'язку та кібербезпеки в Збройних Сил. З огляду на це, авторами було обрано цей актуальний напрям дослідження.

Метою авторської доповіді популяризація досвіду кафедри бойового застосування підрозділів зв'язку з підготовки фахівців на засадах лідерської професійно-ділової гри.

Викладання дисциплін «Бойове застосування систем та комплексів військового зв'язку», як складової курсів професійної військової освіти L-1B (тактичний рівень військової освіти) є одним з найскладніших елементів підготовки курсантів. Це пов'язано з тим, що воно вимагає ґрунтовних теоретичних знань не тільки про призначення засобів зв'язку у складі апаратної, а й про систему зв'язку в цілому з урахуванням взаємодії цих апаратних у системі вузлів зв'язку та їх розташування на місцевості. Подання до вивчення склад апаратної може бути представлено різними способами, починаючи від креслень (фотографій) і закінчуючи тривимірними електронними моделями та натурними макетами, моделями, і вони можуть бути представлені у різний спосіб. Адже засоби мультимедіа вже створюють інтерактивні макети за призначенням, однак потребує вдосконалення методики навчання із застосуванням професійно-ділових ігор.

Підготовки військових фахівців для потреб сектору безпеки та оборони на засадах лідерства та професійно-ділових ігор дозволяє трансформувати існуючу модель навчання у професійну діяльності офіцерів на відповідних посадах у військах, в якій задіяні деякі основні елементи гри. Метою удосконалення роботи викладача ВВНЗ полягає у організації навчання курсантів таким чином, щоб воно стало цікавим та непомітно для курсанта із додержанням принципу «важко в навчанні – легко в бою».

Викладацька діяльність науково-педагогічного працівника на засадах лідерства націлена на спонукання та залучення курсантів до навчання, розуміння змісту дисципліни як потреби. Задля досягнення таких результатів викладацький склад кафедри створює освітнє середовище, у якому курсант залучений у фрагменти майбутньої діяльності, які відповідатимуть його методам викладання задля досягнення бажаних результатів навчання – формування лідерських якостей у курсантів, як майбутніх офіцерів.

Практичні аспекти реалізації полягають у перегляді методики викладання на фаховому курсі тактичного рівня професійної військової освіти (L-1B), не лише дисципліни «Бойового застосування систем та комплексів військового зв'язку», а всього комплексу шляхом переходу від навчання, орієнтованого на викладача, до навчання, орієнтованого на курсанта [2].

Успіх викладачів та досягнення курсантами гарних результатів навчання залежить від якості залучення курсантів до дисципліни, яка викладається. Таке залучення може

бути поверхневим, його ще називають «поверхневим підходом». При такому підході курсант отримує часткові знання від переданої викладачем інформації, докладаючи мінімальних зусиль для отримання позитивної оцінки його знань. Успішним стає той офіцер-лідер, який може застосувати теоретичні знання до практичних проблем при організації бойового застосування підрозділів зв'язку. На нашу думку, таких здібності хочуть бачити не лише викладачі, а в першу чергу замовник.

Безумовно поданий підхід та опис до навчання вимагає, окрім принципово нової роботи викладачів, високоякісних, структурованих результатів навчання. Його називають «глибинним підходом і він надає студентам відчуття задоволення від навчання та глибокого розуміння дисципліни» [3]. Вибір підходу у викладанні викладачем залежить від розуміння змісту викладання.

Таким чином, доцільно організувати науково-педагогічний експеримент на фаховому курсі тактичного рівня професійної військової освіти (L-1B), з дисципліни «Бойового застосування систем та комплексів військового зв'язку» на засадах лідерства в освіті (сумісної діяльності викладачів, курсантів) замість традиційної форми організації групових занять. Курсант має відчути, що він майбутній офіцер, а навчальні заняття це спосіб перетворити набуті теоретичні знання в первинний практичний досвід. Інновацією кафедри є «легко і цікаво в навчанні – професійно і легко діяти в сучасному гібридному бою»!

Список використаних джерел

1. Kokun O. Psychological structure of leadership qualities of the future officer. Bulletin of the National Defense University of Ukraine, 2012. Vol. 4 (29). Pp. 170–174.

2. Kozubtsov I. Methodology of the Professional-Business Game for the Development of a Cadet Leader in Professional Training Courses (L-1B) of the Tactical Level of Military Education. IgMin Research - STEM A Multidisciplinary Open Access Journal. 2023. Vol 1 Issue 2, pp. 160–169. DOI: 10.61927/igmin132.

3. Leadership Foundation for Higher Education. Stimulus paper by Paul Ramsden. Leadership for better student experience. What do senior executives need to know?. 2013. 32 p.

УДК 623.364.4

Поплавець С.І., Гузченко С.В.

ВРАХУВАННЯ ДИФУЗІЙНИХ ПРОЦЕСІВ РОЗПОВСЮДЖЕННЯ РАДІОНУКЛІДІВ ТА НЕБЕЗПЕЧНИХ ХІМІЧНИХ РЕЧОВИН ПІД ЧАС ФОРМУВАННЯ ІНФОРМАЦІЙНИХ МОДЕЛЕЙ РАДІАЦІЙНОЇ ТА ХІМІЧНОЇ ОБСТАНОВКИ

Під час використання масованих ракетних ударів або ведення бойових дій звичайними видами зброї, можливе навмисне чи випадкове зруйнування підприємств атомної енергетики та хімічної промисловості з запасами небезпечних, хімічних речовин (НХР), промислових, транспортних та інших об'єктів з різноманітними небезпечними компонентами, а також не виключено застосування зброї масового ураження (ЗМУ), що може привести до виникнення небезпечної радіаційної, хімічної, біологічної (РХБ) обстановки. Розрахунково-графічні способи прогнозування, які базуються на використанні таблиць і графіків [1,2], та за звичай здійснюються детермінованим методом під час визначення оперативності вироблення та прийняття рішення в умовах радіоактивного та хімічного зараження не дозволяють в короткий термін часу здійснити завчасне оповіщення військ, виконати практичні заходи щодо їх захисту та суттєво знизити втрати

особового складу, озброєння та військової техніки з урахуванням розповсюдження радіонуклідів та НХР в повітрі [3].

В наслідок руйнування радіаційних та хімічно-небезпечних (РХН) об’єктів важливо мати данні, які відповідають реальним умовам в певній точці, в масштабі реального часу, так як лише за допомогою вірних даних можна визначити реальне становище, що склалося після аварії і за допомогою отриманого прогнозу вибрати найбільш раціональний варіант дій [4].

Для формування інформаційної моделі радіаційної обстановки та генерування сценаріїв наслідків руйнування радіаційно-небезпечних об’єктів за основу взята методика прогнозування і оцінці наслідків радіаційної обстановки при руйнуванні (аваріях) атомних електростанцій [1]. Залежно від характеру й обсягу вихідної інформації завдання щодо виявлення й оцінки радіаційної обстановки можуть вирішуватися або методом прогнозування, або за даними радіаційної розвідки [5].

На основі методик прогнозування масштабів зараження при руйнуванні хімічно небезпечних об’єктів [6,7] сформовані алгоритми інформаційної моделі хімічної обстановки при довгостроковому та аварійному прогнозуванні [8].

Дифузійні процеси розповсюдження радіонуклідів і НХР в атмосфері враховуються при моделюванні атмосферної дисперсії в наслідок руйнування РХН об’єктів за допомогою комп'ютерних програм і алгоритмів, що імітують дисперсію забруднювача. Фактори, що мають певний вплив на масштаби поширення забруднюючих речовин об’єднані в одну групу для оптимізації числа вихідних даних процесу зараження довкілля в наслідок руйнування РХН об’єктів. Емпірично-статистичний метод, який застосовується у математичних моделях розсіювання викидів від стаціонарного джерела, при використанні достатньо простих параметрів враховує розсіювання домішок в атмосфері та дозволяє із досить високою точністю розрахувати зону розсіювання від викидів стаціонарного джерела. Дисперсійні моделі використовуються для прогнозування розповсюдження концентрацій під час генерування сценаріїв наслідків руйнування радіаційних і хімічно-небезпечних об’єктів та враховуються до алгоритмів інформаційних моделей радіаційної та хімічної обстановки.

Таким чином, дифузійні процеси розповсюдження радіонуклідів та небезпечних хімічних речовин в атмосфері, що враховуються при моделюванні атмосферної дисперсії під час генерування сценаріїв наслідків руйнування радіаційних та хімічно-небезпечних об’єктів за допомогою комп'ютерних програм і алгоритмів являються вихідними даними для формування інформаційних моделей радіаційної та хімічної обстановки.

Список використаних джерел

1. Методика прогнозирования и оценки последствий разрушений (аварий) атомных електростанций и предприятий химической промышленности. М. : Воениздат, 1991. 92 с.

2. Кузьменко Л.Ф., Блеко А.М., Бацовский О.В. Методика оцінки обстановки при аваріях на ПНО та екологічної обстановки на військовому об’єкті : метод. посіб. К.: НАОУ, 2001. С. 23–35.

3. Поплавець С.І, Гузченко С.В., Нікітін А.А. Деякі погляди щодо визначення обсягу заходів збору, обробки, аналізу, узагальнення та видачи інформації про хімічну, біологічну, радіологічну обстановку. Журнал наукових праць “Соціальний розвиток і безпека”. К.: НУОУ. 2023. Вип. 13, № 3, С. 184–195. https://doi.org/10.33445/sds.2023.13.3.12.

4. Поплавець С.І. Гишко Г.Б., Колмогоров О.В. Інтегрування дифузійних процесів розповсюдження радіонуклідів та небезпечних хімічних речовин до інформаційних моделей хімічної та радіаційної обстановки. Scientific Collection “InterConf”, (42): with the Proceedings of the 1st International Scientific and Practical Conference “Theory and

Practice of Science: Key Aspects" (February 19-20, 2021). Rome, Italy: Dana, 2021. P. 1115–1126. ISBN 978-88-32012-34-7. DOI 10.51582/interconf.19-20.02.2021.

5. Поплавець С. І. Гишко Г.Б., Овчаров О.В Формування інформаційної моделі радіаційної обстановки для генерування сценаріїв наслідків руйнування радіаційно-небезпечних об'єктів. Scientific Collection "InterConf", (41): with the Proceedings of the 7th International Scientific and Practical Conference "Scientific Horizon in The Context of Social Crises" (February 6-8, 2021). Tokyo, Japan: Otsuki Press, 2021. P. 1206–1212. ISBN 978-4-272-00922-0.

6. Про затвердження Методики прогнозування наслідків виливу (викиду) небезпечних хімічних речовин при аваріях на промислових об'єктах і транспорті /спільний наказ МНС України, Мінагрополітики, Мінекономіки, Мінекології № 73/82/64/122 від 27.03.2001 р. [електронний ресурс]. Режим доступу до сайту:http://zakon5.rada.gov.ua/laws/show/z0326-0.

7. Про затвердження Методики прогнозування наслідків виливу (викиду) небезпечних хімічних речовин під час аварій на хімічно небезпечних об'єктах і транспорті [Текст]: наказ Міністерства внутрішніх справ України від 29 лист. 2019 року № 1000. К., 2019. 67 с.

8. Поплавець С.І. Гишко Г.Б., Лазебник С.В. Формування інформаційної моделі хімічної обстановки для генерування сценаріїв наслідків руйнування хімічно-небезпечних об'єктів. Debats scientifiques et orientations prospectives du developpement scientifique: collection de papiers scientifiques "ΛΌГОΣ" aves des matériaux de la l conference scientifique et pratique international (Vol. 2), Paris, 5 février 2021. Vinnytsia-Paris: Plateforme scientifique européenne & La Fedeltà, 2021. P. 123–130. https://doi.org/10.36074/logos-05.02.2021.v2.

Попов М.О., Порохончук О.М., Попова Н.О.

РАДІОТЕХНІЧНА БАГАТОПОЗИЦІЙНА СИСТЕМА ПАСИВНИХ ПРИСТРОЇВ ЯК ДОДАТКОВЕ ДЖЕРЕЛО ІНФОРМАЦІЇ ПРО ПОВІТРЯНУ ОБСТАНОВКУ

Досвід російсько-української війни показав, що виявлення повітряних об'єктів, особливо з невеликою ефективною площею розсіювання та малими висотати польоту, засобами радіолокаційних станцій (РЛС), має деякі складнощі. У зв'язку з цим, не всі цілі можна вчасно виявити, супроводжувати та знищити.

Наряду з тим, досвід також показав, що малопомітний для РЛС повітряний об'єкт являються джерелом додаткової інформації і в залежності від типу випромінює власні сигнали:

- каналу телеметрії;
- каналу передачі цільової інформації.

У зв'язку з тим, авторами запропоновано використання пасивної багатопозиційної системи SDR-приймачів (Software-defined radio – система радіозв'язку, в якій програмне забезпечення використовується як для модуляції, так і для демодуляції радіосигналів) , розміщену додатково поблизу позицій підрозділів, оснащених РЛС у кількості від трьох і більше по периметру або у напрямку найбільш ймовірного напрямку руху безпілотних літальних апаратів (БпЛА).

Найбільш розповсюдженим методом визначення координат в пасивній багатопозиційній системі приймачів є різницево-далекомірний метод (РДМ), який заснований на вимірюванні різниці в часі затримки сигналу, що випромінює БпЛА в напрямку приймачів системи.

Сигнал, що випромінюється БпЛА, буде отриманий приймачами системи в різний час, який залежить від відстані між приймачами та БпЛА. Різниця в часі між двома

приймачами зіставляється з гіперболоїдом (в тримірному просторі), на якому знаходиться БпЛА.

В основі роботи РДМ покладено: вимірювання відносної затримки сигналів, які приймаються в трьох рознесених пунктах прийому, та визначенні лінії переміщення (гіпербол), а також вирахування координат точки перетину ліній переміщень.

Просторове положення БпЛА визначається по трьом різницям дальностей, які були виміряні в приймальних пунктах. Координати БпЛА визначаються як точка перетину гіперболоїдів обертання.

Різницево-далекомірний метод заснований на вимірюванні різниці ходу сигналів до прийомних позицій. Цей метод дозволяє використовувати як імпульсні, так і безперервні сигнали, в тому числі шумові і шумоподібні. Метод особливо ефективний у випадках, коли для обчислення різниці ходу застосовується базовокореляційна обробка, при якій вид сигналів немає значення.

Актуальність даного методу полягає у тому, що система пасивних приймачів може використовуватися як у комплексі з активною РЛС підрозділу, так і окремо, що забезпечує скритність підрозділу (під час вимкнутої РЛС) що підвищує живучість.

В роботі розглядається декілька варіантів використання пасивної багатопозиційної системи SDR-приймачів:

- сумісне використання РЛС та додатково мережі SDR-приймачів;
- окреме використання даної системи, як джерело цілевказівки наряду з цілевказівками РЛС підрозділів радіотехнічних військ.

Сумісне використання окремої РЛС та мережі SDR-приймачів зменшує сумарну похибку розрахунку координат повітряного об’єкту.

Використання пасивної багатопозиційної системи SDR-приймачів підвищую не якість отримання сигналу від джерела випромінювання, а підвищую якість точності виміру координат БпЛА, характеристикою якої являється величина середньоквадратичного відхилення.

Таким чином, використання пасивної багатопозиційної системи SDR-приймачів дозволяє:

- підвищити точність визначення координат повітряного об’єкту;
- забезпечує скритну роботу РЛС;
- підвищує живучість підрозділу.

Недоліками запропонованої системи є:

- необхідність у додаткових приймачах;
- ускладнення апаратної і програмної частини.

УДК: 004.056

Прокопенко Є.В., Мул Д.А.

РОЛЬ ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКИ В ДІЯЛЬНОСТІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

В умовах широкомасштабної збройної агресії російської федерації проти України поряд з протиборством на полі бою гостро постає питання захисту інформаційних та комунікаційних ресурсів держави. Противник не полишає спроб здійснити як комплексні кібернетичні впливи так і атаки з метою моніторингу політики безпеки того чи іншого інформаційного ресурсу. Особливу увагу ворог приділяє кібернетичним ударам по інфраструктурним, військовим, фінансовим та загальнодержавним системам електронних комунікацій.

В сучасних реаліях Державна прикордонна служба стикається зі значними викликами щодо забезпечення безпеки та захисту інформації з одного боку в умовах широкомасштабної збройної агресії російської федерації з іншого боку швидкого розвитку технологій. У зв'язку зі зростаючими загрозами кібернетичної атаки та необхідністю ефективного взаємодії з іншими військовими та правоохоронними органами, важливою стає роль технологій захисту інформації та кібербезпеки.

Державна прикордонна служба стикається з численними викликами, пов'язаними з захистом інформації, включаючи:

– несанкціонований доступ до інформації: – зловмисники можуть намагатися отримати доступ до конфіденційної інформації, такої як дані про прикордонний контроль, особисті дані мандрівників, або дані про операції з протидії контрабанді;

– втрата або крадіжка інформації: – інформація може бути втрачена або вкрадена через людську помилку, технічні збої, або кібератаки;

– пошкодження або руйнування інформації – кібератаки можуть призвести до пошкодження або руйнування інформації, що може мати серйозні наслідки для діяльності прикордонного відомства.

У цій статті розглянемо значення та можливий вплив кіберпротивника на рівні автоматизованих робочих місць, комп'ютерних мереж та радіомереж.

Автоматизовані робочі місця в прикордонній службі використовуються для обробки та аналізу великого обсягу інформації, що стосується пасажирів, вантажів, а також іншої інформації службового (бойового) характеру. З метою забезпечення конфіденційності, цілісності та доступності цієї інформації важливо використовувати сучасні технології захисту даних, такі як шифрування, аутентифікація та контроль доступу. Впровадження систем ідентифікації з двофакторною аутентифікацією та систем моніторингу забезпечує ефективний контроль над доступом до важливої для відомства інформації.

В Державній прикордонній службі України розгорнута та отримала комплексне застосування комунікаційна мережа Інтранет. Вона забезпечує високошвидкісні інформаційні потоки на всіх рівнях управління служби та надає доступ в глобальну мережу Інтернет. Комунікаційна мережа Інтранет прикордонної служби є важливим засобом зв'язку та обміну інформацією як усередині відомства, так і з іншими правоохоронними органами та військовими формуваннями. З огляду на постійно зростаючі загрози кібератак, необхідно використовувати ефективні засоби захисту мережі. В цьому контексті важливо впровадження механізмів виявлення та запобігання вторгнень (Intrusion Detection and Prevention Systems), що дозволяють вчасно реагувати на потенційні загрози та мінімізувати їхні наслідки. Можливими заходами захисту комп'ютерних мереж можуть бути наступні:

– сегментація мережі: – мережа повинна бути сегментована на різні зони з різним рівнем доступу;

– використання VPN: – віртуальні приватні мережі (VPN) повинні використовуватися для захисту конфіденційності даних при їх передачі через Інтернет;

– використання брандмауерів: – брандмауери повинні використовуватися для блокування несанкціонованого доступу до мережі;

– системи виявлення вторгнень (IDS): IDS повинні використовуватися для виявлення підозрілої активності в мережі.

Система радіозв’язку Держприкордонслужби отримала широке застосування не тільки як окремі сигменти радіомереж, а і у варіанті комплексного застосування комплексів радіозв’язку в поєднанні з корпоративною мережею Інтранет. Під час здійснення охорони (оборони) державного кордону радіомережі використовуються для забезпечення інформаційного обміну на відкритих та важкодоступних територіях, де застосування інших технічних засобів передачі інформації може бути недоступними або непрактичними. З огляду на специфіку цих систем, важливо використовувати криптогра-

фічні засоби захисту інформації, такі як шифрування даних та автентифікація користувачів. Забезпечення захищеності радіомереж дозволяє зберегти конфіденційність та цілісність інформації, переданої через ці канали зв'язку.

Розвиток технологій штучного інтелекту відкриває нові можливості для захисту інформації в Державній прикордонній службі України. Інтелектуальні системи можуть аналізувати великі обсяги даних у реальному часі та виявляти аномальні патерни, що вказують на потенційні загрози. Такі системи можуть автоматично реагувати на виявлені загрози або надавати рекомендації персоналу щодо подальших заходів. Використання інтелектуальних систем захисту дозволяє забезпечити високий рівень безпеки та реагувати на загрози швидко та ефективно, що є одним з найперспективніших шляхів розробки сучасних політик безпеки для інформації, яка циркулює в інформаційних системах Державної прикордонної служби України.

УДК 621.391

Прохорський С.І., Бондаренко О.Є., Сергієнко А.В., Бригадир С.П., Гетьман А.В.

ОЦІНКА СИСТЕМИ ПРОГНОЗУВАННЯ ВРАЗЛИВОСТЕЙ ТА ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У теперішній час практично у всіх сферах діяльності суспільства, проблеми інформаційної безпеки потребують першочергового вирішення тому що реалізується велика кількість проектів інформатизації. Переважна кількість реалізованих проектів інформатизації націлені для єдиного телекомунікаційного та інформаційного простору, щоб оптимізувати процеси обробки інформації великих об’ємів.

До шкідливої інформації, яка є проблемою інформаційної безпеки суспільства, відноситься інформація, якою користуються злочинці для інформаційного впливу, розробки нових стратегій спрямованих для залучення нових прихильників та збільшення впливу у соціальних мережах.

Для надійного забезпечення інформаційної безпеки суспільства проводиться аналіз, моніторинг та протидія розповсюдженню шкідливої інформації в соціальних мережах.

Метою тези є оцінка ефективності та адекватності системи прогнозування вразливостей та загроз інформаційної безпеки.

При зростанні засобів комп’ютерної техніки та їх використанням у сфері людської діяльності, обміном інформації в мережі між користувачами, шпигунства, доступу до конфіденційної інформації, конкурентністю у сфері інформаційних послуг суспільства, а також недостатньою кількістю кваліфікованих фахівців у даній сфері з’являється актуальність даної проблеми [3].

У зв’язку з цим є необхідність у проведенні захисту комп'ютерних систем від несанкціонованого доступу до конфіденційних даних та інших небажаних загроз.

Щоб оцінити систему прогнозування вразливостей та загроз інформаційної безпеки та коректності роботи інформаційної системи проводились експерименти з проведенням аналізу щодо потоку повідомлень інтернет-ресурсів [4]:

1. Зібрана класифікація вразливостей і загроз безпеки інформації , яка була отримана експериментальним шляхом, було створено найважливіші загрози та вразливості для інформаційної безпеки конфіденційних даних;

2. Отриманий набір правил, який містить кількість інтернет-ресурсів на форумі та рейтинг авторів від ймовірності виникнення вразливостей та загроз інформаційної безпеки конфіденційних даних;

3. В результаті відбору експертним шляхом форумів інтернет-ресурсів проведено збір текстових повідомлень;

4. За результатами отриманих вразливостей та загроз інформаційної безпеки отримано співвідношення з кількістю записів, які належать до бази знань;

5. Була обчислена кількість текстових повідомлень форумів інтернет-ресурсів, для використання результатів щодо вхідних параметрів інформаційної системи логічного нечіткого виводу;

6. Шляхом фільтрації даних отриманих текстових повідомлень був зроблений статистичний та семантичний аналіз. Для оцінки якості прогнозування інформаційної системи, є показники, які наведені в табл. 1.

Таблиця 1 - Показники якості прогнозування аналітичної системи

№ п/п	Назва, формула, опис
1	*MAPE* – середня абсолютна процентна помилка системи прогнозування $$MAPE = \frac{1}{h}\sum_{i=1}^{h}\left|\frac{f_{T,i} - y_{T+i}}{y_{T+i}}\right| \cdot 100\%, \quad (1)$$ де h - довжина інтервалу, на якому проводиться прогнозування загроз; $f_{T,i}$ - прогнозне значення часового ряду, отримане в момент часу T на i кроків наперед; y_{T+i} - значення часового ряду в момент часу $T+i$
2	*MAE* - середня абсолютна помилка системи прогнозування: $$MAE = \frac{1}{h}\sum_{i=1}^{h}\left| f_{T,i} - y_{T+i}\right|, \quad (2)$$
3	*RMSE* - квадратний корінь із середньої квадратичної помилки системи прогнозування: $$RMSE = \sqrt{\frac{1}{h}\sum_{i=1}^{h}\left(f_{T,i} - y_{T+i}\right)^2}, \quad (3)$$

Процентна помилка (*MAPE*) використовується для оцінки якості прогнозування загроз, а також для їх порівняння.

Щоб оцінити результати, які отримані, проведено розрахунки показників *MAPE, MAE, RMSE* (за формулами 1, 2, 3).

На основі дослідження потоку даних ресурсів реалізовано в інформаційно-аналітичній системі метод прогнозування вразливостей та загроз безпеки інформації, що дозволяє автоматизувати інформаційний процес виявлення загроз, який у свою чергу дає фахівцям з інформаційної безпеки змогу оцінити ступінь захищеності ресурсів та вжити відповідних заходів щодо знешкодження можливих загроз від комп'ютерних атак.

Список використаних джерел

1. Ленков, С.В. Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів / С.В. Лєнков, В.М. Джулій, А.М. Берназ, І.В. Муляр, І.В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2023. – Вип. №78. – С. 123-134.

2. Ленков, С.В. Метод протидії поширенню та виявлення шкідливої інформації в соціальних мережах/ С.В. Ленков, В.М. Джулій, Л.В. Солодєєва // Збірник наукових

праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №77. – С. 103-117.

3. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Сєлюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

4. Джулій, В.М. Модель потоку текстових повідомлень тематичних інтернет-ресурсів системи прогнозування інформаційної безпеки / В. Джулій, Н. Петляк, Ю. Хмельницький, О. Пахар // Вісник Хмельницького національного університету. Технічні науки. – 2022. – № 5. – С. 294-300.

УДК 621.391

Прохорський С.І., Бондаренко О.Є., Сергієнко А.В., Гетьман А.В.

ПРОВЕДЕННЯ АНАЛІЗУ ЗАСОБІВ МЕРЕЖЕВОГО ЗАХИСТУ ТА ЗАХИЩЕНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

На сьогодні, комп’ютерні системи державних та відомчих установ не здатні захиститись від атак навіть найнадійнішими системами захисту. Одна з причин – стандартні механізми захисту: ідентифікація, автентифікація, механізми обмеження доступу до інформації згідно з правами суб’єкта і криптографічні механізми. Тим не менш важливо, щоб дані системи були спроможні протистояти навіть автентифікованому та авторизованому зловмиснику.

Метою тези є висвітлення проблемних питань які виникли при аналізі системи виявлення вторгнень.

Системи виявлення вторгнень (Intrusion Detection Systems, IDS) і виконують дані функції шляхом реагування на загрози, поділяючись на системи виявлення зловживань (Misuse Detection Systems, MDS) і системи виявлення аномалій (Anomaly Detection Systems, ADS), які реєструють відхилення еволюції системи від нормального перебігу.

Засобами технології виявлення мережевих атак (МА) є апаратні та програмні системи виявлення атак, і базуються на сигнатурних та статистичних методиках виявлення на основі мережевих і хостових моделей. Нажаль, сучасні методики виявлення МА досить різнорідні і не зведені до уніфікованого критерію, відповідно якого можливо охарактеризувати ефективність їх застосування.

Важливими факторами створення засобів виявлення і протидії комп’ютерним атакам (КА) є:

1. Прозорість, при якій система виявлення та протидії КА функціонує у фоновому режимі.

2. Оптимальність, при якій розробка системи виявлення та протидії КА проводитися з урахуванням методів, які ефективно та достовірно виявляють комп’ютерні атаки.

3. Адекватність, для реалізації в системі виявлення та протидії КА проєктних рішень.

4. Повнота, яка базується на аналізі та використанні основних параметрів всіх програмних і технічних елементів пунктів управління автоматизованої системи.

5. Адаптивність, для періодичної та поступової зміни складу і характеристик програмних і технічних засобів АС, в залежності від розвитку та мінливості загроз сьогодення.

Система виявлення вторгнень (СВА) розміщується в середині локальної обчислювальної мережі (ЛОМ) таким чином, щоб система мала змогу спостерігати за підконтро-

льними їй сегментами мережі. Спостереженням займаються розташовані в системі кілька сенсорів.

До сенсорів відносяться мережеві інтерфейси та групи мережевих інтерфейсів, якими керує операційна система, як приклад мона навести кластер NIDS. На вхід сегмента встановлюється IDS, які захищені таким чином, щоб весь трафік сегмента проходив через дану систему.

При аналізі засобів мережевого захисту виявлені наступні переваги та недоліки:

– мінімізація вірогідності попадання зловмисного трафіку в сегмент за рахунок проходження всього трафіку через IDS;

– активне реагування на вторгнення зміною комбінацій (правил).

Недоліками є:

– поява ланки, яка при виході з ладу може впливати на працездатність всієї мережі;

– складність масштабування IDS;

– керуючий мережевий інтерфейс.

У мережі засоби мережевого захисту можуть використовувати мережеву, або хостову моделі загроз виявлення мереживих атак (МА). Виходячи з вищевказаного використовуються переваги відповідних моделей (методики та алгоритми), які беруть до уваги характеристики МА, такі як події, що реєструються у журналах (відповідної операційної системи; журналі додатків, які використовуються на хості міжмереживих екранів. Аналіз мережевого трафіку в даних засобах здійснюється безпосередньо у мережі, аналізуючи дані з технічних каналів зв'язку при використанні середовища передачі даних та канал утворюючого обладнання обчислювальної мережі. На сьогодні більшість відомих програмних продуктів відносяться до таких засобів.

Якісні характеристики інформаційної системи поділяються за наступними показниками:

– загальне число зв'язків;

– тимчасові характеристики якості ІС;

– середній час обслуговування;

– надійність обслуговування;

– достовірність передачі;

– можливість доступу.

Характеристики захищеності інформаційної системи включають в себе:

– інформацію, що обробляється в ІС надається вищий гриф секретності;

– перелік і склад устаткування технічних і програмних засобів, які належать до загальної структури схеми і складу ІС;

– тип ІС;

– обсяги основних інформаційних масивів і потоків;

– швидкість і продуктивність;

– відновлення працездатності після збоїв за відповідний проміжок часу та наявність засобів, які підвищують надійність та живучість;

– технічні характеристики каналів зв'язку;

– фізичні параметри компонентів ІС та їх розташування;

– умови експлуатації.

Основні проблемні питання: поєднання до єдиної системи виявлення и протидії атакам усіх принципів створення системи; збільшення переліку загроз; спроможність виявляти тільки деякі види атак; відповідальність за КА та вторгнення відсутня у нормативній законодавчій базі. Відповідно наведені проблемні питання потребують подальших досліджень переліку загроз та класифікації видів атак, а також розробки нормативної законодавчої бази та постійне її наповнення.

Список використаних джерел

1. Куссуль Н. Н., Соколов А. М.. Адаптивное обнаружение аномалий в поведении пользователей компьютерных систем с помощью марковских цепей изменяющегося порядка // Кибернетика и вычислительная техника.

2. J. Allen et al. State of the practice of intrusion detection technologies. TR CMU/SEI-99-TR-028, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, Jan. 2000.

3. D. Wagner and R. Dean. Intrusion detection via static analysis. In Proc. of the 2001 IEEE Symposium on Security and Privacy, pages 156–169, Los Alamitos, CA, May 14-16 2001

Процюк Ю.О., Паламарчук Н.А.,Фомкін Д.В., Куцаєв П.В., Побережець Т.В.

ВИКОРИСТАННЯ GPS-ТРЕКЕРІВ З МЕТОЮ НЕСАНКЦІОНОВАНОГО ОТРИМАННЯ ІНФОРМАЦІЇ ПРО МІСЦЕЗНАХОДЖЕННЯ ОСІБ ТА ПРЕДМЕТІВ

У наш час велику частку загроз для будь-якої інформації становлять засоби несанкціонованого (прихованого) отримання інформації – закладні пристрої (далі – ЗП), тобто штучно створений технічний канал витоку інформації від її джерела до зловмисника.

Найчастіше ЗП використовуються для перехоплення акустичної (мовної) та/або оптичної (видової) інформації, серед них такі як: радіомікрофони, направлені мікрофони, портативні диктофони, приховані відеокамери тощо. Проте, зі стрімким ростом технологій розширюються задачі, для яких використовуються ЗП та розширюються їхні технічні можливості (методи та режими роботи ускладнюються, їх випромінювання маскується на фоні цілком легальних сигналів), що в свою чергу ускладнює виявлення ЗП.

З теорії захисту інформації, ЗП можливо класифікувати за наступними ознаками: за видом інформації, що перехоплюється; за видом датчика перехоплення інформації; за сигналом передавання інформації (середовищем розповсюдження); за періодом роботи; за способом живлення; за способом встановлення; за діапазоном частот передавання інформації; за видом виконання та ін.

Однак, з початком повномасштабного військового вторгнення росії в Україну цінність має не лише перехоплена інформація, а і місцезнаходження певних осіб та/або предметів, маршрут їх переміщення. В цьому випадку, загрозу являють всілякі пристрої для встановлення місцезнаходження, до яких відносяться GPS-трекери, радіомітки, мітки тощо, які в разі несанкціонованого (прихованого) використання можливо застосовувати для відстеження місцезнаходження.

В Україні мали місце випадки використання GPS-трекерів (міток) в посилках для військових, гуманітарних вантажах, на об’єктах критичної інфраструктури та ін., які в подальшому були обстріляні противником. В деяких випадках, GPS-трекери встановлювалися щоб впевнитись, що посилка була доставлена адресату. Також були випадки передачі цивільних автомобілів для потреб військових, в яких з часом знаходили GPS-трекери, які вчасно не знімали власники котрі відстежували свій автотранспорт. Відповідно, зазначені пристрої та варіанти їхнього використання потребують детального вивчення, оскільки первинно являють загрозу життю та здоров’ю громадян.

Аналізуючи ринок “побутових” пристроїв для відстеження місцезнаходження можливо виділити трекер AirTag від компанії Apple, трекер SmartTag виробництва Samsung, розумну GPS-мітку від Xiaomi та ін., які в розрізі даної тематики доцільно розглядати як пристрої подвійного призначення. Загальний принцип їх дії розглянемо на прикладі трекеру AirTag (далі – AirTag, трекер).

AirTag – пристрій, що дозволяє знаходити речі, які знаходяться в безпосередній близькості або ті, що втрачені. В основі технології лежить принцип транслювання захище-

ного сигналу (місцезнаходження AirTag) на iPhone/iPad власника з використанням безпровідної технології Bluetooth. У разі відсутності прямого Bluetooth з'єднання з пристроєм власника, AirTag використовує під'єднання до будь якого ввімкненого Bluetooth iPhone/iPad, які знаходяться в зоні його дії (без їхнього відома). Чужий iPhone/iPad, який допомагає виявити AirTag, залишається анонімним – ні компанія Apple, ні власник трекера не можуть його визначити. Історія трекера та дані про його місцезнаходження на самому AirTag не зберігаються. Інші пристрої iPhone не можуть побачити трекер якщо власник поруч. Відстежити переміщення трекера може лише власник за допомогою ввімкненої функції "Локатора" на його iPhone, за умови що ввімкнені всі дозволи для функції "Локатор", а саме налаштування сповіщення "Локатора" та сповіщення відстеження. Виключення AirTag здійснюється шляхом вилучення з нього елементу живлення.

Розглянемо два варіанти використання AirTag для відстеження місцезнаходження, санкціонований та несанкціонований. Перший, це використання AirTag власником за прямим призначенням, коли він загубив свою річ де був фізично розміщений трекер і за допомогою функції "Локатор" на своєму iPhone може побачити де на даний час знаходиться трекер або останню точку його місцезнаходження. Як зазначалося вище, використовується пряме Bluetooth з'єднання з пристроєм власника або будь якого iPhone/iPad. Якщо трекер протягом тривалого часу знаходиться на з'єднані з будь яким пристроєм (не власника), то з часом (при ввімкненій функції "Локатор") на нього прийде повідомлення *"Знайдено мітку AirTag, що рухається разом із вами"* або трекер подасть звуковий сигнал через свій динамік. При ідентифікації трекера за допомогою функції "NFC" цього iPhone з'явиться повідомлення з посиланням на інформацію про даний трекер: серійний номер трекера, останні чотири цифри номера телефону її власника та повідомлення, що *"Цю річ загублено. Будь ласка, зателефонуйте мені. І номер телефону +**********"*.

Другий варіант, це використання трекера зловмисником, коли його несанкціоновано підкидають сторонній особі для відстеження її місцезнаходження. Перед цим, зловмисник спеціально може видалити механічним шляхом динамік з AirTag, і відповідно, звуковий сигнал не подаватиметься.

У разі, якщо стороння особа проти якої ведуться несанкціоновані дії, має iPhone, то за допомогою включеної функції "Локатор", вона зможе побачити посилання з інформацією про серійний номер трекера та останні чотири цифри номера телефону зловмисника, і детальну інформацію коли і де було здійснено підключення до неї та маршрут за яким вона рухалася (від точки підключення до точки коли прийшло сповіщення). Всі ці заходи щодо локалізації трекерів можливі лише при постійному ввімкнені функцій Bluetooth та геолокації на iPhone, в іншому випадку, сповіщення приходити не будуть і факт використання AirTag буде прихованим.

У пристроях з операційною системою Android пошук трекерів здійснюється через застосунок Google, який функціонально аналогічний до функції "Локатор" на пристроях iPhone.

З метою убезпечення себе від несанкціонованого відстеження місцезнаходження з використанням трекерів AirTag, власникам пристроїв з бездротовими технологіями можливо надати наступні рекомендації:

1) для користувачів iPhone:
   - постійно має бути ввімкнене Інтернет з'єднання; ввімкнений Bluetooth; ввімкнені служби локації;
   - на пристроях мають бути встановлені останні оновлення операційної системи (не нижче версії 14.5) та функції "Локатор" з усіма дозволами;
   - або, періодично вмикаючи Bluetooth та геолокацію для "Локатора" здійснювати моніторинг трекерів.

2) для користувачів з операційною системою Android:

- постійно має бути ввімкнене Інтернет з'єднання; ввімкнений Bluetooth; ввімкнені служби локації;
- на пристроях має бути встановлена операційна система не нижче версії 6.0 та останні оновлення застосунку Google;
- або, у застосунку Google через функцію "Ручне сканування" здійснювати моніторинг трекерів.

UDC 004.896 : 623.746.-519

Parkhomenko D.

FORMALIZATION OF CONTROL OF A INTELLIGENT UNMANNED AERIAL VEHICLES GROUP

The formalization of information technology for intelligent control of a group of heterogeneous unmanned aerial vehicles in an antagonistic environment is considered.

Management of a group of UAVs is carried out using an integrated approach, which includes the development of algorithms, the use of advanced technologies, ensuring safety and compliance with legislation. It is being actively researched and developed in various fields including military, civil aviation, scientific and commercial applications.

To ensure the autonomy of UAV actions in a group that performs a common task, it is necessary to develop decision-making methods for the distribution of tasks and the execution of actions. To do this, it is necessary to formalize the tasks of UAV activity in a group, identify individual subtasks and find methods for solving them.

Decomposition of tasks for controlling UAVs in a group:

Subtask 1. Determining the rational composition of the group to solve the problem. The problem of making a decision in the minds of limitations is solved. Depends on the spatial scope, data on the goals and conditions of action and available resources. It is complicated by the presence of uncertainty in a priori data and the forecast of the level of environmental aggressiveness for the period of the group's flight to its destination.

Subtask 2. Monitoring the operation areas using the information means of the UAV group, identifying target objects and assessing the situation. The task of making a decision to assess the situation is being performed.

Subtask 3. Target distribution - distribution of a group of specific actions over target objects among UAVs. The task of making a decision on target allocation is being performed.

Subtask 4. Monitoring the results of work and the technical condition of group elements. Reconfiguration of the UAV; transition to subtask 3 with new conditions.

The solution to the assigned subtasks is not ordered in time and depends on conditions that change during the task.

The solution to the formalization of the goal distribution subtask is considered in detail. The subtask is solved autonomously, taking into account the importance of each goal and the a priori probabilities of successful servicing by the UAV squad for each distribution option, which corresponds to the maximum integral efficiency indicator.

References

1. Xia, C. and Yudi, A. Multi – UAV path planning based on improved neural network / 2018 Chinese Control and Decision Conference (CCDC). Shenyang, China, 2018. P. 354-359. DOI: 10.1109/CCDC.2018.8407158.

2. Varatharasan, V., Rao, A. S. S., Toutounji, E., et al. Target Detection, Tracking and Avoidance System for Low-cost UAVs using AI-Based Approaches / 2019 Workshop on

Research, Education and Development of Un-manned Aerial Systems (RED UAS). Cranfield, UK, 2019. P. 142-147. DOI: 10.1109/REDUAS47371.2019.8999683.

4. Li, C. Artificial Intelligence Technology in UAV Equipment / 2021 IEEE/ACIS 20th International Fall Con-ference on Computer and Information Science (ICIS Fall). Xi'an, China, 2021. P. 299-302. DOI:10.1109/ICISFall51598.2021.9627359.

Равлюк В.В., Ваврічен О.А.

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ РАДІОЗВ'ЯЗКУ В СИСТЕМІ ЗВ'ЯЗКУ ДЕРЖПРИКОРДОНСЛУЖБИ УКРАЇНИ

Відомо, що сучасні принципи організації зв'язку та технічні характеристики засобів радіозв'язку підрозділів зв'язку Держприкордонслужби України не повністю задовольняють потреби управління органами та підрозділами прикордонного відомства при організації оперативно – службової діяльності так і в сучасному бою.

Організація та підтримання зв'язку під час управління органами та підрозділами Держприкордонслужби України в бойових умовах, при переміщені командирів (штабів), а також зв'язку із прикордонними нарядами які здійснюють охорону державного кордону здебільшого організовується за допомогою засобів радіозв'язку.

При організації зв'язку засобами радіозв'язку виділяють наступні переваги: простота та оперативність організації зв'язку; встановлення зв'язку з підрозділами на значному віддалені, а також місцезнаходження яких невідомо; передача інформаційних повідомлень через територію яка захоплена противником; радіохвилі поширюються на місцевості яка забруднена радіоактивними елементами; встановлення зв'язку з динамічними об'єктами на суші, повітрі та воді; передача команд та сигналів одночасно великій кількості кореспондентів тощо.

На сьогодні існує кілька способів організації радіозв'язку, кожен з яких може бути використаний залежно від конкретних потреб, умов та обставин, серед них способи організації радіозв'язку за радіонапрямком та радіомережею.

Радіонапрямок - це спосіб організації радіозв'язку лише між двома пунктами управління (штабами) при якому для кожного із них виділяється радіостанція що працює на радіоданних встановленних для цього напрямку.

Радіомережа - це спосіб організації радіозв'язку між трьома і більше пунктами управління (командирами, штабами).

В залежності від призначення радіомережі (радіонапрямки) в прикордонному відомстві поділяються на постійно діючі та чергові.

У постійно діючих радіомережах (радіонапрямках) радіообмін між кореспондентами здійснюється безперервно, по мірі необхідності.

При організації чергової радіомережі (радіонапрямку) одна радіостанція безперервно працює на прийом, а інша включається лише для ведення радіообміну.

Вимоги сьогодення диктують потребу у додаткових способах організації радіозв'язку, таких, як резервний та прихований.

При організації резервних радіомереж (радіонапрямків) радіообмін розпочинається за додатковою командою, у разі відсутності можливості обміну повідомленнями в основних радіомережах (радіонапрямках).

Приховані радіомережі (радіонапрямки) призначені для зв'язку із особливо важливими кореспондентами. Їх використовують для передачі найбільш важливих сигналів, команд, наказів та розпоряджень, з дозволу керівника вищого штабу.

Також при організації радіозв'язку взаємодії доцільно будувати наступними способами: створення спеціальних радіомереж (радіонапрямків) взаємодії; спільна робота в

інших радіомережах; за допомогою груп які прибувають для взаємодії з власними засобами зв'язку.

Таким чином, запровадження додаткових способів організації радіозв'язку та взаємодії є одним з тих рішень, що позитивним чином вплине на удосконалення системи зв'язку та забезпечення високої якості зв'язку, та управління органами (підрозділами) Держприкордонслужби України в цілому.

УДК 355.004.

Радзіковський С.А., Колесник В.О.

ДО ПРОБЛЕМ КІБЕРБЕЗПЕКИ ВІЙСЬКОВОЇ ІНФРАСТРУКТУРИ В УМОВАХ ЗБРОЙНОГО ПРОТИСТОЯННЯ

В контексті російсько-української війни, коли рф як держава-агресор є основним джерелом загроз кібербезпеці України, здійснюючи розвідувально-підривну діяльність у кіберпросторі, акції інформаційно-психологічних операцій та інших форм ведення "гібридної війни", процес забезпечення кібербезпеки військової інфраструктури передбачає, з одного боку, добування відомостей та інформації, що циркулює в інформаційних системах і комп'ютерних мережах, у тому числі з використанням несанкціонованого доступу, та їх обробка за допомогою апаратно-програмних засобів, а з іншого боку, виявлення, вивчення та систематизація небезпечних джерел кіберзагроз, що вимагає використання абсолютно нових інформаційних технологій (ІТ) і технічних прийомів.

Внаслідок бурхливого розвитку ІТ і глобальної інформатизації практично всі види озброєння та військової техніки містять електронні та інформаційні компоненти, а бойові дії плануються та здійснюються на єдиному інформаційному фоні за кібернетичними циклами і техніками. До найбільш важливих елементів військової інфраструктури, враховуючи ступінь ефективності управління військами та зброєю завдяки локальним і глобальним інформаційно-комунікаційним системам (ІКС), слід віднести наступні: системи автоматизації, автоматизовані системи управління (АСУ), комплекси оперативного управління силами та засобами (пункти управління, вузли зв'язку, засоби спостереження та навігації тощо), системи управління зброєю. Крім того, інтенсивно розвиваються, впроваджуються та застосовуються технічні системи (засоби) розвідки, робототехнічні (безпілотні, безекіпажні) системи (комплекси) повітряного, наземного та морського (надводного, підводного) базування. Взагалі об'єктивною загальновизнаною реальністю став факт, який засвідчує збереження до певної міри стратегічного балансу, системи противаг і міжнародних угод у сфері звичайних озброєнь і зброї масового ураження, проте питання паритету в кіберпросторі залишається відкритим і проблемним.

Зрозуміло, що показниками інформаційної безпеки (ІБ) військової інфраструктури від кіберзагроз є конфіденційність, доступність і цілісність інформації або комплекс заходів, спрямованих на забезпечення захисту інформації від несанкціонованого доступу. Вплив на будь-який з цих компонентів можна розглядати, як кібератаку. Об'єктом атаки може бути персональна електронно-обчислювальна машина (ПЕОМ), мережевий пристрій, інформаційна мережа або система в цілому. Головною метою кіберзахисту є прогнозування кіберзагроз і відбиття кібератак на відповідний об'єкт військової інфраструктури. Для вирішення цієї мети необхідно знати основні методи добування даних, несанкціонованого доступу (впливу), що використовує противник. Перед нашим військовим керівництвом постає питання щодо зосередження зусиль на мінімізацію наслідків дії потенційних і реальних загроз.

Аналізуючи особливості першочергових заходів кіберзахисту військової інфраструктури, необхідно відмітити найбільш суттєві серед них: створення системи раннього

виявлення інформаційних небезпек (викликів, загроз, впливів); налагодження ефективної системи кіберзахисту військових об'єктів з урахуванням їх категорій за ступенем уразливості; підвищення ефективності інформаційно-аналітичної роботи суб'єктів інформаційної безпеки; створення та постійне оновлення бази даних порушників і порушень. Крім того, необхідно забезпечити умови для дотримання режиму експертного контролю та нерозповсюдження несертифікованих програмно-апаратних засобів і систем, комп'ютерної техніки, оперативного реагування на інциденти, що пов'язані з виведенням із ладу військових ІКС, а також налагодження каналів формального та неформального обміну інформацією стосовно загроз комп'ютерної злочинності та кібертероризму.

Основними пріоритетами підвищення рівня захищеності військової інфраструктури мають бути: забезпечення комплексного підходу до вирішення завдань ІБ з урахуванням необхідності диференціювання її рівнів; розробка паспортів інформаційних небезпек – викликів, загроз, впливів; оцінка уразливості об'єктів; розвиток і вдосконалення захищених засобів обробки інформації; забезпечення ефективного моніторингу стану ІБ тощо.

У рамках протистояння гібридній агресії рф експертне середовище розглядає можливість управління трьома окремими напрямками з різними завданнями, які продиктовані потребами національної безпеки України а саме:

а) кіберрозвідка – має розвідувати загрози національній безпеці в кіберпросторі; здобувати розвідувальну інформацію в інтересах уряду, військово-політичного керівництва держави через кіберпростір; шукати та оцінювати вразливості ІКС противника та критичних елементів його інфраструктури;

б) кібервплив – до його сфери входять: підготовка та проведення стратегічних наступальних кібероперацій; підтримка кібердій оперативного рівня; розробка інструментів кібервпливу, кіберзброї (програмного забезпечення тощо); створенням повного циклу кібервпливу; маскуванням кібердій; демонстраційні дії; пошук та оцінка вразливостей ІКС противника;

в) кіберзахист – має опікуватись: підготовкою та проведенням оборонних кібероперацій; виявленням нових кіберзагроз; розробленням алгоритмів і засобів протидії новим загрозам; виявленням кіберінцидентів та кібератак і реагуванням на них; ліквідацією наслідків кіберінцидентів і кібератак.

Відповідно, шляхами досягнення вагомих переваг у кіберпросторі для забезпечення перемоги у збройному протистоянні з агресором можуть бути:

– підвищення рівня кіберзахисту об'єктів критичної інфраструктури держави, насамперед тих, що розташовані в районах ведення бойових дій;

– вжиття заходів для вдосконалення комплексної системи кібербезпеки, яка виконувала би функції на випередження кібератак, ідентифікації джерел кіберзброї та її фінансування;

– здійснення критичного аналізу кадрового забезпечення підрозділів кібервійськ, їхньої укомплектованості, матеріально-технічної забезпеченості;

– вдосконалення форм і засобів ведення боротьби у кіберпросторі, підвищення ефективності використання кіберзброї.

На завершення слід зазначити наступне:

1) для ведення ефективних дій у кіберпросторі держава повинна володіти необхідними інструментами та можливостями з нейтралізації реальних і потенційних загроз національній безпеці України;

2) російсько-українське протиборство у кіберпросторі продемонструвало необхідність об'єднання кіберструктур усіх складових сил безпеки і оборони держави в єдину систему, подібну до кібервійськ держав-членів НАТО;

3) перемогти Україні у війні, в тому числі у кіберпросторі, допоможе міжнародне партнерство, а напрямом подальших досліджень слід вважати обґрунтування шляхів

об’єднання зусиль суб’єктів національної системи кібербезпеки із відповідними структурами країн-партнерів.

На нашу думку, найефективніший спосіб протиборства в кіберпросторі – збільшення інвестування в кібербезпеку, координація зусиль складових сил безпеки і оборони держави у сфері кібероборони.

УДК 621.396

Раєнко О.С.

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ РАДІООБМІНУ МІЖ ПІДРОЗДІЛАМИ НА ЛІНІЇ БОЙОВОГО ЗІТКНЕННЯ ЗА РАХУНОК ПІДТРИМАННЯ БЕЗПЕКИ ЗВ’ЯЗКУ ТА ІНФОРМАЦІЇ

На сьогоднішній день в умовах сучасної війни використання радіозв’язку є важливим він має свої ризики та потенційні небезпеки. Як відомо, радіо, один з основних засобів зв’язку у всіх арміях світу, а в багатьох випадках – єдиний засіб, здатний при правильній організації ліній радіозв’язку і вмілому їх використанні забезпечити безперервне управління військами в самих складних умовах обстановки та при знаходженні командирів і штабів на місці та під час руху. Дотримання правил безпеки під час використання радіозв’язку допоможе забезпечити ефективну та безпечну комунікацію.

Із самого початку повномасштабної війни проти України РФ почала дуже активно використовувати різні засоби порушення роботи системи управління за рахунок виведення з ладу засобів радіозв’язку.

Радіозв'язок є основою для обміну інформацією з пересувними об'єктами, передача та прийом інформації на відстані з допомогою радіопередавачів і радіоприймачів відбуваються за рахунок розповсюдження радіохвиль у просторі, що забезпечує керування органами та підрозділами.

В умовах сучасного загальновійськового бою роль радіозв'язку ще більш зростає, стає основним засобом управління військами. Це зумовлено насиченням військ колективною швидкодіючою зброєю, ракетно-ядерними і зенітно-ракетними комплексами, армійською авіацією, бойовими машинами піхоти і т.д., бойова ефективність яких знаходиться в прямій залежності від безперервності управління ними. У сучасному бою найважливішою умовою досягнення успіху є чітка взаємодія всіх родів військ і сусідів по меті, місцю і часу. Для того, щоб досягнути поставленої мети, всі повинні діяти погоджено, а це можливо тільки при наявності зв'язку між ними.

Безпека радіозв'язку досягається: застосуванням апаратури зв'язку, що засекречує, дотриманням правил її експлуатації; попереднім шифруванням і кодуванням інформації, використанням таблиць позивних і документів прихованого управління військами; обмеженням кола осіб, що допускаються до ведіння переговорів по дозволених до застосування відкритих каналах зв'язку, застосуванням ефективних способів паролювання і апаратури імітозахисту; перевірки автентичності отриманих повідомлень шляхом зворотної передачі прийнятого тексту; суворим дотриманням правил встановлення зв'язку, ведіння переговорів; виконанням вимог режиму секретності при обробці і зберіганні інформації в автоматизованих системах управлінь, на вузлах, станціях і апаратних зв'язки.

Отже, радіозв'язок може організовуватись по радіонапрямкам і радіомережах. Застосування того або іншого способу його різновиду в кожному окремому випадку залежить від конкретних умов обстановки, призначення даного зв'язку, міри її важливості, специфіки бойових дій даного роду військ, характеру і особливостей організації управ-

ління, потреби в обміні інформацією, необхідність маскування від радіорозвідки противника і захисту від його радіоперешкод, наявності радіозасобів та інших чинників.

УДК 623.4.017

Рафальський Ю.І., Левченко В.С.

АНАЛІЗ ЗАХОДІВ ЩОДО ПЕРЕВІРКИ ГОТОВНОСТІ ОБСЛУГИ РАДІОЛОКАЦІЙНОЇ СТАНЦІЇ ДО ВИКОНАННЯ БОЙОВОГО ЗАВДАННЯ

Досвід ведення війни, що спричинена нападом російської федерації (рф) на Україну свідчить про те, що збройні сили рф використовують велику кількість різних типів засобів повітряного нападу (ЗПН). На момент початку вторгнення російська армія мала значну перевагу в авіації. Повітряно-космічні сили рф налічували понад 130 спеціалізованих важких бомбардувальників, близько 600 спеціалізованих та багатоцільових винищувачів, а також понад 260 штурмовиків; з українського боку їм протистояло приблизно 70 винищувачів та 40 штурмовиків радянських моделей із застарілими радарами та ракетами. Це мало забезпечити панування росії у небі і повну поразку Збройних Сил України (ЗСУ).

Однак російським силам не вдалося в перші дні вторгнення вивести з ладу українську систему наземної ППО через погане планування операцій, недостатнє оснащення літаків, погано навчених пілотів, а також успішні дії ЗСУ. Удари ракетами та дронами стали ключовим засобом ведення росією бойових дій в Україні, проте ця обставина лише наголошує на нездатності російської армії на активні операції з використанням авіації.

Щоб прорвати систему ППО України, атаки включають кілька хвиль: безпілотники, що летять на низькій швидкості, потім дозвукові крилаті ракети і, на останок, балістичні ракети. Для їхнього відображення Україна використовує гібридну систему ППО FrankenSAM, створену за сприяння США та що складається з мобільних підрозділів, оснащених зенітними ракетами Stinger та великокаліберними кулеметами, засобів ППО середньої дальності IRIS-T та SAMP/T, а також комплексів Patriot, які здатні збивати балістичні ракети. Завдяки FrankenSAM Україні вдається перехоплювати переважну більшість російських ракет.

Велику роль в своєчасному виявлені ЗПН рф відіграють радіотехнічні війська Повітряних сил ЗСУ, які призначені для безперервного ведення радіолокаційної розвідки повітряного простору і видачі радіолокаційної інформації на старші, забезпечувані та взаємодіючі КП. Свої завдання РТВ виконують в ході несення бойового чергування. Для цього в РТВ призначаються чергові бойові обслуги (ЧБО) командних пунктів (КП) радіотехнічних бригад і підрозділів, засоби радіолокації та зв’язку, комплекси засобів автоматизації. Підготовка та допуск до бойового чергування осіб чергової бойової обслуги здійснюється згідно відповідних наказів та інструкцій. До підготовки ЧБО обладнаються спеціальні навчальні класи, де напередодні дня заступання на бойове чергування здійснюється підготовка та перевірка осіб бойової обслуги до несення бойового чергування.

В умовах ведення повномасштабної війни рф проти України значна кількість радіотехнічних підрозділів знаходяться на бойових позиціях, місцезнаходження яких постійно змінюється. В цих умовах для підготовки ЧБО необхідно розробити та використовувати тести для перевірки готовності до виконання бойового завдання з відповідними питаннями по функціональним обов’язкам бойових обслуг. Це дозволить підтримувати гідний рівень підготовки осіб бойової обслуги до виконання бойового завдання.

УДК 621.396.96

Рафальський Ю.І., Шишина І.Г.

АНАЛІЗ СПОСОБІВ ЗАХИСТУ РАДІОЛОКАЦІЙНИХ СТАНЦІЙ ВІД ПРОТИРАДІОЛОКАЦІЙНИХ РАКЕТ

Досвід ведення війни, що спричинена нападом рф на Україну свідчить про те, що перевага у повітрі будь-якої із сторін не може бути досконалою без зниження бойових можливостей угрупування протиповітряної оборони (ППО) противника. В ході війни використовувались протирадіолокаційні ракети (ПРР) типу Х-31 та Х-58 з літаків МіГ-29, СУ-27, СУ-34, СУ-35. Головним призначенням ПРР є знищення оглядових РЛС, ЗРК та радіостанції зв'язку.

У системах ППО сучасні оглядові радіолокаційні станції (РЛС) є найважливішими джерелами інформації про повітряну обстановку. За своїм призначенням оглядові РЛС першими вступають у контакт із повітряним противником і нині у зв'язку з бурхливим розвитком високоточної зброї оглядові РЛС перетворилися на першочергові мети поразки. Особливу небезпеку для оглядових РЛС є така високоточна зброя як ПРР. У зв'язку із зростанням застосовуваної кількості ПРР та їх активним удосконаленням підвищується актуальність захисту від них різних радіолокаторів військового призначення. Своєчасне виявлення ПРР сприяє збільшенню промаху при наведенні ПРР на оглядові РЛС (за рахунок проведення спеціальних заходів) та призводить до підвищення ймовірності захисту оглядових РЛС від ПРР.

Значна потужність випромінювання оглядових РЛС та обмежені можливості щодо зміни спектру електромагнітного випромінювання в конкретних РЛС, слабка стійкість до впливу вражаючих факторів боєприпасів, а також відсутність активного захисту від самонавідної зброї обумовлює високу ефективність ПРР.

Найбільш вразливими для ПРР є саме оглядові РЛС, які змушені тривалий час перебувати в увімкнутому стані та не мають засобів активного захисту. Для захисту оглядових РЛС старого парку застосовуються засоби та способи пасивного захисту, а саме відволікаючі пристрої, зміна режимів роботи – вимкнення випромінювання, заборона випромінювання у секторі, режим "Мерехтіння". Очевидно, що ефективне використання засобів захисту від ПРР можливе при своєчасному виявленні та розпізнаванні протирадіолокаційних ракет. Проблема полягає в тому, що ПРР є малорозмірними високошвидкісними цілями, час їх знаходження в зоні видимості складає кілька десятків секунд. Тому так важливо своєчасно виявити ПРР для захисту оглядових РЛС.

Найефективнішим способом захисту є створення комплексної системи захисту оглядових РЛС від ПРР в основу якої покладено способи, що сприяють зменшенню інформації про об'єкт самонаведення-РЛС та зміщенню точки наведення ПРР від місцезнаходження РЛС.

УДК 621.396

Рачок Р.В., Хоптинський Р.П.

ІМОВІРНІСНИЙ ПІДХІД ДО МОДЕЛЮВАННЯ СЕНСОРНОЇ РАДІОМЕРЕЖІ З УРАХУВАННЯМ СТОХАСТИЧНОЇ ПРИРОДИ ОСНОВНИХ ФАКТОРІВ ЯКІ ВПЛИВАЮТЬ НА ВІРНІСТЬ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Охорона кордонів провідними державами світу здійснюється з використанням сучасних інженерних засобів. Державною прикордонною службою України також застосовується значна кількість інженерних засобів. Концепція інтелектуального кордону передбачає ще більше впровадження таких засобів на основі різноманітних датчиків (датчики руху, сейсмічні датчики, камери спостереження тощо). Одним з важливих завдань при цьому є забезпечення ефективної передачі даних, які отримуються в результаті їх роботи. Для вирішення цього завдання, зокрема, можуть бути використані сенсорні радіомережі. Зараз існує багато різних радіомодулів, таких як NRF24L01, які можуть бути використані при створенні сенсорних радіомереж. З метою забезпечення ефективного функціонування цих мереж необхідно врахувати зниження імовірності вірної передачі інформації при збільшенні дальності між їх вузлами.

Оцінка можливості радіозв'язку може бути проведена на аналітичному рівні, з урахуванням потужності передавача, характеристик антен та чутливості приймача. Однак на радіозв’язок може суттєво впливати комплекс стохастичних факторів, таких як погодні умови, рельєф місцевості, радіо-завади. Тому пропонується методика експериментального визначення імовірності наявності зв'язку між вузлами сенсорної радіомережі. Ця методика передбачає передачу тестових повідомлень між вузлами з контролем їх прийому в умовах впливу стохастичних факторів. Із збільшенням відстані між вузлами кількість успішно прийнятих повідомлень почне зменшуватися. Коли це зменшення досягне критичного рівня, відстань фіксується. Такі дослідження в умовах зміни впливу стохастичних факторів повторюються з метою отримання необхідної кількості даних для подальшої обробки. На основі цих даних отримується аналітичний вираз ймовірності наявності зв'язку між вузлами сенсорної радіомережі в залежності від відстані між ними.

Відстань між вузлами сенсорної радіомережі також можна розглядати як випадкову величину. Для отримання функції густини імовірності цієї відстані проведений обчислювальний експеримент в якому в межах заданої смуги вздовж частини державного кордону випадковим чином розміщено N вузлів сенсорної радіомережі. На основі статистичних даних про відстані між сусідніми вузлами проведений їх імовірнісний опис.

Співвідношення щодо залежності імовірності наявності зв’язку від відстані між сусідніми вузлами сенсорної радіомережі разом з імовірнісним описом цієї відстані при заданій густині розподілу вузлів можуть бути використані для раціональної побудови сенсорної радіомережі.

Рижов Є.В.

ПЕРСПЕКТИВНА СИСТЕМА СИТУАЦІЙНОЇ ОБІЗНАНОСТІ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

На сьогоднішній день для ефективного управління військами важливе значення має швидкість надходження, обробка, передача та використання інформації, а також спосіб її зберігання. Командиру для прийняття обґрунтованого і виваженого рішення необхідно отримати, узагальнити та опрацювати великий об’єм різноманітної інформації, яка в

умовах сучасного бою дуже швидко змінюється. Одним із засобів ситуаційної обізнаності, який розробляється в Збройних Силах України є програмно-апаратний комплекс (далі – ПАК) “ICoMWare” призначений для інформаційної підтримки керівників органів управління тактичної ланки, командирів окремих підрозділів (бойових груп, бойових машин, розрахунків та ін.), забезпечення їх ситуаційної обізнаності та підвищення ефективності взаємодії підрозділів в умовах бойової обстановки шляхом створення єдиного інформаційного простору на мережецентричній основі. Зовнішій вигляд ПАК-поано на рис 1.

Рисунок 1 – Вигляд програмно-апаратного комплексу

Кожен із варіантів програмно-апаратного комплексу складається з:
– апаратної компоненти;
– програмної компоненти;
– комплекту кабелів;
– монтажного комплекту;
– комплекту програмної документації;
– комплекту експлуатаційної документації;
– комплекту запасних частин, інструменту та приладдя.

Апаратна компонента ПАК включає:
– тактичний мережевий обчислювальний модуль;
– термінал відображення та введення інформації;
– модуль GPS-навігації.

ПАК “ICoMWare” забезпечує наступні основні сервіси:
– ситуаційну обізнаність (створення єдиної картини тактичної обстановки);
– збір, обробку даних про свої війська та війська противника;
– спільну роботу щодо планування бойових дій;
– інформаційну підтримку прийняття рішень;
– обмін повідомленнями та ведення тактичного чату;
– контроль готовності до виконання завдання;
– контроль стану каналів зв’язку;
– передачу голосових повідомлень;
– синхронізацію тактичної обстановки;
– автоматичне визначення типу та параметрів підключеної радіостанції;
– циркулярний або вибірковий обмін інформацією з іншими тактичними комп’ютерами;
– автоматичний збір даних про топологію радіомережі та автоматичну побудову мережі передачі даних;
– інтеграцію з іншими системами та програмними комплексами;
– підключення датчиків, сенсорів, відеокамер, GPS-навігації тощо;
– підключення засобів електронної розвідки (електронних біноклів, далекомірів,

приладів нічного бачення, тепловізорів, БПЛА) через додатковий інтеграційний модуль;

– ідентифікацію та автентифікацію користувачів в системі;

– розподіл інформації на тактичну та технологічну;

– криптографічний захист інформації;

– моніторинг дій користувачів;

– різні права користувачів (ролі).

Таким чином, сьогодні ” забезпечує широкий спектр можливостей:

– робота з електронною картою (навігація по карті та зміна масштабу карти, вимірювання відстаней, довільне рисування, відображення карти у режимі 3d, фільтрація відображення та обміну інформації по шарам, здійснення пошуку населеного пункту за назвою, або об’єкту за вказаними координатами, підтримка та автоматичний перерахунок різних систем географічних координат тощо) (рис. 2);

Рисунок 2 – Робота з ПАК “ICoMWare

– нанесення тактичної обстановки (з використанням генератору тактичних знаків, шаблонів знаків та їх швидкого пошуку, за допомогою швидкого вибору тактичних знаків, нанесених раніше, коригування тактичних знаків з використанням ампліфікаторів, нанесення площадних знаків, створення довідки тактичного знаку з можливістю додавання фотоінформації);

– прокладання маршрутів по дорогах та пересіченій місцевості з розрахунком довжини маршруту, середньої витрати пального та кількості дозаправок (в залежності від типу транспортного засобу);

– запис треків руху з розрахунком довжини треку, тривалості, середньої швидкості;

– отримання інформації щодо радіусів ураження основною і додатковою зброєю обраної бойової одиниці;

– отримання інформації щодо зон прямої видимості;

– отримання інформації щодо показників боєздатності;

– отримання інформації про швидкість руху, відстань та дирекційний кут на власну бойову машину;

– отримання інформації щодо географічних координат та абсолютної висоти над рівнем моря;

– перегляд показників боєздатності підрозділу;

– внесення показників боєздатності в автоматичному режимі за наявності відповідних датчиків;

– внесення показників боєздатності в ручному режимі;

– спілкування у тактичному чаті (обмін формалізованими текстовими повідомленнями, передача формалізованих команд, формування та передача сигналів бойового

управління та оповіщення, обмін тактичною обстановкою, обмін графічними повідомленнями);

– використання встановлених на борту (шоломі військовослужбовця) відеокамер (при наявності), надсилання знімків, знімки з камери та нанесення на них позначок;

– забезпечення сумісності з різними типами БпЛА («Лелека-1000», «Фурія») та програмами («Термінал», «Кропива»).

Враховуючи та узагальнюючі наведене вище, можна сказати, що ПАК "ICoMWare" дозволяє:

– створити єдине інформаційне середовище в підрозділах тактичної ланки управління;

– забезпечити інформаційну підтримку командирів окремих підрозділів (бойових груп, бойових машин, розрахунків та ін.) в ході бойових дій в режимі реального часу;

– підвищити в рази ефективність управління, бойових можливостей підрозділів та ведення бойової роботи особовим складом тактичної ланки, взаємодії підрозділів в умовах бойової обстановки шляхом створення єдиного інформаційного простору на мережецентричній основі;

– автоматизувати процеси управління підрозділами у режимі реального часу (обміну текстовою, графічною та іншою інформацією);

– суттєво зменшити час на розробку, доведення та отримання команд (розпоряджень), цілевказання, повідомлень, сигналів бойового управління тощо;

– створити систему захисту інформації;

– забезпечити дієвий контроль за своїми підрозділами та виконанням управлінських рішень.

Таким чином, одним із пріоритетних завдань оборонної реформи та забезпечення підвищення ефективності управління військами (силами) є створення сучасної системи управління Збройними Силами України. Важливу роль у реалізації цього завдання належить комплексній автоматизації процесів оперативного (бойового) управління, зв'язку, розвідки та спостереження.

Як показує практика, на цей час існуюча система управління Збройними Силами України в цілому не автоматизована, а окремі функції (процеси), які автоматизовані, не охоплюють замкнутого циклу управління за всіма напрямами діяльності Збройних Сил України.

УДК 681.3.06

Рижов Є.В., Сакович Л.М.

ВИЗНАЧЕННЯ НАУКОВО-ТЕОРЕТИЧНИХ НАПРЯМКІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ ВІЙСЬКОВОЇ ТЕХНІКИ ЗВ'ЯЗКУ

Метрологічне забезпечення – комплекс науково-технічних заходів, а також діяльність відповідних організацій і фахівців, спрямований на забезпечення єдності та точності вимірювань для досягнення необхідних характеристик функціонування технічних пристроїв.

Бойові дії в України показали не повну відповідність існуючого метрологічного забезпечення військової техніки зв'язку сучасним вимогам і реаліям, що потребує подальших досліджень для усунення встановлених протиріч.

Сучасна програмно-керована військова техніка зв'язку з цифровою обробкою сигналів відноситься до багаторежимних об'єктів зі змінною структурою, технічне обслуговування яких в польових умовах доцільно виконувати за станом, чого не враховує іс-

нуюче метрологічне забезпечення. Тому виникає актуальна наукова проблема, яка полягає в подоланні встановлених протиріч між існуючим метрологічне забезпеченням і вимогами до нього системи технічного обслуговування і ремонту перспективних зразків військової техніки зв'язку завдяки отримання і впровадження нових методів, спрямованих на уніфікацію засобів вимірювальної техніки з мінімально необхідними значеннями метрологічних характеристик при задоволенні показників щодо надійності військової техніки зв'язку. Тобто мета проведених досліджень – скорочення витрат на метрологічне забезпечення ремонту і технічне обслуговування сучасної військової техніки зв'язку при забезпеченні вимог до показників її надійності.

В результаті оцінки впливу метрологічної надійності засобів вимірювальної техніки на час виконання технічного обслуговування військової техніки зв'язку за станом запропоновано метод визначення послідовності перевірки і кількості параметрів без зниження якості робіт щодо оцінки і підтримки рівня технічного стану. При цьому обґрунтовано метод завдання мінімально припустимого значення ймовірності оцінки результату перевірки параметрів військової техніки зв'язку під час її технічного обслуговування і ремонту.

Особлива увага приділена відновленню працездатності військової техніки зв'язку з аварійними та бойовими пошкодженнями слабкого ступеню в польових умовах силами екіпажів апаратних зв'язку і фахівців військових ремонтних органів. Для цього запропоновано методика обґрунтування вимог до засобів вимірювальної техніки як аналогових, так і сучасних цифрових, яку доцільно використовувати при комплектуванні перспективних апаратних технічного забезпечення [1].

Для впровадження результатів досліджень обґрунтовано науково-практичні рекомендації щодо перспективних напрямків удосконалення метрологічного забезпечення сучасної військової техніки зв'язку при її технічному обслуговуванні і ремонті у військових умовах. Проведено оцінку ефективності використання обґрунтованих методів і методик:

- врахування метрологічної надійності військової техніки зв'язку уточнює час виконання технічного обслуговування за станом військової техніки зв'язку від 9% до 22%. У доповіді зазначено, що особливість використання засобів вимірювальної техніки під час технічного обслуговування за станом військової техніки зв'язку обумовлена забезпеченням їх безвідмовності, переважно за прихованими метрологічними відмовами. Як показник метрологічної надійності засоби вимірювальної техніки використовують ймовірність збереження значень метрологічних характеристик у заданих межах протягом міжперевірочного інтервалу. Необхідний рівень метрологічної надійності суттєво залежить від сфери застосування засобів вимірювальної техніки і обирається з умови забезпечення необхідної ефективності функціонування військової техніки зв'язку. Як правило, цей рівень для робочих засобів вимірювальної техніки становить 0,85…0,99, а для зразкових – 0,90…0,99 [2];

- використання методики визначення послідовності перевірки військової техніки зв'язку при її технічному обслуговуванні за станом дозволяє до 43% скоротити кількість перевірок при заданій ймовірності оцінки технічного стану виробу. Зазначено, що методика призначена для обґрунтування послідовності перевірки працездатності підсистем радіоелектронних комплексів великої розмірності, які складаються з десятків і сотень тисяч електрорадіоелементів. Її сутність полягає в комплексному врахуванні показників надійності підсистем, вартості і часу перевірки їх працездатності, часу усунення несправності (або резервування підсистем), а також метрологічної надійності засобів вимірювальної техніки [3];

- впровадження рекомендацій щодо вибору засобів вимірювальної техніки для поточного ремонту військової техніки зв'язку в польових умовах занижує вимоги до ймовірності правильної оцінки результату виконання перевірки до 11%, що знижує вартість засобів вимірювальної техніки. Зазначено, що сутність методу полягає в обґрунтуванні

мінімально припустимого значення імовірності оцінки результату перевірки параметрів з врахуванням метрологічної надійності засобів вимірювальної техніки, що забезпечить зменшення витрат на технологічне обладнання ремонтних органів [4];

- впровадження сукупності отриманих рекомендацій в практику поточного ремонту військової техніки зв'язку в польових умовах дозволяє знизити до 18% середній час відновлення працездатності. У доповіді обґрунтовано мінімально необхідні вимоги до засобів вимірювальної техніки при двоступеневій системі діагностування в процесі поточного ремонту військової техніки зв'язку, що забезпечує зменшення часу її відновлення за рахунок вдосконалення діагностичного забезпечення [5];

- врахування властивості військової техніки зв'язку змінювати структуру під час використання за призначенням при обґрунтуванні її поточного ремонту зменшує середній час відновлення до 44%. Зазначений метод, призначений для обґрунтування вимог до засобів вимірювальної техніки при поточному ремонті об'єктів зі змінною структурою. Сутність методу полягає у виборі засобів вимірювальної техніки з мінімально необхідним значенням ймовірності правильної оцінки діагностичного параметру при задоволенні вимог до надійності виробу [6];

- при усуненні бойових пошкоджень військової техніки зв'язку слабкого ступеня завдяки перерозподілу зусиль на дефектування і діагностування з запропонованим метрологічним забезпеченням можливе скорочення середнього часу відновлення до 25%. Зазначено, що дефектація військової техніки зв'язку полягає у визначенні ступеня пошкодження техніки за зовнішніми ознаками і усуненні несправностей для обґрунтованого висновку про доцільність ремонту, його виду і місця виконання робіт. Використання запропонованого процесу формалізації раціонального розподілу зусиль бригади фахівців апаратної технічного забезпечення при відновленні військової техніки зв'язку зі слабким ступенем пошкоджень дозволяє у кожному конкретному випадку залежно від реальних умов ремонту отримувати рекомендації щодо досягнення мінімального часу відновлення працездатності [7].

Ці результати отримано з використанням математичного апарату теорії дискретного пошуку, надійності и метрології. Обмеження і допущення на їх використання відповідають реальним умовам відновлення працездатності техніки в польових умовах фахівцями екіпажів апаратних зв'язку і технічного забезпечення. При цьому вважають, що кваліфікація фахівців відповідає штатному розкладу, засоби вимірювальної техніки та інше обладнання апаратних технічного забезпечення заздалегідь справні. Отримані результати доцільно використовувати під час розробки метрологічного та діагностичного забезпечення існуючих та перспективних зразків військової техніки зв'язку, а також при проектуванні сучасних апаратних технічного забезпечення модульного типу з використанням інформаційних технологій.

В усіх перерахованих прикладах ефект досягається науково обґрунтованим вибором метрологічного забезпечення ремонту і технічного обслуговування за станом існуючої і перспективної військової техніки зв'язку з використанням сучасних інформаційних технологій.

Подальші дослідження доцільно направити на підвищення ефективності усунення бойових пошкоджень слабкого ступеня в польових умовах завдяки удосконаленню метрологічного и діагностичного забезпечення ремонту впровадженням досягнень інформаційних технологій в процес визначення реального технічного стану при пошуку кратних дефектів.

Список використаних джерел

1. Yevhen Ryzhov, Lev Sakovych, Petro Vankevych, Maksym Yakovlev, Yuriy Nastishin. Optimization of requirements for measuring instruments at metrological service of communication tools. Measurement. Journal of the International Measurement

Confederation, Volume 123 (July 2018) pp. 19–25. DOI: https://doi.org/10.1016/j.measurement.2018.03.055.

2. Yevhen Ryzhov, Lev Sakovych, Yurii Myroshnychenko, Volodymyr Hrabchak, Yuriy Nastishin, Anatolii Volobuiev. (2021). Metrological support of maintenance by the technical state of communication means. Ukrainian Metrological Journal, No.3 pp. 17–23. DOI: https://doi.org/10.24027/2306-7039.3.2021.241573.

3. Сакович Л.М., Рижов Є.В., Настишин Ю.А., Мирошниченко Ю.В., Коротченко Л.А. Методика визначення послідовності перевірки радіоелектронних комплексів при технічному обслуговуванні за станом. Військово-технічний збірник. – 2020. – № 22. – С. 66-73. DOI: https://doi.org/10.33577/2312-4458.22.2020.66-73.

4. Рижов Є.В., Сакович Л.М. Метод обґрунтування мінімально припустимого значення ймовірності оцінки результату перевірки параметрів. Вісник Національного технічного університету України "Київський політехнічний інститут". Серія ПРИЛАДОБУДУВАННЯ. – 2017. – Вип. 54(2). – С. 96-106. DOI: https://doi.org/10.20535/1970.54(2).2017.119562.

5. Рижов Є.В., Сакович Л.М., Настишин Ю.А., Кирилова Н.В. Обґрунтування мінімально необхідних вимог до засобів вимірювань при двоступеневій системі діагностування в процесі поточного ремонту військової техніки зв'язку. Науково-технічний журнал ЦНДІ ОВТ ЗС України. – 2018. – № 4(20). – С. 54-58.

6. Ryzhov Ye., Sakovych L., Kuriana Ya., Slisarchuk O., Volkov O., Nastishin Yu. Method of justification of the requirements for metrological support of repair of objects with variable structure. Ukrainian Metrological Journal, 2023. № 3. P. 16-23. DOI: https://doi.org/10.24027/2306-7039.3.2023.291931

7. Сакович Л.М., Рижов Є.В., Курята Я.Е., Гиренко І.М. Настишин Ю.А. Відновлення військової техніки зв'язку з бойовими пошкодженнями. Військово-технічний збірник. 2023. № 28. С. 107-113. DOI: https://doi.org/10.33577/2312-4458.28.2023.107-113.

УДК 621.396.96

Руденко А.Р., Ковалевський С.М.

РОЗРОБКА СПОСОБУ ВИЯВЛЕННЯ ТА ВИДАЧІ КООРДИНАТ БПЛА З ВИКОРИСТАННЯМ МЕТОДІВ БАГАТОПОЗИЦІЙНОЇ РАДІОЛОКАЦІЇ

Зараз йде російсько-Українська війна, атаки противника не припиняються. Тому робота протиповітряної оборони необхідна як ніколи, а саме хотів би підкреслити роботу радіотехнічних військ.

Основні засоби нападу агресора в конфлікті є безпілотні літальні апарати. Проаналізувавши їх тактико-технічні та тактичні характеристики, встановлено, що вони мають нестандартну тактику дії.

Проведена оцінка можливостей виявлення БПЛА оперативного та тактичного рівня радіолокаційними станціями радіотехнічних військ. Особливостями радіолокаційного виявлення малорозмірних ПО є:

- мала дальність виявлення;
- знаходження БПЛА в зоні за світок від місцевих предметів, що вимагає включення апаратури захисту від пасивних завад, що в свою чергу зменшує дальність виявлення;
- відсутність оповіщення безпілотних літальних апаратів від інших підрозділів.

Малорозмірні БПЛА, що діють на малих та гранично малих висотах, засобами РТВ в ході ведення РУВ можуть не виявлятися.

Проведена оцінка РЛС метрового та дециметрового діапазону та встановлено, що сучасні РЛС РТВ не вспромозі виявляти безпілотні літальні апарати з заданими показ-

никами якості. Розробляються шляхи підвищення виявлення БПЛА оперативного та тактичного рівня.

Проведено аналіз відомих методів виявлення малорозмірних та малопомітних ПО. Встановлено, що відомими організаційними та технічними шляхами підвищення ефективності ведення РЛР малопомітних та малорозмірних цілей є:

- підвищення енергетичного потенціалу та покращення ТТХ РЛС;
- ущільнення розташування РЛС на небезпечних напрямках (створення смуг виявлення);
- одночасне використання радіолокаційних станцій різних діапазонів частот та інші.

Встановлено, що альтернативними (перспективними) шляхами підвищення ефективності виявлення БПЛА є:

- використання енергії сторонніх джерел випромінювання та реалізації режимів рознесеного прийому;
- використання властивості резонансного відбиття електромагнітних хвиль від ПО при використанні довжин хвиль, які порівняні із розмірами об'єкта;
- використання властивостей бістатичної ЕПР при рознесеному прийомі.

Sadovnykov B., Pastushenko V.

EXPERIMENTAL STUDY OF OPTIMIZED FACE RECOGNITION ALGORITHMS FOR RESOURCE – CONSTRAINED

The existing face recognition algorithms were studied, and the effectiveness of the best of them was substantiated according to a set of criteria, namely: checking accuracy, speed and reliability when working on devices with limited resources, such as embedded devices. Mathematical modeling of the face recognition algorithm designed to work in systems with limited resources was carried out. A study of facial recognition methods was conducted with the aim of choosing the most effective ones for further optimization. It is substantiated that the most effective method of face recognition is mixed convolutional neural networks, namely the method using the FaceNet neural network. A series of experiments was conducted to determine the difference between optimized versions deployed on an embedded device and non-optimized versions.

According to the results of experiments, it has been proven that the static quantization model has the best results. Its advantages are: no need to additionally train the model or train it from the beginning, the possibility of optimizing any model according to this principle. It is justified that static quantization eliminates the need to select the loss function and training parameters, as in the case of knowledge distillation or network pruning. It has been proven that from a practical point of view, quantization is the simplest method of optimization, and in terms of accuracy, the experiment proved only minor losses that do not affect the final result.

УДК 623.7

Самокіш А.В., Таран Д.О., Стаднік В.В., Крепко А.В.

ДОСЛІДЖЕННЯ МЕТОДІВ ШИФРУВАННЯ МЕРЕЖ З ВІДДАЛЕНИМ ДОСТУПОМ ДЛЯ ОБМІНУ ДАНИМИ В РЕАЛЬНОМУ ЧАСІ

Постійний процес цифровізації сучасного світу, потребує вирішення проблем із забезпечення безпеки та конфіденційності даних у мережах під час обміну інформацією Розвиток інформаційних технологій, поява нових методів здійснення кібератак, зумов-

лює зростання кількості кіберзагроз. Забезпечення високого рівня безпеки мережевих комунікацій стає важливою передумовою для стійкого розвитку сучасного суспільства. Тому актуальним питанням є постійне удосконалення засобів захисту інформації. Тому методи шифрування мереж стають ключовим елементом у забезпеченні надійності та конфіденційності передаваних даних.

Технологія VPN дозволяє організувати захист на різних рівнях моделі OSI. На канальному рівні, засоби VPN, будує віртуальний тунель типу «точка-точка» та забезпечують інкапсуляцію трафіку. На мережевому рівні виконується інкапсуляція IP в IP, а на сеансовому використовується метод «circuit proxy», який ретранслює трафік із захищеної мережі в загальнодоступну мережу Internet. Реалізувати VPN можна на основі мережевої операційної системи, міжмережевого екрану, маршрутизаторів, програмних рішень або спеціалізованих апаратних засобів з вбудованими шифропроцесорами.

В дослідженні розглянуті захищенні за допомогою протоколів PPTP, L2TP, SSL, TLS та IPSEC мережі. Протокол L2TP не прив'язаний до протоколу IP, на відміну від PPTP, тому він може бути використаний в мережах з комутацією пакетів. Також, в протокол L2TP додана важлива функція управління потоками даних. В залежності від ролі вузла в якому працює IPSec, застосовується тунельний або транспортний режим. Загалом розрізняють три схеми застосування IPSec: хост-хост, шлюз-шлюз та хост-шлюз.

Доповідь присвячена дослідженню методів шифрування мереж. Основні цілі дослідження включають аналіз сучасних тенденцій у галузі криптографії, оцінку ефективності та безпеки існуючих підходів до шифрування, а також розгляд можливостей застосування квантового шифрування. Зроблено висновок щодо їх переваги, недоліків та рекомендації для оптимального вибору залежно від конкретних вимог та умов використання.

УДК 621.396.96

Селезньов Д.Д., Сердюк О.В.

АНАЛІЗ МОЖЛИВОСТЕЙ ПОКРАЩЕННЯ НАПРЯМКІВ ПІДГОТОВКИ ОПЕРАТОРІВ РЛС

В реаліях сучасної війни, час на підготовку операторів РЛС значно зменшується, через потребу постійного поновлення кадрів, тому ми розглядаємо покращення напрямків підготовки спеціалістів, а саме, через створення інтерактивного додатку.

Інтерактивний додаток, скоротить час навчання, та полегшить постійний доступ до потрібної інформації.

Електронна презентація – це сучасний спосіб представлення інформації різноманітного спрямування. Як правило, в ній задіяні всі сучасні мультимедійні можливості: графіка і анімація, текст і таблиця, фото-, відео- і аудіоматеріали.

Враховуючи розвиток засобів мультимедіа, презентації бувають двох типів – інтерактивні та неінтерактивні. У неінтерактивних презентаціях користувач не може впливати на порядок перегляду. Інтерактивні презентації володіють системою навігації, тобто дозволяють користувачеві самому вибирати розділи, що цікавлять його, і проглядати їх в довільному порядку. Така презентація дозволяє створювати інтерактивні електронні дидактичні засоби.

Для розробки інтерактивних презентацій сьогодні створено дуже багато різних програмних продуктів. Одні з них вимагають рівня просунутого користувача, інші доступні і початківцям.

Canva – інструмент графічного дизайну, що надає доступ до фотографій, векторних зображень, графіки та шрифтів.

Prezi – хмарний сервіс для створення інтерактивних презентацій в режимі онлайн. ...

PowerPoint – сервіс для створення та відтворення презентацій, що є частиною Microsoft Office.

Кожна з цих програм є багатоцільовою за застосуванням та має виконувати такі функції:

1.Забезпечення високої ступені наочності матеріалу;

2.Використання мультимедійних ресурсів;

3.Проста та зручна навігація;

4.Можливість редагування та оновлення інформації з боку розробника.

Серед найбільш доступних програм — MS PowerPoint. Ця програма є простою в освоєнні і дуже потужним інструментом створення спеціалізованих інтерактивних додатків, що відповідають будь-яким вимогам.

Тож, використання інтерактивних презентацій скоротить час підготовки операторів РЛС, облегшить роботу командирів, відкриває можливість швидкого оновлення інформації, так як, в реаліях сьогоднішньої війни, тактика змінюється, що не кожного дня, надає зручність використання будь-де, з телефону, планшету чи ноутбуку.

Серватинський М.Р., Толкаченко Є.А.

ДОСЛІДЖЕННЯ ВПЛИВУ АРХІТЕКТУРНИХ ПАРАМЕТРІВ НА ПРОДУКТИВНІСТЬ НЕЙРОННИХ МЕРЕЖ

У сучасних реаліях, на тлі агресивної війни, розв’язаної російською федерацією використання високих технологій стає найбільш вирішальним для скорочення втрат Сил Оборони та завдання великих втрат ворогу. Саме тому дослідження в галузі штучного інтелекту є актуальними та перспективними. В даній доповіді розглядається вплив архітектурних параметрів нейронних мереж на їх продуктивність з метою використання в автономних рішеннях з обмеженими енергетичними та обчислювальними ресурсами. Представлений аналіз різноманітних автономних платформ для запуску штучного інтелекту, що доступні на світовому ринку, а також моделі нейронних мереж для роботи в автономних системах. Проаналізовано архітектурні особливості та параметри, які можуть дозволити підвищити швидкодію під час роботи нейронної мережі в режимі висновку та можливості використання подібних систем для потреб Сил Оборони.

УДК 378.1:004.8

Сидоренко І.І.

ШТУЧНИЙ ІНТЕЛЕКТ GHATGPT ЯК ІНСТРУМЕНТ РОЗРОБКИ ЗАНЯТЬ З ВИЩОЇ МАТЕМАТИКИ

Сучасний світ перебуває на порозі IV промислової революції, яку визначає штучний інтелект та розумні машини. Технології на основі штучного інтелекту мають хоча ще й недостатньо вивчений, проте величезний потенціал до використання. Вони поступово і неминуче змінюють світ, а разом з цим і технології навчання. Тому у викладацькому середовищі активно обговорюється можливість його використання у навчальному процесі.

ChatGPT – це чат-бот з великою мовною моделлю, розроблений OpenAI на основі GPT-3.5. Він використовує модель обробки природної мови та генерує відповіді на запити користувачів. Він спроможний структурувати тексти, генерувати історії, вірші,

жарти, переклади, редагувати текст та виконувати розрахунки. Даний інструмент сконструйований за принципом автовідповідача у сучасних мобільних телефонах та оснований на прогнозуванні наступного слова, яке виявляється найбільш ймовірним з аналізу попереднього тексту, що складається з так званих, промптів – підказок-запитів які користувач надає чатові GPT. У такий спосіб ChatGPT зручно використовувати як асистента при розробці занять.

Застосування функції асистента ChatGPT виявилося корисним при розробці занятть з Вищої математики. Система була спроможною надати результат за такими промптами: «Запропонуй план заняття на тему «Диференціальні рівняння першого порядку», «Напиши вірш до чотирьох рядків для запам'ятовування формули», «Структуруй інформацію про типи диференціальних рівнянь першого порядку», «Розбий інформацію на слайди до презентації», «Напиши тези до слайдів».

При наявності готових вправ або задач, для складання тестових завдань у ChatGPT можна надати запит згенерувати таблицю, де в одному стовпці будуть вправи, а в іншому – описання інструменту для виконання цих вправ. Можливості ChatGPT дозволяють перенести таку таблицю на інші платформи (наприклад Exel) і з нею надалі можна працювати.

Використання чату GPT також дозволяє складати тестові завдання з готовою відповіддю, що значно економить час на перевірку. Наприклад, промпт «Намалюй графік функції …» виявився корисним при перевірці завдання «Дослідження функції»; промпти «Опиши етапи розв'язання рівняння …», «Напиши задачу, в якій є три стратегії, одна з яких справжня, а дві інших – фейкові. Вкажи правильну відповідь» оптимізували витрати робочого часу на розробку методичних матеріалів для викладачів на етапі складання банку відповідей на завдання контрольних робіт [3].

У чаті GPT є набір загальних функцій, які можливо застосовувати для організації роботи здобувачів на занятті без прив'язки до конкретної дисципліни. Наприклад, промпт «Запропонуй дві вправи, щоб розбити студентів на трійки випадковим чином».

З недоліків можна назвати той, що обсяг тексту, що можна відправити до чату, лімітований. Отже є певні незручності з тим, що великі тексти потрібно розбивати на частини. Однак така вада компенсується тим, що чат пам'ятає розмову у межах одного діалогу. Також досить зручною є функція розшифрування відео Freesubtitles, добре адаптована під українську.

Отже, ChatGPT можливо використовувати викладачам, як допоміжний засіб при розробці занять. Для здобувачів він має працювати, як персональний тренажер, проте має сенс донести до слухачів, що штучний інтелект не є аналогом вікпедії або наукових джерел інформації. Внаслідок того, що ChatGPT працює на прогнозуванні найбільш ймовірній відповіді, чат може помилятися або видавати неіснуючі факти. Тому не слід використовувати відповіді, що він видає, без аналізу. Тобто, на сучасному етапі розвитку інструментів штучного інтелекту, найбільш доцільно використовувати такий інтелект для структурування інформації, а не як її джерело.

Список використаних джерел

1. Мар'єнко М., Коваленко В. Штучний інтелект та відкрита наука в освіті. *Фізико-математична освіта.* 2023. Том 38, № 1. С. 48–53.

2. Драч І., Петроє О., Бородієнко О., Регейло І., Базелюк О. та ін. Використання штучного інтелекту у вищій освіті. *Міжнародний журнал «Університет і лідерство».* 2023. № 15. С. 66–88.

3. Візнюк І.Н., Буглай Н.М., Куцак Л.В., Поліщук А.С., Киливник В.З. Використання штучного інтелекту в освіті. *Сучасні інформаційні технології та інноваційні методики в підготовці фахівців: методологія, теорія, досвід.* 2021. Вип. 59. С. 14–22.

УДК 004.732

Симоненкова І.В., Лукаш Р.В., Симоненков В.М.

ШЛЯХИ ПОБУДОВИ ПЕРСПЕКТИВНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ДЛЯ ПОТРЕБ ПІДГОТОВКИ ТА ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ НА ОСНОВІ ВПРОВАДЖЕННЯ ХМАРНИХ ТЕХНОЛОГІЙ

Одним з основних пріоритетів розвитку Збройних Сил України на найближчі 10 років та в подальшому визначена необхідність створення інформаційних мереж в інтересах підготовки та діяльності сил охорони правопорядку, які будуть забезпечувати набуття інформаційних спроможностей для отримання, опрацювання, зберігання, передачі, контролю та надання інформації на вимогу командувачів (командирів) та штабів (тактичного, оперативного, стратегічного рівнів) об'єднаних сил, у тому числі забезпечення їх взаємосумісності зі збройними силами держав-партнерів.

Вищі військові навчальні заклади, військові навчальні та наукові підрозділи закладів вищої освіти об'єднуються в єдину систему під загальним керівництвом підрозділу підготовки (J-7) Генерального штабу Збройних Сил України, основна увага, при цьому, буде приділятися самостійному покращенню рівня професійної майстерності та широкому застосуванню дистанційного режиму доступу до інформаційних ресурсів, у тому числі даних й документів, засобів сумісної роботи, програмного забезпечення, що працює на віддалених серверах, та обчислювальних можливостей.

На даний момент, термін «віртуалізація» трактується як перетворення апаратних засобів у «програмний вигляд», при цьому, низка віртуальних машин сумісно використовують спільні апаратні ресурси. Такий підхід полягає у визначенні програмного шару у операційному середовищі шляхом розподілу наявних ресурсів апаратних засобів та створення віртуальних машин – окремих робочих місць. Завдяки розвитку мережевих технологій, «звичайна віртуалізація» перетворюється у технологію «хмарних обчислень» (cloud computing), що розширюють можливості технологій віртуалізації.

Хмарні обчислення або хмарні технології – це модель забезпечення доступу «на вимогу» через відповідну інформаційно-телекомунікаційну мережу до спільного пулу обчислювальних ресурсів (серверів, комунікаційних засобів, засобів збереження даних, прикладних додатків та сервісів тощо), які можуть бути надані з мінімальними управлінськими затратами.

Інформаційна інфраструктура на базі віртуальних машин максимально відповідає вимогам застосування в умовах дистанційного режиму праці та є найбільш перспективним напрямком застосування інформаційних технологій шляхом впровадження хмарних технологій під час організації інформаційних процесів у сфері освіти та проведення наукових досліджень.

В ході досліджень на базі наукового центру Військової академії (м. Одеса) було розгорнуто експериментальний стенд із використанням технологій приватної хмари та тонких клієнтів. На наш погляд, технології «хмарної обробки даних» є потужним інструментом модернізації інформаційно-телекомунікаційних мереж для потреб підготовки та діяльності сил охорони правопорядку держави.

Syvolovskyi I.

RESEARCH OF MODERN DATABASES TO SIMPLIFY THE PROCESS OF THEIR DESIGN

The amount of data on the Internet is growing at a tremendous rate, as users add thousands of gigabytes of data to social networks every second. It is not surprising that relational databases cannot cope with such modern arrays of information, even though they have been successfully dealing with data processing tasks for several decades. This problem has led to the need to introduce new approaches of data storing and processing in large systems. NoSQL databases coped with this task, as they allowed replacing expensive vertical scaling with efficient horizontal scaling. They also had better performance, a more flexible data model, and open-source code.

However, without unified approaches to database selection and schema implementation, application developers make mistakes at the system design stage, which can lead to additional costs and problems.

Given the urgency of the problem, the paper explores modern NoSQL databases, which may be the key to improving the overall performance of server systems.

УДК [001.8/.816/.817] + 001.92 + [371.315.5/.315.6/.335] +655.52

Сілко О.В., Козубцов І.М., Саєнко О.Г. Логвіненко Н.М.

МЕТОДИКА ВИКЛАДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ПСИХОЛОГО-ПЕДАГОГІЧНІ ОСНОВИ ОСВІТНЬОЇ ТА НАУКОВОЇ ДІЯЛЬНОСТІ» ЗДОБУВАЧАМ ДРУГОГО ОСВІТНЬОГО РІВНЯ У ФОРМІ ЛІДЕРСЬКОЇ ПРОФЕСІЙНО-ДІЛОВОЇ ГРИ

Ключовим пріоритетом Національної доктрини розвитку освіти в Україні є підготовка кваліфікованих кадрів, здатних до творчої праці, професійного розвитку, освоєння та впровадження інформаційних технологій, конкурентоспроможних на ринку праці. Забезпечити виконання цього складного завдання можуть лише викладачі-професіонали, покликані розвивати задатки, виявляти таланти, зберігати індивідуальність кожного курсанта. Підвищення професіоналізму майбутніх наукових та науково-педагогічних працівників для потреб Збройних Сил України є важливим завданням в системі сучасної вищої військової освіти. Цьому сприяє навчальна дисципліна «Психолого–педагогічні основи освітньої та наукової діяльності». Проте виникає потреба у прикладному спрямуванні при викладанні окремих освітніх компонентів військово-гуманітарного циклу для ад'юнктів технічних військових вищих навчальних закладів (ВВНЗ).

Мета доповіді полягає у вивченні особливості викладання навчальної дисципліни «Психолого-педагогічні основи освітньої та наукової діяльності» здобувачам другого (магістерського) рівня ВВНЗ спеціальностей 126 «Інформаційні системи та технології» та 255 «Озброєння та військова техніка».

Виклад основного матеріалу дослідження. З огляду на необхідність підняття рівня психологічної, педагогічної та методичної підготовки викладача вищої школи і запропонована комплексна дисципліна «Психолого-педагогічні основи освітньої та наукової діяльності», в якій визначаються психологічні основи педагогічного процесу у вищій школі, розкриваються як загальні основи педагогіки вищої школи, так й питання дидактики та методики вищої школи. Основна увага зосереджена на методичних та технологічних аспектах викладання.

В умовах війни система освіти України за функціонувала в екстремальних умовах, оскільки в цей період необхідно поєднання виконання важливих завдань, що тягнуться з минулого та потребують свого логічного завершення [1, с. 163]. Військова агресія не завершилась, а тому є потреба адаптуватися до реалії війни за якої необхідно продовжувати освітній процес з підготовки здобувачів вищої освіти для потреб національної економіки. Всі ці 2 академічні години за розкладом занять актором і режисером лишається викладач на якого додатково покладається зобов'язання щодо дотримання режиму збереження життя здобувачів за умови надходження сигналу оповіщення про повітряну тривогу [2].

Для успішного засвоєння навчального матеріалу освітніх компонентів потрібно створити здобувачам освіти умови до комбінування форм проведення занять. Вибір педагогічних технологій навчання є ключовою проблемою – суб'єкта освітнього процесу, тобто викладача [2]. Одночасно відсутність рекомендацій щодо формалізації у їх виборі, розширює ступінь свободи педагогічної майстерності лектора у творчому пошуку і експериментуванню.

Як правило внаслідок повітряної тривоги відбувається скорочення аудиторного часу (лекцій, практик / семінарів), в результаті чого порушується логіка навчального процесу. Для забезпечення збалансованості пропонується змішане навчання за технологією «випереджаючого навчання» або «перевернутий клас» [3].

Схема реалізації освітнього процесу подана на рис. 1 та раніше апробовано на фаховому курсі тактичного рівня професійної військової освіти (L-1B), з дисципліни «Бойового застосування систем та комплексів військового зв'язку» [3].

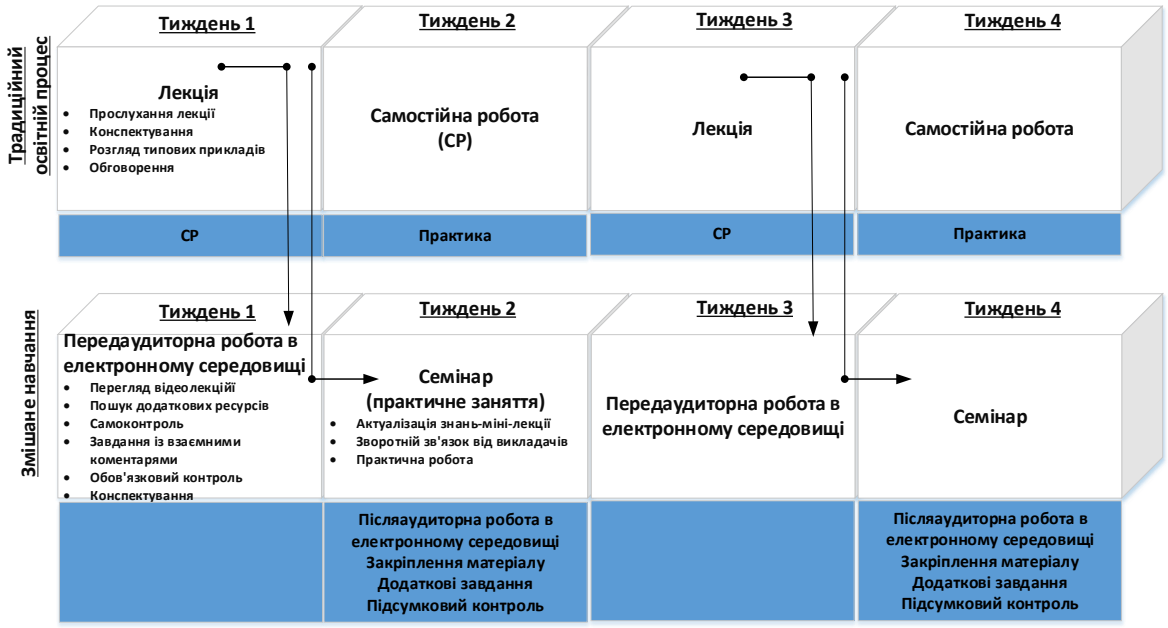


Рисунок 1 - Схема реалізації навчального процесу

За даною методикою курс лекцій дисципліни викладається здобувачам освіти завчасно для самостійного опрацювання. На аудиторному занятті здобувачі за професійно-ділової гри займають роль викладача-початківця. Після їх лекційного дебюту продовжують наступне обговорення лекційного матеріалу у форматі брифінгу (семінару).

Запропонована методика проведення занять у формі лідерської професійно-ділової гри підтвердила набуття здобувачами первинного досвіду з науково-педагогічної діяльності.

Застосування форми навчання на випередження забезпечує безперервність виконання навчального плану викладачу, а здобувачам опанування освітньої компоненти. В цілому унікальний комплекс заходів націлений на реалізацію державної політики по

збереженню життя і здоров'я кожного учасника освітнього процесу в умовах війни.

Список використаних джерел

1. Освіта України в умовах воєнного стану : інформаційно-аналітичний збірник. К.: Інститут освітньої аналітики, 2022. 358 с.

2. Ліщина В., Козубцов І., Козубцова Л. Вибір педагогічних технологій навчання як ключова проблема викладач – суб'єкта освітнього процесу. Міжнародна науково-методична конференція «Інноваційні технології у військовій освіті», (Одеса, 25 червня 2021 р.). Одеса: Військова академія. 2021. С. 225 – 226.

3. Kozubtsov I. Methodology of the Professional-Business Game for the Development of a Cadet Leader in Professional Training Courses (L-1B) of the Tactical Level of Military Education. IgMin Research - STEM A Multidisciplinary Open Access Journal. 2023. Vol 1 Issue 2, pp. 160–169.

УДК 621.396.96

Скавронов О.С., Райков Р.Ю.

ПІДВИЩЕННЯ НАДІЙНОСТІ СИСТЕМИ УПРАВЛІННЯ ОКРЕМОГО РАДІОЛОКАЦІЙНОГО ВЗВОДУ В УМОВАХ СУЧАСНОЇ ВІЙНИ

Одним з основних принципів бойового застосування радіотехнічних військ є чітке і безперервне управління.

Управління окремим радіолокаційним взводом – процес цілеспрямованого впливу командира на підпорядкований особовий склад, що здійснюється для підтримання готовності підрозділу до виконання завдань за призначенням, підготовки та успішного виконання ними завдань під час бойового застосування.

До управління окремим радіолокаційним взводом, як процесу, пред'являються вимоги, виконання яких є необхідною передумовою досягнення його мети. Основними з них є: оперативність, стійкість, безперервність, скритність, якість.

Стійкість і безперервність управління окремим радіолокаційним взводом тісно взаємопов'язані та досягаються:

а) створенням пункту управління, його захистом від засобів ураження, оснащенням технічними засобами управління і життєзабезпечення, маскуванням та інженерним обладнанням району розташування;

б) підтриманням пункту управління в постійній готовності до роботи та своєчасною зміною його розташування під час бойового застосування;

в) вмілою організацією роботи особового складу;

г) приховуванням об'єктів системи управління від розвідки противника та захистом їх від впливу різних видів зброї;

д) забезпеченням електромагнітної сумісності радіоелектронних засобів управління, захистом їх від подавлення засобами радіоелектронної боротьби противника;

е) комплексним застосуванням і забезпеченням надійної роботи засобів зв'язку і системи обробки та видачі радіолокаційної інформації;

ж) своєчасним нарощуванням системи зв'язку та інформаційних систем;

и) надійною охороною і обороною об'єктів системи управління;

к) відновленням порушеного управління у стислі строки та будь-яких умов обстановки.

На командира окремого радіолокаційного взводу під час бойового застосування покладаються такі завдання:

а) аналіз повітряної обстановки;

б) підготовка пропозицій та необхідних даних для прийняття рішення;

в) управління бойовою обслугою, координація дій з діями взаємодіючих підрозділів та підрозділів, що забезпечуються;

г) доведення до підлеглих рішення на виконання бойового завдання і контроль за його виконанням;

д) контроль за загальною повітряною обстановкою та видачею розвідувальної інформації;

е) узагальнення даних про повітряну обстановку;

ж) здійснення заходів для забезпечення безперервності управління;

з) підготовка підсумкових даних про бойове застосування.

Таким чином, підвисити надійність управління окремим радіолокаційним взводом можна шляхом обладнанням захищеного пункту управління (бліндаж, захисна споруда), автоматизацією процесу знімання інформації з РЛС та передачею її на робоче місце оператора вводу (з використанням АЦПРЛ та бездротової передачі на робоче місце оператора вводу), використанням декількох каналів зв’язку (сучасні засоби радіозв’язку, супутниковий зв'язок, LTE модеми).

Скакун А.О., Кулабухов О.М.

ОСОБЛИВОСТІ ФОРМАЛІЗАЦІЇ ЗНАНЬ ДЛЯ ВИЗНАЧЕННЯ ТЕХНІЧНОГО СТАНУ ЗАСОБІВ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ

На сьогоднішній день, для успішного здійснення управління військами (особливо в умовах ведення бойових дій) важливе значення має швидкість отримання, обробки, перетворення, передачі та використання інформації, а також спосіб її зберігання. Ефективне виконання цих завдань не можливе без застосування сучасних комплексів засобів автоматизації (КЗА) зі спеціальним програмним забезпеченням.

Комплекси засобів автоматизації відносяться до складних технічних об’єктів, технічний стан яких змінюється у ході застосування і потребує різних експлуатаційних рішень. Особа, яка експлуатує КЗА, повинна мати знання щодо процесу діагностування поточного технічного стану комплексу та подальшого прийняття якісних рішень в разі виявлення несправності.

На цей час оцінка технічного стану елементів КЗА, що знаходиться у підрозділах ЗСУ, здійснюється неавтоматизовано шляхом перевірки техніки за допомогою вмонтованих системам контролю та індикаторних приладів у відповідності до інструкцій з експлуатації. Здійснюється порівняння інформації про фактичний стан техніки із нормативними встановленими значеннями параметрів, які визначені експлуатаційною та нормативною документацією, та приймається рішення щодо стану комплекса. Однак актуальним є прогнозування зміни технічного стану та розрахунок числових показників готовності, боєздатності, справності комплексу на основі фактичної інформації про технічний стан об’єкту, умов експлуатації техніки, факторів зовнішнього середовища та впливу. Тому є доцільним та необхідним впровадження методики оцінки та прогнозування технічного стану КЗА в умовах невизначеності.

Аналіз показав, що використання підходу, який заснований на принципах придбання, обробки та формалізації знань для визначення технічного стану КЗА є актуальним.

Для ефективного вивчення та систематизації методів формалізації знань, їх застосування в контексті визначення технічного стану може бути розділено на кілька ключових напрямків. Експертні системи використовують знання експертів для моделювання та розв'язання проблем. В контексті технічного стану, експертні системи можуть використовуватися для автоматизованого аналізу симптомів та визначення можливих несправностей. Машинне навчання дозволяє системам навчатися на основі даних та роби-

ти прогнози. В контексті технічного стану, це може включати в себе класифікацію стану пристроїв на основі великого обсягу даних про їхню роботу. Логічне програмування може бути застосоване для створення правил та умов, які визначають технічний стан системи, з використанням формальної логіки для визначення стану системи. Бази даних дозволяють ефективно організовувати та аналізувати великі обсяги даних, що визначають стан систем. Застосування гібридних методів для комбінації різних методів формалізації знань для отримання комплексного підходу для точного визначення технічного стану. Так, використання системи моніторингу та діагностики використання датчиків та систем збору даних для постійного моніторингу стану пристроїв може бути формалізованим для виявлення аномалій та передбачення можливих несправностей.

Отже, проведене дослідження дозволяє стверджувати, що вирішення задачі визначення технічного стану КЗА неавтоматизованим способом в сучасних умовах швидкої зміни бойової обстановки, не є ефективною. Проведений аналіз підходів щодо автоматизації задачі оцінки технічного стану комплексу та подальшого його прогнозування обґрунтовує застосування нових інформаційних технологій, а саме експертних систем, систем, заснованих на машинному навчанні та логічному програмуванні, що забезпечить оперативну видачу якісної рекомендації особі, яка приймає рішення, для визначення технічного стану елементів КЗА.

УДК 681.518.2, 681.514

Скачков В.В., Чепкій В.В., Єфимчиков О.М., Набок В.К., Єльчанінов О.Д.

РІШЕННЯ ПРОБЛЕМИ ОБЧИСЛЮВАЛЬНОЇ СТІЙКОСТІ ЗВОРОТНИХ ЗАДАЧ МЕТОДОМ ДИНАМІЧНОЇ РЕГУЛЯРИЗАЦІЇ ВИБІРКОВИХ ОЦІНОК КОРЕЛЯЦІЙНОЇ МАТРИЦІ СПОСТЕРЕЖЕНЬ

Вступ. Аналізується проблема обчислювальної стійкості зворотних задач, за якої незначні варіації спостережуваних процесів призводять до непередбачених результатів їх рішення. Подібні задачі належать до класу некоректних або умовно коректних задач. Розв’язання таких задач в додатках спектрального аналізу, обробки просторово-часових сигналів, теорії прогнозування та прийняття рішень здійснюється методом регуляризації А.М. Тихонова та його модифікаціями [1-4]. Зазначені методи базуються на додаванні деякого фіксованого позитивного числа – параметра регуляризації μ в діагональні елементи оцінки N-мірної кореляційної матриці $\hat{\mathbf{A}}(L)$. Остання формується за L вибірками вектору спостережень $\mathbf{U}(L)$ шляхом прямого або рекурентного підсумування ермітових матриць одиничного рангу. В цьому контексті матрицю $\hat{\mathbf{A}}(L)$ можна віднести до класу ермітових з рангом, який монотонно зростає за N ітерацій від одиниці до N. Відповідно, в діапазоні вибірок $1<L<N$ інверсія матриці $\hat{\mathbf{A}}(L)$:$\hat{\mathbf{A}}^{-1}(L)$ є нестійкою за критерієм Адамара. Клас матриць з такою властивістю рангу потребує нестандартного підходу до їх регуляризації [5].

За класичного підходу параметр регуляризації μ повинен мати оптимальне значення. Даний тип регуляризації носить статичний характер. Вибір оптимальної величини параметра статичної регуляризації μ дає можливість змінювати вклад апріорної інформації щодо рішення задачі в атрибутах критеріальної функції $J(\mathbf{W},\mu)$, де $\mathbf{W}$ – вектор рішення, якому відповідає матриця спостережень $\hat{\mathbf{A}}(L)$. Разом з тим:

−підвищення параметра μ порушує узгодженість рішення $\mathbf{W}$ з вихідними даними;

−тривіальність властивостей статичної регуляризації обмежує можливості природної регуляризації (саморегуляризації), за якої некоректна задача розв’язується методами, що допускають управління мірою близькості отриманого рішення до точного за рахунок зростання обсягу вибірки L векторного процесу $\mathbf{U}(L)$;

−відсутність на поточний момент універсального алгоритму для визначення величини параметра статичної регуляризації μ оцінки кореляційної матриці спостережень $\hat{\mathbf{A}}(L)$, яка оптимальна для всього об'єму вибірки L.

В доповіді висвітлюється проблема обчислювальної стійкості зворотних задач методом динамічної регуляризації вибіркових оцінок кореляційної матриці $\hat{\mathbf{A}}(L)$ з рангом, який монотонно зростає в масштабі реального часу.

Основна частина. В загальному випадку процес обчислення оцінки ермітової кореляційної матриці $\hat{\mathbf{A}}(L)$, з наступними її обертанням $\hat{\mathbf{A}}^{-1}(L)$ на кожній ітерації, здійснюється шляхом опрацювання інформаційного процесу в масштабі реального часу за схемами прямого або рекурентного підсумування N-мірних матриць одиничного рангу, а саме вироджених матриць. Отримані оцінки матриць $\hat{\mathbf{A}}(L)$ та $\hat{\mathbf{A}}^{-1}(L)$ в асимптотичному сенсі збігаються до істинних величин $\mathbf{A}$ та $\mathbf{A}^{-1}$, ступень наближення яких відображають поведінкові функції $G(L)$. У зв'язку з постійним значенням параметра μ слушність цих оцінок не типова для методів статичної регуляризації.

Конзистентність, незміщеність та ефективність оцінок кореляційних матриць $\hat{\mathbf{A}}(L)$ та $\hat{\mathbf{A}}^{-1}(L)$ гарантує запропонований метод динамічної регуляризації. Зобов'язуюча сутність метода полягає в збіжності значення параметра $\mu(L)$, як монотонної функції регуляризації, до нульового рівня за умови надходження інформації в масштабі реального часу та відсутності потреби в попередньому прогнозуванні [6-8].

Специфіка дослідження відомих методів регуляризації полягає у визначенні виключно асимптотичних значень, що потребує необмеженого обсягу вибірок L. Як наслідок, ускладнюється аналітичний опис процесу обчислення оцінок кореляційних матриць $\hat{\mathbf{A}}(i)$ та $\hat{\mathbf{A}}^{-1}(i)$ на довільній ітерації $i \in [1, L]$. Отримати аналітичну залежність проблемно, а де-факто неможливо за наявності:

−по-перше, невизначеності результатів оцінки $\hat{\mathbf{A}}(i)$ та $\hat{\mathbf{A}}^{-1}(i)$, внаслідок цього виродження випадкових N-мірних матриць не повного рангу, коли $i<N$;

−по-друге, складності представлення статистичного розподілу власних значень та унітарних векторів випадкових матриць для будь-якої довільної ітерації $i \in [1, L]$.

Перспективний напрямок подоланням зазначених обмежень афілійований з імітаційним моделюванням, яке дозволяє отримати достовірні результати в сенсі їх збіжності до асимптотичних розподілів та оцінок. Така збіжність результатів наочно ілюструє ефективність процесу статичної та динамічної регуляризації за критерієм конзистентності та обчислювальної стійкості вибіркових оцінок кореляційних матриць $\hat{\mathbf{A}}(L)$ та $\hat{\mathbf{A}}^{-1}(L)$. З метою визначення поведінкових функцій $G(L)$ регуляризованих оцінок кореляційних матриць $\hat{\mathbf{A}}(L)$ та $\hat{\mathbf{A}}^{-1}(L)$ організовано обчислювальний експеримент. В ході експерименту на кожній ітерації генерувались незалежні N-мірні стаціонарні гаусові вектори корисного просторово-часового сигналу $\mathbf{S}(i)$ та внутрішнього шуму $\mathbf{n}(i)$ за умови, що розмір кореляційної матриці перевищує число джерел корисного сигналу. У підсумку отримано оптимальну за критерієм конзистентності оцінок монотонну функцію регуляризації $\mu(L)$. Для дослідження динаміки наближення в евклідовому просторі оцінок матриць $\hat{\mathbf{A}}(L)$ і $\hat{\mathbf{A}}^{-1}(L)$ до істинних значень $\mathbf{A}$ і $\hat{\mathbf{A}}^{-1}$ методами статичної та динамічної регуляризації побудовано поведінкові функції $G(L,\mu)$ та $G[L,\mu(L)]$. Порівняльний аналіз функцій $G(L,\mu)$ та $G[L,\mu(L)]$ показує:

−поведінкова функція $G(L,\mu)$ не досягає нульового рівня, а за деякого обсягу L збігається до межі, рівень якої визначається значенням статичного параметра регуляризації μ та структурою спектра (обумовленістю) кореляційної матриці $\mathbf{A}$. Динаміка поведінкової функції $G(L,\mu)$ переконливо підтверджую не оптимальність метода статичної регуляризації в сенсі критерію конзистентність оцінок $\hat{\mathbf{A}}(L)$ і $\hat{\mathbf{A}}^{-1}(L)$;

−функція $G[L,\mu(L)]$ за умови зростання L монотонно збігається до нульової межі незалежно від структури спектра матриці $\hat{\mathbf{A}}(L)$. Даний факт ще раз підкреслює конзистентність оцінок, які були отримані методом динамічної регуляризації;

−метод динамічної регуляризації не передбачає використання трудомістких обчис-

лювальних алгоритмів для вибору оптимальної величини статичного параметра регуляризації μ. Зазвичай, такі алгоритми носять локальний характер і практично не можуть бути реалізовані в масштабі реального часу.

Теоретичні дослідження конзистентності максимально правдоподібної оцінки $\hat{\mathbf{A}}^{-1}(L)$ та проведений експеримент, враховуючи монотонність спадання параметра $\mu(L)$ за умови зростання вибірки L, описують алгоритм обчислення оптимального значення ваги динамічної регуляризації у вигляді: $\mu(L)_{opt} = NL^{-1}$ з такими властивостями [6, 7]:

−оптимальність параметра динамічної регуляризації $\mu(L)_{opt}$ визначається виключно розмірністю кореляційної матриці спостережень $\hat{\mathbf{A}}(L)$;

−простота обчислень в реальному часі за відсутності апріорної інформації;

−інваріантність оптимального параметра динамічної регуляризації до умов апріорної невизначеності відносно вихідних даних обчислювальної процедури.

Головна перевага динамічної регуляризації $\mu(L)_{opt}$ у розв'язанні зворотних задач полягає в задоволенні критерію «обчислювальна стійкість - конзистентність» вибіркової оцінки кореляційної матриці $\hat{\mathbf{A}}^{-1}$ за умови довільної розмірності N [6, 8].

Висновки. Результати дослідження порушують лише одне із проблемних питань пошуку оптимальних рішень зворотних задач в умовах апріорної невизначеності.

Заявлено оптимальний за середньоквадратичним наближенням алгоритм динамічної регуляризації вибіркових оцінок кореляційної матриці спостережень, в якому параметр вагової функції визначається розмірністю адаптивної інформаційної системи.

Метод динамічної регуляризації з оптимальним параметром володіє властивістю саморегуляризації вибіркових оцінок кореляційної матриці і подається як альтернатива для статичної регуляризації. Окрім того, даний метод дозволяє:

− виключити із рішення зворотної задачі область обчислювальної нестійкості, в якій інформаційні втрати максимальні;

− отримати рішення зворотної задачі в реальному часі без прогнозування та додаткових обчислювальних витрат на пошук оптимального параметра регуляризації.

Запропонований підхід відкриває перспективи для практичного рішення некоректних зворотних задач в сфері інформаційних та радіотехнічних додатків.

Список використаних джерел

1. Тихонов А. Н. Численные методы решения некорректных задач / А. Н. Тихонов, А. В. Гончарский, В. В. Степанов и др. М.: Наука, 1990. 231 с.

2. Lekhovytskiy D. I. To the theory of adaptive signal processing in systems with centrally symmetric receive channels. *EURASIP J. Advances Signal Process*. 2016. Vol. 33. P. 1–11. DOI: https://doi.org/ 10.1186/s13634-016-0329-z.

3. Абрамович Ю. П. Регуляризованный метод адаптивной оптимизации фильтров по критерию максимума отношения сигнал/помеха. *Радиотехника и электроника*. 1981. Том 26. №3. С. 543–551.

4. Черемисин О. П. Эффективность адаптивного алгоритма с регуляризацией выборочной корреляционной матрицы. *Радиотехника и электроника*. 1982. Том 27. №10. С. 1933–1942.

5. Осипов Ю.С., Васильев Ф.П., Потапов М.М. Основы метода динамической регуляризации. М.: Изд-во МГУ, 1999. 237 с.

6. Skachkov V., Chepkyi V., Efimchikov O., Korkin O., Dudush A. Dynamic Regularization Parameter Optimization of a Sample Estimate of the Correlation Matrix of Observations by the Criterion «Computational Stability – Consistency». 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), July 2-6, Lviv, Ukraine. IEEE, 2019. P. 18-23. DOI: https://doi.org/ 10.1109/UKRCON.2019.8879946.

7. V.V. Skachkov, V.V. Chepkii, O.M. Yefymchykov, O.Yu. Korkin, & A.A. Goncharuk. Solving the Problem of Forming Stable and Consistent Estimates of a Correlation Matrix of Observations Using the Method of Dynamic Regularization. *Cybernetics and Systems*

Analysis. 2021. Vol. 57. P. 82–90. DOI: https://doi.org/10.1007/s10559-021-00331-3.

8. Skachkov V, Chepkii V., Yefymchykov O., Nabok V., Yelchaninov O. Asymptotic optimality of adaptive systems with alternative standards in unclassified learning situations. *Cybernetics and Systems Analysis.* 2023. Vol. 59. No. 4. P. 624–632. DOI: https://doi.org/10.1007/s10559-023-00597-9.

Собецький Я.С., Несміян О.Ю., Гладишев М.Г.

АНАЛІЗ ПРОЦЕСІВ ОБРОБКИ ІНФОРМАЦІЇ НА КОМАНДНОМУ ПУНКТІ ПОВІТРЯНИХ СИЛ

Аналіз методів та моделей інформаційної підтримки процесів прийняття рішень, показав, що система підтримки прийняття рішень (СППР) має суттєве значення та використовується при прийнятті рішень, полегшуючи взаємодію між даними, процедурами аналізу та обробки даних, і моделями прийняття рішень. Також надається допоміжна інформація, особливо для виконання неструктурованих або слабоструктурованих завдань, де важко заздалегідь визначити дані та процедури для прийняття рішень.

СППР складається з двох основних підсистем - людей, що приймають рішення, та комп'ютерної системи. Модель прийняття рішень є формальним поданням задачі та процесу прийняття рішень на яку впливає багато різноманітних факторів, одним з яких є невизначеність інформації, що надходить на вхід СППР.

Невизначеність відіграє суттєву роль при плануванні військових операцій та під час управління Повітряними Силами, виникаючи з різноманітних джерел та обставин. Існує значна кількість причин невизначеності, розв'язання яких може сприяти ухваленню точних та обґрунтованих рішень, спрямованих на зменшення непередбачуваних ситуацій. Бойовий простір, в якому проводять операції Повітряні Сили, характеризується великою динамікою, постійними змінами та невизначеністю, що впливає на стратегії, тактику та прийняття рішень. Невизначеність виникає через обмежену кількість інформації. Якщо даних недостатньо або якщо інформація не повна, прогнозування стає складним завданням. Ключовою причиною невизначеності є випадковість багатьох явищ, яка визначається їхньою природою та стохастичністю.

Нестохастичні чинники, також спричинюють невизначеність, через недостатню інформацію про явища, що не є випадковими. В контексті прийняття рішень на командних пунктах, існують такі причини невизначеності, як неможливість повного передбачення процесів, відсутність повної інформації та вплив суб'єктивних факторів. Помилки в інформації, невідповідна інформація від радіолокаційних систем та нестабільність бойової обстановки також вносять свій вклад у виникнення невизначеності. Взаємодія цих факторів спричиняє виникнення невизначеності на командних пунктах тому розуміння цих причин є ключовим для розробки стратегій та технологій управління повітряними силами в сучасних умовах ведення бойових дій.

УДК 621.39:623.1/.7

Соболь М.Р., Кущ П.С., Сургай М.В., Мокряк А.Г.

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ВПРОВАДЖЕННЯ АКТИВНОЇ ФАЗОВАНОЇ АНТЕННОЇ РЕШІТКИ В БАГАТОКАНАЛЬНУ СТАНЦІЮ НАВЕДЕННЯ РАКЕТ 9С32 ТА ОБҐРУНТУВАННЯ МОЖЛИВОЇ ДО ВИКОРИСТАННЯ ЕЛЕМЕНТНОЇ БАЗИ

Багатоканальна станція наведення ракет (БСНР) 9С32 відіграє важливу роль під час виконання ЗРК С-300В1 завдань за призначенням. Разом з тим, на сьогоднішній час залишковий ресурс наявних станцій є мінімальним, тому постає питання щодо пошуку шляхів усунення наведеного недоліку [1-16].

Аналіз пропозицій щодо підвищення характеристик станції показав, що окремо розглядаються питання удосконалення приймальної, передавальної або антенно-хвильоводних систем. Разом з тим, це дозволить вирішити проблемне питання стосовно лише однієї з систем станції, а не проблемпе питання в цілому.

Перспективним шляхом збільшення наявного ресурсу, покращення характеристик приймальної, передавальної та антенно-хвильоводної систем є використання в БСНР 9С32 активної фазованої антенної решітки (АФАР).

Суттєвою перевагою застосування АФАР є відносно низькі втрати енергії при генерації потрібних сигналів, спрощення цифрової обробки та інші.

В доповіді наведено результати аналізу особливостей побудови, функціонування та характеристик існуючих та перспективних АФАР.

За результатами досліджень було прийнято рішення щодо доцільності застосування в БСНР 9С32 ЗРК С-300В1 АФАР.

Наведено, що реалізація запропонованого рішення дозволить покращити характеристики "застарілих" ЗРК, що знаходяться на озброєнні зенітних ракетних військ Повітряних Сил Збройних Сил України.

Наведені пропозиції щодо побудови та елементної бази АФАР.

Список використаних джерел

1. Dzhus, V., Roshchupkin, Y., Kukobko, S., Herasymov, S., Drob, N., & Trofymova, M. Estimation of noise radiance point sources multichannel direction finding systems resolution by linear prediction method. Sistemi obrobki ìnformacìï. 2021. № 4(167). С. 19-26. https://doi.org/10.30748/soi.2021.167.02

2. Сухаревский О.И., А.Ю. Шрамков & Рощупкин Е.С. (2005). Высокочастотный метод расчета диаграммы направленности антенны с учетом неоднородностей рельефа местности на позиции РЛС. Моделювання та інформаційні технології, (33), 174-181.

3. Рощупкин, Е.С., & Беляев, Д.Н. (1999). Измеритель коэффициента стоячей волны в виде ответвителя дециметрового диапазона волн. Збірник наукових праць за матеріалами 3-го міжнародного молодіжного форуму "радіоелектроніка і молодь у XXI столітті" 20-23 квітня 1999 р., 1, 52–55. https://doi.org/10.5281/zenodo.5591877

4. Крючков, Д. М., Рощупкін, Є. С., Калита, О. В., & Дранник, П. А. (2023). Пропозиції щодо підвищення ефективності відновлення сукупності різнотипних радіоелектронних засобів спеціального призначення при їх використанні в різних умовах. XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023), Kharkiv. https://doi.org/10.5281/zenodo.10257044

5. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2006). Алгоритмы когерентной обработки широкополосных сигналов на промежуточной частоте с использованием схем фазонастраивающих контуров с управляемыми дисперсионными линиями задер-

жки в крупноапертурных антенных решетках и многопозиционных системах. Прикладная радиоэлектроника, (Т.5, №2), 250-254.

6. Маслов А.Ф., Рощупкин Е.С. & Шрамков А.Ю. (2005). Организация когерентной обработки на промежуточной частоте при приеме широкополосных сигналов крупноапертурными антенными решетками и многопозиционными системами. Прикладная радиоэлектроника, (Т.4, №4), 437-440.

7. Бєляєв, Д.М. Застосування векторних аналізаторів сигналів для забезпечення електромагнітної сумісності радіоапаратури / Д.М. Бєляєв, С.В. Герасимов, С.В. Кукобко [та ін.] // Збірник наукових праць ЦНДІ ОВТ ЗС України, - 2016. №3(62), -с. 77-84.

8. Tymchenko, S., Kaplun, Y., Roshchupkin, E., Kukobko, S. (2023). Substantiation of Time Distribution Law for Modeling the Activity of Automated Control System Operator. In: Shkarlet, S., et al. Mathematical Modeling and Simulation of Systems. MODS 2022. Lecture Notes in Networks and Systems, vol 667. Springer, Cham. https://doi.org/10.1007/978-3-031-30251-0_9

9. Рощупкін Є.С. Великоапертурна (рознесена) радіолокаційна система: пат. 148518 Україна : G01S7/42, H01Q21/00 / Є.С. Рощупкін, С.В. Герасимов, С.В. Кукобко, М.В. Борисенко, Ю.О. Крихтін, О.Ф. Галицький, Б.В. Гайбадулов, В.В. Джус, І.В. Помогаєв, В.В. Борисов, Ю.О. Чміль, А.Ю. Задорожна. – u 202100336; заявл. 29.01.2021; опубл. 18.08.2021, бюл. № 33/2021, – 7 с.

10 Herasimov S., Roshchupkin E. (2022). Parameters of monitoring the technical condition of airspace radio engineering monitoring systems. International scientific and practical conference "Application of information technologies in the preparation and operation of law enforcement forces", Kharkiv.

11. Рощупкін, Є. С., Гречка, О. В., Галицький, О. Ф., & Гайбадулов, Б. В. (2023). Аналіз факторів, що впливають на ефективність відновлення різнотипних радіотехнічних засобів складної системи під час виконання завдань за призначенням в екстремальних умовах. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей тринадцятої міжнародної науково-технічної конференції. Том 1: секції 1, 3, 4, Баку-Харків-Жиліна. https://doi.org/10.5281/zenodo.7868194.

13. Кукобко С.В., Місценко Р.В., Бритов Д.М., Рощупкін Є.С., & Гайбадулов Б.В. (2023). Пропозиції щодо автоматизації процесу прийняття рішення при класифікації ситуацій у повітряному просторі. Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку", Харків

14. Кукобко С.В., Рощупкін Є.С. (2022). Моделювання системи технічного обслуговування безпілотних літальних апаратів. Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2022): тези доповідей XII Міжнародної науково-практичної конференції, Чернігів

15. Herasimov, S., Borysenko, M., Roshchupkin, E. et al. Spectrum Analyzer Based on a Dynamic Filter. J Electron Test 37, 357–368 (2021), https://doi.org/10.1007/s10836-021-05954-0

16. Herasimov S.V. Assessment of possibilities of detection and tracking of drones the system of radiolocation stations of antiaircraft defense / S.V. Herasimov, S.V. Kukobko, E.S. Roshchupkin, A.E. Roshchupkina// Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXVIII міжнародної науково-практичної конференції MicroCAD-2020, 28-30 жовтня 2020 р.: у 5 ч. Ч. V. / за ред. проф. Сокола Є.І. – Харків: НТУ "ХПІ". – С. 270.

Sovhar O.

USING INTERACTIVE METHODS OF LEARNING TO FORM FUTURE ARMED FORCES OFFICERS' FOREIGN LANGUAGE COMMUNICATIVE COMPETENCE

In the light of current situation in Ukraine and the state's strategic course on Euro-Atlantic cooperation the problem of creating and retaining strong, combat-ready, mobile armed forces is of paramount importance. The foundation of such an army should be military professionals capable of effectively carrying out assigned tasks in both peace and wartime. To this end, effective training system of such professionals has to be established in which language training is duly prioritized. This created the necessity to intensify the educational process in conditions of high informational and psychophysiological load in order to enhance the effectiveness of education, although not through a simple increase in labor costs, time of teachers, students, and material resources, which is characteristic of extensive development, but primarily due to their more rational application and the creation of favorable conditions for the perception of educational material. The goal of training intensification at the higher military institutions is to meet modern practice requirements for the training of highly qualified military specialists through the integrated use of the most effective forms, methods and means of training, as well as the organization of close interaction between learning process stakeholders.

In this context, an important aspect is the improvement of the system of language training in order to increase the level of foreign language communicative competence of military personnel. The learning outcomes here include knowledge of professionally oriented terminology; the ability to communicate with partners from different national forces, knowledge of relevant structures and specifics of international documentation in the context of international cooperation; gaining command of the English language, which enables service members to be interoperable in the international military community; an opportunity to improve the level of foreign language command for military personnel who have successfully passed tests at language (professional) courses abroad. At the same time, fluency in foreign language (most often English) provides an opportunity for Ukrainian soldiers and officers to participate in international exercises and training that take place on the territory of Ukraine and outside its borders, and also enables officers involved in research to participate in the development of military science by publishing their scientific achievements in various foreign publications, and sharing their valuable experience, which becomes indispensable a step in career growth. The improvement of the system of language training of military specialists should take place in an integrated manner, in combination with the psychological and pedagogical disciplines to achieve the goal of forming the ability of milirary men and women to communicate at the international level.

If traditionally training methods of learning prevailed in educational practice, now it is more productive to use creative, interactive, projective, innovative methods. The effectiveness of foreign language learning depends on the choice of teaching approaches. Interactive methods activate educational activities, which will ensure the competion of learning tasks, interaction and mutual understanding. The basic principle of the interactive method is the principle of collective interaction, according to which cadets achieve communicative goals through social-interactive activities: discussions, debates, role-playing, simulation games, etc. The educational role-playing game is based on the following principles: correlation of the content with the structure of the educational role-playing game; inter-subject and inter-cycle links of learning content; principle connections of the content of the game with the conditions of professional activity of future officers. Thanks to the abovementioned principles, the main tasks of the educational role-playing game are achieved, namely the formation of a system of knowledge, abilities, and skills of communicative activity in a foreign language; development of creative and cognitive activity; implementation of the connection of theoretical

professional knowledge with the foreign language practice of future officers. Therefore, educational role-playing is an effective method of forming professional foreign language communicative competence, which makes it possible to improve the knowledge, skills, and abilities of cadets in a foreign language.

A simulation game is a type of role-playing game, an imitation of a situation of professional communication, which is implemented using the means of a foreign language. This game allows you to simulate a real professional environment and its problems. The presence of real roles in such a game, simulation of real conflict situations, close to reality, contribute to the creation of controlled emotional tension.

In the game, the future officers perform the assigned tasks drawing on their own experience and reproducing the knowledge, skills, and abilities they have acquired during professional training. After all, the simulated situations in the games imitate the problems of professional communication well known to the cadets. The following simulation games could be organized for the cadets in practical foreign language classes: "Patrolling", "Convoys", "Joint training of Ukraine and other nations". They are conducted in order to practice military-technical and military-political terminology and vocabulary, speech etiquette of service members, overcome difficulties that arise when communicating with foreign military personnel, performing combat missions. The simulation game performs the following functions:

- motivational, which involves the presence of a goal, roles, a dynamic game situation, certain attitudes, rules of the game, duties and responsibilities of cadets;
- informational and analytical, the essence of which is that role-playing games are the final stage of comprehensive understanding of the various theoretical knowledge that cadets have mastered earlier within a certain topic. The final lesson conducted at the end of logically related topics in the form of a role-playing or simulation game allows cadets to practice the transition from acquiring theoretical knowledge to applying it in practice;
- organization and management, the heuristic function of which consists in the purposeful management by the teacher of the mental activity of the cadets, as well as in the formation of such cognitive structures that allow the cadets to independently regulate their thinking and make decisions;
- developmental and educational, enabling to reveal the creative and critical thinking skills potential of the cadets, providing them comprehensive development and formation of value orientations;
- communicative as it develops communicative competence (cadets learn to cooperate with other people, correctly perceive their opinion, master psychology and ethics);
- assessment-reflective-evaluative − enables cadets to analyze their own actions and state , overcoming psychological barriers, fears, and mastering the skills of emotional self-regulation.

The benefits of using simulation and role-playing games during the formation of professional foreign language communicative competence of future officers are increasing the personal and professional motivation of cadets; developing systematic critical thinking thanks to the assimilation of the theoretical and practical knowledge, forming interdisciplinary and intercyclical connections; stimulation of creative activity and independence; formation of educational cooperation and partnership between cadets and the teacher; development of unrehearsed speaking skills, overcoming the barrier between learning a foreign language and its practical application; acquisition of social interaction skills, professional traits and qualities of a competent professional capable of foreign language communication.

УДК 621.396.96

Соколко К.В., Бакуменко Б.В.

ДОСВІД ВИКОРИСТАННЯ СПЕЦІАЛЬНОГО ПРОГРАМНОГО МАТЕМАТИЧНОГО ЗАБЕЗПЕЧЕННЯ (ВІРАЖ-ПЛАНШЕТ) ДЛЯ ОЦІНКИ ПОВІТРЯНОЇ ОБСТАНОВКИ

Досвід російсько-української війни показав важливість оцінки повітряної обстановки з метою підвищення якості своєчасного виявлення та супроводження повітряних цілей. Оцінка повітряної обстановки є одною зі складових процесу прийняття рішення на виконання бойового завдання.

Оцінювання обстановки командиром включає оцінку: повітряного і наземного противника; бойові можливості забезпечуваних і взаємодіючих частин і підрозділів; бойові можливості свого підрозділу; вимоги до розвідувальної і бойової інформації; стан видів забезпечення; умови місцевості, їх вплив на виконання завдання.

Для радіотехнічних підрозділів найбільш важливе значення оцінювання обстановки має оцінка повітряного та наземного противника, особливо в ході безпосереднього виконання бойового завдання.

Аналіз виконання завдань в ході російсько-української війни окремими радіолокаційними взводами (ЗвП) чи окремими РЛС показав, що практично всі вони змінювали свої позиції. Розгортання їх здійснювалося в більшості у першому ешелоні чи на лінії зіткнення, при цьому слід враховувати дальність ураження зенітно-артилерійськими засобами противника. Дальність до вогневих засобів противника можливо визначити використовуючи «Віраж-Планшет».

Для оцінки повітряного противника необхідно знати: типи літальних апаратів, що задіяні в ударі; ЛТХ засобів повітряного нападу; підлітний час засобів повітряного нападу; напрямок основного удару. Оперативне проведення розрахунків зони виявлення РЛС (зони інформації підрозділу) надають можливість оцінити не тільки правильність вибору позиції, а також рубежі виявлення ЗПН, особливо БпЛА.

Використовуючи програмне математичне забезпечення «Віраж-РД, -П», та оперативне введення вихідних даних вибраної позиції, можливо в короткі терміни розрахувати рубіж виявлення цілей на заданій висоті та визначити напрямок головного удару повітряного противника. В ході виконання бойового завдання виявлення розвідувального БпЛА (типу «Орлан, Зала») після оцінки обстановки дають можливість своєчасно прийняти рішенні на зміну позиції РЛС з метою виведення з під удару від БпЛА (типу «Ланцет»).

Запропоновані пропозиції для оцінки повітряної обстановки підвищать можливість своєчасно виявлення повітряного противника, вірного визначення режимів бойової роботи ЗРЛ, своєчасної зміни позиції для збереження особового складу та РЛС.

УДК 004.93

Стасєв Ю.В., Гончаренко К.Г.

РОЛЬ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ ДЛЯ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ

У сучасному цифровому середовищі попит на безпечні та надійні методи автентифікації досяг безпрецедентного рівня. Паролі, які раніше були основним засобом перевірки особи, поступово піддаються підвищеній уразливості до кіберзагроз. У зв’язку з цим

почалися пошуки альтернативних механізмів автентифікації. Розробники сучасних систем захисту зосередили свої зусилля на біометричних методах автентифікації. Біометричні методи захисту охоплюють використання відмінних фізичних або поведінкових атрибутів для цілей ідентифікації користувачів та мають значний потенціал для зміни парадигми кібербезпеки. Біометричні атрибути включають відбитки пальців, риси обличчя, голос, сканування райдужної оболонки, сітківки ока та навіть ритми друку. На відміну від паролів чи токенів, які легко загубити або вкрасти, біометричні дані є ексклюзивними для кожної особи, тому їх складно підробити чи відтворити.

Враховуючи досягнення науково-технічного прогресу, кіберзлочинці адаптують свою тактику, щоб використовувати вразливості в системах безпеки. Для інформаційних систем (ІС) вкрай важливо встановити надійні протоколи кібербезпеки, щоб захистити свою конфіденційну інформацію.

Проведені дослідження, в тому числі з участю авторів показали, що ключовим елементом у цій боротьбі з кіберзагрозами є біометрична технологія, яка забезпечує відмінні та безпечні методи автентифікації користувачів. Біометричні системи (БС) відіграють важливу роль у захисті ІС, використовуючи унікальні фізіологічні чи поведінкові особливості для ідентифікації та автентифікації користувачів. Інтеграція БС у захист ІС пропонує потужне рішення для підвищення безпеки, зменшення залежності від вразливих методів автентифікації та забезпечення більш надійної та зручної роботи в різних програмах, від контролю фізичного доступу до захисту цифрових даних.

В доповіді приводиться аналіз існуючих біометричних систем. Встановлено, що ІС з БС захисту повинні відповідати таким вимогам, як: унікальність і незамінність, покращена безпека, зменшення ризику несанкціонованого доступу, безпечний контроль доступу, безпека біометричних баз даних, багатофакторна автентифікація, зручність для користувача, неможливість передачі, відповідність положенням про конфіденційність, безперервний моніторинг, інтеграція з системами контролю доступу та повинні мати розширені заходи проти спуфінгу.

В доповіді авторами розглянуто значення біометрії в сфері кібербезпеки, досліджено ризики, з якими вони стикаються і доступні рішення для протидії цим викликам, проаналізовано, що деякі БС підтримують постійну автентифікацію, постійно перевіряючи особу користувача під час активного сеансу, біометричні системи можуть бути інтегровані з системами контролю доступу, підвищуючи фізичну та логічну безпеку.

УДК 004.056.53

Стасєв Ю.В., Козюберда К.В.

АНАЛІЗ МЕТОДІВ СТАТИСТИЧНИХ АТАК НА СТЕГАНОСИСТЕМУ У ВИГЛЯДІ ЗОБРАЖЕННЯ

У минулі роки зацікавленість у використанні стеганографічних методів значно зросла. Це пояснюється можливістю передавати інформацію через відкриті канали зв'язку. З урахуванням цього факту, зловмисник старається виявити факт передачі конфіденційної інформації через відкриті файли та здобути доступ до передаваної інформації.

Одночасно помітно розвивається стеганоаналіз, основне завдання якого – встановлення факту присутності в контейнері прихованої інформації. Під час вирішення цього завдання стеганоаналітиком використовуються різні методи аналізу. Проте при спробі автоматизації процесу на множині контейнерів виникає проблема вибору методу аналізу, оскільки реалізації різних методів можуть давати протиріччя у результаті, що обумовлено, насамперед, нерівністю ймовірностей виникнення помилок розпізнавання для цих реалізацій. Крім того, в умовах апріорної невизначеності щодо типу стеганосисте-

ми значну складність представляє питання вибору вихідних даних для аналізу. Зменшення обсягу аналізованих даних потенційного контейнера призводить до збільшення ймовірності виникнення помилки першого роду, що, в свою чергу, збільшує ймовірність виникнення помилок другого роду. Зміна правил вибірки аналізованих даних призводить до зростання помилок розпізнавання.

Таким чином, на даний момент для вирішення завдання стеганоаналізу та подальшого вилучення прихованої інформації необхідний комплексний підхід, що дозволяє виділити на множині результатів ті з них, які сприяють мінімізації ймовірності помилки другого роду за заданим рівнем ймовірності помилки першого роду. Статистичні методи базуються на понятті “природного” контейнера. Суть методів полягає в оцінюванні ймовірності існування стегоповідомлення на основі критерію оцінки близькості досліджуваного контейнера до “природного”. Основним недоліком методів цього класу є саме припущення про існування “природного” контейнера.

Авторами розглянуто основні методи статистичного стегоаналізу, а саме:

Метод хі-квадрат: Цей метод ґрунтується на порівнянні спостережуваних та очікуваних значень в певному контексті. В стеганоаналізі він використовується для оцінки статистичної значущості різниці між фактичним розподілом даних та очікуваним розподілом у випадку відсутності прихованої інформації. Переваги методу у відносно простий у реалізації та розумінні, а також він добре підходить для виявлення загальних аномалій у розподілі даних. Недоліки: чутливий до розміру вибірки даних, може недооцінювати аномалії в складних розподілах.

Метод аналізу перетворень відліку (LSB analysis): цей метод стосується аналізу найменших значущих бітів (LSB) в цифрових даних, зазвичай у зображеннях чи аудіофайлах. Він базується на припущенні, що прихована інформація часто вбудовується, змінюючи найменш значущі біти даних. Переваги: ефективний для виявлення вбудованої інформації у зображеннях та аудіофайлах. Недоліки: не ефективний для виявлення вбудованої інформації у бінарних даних або даних інших форматів; може бути обмежений при застосуванні до дуже маленьких або дуже великих зображень.

Метод кореляції: цей метод полягає в аналізі статистичної залежності між різними частинами даних. У стеганоаналізі кореляція може бути використана для виявлення прихованої інформації, яка може впливати на статистичні зв'язки в даних. Переваги: ефективний для виявлення статистичних зв'язків між частинами даних. Недоліки: може бути чутливий до шуму в даних та вимагає великої кількості даних для надійних результатів.

Метод аналізу фільтрів: Цей метод включає в себе використання цифрових фільтрів для виділення певних характеристик сигналу, які можуть бути специфічні для прихованої інформації. Цей метод е фективний для виділення певних характеристик сигналу. Проте може бути обмежений до використання в конкретних ситуаціях та вимагає налагодження параметрів фільтрів.

Провівши аналіз, автори зробили наступні висновки. Існує широка різноманітність статичних методів, кожен з яких має свої переваги та обмеження. Важливо вибирати методи залежно від типу даних та природи прихованої інформації. Використання комплексного підходу методів може підвищити ефективність стеганоаналізу та знизити ймовірність помилок. Деякі методи можуть вимагати налагодження параметрів для досягнення оптимальних результатів. Важливо ретельно налаштувати параметри з урахуванням конкретних умов та вимог задачі.

Стовба Р.Л., Коба А.С., Міщеряков Ю.Г.

РОЗШИРЕННЯ ІНФОРМАЦІЙНИХ МОЖЛИВОСТЕЙ В УМОВАХ ПІДГОТОВКИ ТА ДІЯЛЬНОСТІ СИЛОВИХ СТРУКТУР ПРИ ЗАСТОСУВАННІ МЕТЕОКАНАЛІВ У РЛС РТВ БОЙОВОГО РЕЖИМУ

Досвід російсько-української війни та сучасних військових конфліктів переосмислив весь етап підготовки та вніс певні зміни у форму ведення бойових дій. Невід'ємною частиною, стало широке застосування, як противником так і Силами Оборони, безпілотних летальних апаратів (БПЛА). На полі бою в інтересах силових структур БПЛА можуть вирішувати такі задачі: ведення повітряної розвідки й визначення координат цілей, радіоелектронна розвідка, радіоелектронне подавлення, перенавантаження зон ППО хибними цілями; видача цілевказування системам зброї з лазерним наведенням; корегування вогню артилерії; ураження наземних цілей, включаючи засоби їх радіолокаційного виявлення – радіолокаційні станції (РЛС); забезпечення радіорелейного зв'язку; пошук замінованих ділянок місцевості.

Але на відміну від великої кількості переваг застосування БПЛА, можливо виділити і ряд недоліків БПЛА:

– є певні обмеження з застосування БПЛА у залежності від часу доби й погодних умов;
– обмежений функціонал дій у автономному режимі;
– низька прихованість каналів радіокерування й передачі даних;
– схильність каналів управління й каналу супутникової навігації БПЛА до впливу радіоелектронних завад.

У пілотів комплексів БПЛА часто виникає необхідність здійснювати планування та безпосередньо виконувати польотне завдання, з урахуванням метеорологічної обстановки в зоні дії БПЛА та наслідків впливу метеоутворень на технічні та тактичні характеристики БПЛА. Знання командиром метеорологічної обстановки впливає на визначення варіантів цільового навантаження та програмування польотного завдання. Всебічне забезпечення метеоінформацією дасть змогу найкраще виконувати поставлені завдання. З іншої сторони, для виявлення ворожих БПЛА в зоні відповідальності Сил оборони, використовуються радіолокаційні станції окремих радіотехнічних батальйонів, що несуть безперервне бойове чергування, в наслідок чого, стають пріоритетними цілями для противника. Враховуючи інформацію про погодні умови, можливо досягти зменшення часу роботи РЛС на випромінювання, з метою виявлення БПЛА противника, тим самим підвищуючи живучість підрозділів радіотехнічної розвідки.

На сьогодні можливості з отримання метеорологічної інформації у Повітряних Силах суттєво обмежені, в наслідок використання метеорадарів старого парку. За умови обладнання РЛС радіотехнічних військ (РТВ) спеціальними метеоканалами, такі можливості будуть суттєво розширені. Дослідженнями доведено, що використання нових методів й алгоритмів обробки відбитих сигналів від метеоутворень, як корисних сигналів, а не придушення їх, як завад, дозволить ефективно підвищити тактичні спроможності Сил оборони, використовуючи метеоінформацію від РЛС РТВ в зоні їх виявлення. Цю метеоінформацію силові структури можуть отримувати через систему збору, обробки, відображення та аналізу інформації про повітряну обстановку «Віраж-планшет».

Стрельбіцький М.А.

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Оперативно-службова діяльність Держприкордонслужби України в умовах стрімкого розвитку інформаційних технологій вимагає наявності високоефективних інформаційних систем (ІС). Зазначені системи являють собою складні організаційно-технологічні структури, створення яких вимагає вирішення комплексу системних задач.

Визначення кількісних та якісних оцінок ефективності як об'єктивного підтвердження якості ІС є достатньо складним завданням, що залежить від їх призначення, умов функціонування, типу інформації яка циркулює в ній, тощо.

Загалом ефективність ІС як складного комплексу програмно-апаратних засобів, технічних, організаційних та інших методів і заходів – це здатність системи протистояти негативним впливам дестабілізаційних факторів.

На сучасному етапі розвитку інформація є одним з найцінніших ресурсів, який визначає рівень національної безпеки держави. З розвитком інформаційних технологій і зростанням значущості технічних засобів зв'язку ІС піддаються все більшій кількості інформаційних дестабілізаційних впливів, які за умови їх реалізації можуть призвести до збитків національного масштабу.

Оцінюючи ефективність ІС необхідно звернути увагу на те, що це властивість саме процесу функціонування, а не самої системи. Тому в подальшому під поняттям ефективності ІС будемо розуміти комплексну властивість цілеспрямованого процесу, який характеризується ступенем досягнення мети системи.

Оцінюючи якість ІС, яка описується n-вимірним векторним показником $Y_{\langle n\rangle}$, необхідно визначити сукупність критеріїв, які належать класу критеріїв придатності $\{G\}$, математичне формулювання якого має вигляд

$$G:\left(Y_{\langle n\rangle}\in\left\{Y_{\langle n\rangle}^{A}\right\}\right), \tag{1}$$

де $Y_{\langle n\rangle}$ – показник якості ІС;

$\left\{Y_{\langle n\rangle}^{A}\right\}$ – множина допустимих значень показника якості ІС.

Отже, ІС, для якої виконується умова (1), придатна до використання за призначенням та виконує свої функції.

Серед множини властивостей ІС істотними є ті, які визначають якість процесу її функціонування. Разом із тим у процесі функціонування ІС витрачаються певні ресурси. Отже, ІС у будь-який момент часу можна охарактеризувати трійкою властивостей:

– результативністю – властивістю системи виконувати власні функції;

– ресурсоємністю, яка характеризується витратою ресурсів системи (матеріально-технічних, часових, енергетичних, фінансових, людських тощо);

– оперативністю – властивістю системи забезпечувати виконання функцій в межах визначеного часу.

Із зазначеного вище можна зробити висновок, що якість ІС не може бути охарактеризована окремими властивостями, а визначається тільки їх сукупністю, тобто трійкою властивостей.

Введемо позначення цих властивостей: $V_{\langle n_1\rangle}$ – показник результативності; $R_{\langle n_2\rangle}$ – показник витрат ресурсів; $T_{\langle n_3\rangle}$ – показник часу.

Тоді, показником якості ІС буде n-вимірний вектор, що містить три групи властивостей:

$$Y_{\langle n\rangle} = \left\langle V_{\langle n_1\rangle}, R_{\langle n_2\rangle}, T_{\langle n_3\rangle} \right\rangle, \tag{3}$$

де $n = n_1 + n_2 + n_3$.

Необхідно врахувати, що при згортанні різнорідних показників узагальнений показник губить фізичний сенс, тому при багатокритеріальному аналізі коректним є згортання показників тільки всередині груп показників результатів. Згортання показників якості функціонування систем із різних груп є неприпустимим.

Для оцінювання якості необхідно розробити показник ефективності процесу функціонування ІС, який повинен відповідати основним вимогам: показовість (адекватність), критичність (чутливість), комплексність (повнота), стохастичність, простота.

Показовість дозволяє оцінити ефективність функціонування ІС з точки зору виконання нею основного завдання. Отже, мета системи повинна явно міститись у показникові ефективності системи.

Критичність показника показує, наскільки він чутливий до змін у характеристиках процесу забезпечення ІС.

Комплексність показника дозволяє вирішити завдання визначення ефективності системи без залучення інших її характеристик.

Стохастичність дозволить урахувати невизначеність умов функціонування системи, впливу ДФ, які мають випадковий характер.

Простота показника ефективності сприяє доступності його сприйняття, а також аналізу якості функціонування ІС.

На показники результативності ІС впливають зовнішні та внутрішні фактори, які визначаються середовищем її функціонування.

Кожна з компонент вектора Y залежить від характеристик ІС та її організації, умов функціонування та умов застосування системи.

$$Y = Y\left(A_1, A_2, B_1, B_2\right), \tag{4}$$

де A_1 – характеристики ІС;

A_2 – характеристики організації процесу забезпечення ІС;

B_1 – характеристики умов функціонування ІС;

B_2 – характеристики умов застосування ІС.

У свою чергу компоненти вектора Y^A допустимих значень теж залежать від умов застосування системи і визначаються керуючою системою

$$Y^A = Y^A\left(B_2\right). \tag{5}$$

У загальному випадку на характеристики ІС, її організації, умови функціонування та застосування діє множина випадкових факторів, що визначає зазначені величини як випадкові. Разом із тим апріорі випадковими є і допустимі значення вектора Y^A, який залежить від умов застосування системи, оскільки завчасно невідомо, які повинні бути результати роботи ІС, щоб забезпечити необхідний рівень її функціонування. Окремі дослідження при визначенні умов застосування та функціонування ІС приймають припущення про найгірший їх варіант, тобто величини B_1 та B_2 є не випадковими. Зазначене припущення призводить до неправомірно великих витрат ресурсів.

Усі складові вектора показників якості функціонування ІС носять ймовірнісний характер, тому

$$\hat{Y} = Y\left(\hat{A}_1, \hat{A}_2, \hat{B}_1, \hat{B}_2\right), \tag{6}$$
$$\hat{Y}^A = Y^A\left(\hat{B}_2\right).$$

У результаті реальних умов експлуатації ІС критерій придатності (1) прийме вигляд

$$G:\left(\hat{Y}\in\left\{\hat{Y}^{A}\right\}\right). \quad (7)$$

З виразу (7) можна зробити висновок, що придатність процесу функціонування ІС – випадкова подія, яка безпосередньо не може відображати якість процесу. Тому характеристикою якості ІС є ймовірність випадкової події

$$P_{ДМ}=P\left(\hat{Y}\in\left\{\hat{Y}^{A}\right\}\right). \quad (8)$$

Отже, ймовірність $P_{ДМ}$ – це показник ефективності ІС, який визначає ступінь виконання нею своїх функціональних завдань. На її основі формується критерій придатності системи, тобто $P_{ДМ}\geq P_{ДМ}^{НОРМ}$.

Табенський С.М., Бабарика А.О., Лазоренко О.В., Кожушко В.Ю.

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ HTML5 PACKAGE ДЛЯ СТВОРЕННЯ ІНТЕРАКТИВНОГО НАВЧАЛЬНОГО КОНТЕНТУ

Організація навчального процесу в сучасних умовах практично не можлива без використання інформаційних технологій комунікації та взаємодії між людьми. Сьогодні зростає обсяг знань і технологій, що відповідно трансформуються в усі ланки життя суспільства, в тому чисті і в освітню діяльність, що вимагає застосовувати нові, зокрема інтерактивні технології навчання.

Інтерактивним називається весь той контент, який має на увазі безпосередню взаємодію користувача з сайтом.

Для створення інтерактивного контенту використовуються спеціально створені інформаційні системи, які призначені для розробки та збереження електронних навчальних матеріалів і програм та здійснення автоматизованого адміністрування навчальним процесом. Вони також створюють умови для спілкування в електронному середовищі курсантів між собою, курсантів та викладача, викладачів.

В освітньому середовищі існує велика кількість різноманітного програмного забезпечення та ресурсів, які дозволяють здійснювати інтерактивне наповнення занять, наприклад інтерактивні презентації (Prezi, Haiku Deck, Slides тощо), інтерактивні опитування (Mentimeter, Kahoot!, Quizalize тощо), інтерактивні дошки (Twiddla, MIRO, Trello тощо) та багато інших. Проте використання під час занять таких вузькоспеціалізованих ресурсів є складним як для викладача, так і для курсантів, адже кожен з них має різний інтерфейс, логіку роботи та потребує окремої реєстрації.

Тому, на сьогоднішній день, найбільш розповсюдженою навчальною платформою у світі, яка також використовується в Національній академії Державної прикордонної служби України імені Богдана Хмельницького, є Moodle (Modular Object-Oriented Dynamic Learning Environment — модульне об'єктно-орієнтоване динамічне навчальне середовище) — навчальна платформа призначена для об'єднання педагогів, адміністраторів і учнів (курсантів) в одну надійну, безпечну та інтегровану систему для створення персоналізованого навчального середовища.

Слід звернути увагу, що зазначена платформа містить ряд ресурсів та діяльностей, які дозволяють реалізовувати різноманітні інтерактивні елементи, для покращення засвоєння матеріалу здобувачів освіти.

Одним з модулів, який з’явився в Moodle після оновлення є H5P (HTML5 Package) - це новий безкоштовний засіб створення, обміну й використання інтерактивного мультимедійного навчального контенту. Створення і редагування контенту відбувається безпосередньо в браузері, конструктор вбудований в Moodle і не вимагає стороннього програмного забезпечення ,що полегшує роботу користувачеві.

H5P пропонує широкий спектр типів контенту, включаючи інтерактивні відео, презентації, тести, ігри та інше.

Серед яких можна виділити:

1. Image Hotspot (Зображення з «гарячими ділянками») – інструмент, який дозволяє створювати інтерактивні зображення з точками гарячих ділянок. Цей інструмент дозволяє користувачам розміщувати точки (або "гарячі ділянки") на зображенні та додавати до них відомості, текст, зображення чи навіть відео. Коли користувач наводить курсор на гарячу ділянку, з'являється випливаюча підказка з додатковою інформацією. Це дуже корисний засіб для створення інтерактивних навчальних матеріалів, мап та багатьох інших застосувань, де потрібно показати або пояснити певні області на зображенні.

2. Agamotto – інструмент, який дозволяє реалізувати інтерактивну послідовність зображень, а здобувач освіти має можливість здійснювати перехід між ними використовуючи перетягування вказівника, за бажанням до окремого зображення можна додати деталі у вигляді тексту, які його характеризують. Цей ресурс можна використовувати під час викладення матеріалу про певну послідовність дій різних процесів. Наприклад, порядок налаштування радіостанції, порядок проведення прикордонного контролю.

3. Course Presentation (Презентація курсу) - це інструмент H5P, який дозволяє створювати інтерактивні курси та презентації з різноманітними модулями та завданнями. Цей інструмент надає можливість створювати сторінки з різними типами контенту, такими як текст, зображення, відео, аудіо, питання та завдання.

4. Interactive Video (Інтерактивне відео) - це інструмент H5P, який дозволяє створювати інтерактивні відеоролики з додатковими елементами, такими як питання, коментарі та інші взаємодійні елементи. При цьому здобувачі освіти можуть взаємодіяти з відеороликом, відповідаючи на питання та перевіряючи свої знання під час перегляду, що значно підвищує засвоєння матеріалу.

5. Drag and Drop (Перетягни і Постав) - це інструмент H5P, який дозволяє створювати інтерактивні завдання, де здобувачі освіти можуть перетягувати елементи на визначені місця. Таким чином зазначений інструмент може бути використаний для засвоєння різних понять, логічного мислення, розвитку навиків прийняття рішення та інших напрямках.

6. Flashcards (Картки) - це інструмент H5P, який дозволяє створювати навчальні картки для вивчення нових слів, термінів, визначень та є ефективним засобом для навчання та тренування, в тому числі і в питаннях прийняття рішень.

7. Dialog Cards (Картки діалогів) - це інструмент H5P, який дозволяє створювати інтерактивні навчальні матеріали, що містять діалогові сценарії або розмови. Картки діалогів можуть містити текстові репліки, а також зображення персонажів або ситуацій, що допомагають ілюструвати сценарій.

8. Grouping (Групування) - це інструмент H5P, який дозволяє створювати завдання, де користувачі повинні групувати елементи за певними критеріями або властивостями. Цей засіб допомагає розвивати логічне мислення, класифікаційні навички, навики прийняття рішення та вміння робити висновки.

Окрім зазначених інструментів сервіс H5P пропонує ще цілий ряд інших засобів, використання яких забезпечує інтерактивне наповнення занять.

Таким чином, використання H5P для покращення засвоєння матеріалу при підготовці представників силових структур має безліч переваг:

Інтерактивність. Дозволяє створювати інтерактивний контент, такий як відео з вбудованими питаннями, інтерактивні тести, перетягування елементів тощо. Це дозволяє здобувачам освіти активно залучатися до навчання та більше сприймати матеріал.

Зацікавленість. Завдяки різноманітним типам контенту, створеним за допомогою H5P, можна привернути увагу учнів та збільшити їх зацікавленість у процесі навчання.

Адаптивність. H5P дозволяє створювати контент, який може адаптуватися до різних рівнів навчальної підготовки та потреб здобувачів освіти.

Миттєвий зворотний зв'язок. Багато типів контенту в H5P надають миттєвий зворотний зв'язок, що дозволяє здобувача освіти швидко перевіряти свої знання та отримувати негайну відповідь на свої дії.

Спільне навчання. H5P дозволяє легко обмінюватися та використовувати створений контент іншими викладачами та здобувачами освіти, що сприяє спільному навчанню та обміну ідеями.

Доступність. Контент, створений у H5P, може бути легко доступний з будь-якого пристрою з підключенням до Інтернету, що дозволяє здобувачам освіти вчитися в будь-який час і в будь-якому місці.

УДК 355.42

Телюков С.М., Зливка Г.А., Дроль О.Ю., Гатченко Є.С., Лук'янов С.М.

ПОСЛІДОВНИЙ СПОСІБ РОЗРАХУНКУ ЧАСУ НА ПІДГОТОВКУ БОЮ (ДІЙ)

Пропонується послідовний спосіб та рекомендації, щодо проведення розрахунку часу на підготовку бою (дій), з урахуванням принципів тайм-менеджменту та методів планування та управління проектами

Обґрунтований розрахунок часу (timeline) може бути виконаний, коли особа або колектив людей представляють логіку, взаємозв'язок та послідовність виконання всіх робіт, що виконуються кожним виконавцем.

Розрахунок (розподіл) часу на організацію бою та підготовку бою (дій) в цілому виконується під час усвідомлення завдання, а також під час процедур Receive and analyse the mission (отримання та аналіз завдання) та Receipt of mission (отримання завдання) для Troop Leading Procedures (процедури управління підрозділом) та Military Decision-making Process (процес прийняття військового рішення) відповідно. Розрахунок часу служить орієнтиром для командирів щодо вчасності виконання етапів (процедур) по підготовці (у т.ч. організації бою), виконання етапів планування (прийняття рішення).

Раціональний та послідовний спосіб розрахунку часу повинен ґрунтуватися на принципах тайм-менеджменту, а саме складання списку справ (робіт) з визначенням їх пріоритетів (наприклад, як це реалізовано в методі Альпи). Також для можливості оптимізації та розподілу часу між виконавцями, з урахуванням специфіки робіт, пропонується: використання методів мережевого (сіткового) та календарного планування (наприклад, на основі Діаграма Ганта). З метою автоматизації процесу розподілу часу відповідно роботам, забезпечення відстежування прогресу і аналізу обсягів робіт, може бути використане програма Microsoft Project, яка є системою управління проектами, що розроблена корпорацією Microsoft.

З урахуванням принципів тайм-менеджменту, математичних та графічних методів планування, пропонується послідовність розрахунку часу на підготовку бою (у т.ч. на організацію боя):

1. Визначається кількість часу, що є в наявності на підготовку боя.
2. Визначаються (уточнюються) строки виконання заходів, що вказані в наказі старшого командира.
3. Наявний час розподіляється на денний та нічний періоди.
4. Складається перелік основних робіт (заходи підготовки бою).
5. Визначаються виконавці за напрямками робіт.
6. Здійснюється приблизна розстановка часу, що витрачається на кожний вид роботи.

7. Визначаються роботи, що можуть виконуватися паралельно (тобто в один і той же час), при умові наявності виконавців.

8. Згруповуються роботи, що виконуються у нічний час (в темну пору доби).

9. Остаточно уточняються строки проведення всіх основних заходів.

10. Складається розрахунок часу за встановленою формою.

Нижче надаються рекомендації, щодо виконання послідовного розрахунку часу на підготовку бою.

Визначення кількості часу, що є в наявності на підготовку боя, полягає у визначенні загальної кількості часу з моменту отримання завдання від старшого командира та до визначеного ним же терміну готовості до виконання завдання.

При визначені строків виконання заходів, що вказані в наказі старшого командира, уточнюються вузлові етапи та строки їх виконання (deadline). Такими вузловими етапами можуть бути, наприклад:

– час, до якого необхідно висунутися та зайняти місцевість (або вийти на відповідний рубіж),

– надання доповіді про свій замисел старшому командиру,

– доповідь свого рішення та про готовність системи вогню старшому командиру,

– час, до якого підлеглі повинні бути готовими до виконання бойового завдання, і т.ін.

Розподіл наявного час на денний та нічний періоди рекомендується виконувати для подальшого врахування маскувальних заходів при виконанні робіт, організації відпочинку особового складу та чергування. Також, визначення нічного періоду дасть можливість в подальшому раціонально розподілити роботи або їх об’єднати, якщо це необхідно.

Перелік основних робіт визначається відповідно заходам підготовки підрозділів до виконання завдань, а також на підставі визначеного методу роботи командира, після отримання завдання. При складанні переліку основних робіт (списку задач) необхідно:

– чітко визначити результат виконання роботи (робіт),

– визначити першочергові дії, які будуть забезпечувати виконання подальших робіт,

– визначити конкретні задачі підлеглим, на підставі виданих вказівок.

При визначені виконавців необхідно враховувати, функціональне призначення кожного виконавця та його компетентності, а також приблизно намітити роботи, які будуть виконуватись групою осіб. Командир взводу або роти, як правило, працюють одноосібно. Але для виконання робіт по організації бою командир взводу (роти) може залучати необхідний йому підлеглий особовий склад, наприклад, для виконання допоміжних робіт, для безпосереднього виконання окремих заходів прийняття рішення та організації бою в цілому (в залежності професійних та індивідуальних якостей підлеглих).

Час на виконання тієї або іншої роботи, залежить від:

– характеру (виду або різновиду бою, комплексу дій і т.ін.) та змісту завдання,

– об’єму роботи по організації та підготовці бою,

– необхідних та наявних ресурсів і умов для виконання роботи (наявність: персоналу для виконання робіт, інформації про обстановку, матеріально-технічних засобів та умов для роботи),

– спроможності (компетентність, досвід, морально-психологічний стан) особи (осіб) щодо виконання відповідної роботи.

Приблизна розстановка часу на кожний вид роботи, з урахуванням розподілу виконавців за напрямками робіт може бути виконана також з урахуванням:

– нормативних показників на виконання робіт,

– досвіду застосування інших підрозділів в бойових діях та організації бою,

– власної інтуїції (відчуття) командира (офіцера управління) спираючись на попередній власний досвід та свої знання.

Проаналізувавши етапи підготовки до бою (дій), розподіл виконавців робіт та орієнтовний розподіл часу, можна розподілити роботи по виконавцям та організувати спорідненні роботи паралельно. Час, який перевизначено для паралельних робіт, повинен дорівнюватися часу найбільшої роботи.

При визначені робіт, що виконуються у нічний час необхідно організувати та розподілити роботи так, щоб впровадити виконання маскувальних заходів, відпочинку, чергування, бойова охорона і т.ін. Відпочинок це те ж зброя, якщо можливо то організувати почерговий відпочинок особового складу.

Остаточне уточнення строків проведення всіх основних заходів полягає у корегуванні всіх робіт з урахуванням резерву та дефіциту часу на кожному етапі підготовки бою (дій). В ході остаточного уточнення не слід одразу розподіляти всі резерви часу. Головне усунути дефіцит (дефіцити) часу, а резерв мати для можливого маневру цим часом.

Розрахунок часу, як документ, підписується начальником штабу і затверджується командиром. Перед складанням розрахунку часу за встановленою формою необхідно обов'язково уточнити, яка саме форма документу затверджена старшим командиром або встановлена вищим командуванням.

Також необхідно враховувати і обов'язково використовувати основне правило розрахунку часу – більше часу на підготовку до бою необхідно виділяти для підлеглих, наприклад, може бути застосовано правило 1/3 та 2/3. Дане правило реалізується при виконанні Troop Leading Procedures та Military Decision-making Process. Сутність даного правила полягає в тому, що від загального часу 1/3 виділяється для роботи командира (штабу), 2/3 підлеглим підрозділам.

На основі затвердженого командиром розрахунку часу штаб (або сам командир) може корегувати терміни виконання заходів підготовки бою, якщо це необхідно.

З набуттям практичного досвіду, на основі власної інтуїції, розуміння ситуації і т.ін., командир (офіцера управління) спираючись на логіку та послідовність розрахунку часу, спроможний виконати розрахунку часу навіть за час, що передбачений нормативними вимогами.

УДК 004.49

Терещенко К.В., Штонда Р.М., Черниш Ю.О., Терещенко Т.П., Бондаренко Т.В.

РОЛЬ І МІСЦЕ ФІШИНГУ В СУЧАСНОМУ КІБЕРПРОСТОРІ ПІД ЧАС ВЕДЕННЯ ГІБРИДНОЇ ВІЙНИ

Стрімке розширення загроз національній безпеці у XXI столітті покладає на органи держаної влади завдання щодо їх попередження, виявлення та нейтралізації. Серед найбільш небезпечних загроз для України – кіберзлочинність, яка реалізується через мережу Інтернет. І це зрозуміло. На сучасному етапі і у подальшій перспективі розвиток як окремих суспільств і держав, так і загалом світу буде здійснюватися відповідно до концепції інформаційного суспільства, що пов'язана з використанням інформаційних, комунікаційних та інформаційно-комунікаційних технологій у придбанні, зберіганні та обробці інформації із повсякденного життя [1; 2].

Актуальність теми обумовлена вразливістю кіберпростору та його базової інфраструктури до різного роду кібератак (порушення корпоративної безпеки, фішинг, вимагання в соціальних мережах тощо), які перетворилися на одну з найнебезпечніших загроз для особистої, національної, регіональної і глобальної безпеки.

Кібербезпека більше не є проблемою винятково комп'ютерної безпеки. У її забезпеченні зацікавлені усі держави, оскільки від її стану залежить, чи буде продовжувати ефективно функціонувати кіберпростір під час здійснення цієї кібератаки.

Інтернет дав потужний поштовх для розвитку масової комунікації, торгівлі та обміну інформацією. Разом з тим сьогодні він є тією сферою, де здійснюється чимало правопорушень. Знеособлений характер цифрової інфраструктури зробив крадіжку ідентичності природним і надзвичайно привабливим проєктом. Кіберзлочинці активно використовують різні засоби викрадення інформації, зокрема фішинг.

Фішингові атаки стали головним інструментом злочинців останніх років та становлять 41% від усіх кіберзагроз. Кількість кібератак збільшується паралельно з пришвидшенням цифровізації суспільства та бізнесу. Впродовж останнього десятиріччя 30% всіх світових кібератак проводили росія та Китай. Одним із прикладів фішингу є створення шахраями підробного сайту "Повернись живим" з підробленими реквізитами. Російські хакери продовжують полювати за персональними даними українців, намагаються зламати аканти українців у месенджері SIGNAL, яким користуються чимало військовослужбовців. Також ними було розроблено шкідливе програмне забезпечення, розраховане на крадіжку інформації з пристроїв Android бійців армії України. У 2023 році фішинг набуває масового прояву в українському сегменті соціальних мереж на рівні з дезінформацією та чинить деструктивний тиск на українське суспільство [3].

На тлі війни з росією проблема фішингових атак є особливо актуальною, адже противник не тільки отримує додатковий важіль емоційного впливу на цивільне населення, але може використовувати здобуті дані для диверсійної діяльності проти України. З 2014 року кількість кібератак з території росії суттєво збільшилась. Перед початком повномасштабного вторгнення передувала лавина повідомлень про мінування та спроби здійснити атаки на державні підприємства й об'єкти інфраструктури. Наразі зберігається висока ймовірність як кібератак з боку росії, так і звичайних побутових фішингових атак від людей, що прагнуть скористатися вразливістю українців під час війни.

Кібербезпека все частіше розглядається, як фундаментальна проблема держави, що комплексно зачіпає її безпеку і оборону, економіку, окремі сфери суспільного життя, зокрема, енергетику, охорону здоров'я, що обумовлена проблемами кількості зростання кіберзагроз та кількістю виникнення кіберінцидентів в кіберпросторі. Задля поліпшення кібербезпекових спроможностей України в сучасних умовах ведення рф гібридної війни слід використовувати досвід провідних країн світу, організовувати міжнародне співробітництво, постійно покращувати рівень кібергігієни громадян України.

Надійна робота мереж передачі даних, комп'ютерних систем та мобільних пристроїв є обов'язковою умовою для ефективного ведення бойових дій під час війни, функціонування держави і суспільства, життєдіяльності окремого індивіда. Надійність роботи ключових інформаційних систем загального користування залежить від багатьох чинників: кібератак, збою апаратного та програмного забезпечення, різного роду помилок. Суттєве зростання кількості інцидентів у кіберпросторі обумовлює необхідність системного аналізу джерел виникнення загроз, на перше місце серед яких виходить фішинг.

Список використаних джерел

1. Antonelli, C., Geuna, A., Steinmueller, W.E. (2000). Information and Communication Technologies and the Production, Distribution and Use of Knowledge. International Journal of Technology Management, Vol. 20 (1–2), 72-94.

2. Mansell, R. (2010). The life and times of the information society. Prometheus. Vol. 28 (2), 165–186. doi: 10.1080/08109028.2010.503120.

3. Медіа експерт розповів, чому фішинг став негативним трендом у соцмережах [Електронний ресурс]. Доступно: https://ms.detector.media/internet/post/34071/2024-01-26. Дата звернення: 07.02.2024.

UDC 621.396

Tymchenko S.

DEVELOPMENT OF A MODEL OF THE FORMATION PROCESS OF A REFLECTIVE TRANSPARENCY WITH A CHANGE OF THE FORM OF THE DIAGRAM OF DIRECTIVITY AND FREQUENCY OF RADIATION OF RADIO COMMUNICATION MEANS

A survey of the use of radio communication tools in the conditions of the operation of radio electronic warfare tools by the troops of the Russian Federation showed the need to improve the factory-protected radio communication system. The effectiveness of the radio equipment directly depends on the antenna systems of the radio communication equipment that are in service with the military units. Previous studies indicated the possibility of creating antenna systems based on the polarization holographic effect. Polarization holography requires placement on a polarization hologram, which is made in the form of an anisotropic system and an emitter and differs in that the elements of an anisotropic system have a geometric shape that corresponds to the distribution of the polarization vector of the total interference field of the interaction of the electromagnetic field of a plane wave and the electromagnetic field of the emitter. Currently, there is no scientific and methodological apparatus that will ensure the determination of the exact shape of the polarization hologram. Solving this problematic issue is possible due to the creation of a mathematical model of the process of forming a reflector banner.

Therefore, modeling the process of the formation of a transparent reflector when changing the shape of the directional diagram and the frequency of radiation of radio communication means is an urgent scientific task.

The report is devoted to highlighting the issue of increasing the accuracy of creating the form of a polarization hologram due to the use of measuring signals based on triangular time-pulse modulation.

The following general blocks are proposed.

Block 1. Formation of the conditions of the situation and parameters of the radio means of the radio communication system.

Block 2. Calculation of performance indicators of the radio communication system.

Block 3. Calculation of radio communication system immunity indicators.

Block 4. Block for forming the parameters of the antenna systems of the system.

Block 5. Unit for calculating the electromagnetic compatibility criterion.

Block 6. Calculation of system immunity indicators.

Block 7. Performs the formation of a conclusion on the execution of a combat task.

Output data: the value of the general criterion for ensuring the immunity of the radio communication system; the value of the radio communication system immunity indicator.

The received simulation model of the protection of the radio communication system can be used as the main mechanism for determining the states of the radio communication system under the conditions of the enemy's EW.

The direction of further research is the development of a method of synthesizing antennas of a given directional pattern to protect the radio communication channel from intentional interference.

УДК 654.01

Тимчук В.Ю., Бортнік Л.Л., Дацик В.В., Яшник В.С.

ДОСВІД УКРАЇНИ У СТВОРЕННІ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ

Короткі державотворчі потуги українського народу в ХХ ст. з об'єктивних причин пріоритетності щодо викликів не знайшли відображення в науково-інженерній сфері людської діяльності. Можна лише припустити, що такі світила як математики Д. Граве і М. Кравчук, фізик Й. Косоногов і політекономіст Б. Кістяківський (батько Дж. Кістяківського), які стали у витоків українського академічного життя в Українському народному університеті (1917–18), а також В. Вернадський, в інших реаліях нашої історії могли б закласти серйозні наукові школи, яким по силі було би конкурувати з передовою думкою і винахідництвом у світі.

Тож повернення українського обличчя науці на теренах України почало поступово відбуватися з 1991 р. Очевидно, що збережені від СРСР конструкторські бюро, наукові колективи та університетські катедри і лабораторії продовжували розвивати свої напрямки.

В умовах погіршення стану національної економіки основні результати мали переважно теоретичний характер. Практичні реалізації складних систем були поекземплярними (переважно на виконання інозамовлення (КНР, держави Аравійського півострова) або складовими міждержавних кооперацій (космічні та антарктична програма). Яскравим прикладом цього є розробки ракетного комплексу у кооперації КБ «Південне» та інші організації («Сапсан», «Грім-2»).

Спостерігалося дослідження теоретичних обґрунтувань для багатосистемних рішень, як-от у Ю. Каткова, 2004 (щодо воєнно-інформаційних систем), О. Барабаша, 2005 (щодо розподілених інформаційних систем), П. Сніцаренка, 2008 (складних військових систем дистанційного моніторингу), А. Зінченка, 2017 (щодо інтегрованих систем). Також увагу українські науковці в галузі розробки ОВТ зосереджували на напрямках автоматизації та систем підтримки прийняття рішень: А. Воронін, 1990, А. Перм'яков, 1999, В. Савченко, 2012, С. Ковбасюк, 2015, С. Микусь, 2020, Ю. Прибилєв, 2021, та ін.

З різних причин, фінансових, політичних і організаційних, чимало масштабних проєктів не реалізували. До небагатьох винятків практичного втілення розробок можна віднести роботи Інституту проблем математичних машин і систем НАНУ щодо створення ситуаційних центрів для вищих органів державного управління та Єдиної автоматизованої системи управління.

На кардинальні зміни спонукала російсько-українська війна. Прикметою особливістю стало те, що кожна пропонована інформаційна технологія (ІТ) тестувалися споживачами — у військах. У підсумку на початок 2022 року навіть без усталеного циклу приймання систем (зразків) на озброєння вже невід'ємними у штабах (і у нижчих ланках управління) такі ІТ як «Кропива» («Мапа)», «Віраж», «Термінал», «Дельта». Окремі з названих ІТ де-факто набувають статусу бойових систем, не лише забезпечуючи творення ситуаційної обізнаності, а і реагуючи на протидію ворога, в т. ч. через застосування ним кіберзброї для дискредитації (порушення функціонування) системи.

Отже, за росту великої кількості різних функціональних систем озброєння, ІТ, спеціалізованого програмного забезпечення, інформаційних каналів тощо, а також в умовах постійної протидії ворога, розробка автоматизованих, консолідованих та інших інформаційних систем виходить на новий рівень викликів і потреб розв'язування проблем.

УДК 654.01

Тимчук В.Ю., Галенко І.В.

ДОСВІД СРСР У СТВОРЕННІ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ, СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ І СИСТЕМ ОЗБРОЄННЯ

В XX ст. Російська імперія вступила переважно аграрно-сировинним конгломератом, який геополітичні завдання вирішував через розрахунок на тотальну мобілізацію населення та ресурсів. Технічна відсталість імперії проявилася в російсько-японській війні 1903–1905 рр. Незважаючи на певні іміджеві суперечки щодо піонерства в окремих нових наукових напрямках («Яблочков vs. Едісон», «Попов vs. Марконі», «капітан Бенуа vs. Булл-Нордманн-Бреґґ», «Ціолковський vs. Оберт» та ін.), Російська імперія не встигала за розвитком наукових ідей і винахідництвом в Європі та США, тож переважно скупляла готові рішення для військового використання, наприклад Argo Clock, по суті, перший електрично-керований механічний аналоговий комп'ютер, який винайшов британець А. Поллен для задач розрахунку вогню артилерії.

Після більшовицького перевороту прірва у розвитку технологій ще більше поглибилися, посилена спочатку втечею вчених і офіцерів в еміграцію, а затим репресіями (наприклад щодо того ж Н.-К. Бенуа, заявленого творця станції звукометричної розвідки в артилерії, Ю. Кондратюка та ін.). Окремі розробки, наприклад телетанку (ТТ-18), були довготривалими, оскільки надійність і глибина дій озброєння в бойових умовах залишалися незадовільними.

По суті, підвалини для зменшення розриву заклала Друга світова війна, коли в СРСР по ленд-лізу із США, Великобританії передали набагато ефективніші за радянські аналоги зразки різного озброєння та військової техніки, а також коли після завершення війни Союз «набув» інших технологічних на той час зразків Німецького Рейху (включно з інженерами, які потрапили в радянську зону окупації). Додатково «паралельність» розвитку науки на деякий період вдалося забезпечити внаслідок розвідувальних заходів радянським спецслужб, які опиралися на антимілітарні настрої західних науковців після великої жахітної війни.

Власне в цей період — в 1950–70-ті — почали формуватися відомі на теренах Союзу наукові школи, у витоків яких стали С. Корольов, П. Ощєпков, Ю. Кобзарєв, Л. Канторович, Ю. Тихомиров, С. Лєбєдєв, І. Брук, А. Берґ, А. Колмогоров, А. Кітов, В. Ісаєв, В. Глушков, А. Ярошенко, Г. Поспєлов, М. Цетлін, В. Варшавскій, І. Ґельфанд, В. Арґольд, В. Успєнскій, Б. Лєвін, В. Кунцевич та ін.

Наукові рішення відповідних шкіл лягали в розробку систем озброєння, серед яких з певною часткою автономності та інтелектуалізації можна виокремити професійні персональні ЕОМ серії МІР, різнопланові, у т.ч. комплексні, автоматизовані системи керування (наприклад, бортові комплекси керування зльотом і посадкою «Крос-2, -1» літаків «МІГ-29» і «СУ-27» на палубу авіаносців і т.д.). Загалом зміна ТТХ зразків озброєння обумовлювала необхідність вирішення питання прискорення прийняття управлінських рішень. Велика маса інформації та фактор часу обумовлювали потребу автоматизації процесів. У військах ППО впроваджується перша комплексна АСУ в стаціонарному і мобільному варіантах «Воздух-1п». Система здійснювала напівавтоматичне знімання, автоматичну передачу, відображення і узагальнення даних повітряної обстановки на індикаторні пристрої; прилади апаратного наведення літаків на виявлені повітряні цілі; управління і оповіщення військ і з'єднань ППО.

В цілому, можна на сьогодні констатувати, що розробки в СРСР істотно не вплинули на технологічні винаходи в сферах автономних систем і робототехніки, незважаючи на надмірне фінансування в умовах планової економіки, залишившись у теоретичних обґрунтуваннях.

Тим не менше наукові школи стали основою для досліджень у післярадянських країнах.

УДК 654.01

Тимчук В.Ю., Галенко І.В., Триснюк В.М.

ОСНОВНІ ТЕНДЕНЦІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ У ПРАГНЕННІ ДОСЯГНУТИ ПАРИТЕТУ ІЗ США ЩОДО ТЕХНОЛОГІЧНОГО РОЗВИТКУ

Оговтавшись від свободи, принесеної п'янким «wind of changes» разом із деморалізацією армії на тлі поразки у Першій чеченській війні, Кремль із новим президентом повернувся до політики домінування принаймні на «своїй», як він вважав, території СНД. Оскільки колишні республіки СРСР були в схожих економічних і соціальних умовах, на певні успіхи у заганяння сусідів у фарватер зовнішньої та спільної (чи тісно-зв'язаної) економічної і оборонно-промислової політики Москва спромоглася. Щоб закріпити ці свої сфери впливу, їй потрібно було, принаймні для внутрішнього сприймання, виглядати сильним і переконливим у світі, зокрема у контактах із США, Великобританією, ФРН, Францією, Японією. Цим самим, Москва взялася мобілізовувати власні ресурси, в т. ч. кадрові та науково-технічні, для технологічного конкурування з провідними державами світу.

Не володіючи пріоритетом у створенні технологій і інновацій, Росія могла успішно тільки копіювати ідеї, загортаючи їх в національну обгортку та за допомогою державної протекції масштабуючи її на свої сфери впливу. Приклади таких наслідувань, які є важливими для сектору безпеки та оборони України: розробка Спартаком Никаноровим теорії концептуального управління та методів «управління управлінням» (для створення систем ППО і ПРО) як подальшого осмислення американської системи проектування PERT; розробка альтернативи для геоінформаційної системи «ArcGIS» (яка є основою для роботи штабів НАТО) у вигляді ГІС «Панорама» (деякий час її використовували в Повітряних Силах України, у воєнізованих формуваннях України як-от Внутрішні війська МВС України тощо); розробка альтернатив інформаційним технологіям (замість Gmail, Фейсбук, WhatsApp — mail.ru, Одноклассники, Vkontakte, Telegramm), які є середовищами не тільки для OSINT, а і для проведення інформаційних операцій і кібервійни. Підтвердженням домінування власне системного наслідування найкращого у сфері розробки технологій і створення зразків ОВТ стала російсько-українська війна в її повномасштабній фазі, коли у трофейних або уражених зразках ОВТ найскладніші системи (конструкти) належали іноземному виробникові.

Тим не менше наукові, дослідні і дослідно-конструкторські розробки в сучасній російській федерації проводяться. В їх фундаменті — успадковані від СРСР наукові школи з поєднанням наукових зв'язків із західними, а також із китайськими інституціями. Тому переймання ідей і їх подальший розвиток відбувається також внаслідок відлагодженої системи перекладів патентної документації і наукової літератури (зокрема такими потужними суб'єктами видавничої та винахідницької діяльності як «Концепт», «Питер», «Радио и связь», «Роспатент» та ін.).

Щодо конкретних систем, то для прикладу наведемо такі дані: тривалі дослідження щодо проектування складних систем в т. ч. АСУ (Никаноров С. П., Солнцев С. В. та ін.) лягли в основу аванпроєкту національною обороною російської федерації, прийнятою в 2013 р. на озброєння. Налагодження АСУ тривало усі наступні роки.

УДК 654.01

Тимчук В.Ю., Коцемир О.В., Поляков А.Ю., Триснюк В.М.

ЗАРОДЖЕННЯ ТРАДИЦІЙ СТВОРЕННЯ ВИСОКОТЕХНОЛОГІЧНИХ СИСТЕМ ОЗБРОЄННЯ У ЄВРОПЕЙСЬКИХ ДЕРЖАВАХ

В XX ст. Європа ввійшла найпередовішою щодо науки і технологій частиною світу. Класичні європейські наукові школи дозволяли плеядам вчених по суті «перевертати наукові світи». Самі ж наукові досягнення майже без затримки комерціалізувалися, впроваджувалися у практичні винаходи, в т. ч. і у світі озброєння.

Для прикладу, британський винахідник А. Поллен (Arthur Pollen) у 1912 р. створив Argo Clock, який вважають першим електрично-керованим механічним аналоговим комп'ютером. Італійський винахідних Е. Паскаль (Ernesto Pascal) у 1912 р. розробив інтеграф, який дозволяв проводити складні диференційні розрахунки, що було потрібно для артилерії, і подібні винаходи знаходили втілення вже у перших системах керування стрільби — нею вважають систему Дреєра 1916 р. (за ім'ям флаґ-капітана Королівського флоту Великобританії Ф. Ч. Дреєра, пізніше адмірала, удостоєного лицарства) Dreyer Table fire control system.

І світова війна активізувала розробку і інших «інтелектуалізованих» засобів для ефективної боротьби. Так, у цілях точнішого повітряного бомбометання Г. Вімперайз (Harry Wimperies) у 1916 р. розробив механічний пристрій Drift Sight, який вимірював швидкість вітру і вираховував параметри бомбометання. У 1917 р. він модернізувався у систему озброєння CSBS Mk. IX для літаків Королівських морських ВПС для боротьби з підводними човнами та кораблями.

Оскільки артилерія виявилася спроможною уражати цілі з-за меж прямої видимості, то зародилися дві практично-наукові проблеми: з одного боку, розрахунки точності вогню, з іншого — виявлення місця неспостережної артилерії противника. Французькі фотограф Л. Булл (Lucien Bull) і астроном Ч. Нордманн (Charles Nordmann) розробили реєстрацію сигналів, зумовлених артилерійськими вибухами, на плівку. Австралійський вчений і нобелівський лауреат Л. Брегґ (Sir William Lawrence Bragg) спільно з Ч. Ґ. Дарвіном (Charles Galton Darwin), В. С. Такером (William Sansome Tucker), Е. Ендрейдом (Edward Andrarade) та ін. виявили низько-частотну акустичну хвилю від пострілу, що уможливило створення у 1916 р. звукометричної системи. В цьому ж році, врахувавши метеорологічні фактори впливу та геометрію акустичної бази (для розстановки мікрофонів) військові вчені досягнули точності визначення місця пострілу на рівні 25…50 м (формулярної і до цього часу). У протилежній армії мобілізований на війну австрійсько-єврейський хімік Л. Льовенштайн (Leo Löwenstein) на тільки здобув у чині капітана Залізний хрест, а і розробив часово-різницевий метод вимірювання відстані до джерела звуку (позиції гармати) за допомогою акустичної бази з чотирьох мікрофонів. Після війни науковець запатентував десятки винаходів у царині зв'язку та розробки керованих ракет, хоча науковий пріоритет у нацистській Німеччині закріплювався за іншими підходами.

Д. Гартрі (Douglas Hartree) у 1935 р. в Манчестерському університеті розробив інтегратор, який дозволив реалізувати повністю автоматизовану систему керування вогнем «Kerrison Predictor», яку почав виготовляти збройний концерн Vickers для поєднання зі шведською 40-мм гарматою Bofors L60.

УДК 654.01

Тимчук В.Ю., Коцемир О.В., Шарапа В.В., Хахула В.В.

ЄВРОПЕЙСЬКИЙ ДОСВІД У СТВОРЕННІ АВТОМАТИЗОВАНИХ І РОБОТИЗОВАНИХ СИСТЕМ ОЗБРОЄННЯ

В ІІ світовій війні питання роботизації зразків озброєння зацікавило передусім нацистську Німеччину.

Систему військової науки в нацистській Німеччині, яка зосередили в Армійському дослідницькому центрі (HVP, Heeresversuchsanstalt Peenemünde). Саме там в 1942 р. Г. Гьолзер (Helmut Hölzer) розробив повністю електронний аналоговий комп'ютер для розрахунку та моделювання траєкторії ракети «Фау-2». Внаслідок післявоєнної операції «Скріпка» його знання, як і інших розробників РЛС, систем, зв'язку тощо, вочевидь, знадобилися в США.

Німеччина була єдиною, хто серійно виготовляв самохідні спецмашини Найпоширенішим зразком озброєння були наземні гусеничні самохідні міни серії Sd.Kfz. (Sonderkraftfahrzeug). Безекіпажні, дистанційно керовані за допомогою дротяного зв'язку на дальностях до 1000 м танки-підривники («Голіаф», «Springer», «Borgward IV») у Вермахті використовували для боротьби з танками і загородженнями противника.

Саме ІІ світова війна спонукала продовження розвитку технологій в Європі, залишаючи її лідером інновацій. Але все ж у повоєнний період безекіпажні системи розроблялися, насамперед, для вивчення космосу та для роботи в умовах підвищеної небезпеки, що показало свою практичну доцільність після Чорнобильської катастрофи. В Європі є чимало подібних об'єктів і основні дослідження зосереджували в надрах таких корпорацій як CEA (French Atomic Energy Commision), MATRA, Aerospatiale, British Aircraft Corporation та ін. Яскравим прикладом створення потужної надсистеми є ANALAC (Франція, 1960-ті рр.).

Після зникнення комуністичної загрози розробка систем і технологій у мілітарній сфері не була пріоритетом у національних економіках європейських держав, яка, з одного боку, дозволяла такі дослідження тільки потужним корпораціям за рахунок власних резервів і комерційної діяльності на ринку озброєнь, але з іншого боку вимагала пошуку балансу між ефективністю системи озброєння та її вартістю виготовлення та експлуатації. Тож окремі «європейські» зразки озброєння (системи керування зброєю, системи виявлення (РЛС, оптико-електронні та акустичні системи тощо) були доволі технологічними, незважаючи на начебто давній час розробки. Подібні системи з 2022 року постачалися в Україну і засвідчили свою бойову ефективність (Bayraktar, ARTHUR, HALO, Heidrun, CEASAR, PzH, AHS Krab, Storm Shadow / SCALP EG і т. д.).

Власне масштабність, інтенсивність і динамізм, який є характерним для російсько-української війни, призвів до відновлення розробки автоматизованих і роботизованих систем озброєння. Конкретні розробники із зрозумілих причин не афішуються, але успіх безекіпажних катерів і роїв із безпілотних літальних апаратів дозволяє констатувати високу частку автоматизації у зразках озброєння, які мають мати високоманеврові характеристики, діяти в умовах радіоелектронних перешкод і в умовах функціонування дистанційно підтримуваних мереж.

УДК 654.01

Тимчук В.Ю., Тимчук О.С.

ФОРМУВАННЯ ПЕРЕДУМОВ СВІТОВОГО ЛІДЕРСТВА СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ У РОЗВИТКУ ПРОРИВНИХ ТЕХНОЛОГІЙ

XXI ст. США зустріло світовим лідером у проєктуванні складних систем озброєнь, у яких домінує інтелектуальна частка.

«Сплав» технічної революції кінця XIX ст. та «Чотирьох свобод», на яких заснувалися США, створив ґрунт для інноваційного вибуху невдовзі. Підприємницька спрямованість, патентування за умов об'єктивного відстоювання наукового пріоритету в судовому порядку, масштабування виробництва, що вимагало спрощення конструктивних рішень із дотриманням вимог до функціональності, живило інтелект інженерів і теоретиків.

Наукові постулати, сформовані Теслою, Айнштайном, Оппенгаймером, Шенноном, Вінером, Атанасовим і багатьма іншими, дозволили вже одразу по суті після завершення Другої світової війни взятися за створення систем із деякою, в ідеалі — високою або абсолютною – часткою машини у забезпеченні функціонування системи.

Розвиток комп'ютерів як технічної та керівної основи для систем із автономними діями пов'язаний із цілою плеядою імен в американській академічній спільноті як-от К. Шеннон, Дж. Маккарті, М. Мінскі, А. Ньюелл, Н. Рочестер, Г. Саймон, Д. Енгельбергер та ін.

З їх робіт і винаходів (з урахуванням досліджень науковими школами та конструкторськими бюро інших держав, а також внаслідок операції «Скріпка» (Robert Lusser, Helmut Hölzer)) поставали бортові комп'ютери, програмування, автоматизовані системи, системи підтримки прийняття рішень, штучний інтелект, IBM, робототехніка тощо.

Зрозуміло, що пріоритетний інтерес до розробок проявляло військове відомство США, яке з урахуванням досліджень і розробок від своїх відомчих інженерних колективів закритого типу, що завжди було вимогою в умовах міждержавного протистояння і розпочата доба Холодної війни це тільки посилила (реакцією США на запуск СРСР першого у світі штучного супутника було створення двох інституцій, які, по суті, визначили подальший технологічні прориви в оборонній сфері — NASA та ARPA), впроваджувало наукові та інженерні рішення в проєктовані системи та, відповідно, створювало нові системи озброєння. При цьому військові розробники опиралися на історичні системи озброєння, в яких передбачалися пристрої для механічних розрахунків або небезпосереднього управління (те, що пізніше стало БПЛА), наприклад:

- Whistler-Hearn Plotting board, модель 1904 р. — засіб берегової артилерії для розрахунку курсу рухомої цілі (корабля) для її наступного ураження вогнем;
- A.F.C.T., подальша модернізація 1927 р. балістичних пристроїв у вигляді вже аналогового комп'ютера для керування кутами повороту корабельних гармат;
- Norden Mk. XV, 1931 р. — пристрій для контрольованого бомбометання;
- JB-4, 1944 р. — керована ракета «Повітря – Земля» із теле-/радіо-каналами керування;
- ENIAC, 1945 р. — цифровий комп'ютер для розрахунку таблиць стрільби і т. д.

Отож, корпораційні та спадкові підходи дозволи США створювати надскладні ефективні системи озброєння, яскравими прикладами яких є:

- РЛС із синтезованою апертурою розробки К. Вілея, 1951 р.;
- система FADAC M18, 1960 р. — перший балістичний комп'ютер на транзисторах;
- 474L System, 1961 р. — система раннього попередження про застосування балістичних ракет, яка поєднала РЛС раннього виявлення, комп'ютер і систему управління та зв'язку.

В цей самий час науковці та інженери досліджували у своїх лабораторіях подальші можливості комп'ютерів, закладаючи основи для штучного інтелекту, робототехніки та автоматизації обробки інформації.

УДК 654.01

Тимчук В.Ю., Шарапа В.В., Семитківський М.В.

ДОСВІД СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ У СТВОРЕННІ АВТОМАТИЗОВАНИХ І РОБОТИЗОВАНИХ СИСТЕМ ОЗБРОЄННЯ

Отже, в другій пол. XX ст., США, спершись на фундаментальний науковий потенціал, залучений в рамках організації шляхів ефективного ведення війни проти нацистського Рейху під час Другої світової війни, започаткувало нові наукові напрями, зорієнтовані на домінування в майбутніх потенційних війнах.

В 1958 р. рішенням Президента США були засновані Національне управління з аеронавтики та дослідження космічного простору та Агентство перспективних наукових досліджень — відповідно NASA та ARPA (згодом DARPA). Саме в надрах цих двох інституцій створювалися перші прототипи різних автоматизованих і роботизованих систем озброєння. Слід розуміти, що окрім власних досліджень, інституції організовували та супроводжували кооперацію із багатьох інших університетських лабораторій, дослідницьких центрів, конструкторських бюро корпорацій і потенційних користувачів з оборонного сегменту.

Так, з ARPANET, налагодженого у 1969 р. у співпраці з університетськими лабораторіями, у 1983 р. «виокремилася» військова комп'ютерна мережа MILNET (паралельно «визрівав» і Інтернет, поява якого в умовах американських свобод очікувана).

В DARPA на основі даних спостереження за «Спутніком-1» розробили основи для GPS, глобальної позиційної системи, реалізованої в 1973 р. Р. Істоном, І. Ґеттінгом, Б. Паркінсоном.

З початку XXI ст. в рамках масштабних програм:

- J-UCAS (Joint Unmanned Combat Air Systems) щодо загальновійськової бойової безпілотної системи з виготовленими прототипами X-45A (2002 р.), X-47B (2011 р.), яку трансформували в програму UCLASS (The Unmanned Carrier-Launched Airborne Surveillance and Strike);

- JASSM-ER (Joint Air-to-Surface Standoff Missile) та LRASM (Long Range Anti-Ship Missile) — складові програми щодо автономного цілевідбору у протикорабельних ракетах великої дальності AGM-158B (1998 р.), AGM-158C (2017 р.), що розробляються «Lockheed Martin Missiles and Fire Control»;

- CODE (Collaborative Operations in Denied Environment), 2015 р., щодо спільних операцій у недоступному середовищі;

- FLA (Fast Lightweight Autonomy), 2016 р., щодо дослідження високошвидкісної автономної навігації в перевантажених середовищах;

- ACTUV (Anti-Submarine Warfare Continuous Trail Unmanned Vessel), 2016 р., щодо створення безекіпажного корабля вистежування підводних човнів під назвою «Sea Hunter» виробництва «Vigor Industrial»,

а також інших досліджуються та створюються зразки озброєння, головною та спільною концепцією яких є поєднання в рамках єдиної системи різних інших функціональних систем в цілях забезпечення часткової, а інколи і повної, автономності дій.

Вочевидь, що відповідно до таких головних викликів — по-перше, усунення людини (оператора, пілота, екіпажа) із зони ризику ураження, по-друге, втілення цілей зброї, у т.ч. через автономні процеси, розробляються та досліджуються різні інформаційні тех-

нології, як-от консолідованої обробки інформації, прогнозування розвитку ситуації, контролю тощо.

УДК 654.1

Ткаченко К.М., Ткаченко М.Д.

ПРОБЛЕМА ВИКОРИСТАННЯ ВІДДАЛЕНИХ ТОЧОК ДОСТУПУ ДО МЕРЕЖІ ІНТЕРНЕТ ТИПУ WiFi В ЗОНІ ВЕДЕННЯ БОЙОВИХ ДІЙ В УМОВАХ ЗАСТОСУВАННЯ ПРОТИВНИКОМ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ

Розвиток технологій сьогодні дозволяє виявляти місце розташування джерела радіо випромінювання на дуже великих відстанях. Єдиною проблемою на шляху до цього є наявність відповідного обладнання, фахівців та часу. Досі однією із головних проблем, яку життєво необхідно усвідомити кожному військовослужбовцю, залишається розуміння того, що виявлення мобільного телефону або точки доступу WiFi для противника, із наявними у нього засобами радіоелектронної розвідки, не є проблемою, а лише питанням часу.

Варто розуміти, що випромінювати WiFi сигнал може не лише точка доступу (мобільна чи стаціонарна), але і будь-який сучасний гаджет: смартфон, пульт керування дроном, сам дрон, ноутбук, і, навіть, портативна колонка. Одні пристрої передбачають повне вимкнення передавача сигналу, а інші (наприклад, гаджети виробництва Apple) – ні.

Думка про те, що портативний модем з відстані декількох сотень метрів залишиться непоміченим є оманливою і може коштувати життя під час ведення бойових дій. Виявлення джерела випромінювання і підключення до точки доступу WiFi це принципово різні речі – якщо не вдається встановити з'єднання з роутером, тут відстань має бути невеликою, не означає, що його не “бачать” засоби радіорозвідки, які перебувають на значно більших відстанях.

Технології WiFi пройшли певну еволюцію і сучасні 802.11 ac/ax чи, навіть, 802.11 n мають дуже малу потужність. Як правило, для обміну даними використовуються частоти 2.4 ГГц або 5 ГГц, на яких сигнал затухає дуже швидко на невеликій відстані. Проте, більшість комерційних БПЛА, які в останні два роки були пристосовані до виконання військових завдань, працюють саме на цих частотах, а і при умові управління в межах прямої видимості, вони можуть подолати достатньо великі відстані – до 5-7 кілометрів в одну сторону.

Велика кількість пристроїв, які можна побачити у військовослужбовців в зоні ведення бойових дій, зазвичай, оснащені більш сучасними модулями доступу до бездротової мережі стандартів 802.11 a/b/g, а вони мають значно вищу потужність випромінювання, про що більшості, навіть, і думка в голову не приходить. До них відносяться: телевізори (в яких наявна функція smart TV), розумні годинники та пульсоміри, портативні колонки, мобільні телефони та планшети, ноутбуки тощо. Цей список сягне нескінченності.

В умовах нестійкого прийому або передачі сигналу такі гаджети здатні автоматично переводити пристрій на потужніший стандарт для забезпечення більш якісного з'єднання, не сповіщаючи про це користувача. І тут можна просто уявити собі наслідки від такої “допомоги”, тому що для спеціалізованих засобів радіоелектронної розвідки, наприклад Лєєр-3, той маленький модем буде світитися, як новорічна ялинка, на відстані до 20 кілометрів.

Звісно, трапляється безліч ситуацій, коли використання “розумних” гаджетів може вирішити хід бою або стати єдиним можливим варіантом на шляху до досягнення певних цілей. В такому випадку слід пам’ятати про власну безпеку і застосовувати всі можливі способи для надійного шифрування каналу обміну даними, авторизації користувачів тощо.

Сьогодні використовується безліч керівних документів та нормативів для врегулювання питань безпеки зв'язку, правил ведення радіообміну, дотримання кібергігієни тощо. Всі їх можна піддавати сумніву, нехтувати тими правилами, які в них прописані, але варто пам'ятати, що кожна незначна помилка, кожен коротенький дзвінок, кожне відвідування власної сторінки в соціальній мережі може коштувати життя не тільки тому, хто припустився помилки, а й тим, хто знаходиться поруч. Таким чином, всі командири підрозділів повинні чітко орієнтуватися в цих питаннях, суворо дотримуватися заходів безпеки і вимагати цього від своїх підлеглих.

УДК 796:355.5

Ткачук О.А., Мелешенко О.В, Скопінцев О.О., Оборонов М.І., Шулежко В.В.

ОСОБЛИВОСТІ ПІДГОТОВКИ ОСОБОВОГО СКЛАДУ ПОСТІВ ВІЗУАЛЬНОГО СПОСТЕРЕЖЕННЯ ТА МОБІЛЬНИХ ВОГНЕВИХ ГРУП ДО ВИКОНАННЯ ЗАВДАНЬ ЗА ПРИЗНАЧЕННЯМ В УМОВАХ ВЕДЕННЯ МАНЕВРЕНОЇ ПРОТИПОВІТРЯНОЇ ОБОРОНИ

Аналіз робот, присвячених організації та проведення особового складу до виконання завдань за призначенням свідчать, що основна увага приділяється тренуванню виконання завдань в засобах балістичного захисту, підвищенню навченості в виконанні функціональних обов’язків за посадою, наданню першої медичної допомоги та ліквідації наслідків ураження. Разом з тим, питання підготовки до виконання позаштатних обов’язків розкрити не достатньо повно [1-10]. На цей час одним з розповсюджених прикладів є виконання обов’язків у складі мобільних вогневих груп (МВГ) та постів візуального спостереження (ПВС).

Для забезпечення виявлення та знищення низькошвидкісних засобів повітряного нападу (ЗПН) з малою ефективною поверхнею розсіювання, такі як крилаті ракети та безпілотні літальні апарати, утворюються МВГ та висуваються ПВС на напрямки, найбільш імовірні для шляхів підльоту ЗПН. Ймовірно, що загальна кількість загрозливих напрямків буде перевищувати кількість наявних сил та засобів. Одним з шляхів розв’язання цього проблемного питання є розміщення особового склад та засоби ПВС та МВГ в місцях, висування з яких забезпечить мінімізацію часу розгортання на напрямках, що відповідають нанесенню удару за результатами оповіщення. Але реалізація цієї пропозиції фактично потребує від особового складу виконання не властивих обов’язків в стресових умовах після фізичного навантаження.

В доповіді наведено пропозиції щодо програми спеціальної фізичної підготовки особового складу МВГ та ПВС, яка забезпечує формування потрібних фізичних якостей, підвищує стресостійкість та здатність виконання завдань за призначенням. Запропоновані вправи, що забезпечать успішне застосування стрілецької зброї та переносних зенітних ракетних комплексів для ураження ЗПН після здійснення маршу.

Заходи, що пропонуються, повинні забезпечити успішність виконання поставлених перед особовим складом ПВС та МВГ завдань при веденні мобільної протиповітряної оборони.

Список використаних джерел

1. Васильєва, Н.М., Ткачук, О.А., Резніченко, О.А., Помогаєв, І.В., & Овчаренко, О.Ю. (2022). Аналіз досвіду відпрацювання питань тактичної медицини в ході проведення тактичних (тактико-спеціальних) навчань військових частин (підрозділів) зенітних ракетних військ при підготовці до дій в особливих умовах. XVI Міжнародна науково-практична конференція магістрантів та аспірантів "Теоретичні та практичні дослідження молодих вчених" (TPRYS-2022), Харків. https://doi.org/10.5281/zenodo.7454944

2. Джус В, Шулежко В, Рощупкін Є, Гречка О, & Сургай М. (2020). Особливості організації та проведення практик курсантів факультету зенітних ракетних військ, що навчаються за спеціалізацією зенітні ракетні комплекси та системи середньої дальності, на державних підприємствах. Освітній процес: методика, досвід, проблеми, 3-4 (157-158), 70–74. https://doi.org/10.5281/zenodo.6618969

3. Резніченко, О., Шулежко, В., Удовенко, А., Рощупкін, Є., Крючков, Д., & Титаренко, Р. (2021). Досвід активізації та мотивації навчально-пізнавальної діяльності курсантів при підготовці фахівців за спеціалізацією «зенітні ракетні комплекси та системи середньої дальності» (за напрямком С-300В1) в умовах карантинних обмежень. Освітній процес: методика, досвід, проблеми, 3-4 (161-162), 61–69. https://doi.org/10.5281/zenodo.7273873

4. Васильєва, Н.М., Ткачук, О.А., Мелешенко, О.В., Романюк, М.М., & Шарапа, І.А. (2022). Урахування досвіду тактичних (тактико-спеціальних) навчань військових частин (підрозділів) зенітних ракетних військ з питань тактичної медицини при організації та проведенні занять з спеціальної фізичної підготовки. XVI Міжнародна науково-практична конференція магістрантів та аспірантів "Теоретичні та практичні дослідження молодих вчених" (TPRYS-2022), Харків. https://doi.org/10.5281/zenodo.7455049

5. Ткачук, О.А., Рощупкін, Є.С., Помогаєв, І.В., Калита, О.В., & Крючков, Д.М. (2022). Особливості фізичної підготовки військовослужбовців частин (підрозділів) зенітних ракетних військ у процесі відпрацювання питань відновлення озброєння та військової техніки на тактичних (тактико-спеціальних) заняттях. VI Міжнародна науково-практична конференція "Сучасні тенденції та перспективи розвитку фізичної підготовки та спорту Збройних Сил України, правоохоронних органів, рятувальних та інших спеціальних служб на шляху євроатлантичної інтеграції України", Київ. https://doi.org/10.5281/zenodo.7501178

6. Ткачук, О.А., Васильєва, Н.М., Мелешенко, О.В., Гайбадулов, Б.В., & Овчаренко, О.Ю. (2022). Особливості реабілітації військовослужбовців засобами фізичної підготовки при контузіях головного мозку. VI Міжнародна науково-практична конференція "Сучасні тенденції та перспективи розвитку фізичної підготовки та спорту Збройних Сил України, правоохоронних органів, рятувальних та інших спеціальних служб на шляху євроатлантичної інтеграції України", Київ. https://doi.org/10.5281/zenodo.7501557

7. Палевич, С., Піддубний, О., Ткачук, О., & Золочевський, В. (2018). Стан проблеми та напрями удосконалення спеціальної фізичної підготовки військовослужбовців Повітряних сил Збройних Сил України. Спортивна наука України, № 1(83), 15–25. Вилучено із http://repository.ldufk.edu.ua/handle/34606048/12131

8. Ткачук, О.А. (2016). Фізична підготовка як засіб адаптації до стресових умов бойової і навчально-бойової діяльності військовослужбовців. Актуальні проблеми фізичного виховання різних верств населення, 195–199. http://journals.uran.ua/hdafk-tmfv/article/view/71804

9. Васильєва Н.М., Ткачук О.А., Мелешенко О.В, Шевченко О.С., & Овчаренко О.Ю. (2022). Особливості підготовки військовослужбовців до виконання завдань за призначенням в засобах індивідуального захисту. Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку", Харків

10. Помогаєв, І. В., Рєзнік, Д. В., Ткачук, О. А., Мелешенко, О. В., & Овчаренко, О. Ю. (2023). Пропозиції щодо підвищення ефективності підготовки спеціалізованого персоналу військових формувань для виконання службових обов'язків в особливих умовах та оцінювання за результатами діяльності. XVII Міжнародна науково-практична конференція магістрантів та аспірантів "Теоретичні та практичні дослідження молодих вчених" (TPRYS-2023), Kharkiv. https://doi.org/10.5281/zenodo.10257653

Толмач Г.А.

ПРОБЛЕМНІ ПИТАННЯ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ ПРИ КАЛІБРУВАННІ (ПОВІРЦІ) ЕЛЕКТРОННО-ЛІЧИЛЬНИХ ЧАСТОТОМІРІВ

В умовах реформування та нових економічних взаємовідносин з виробниками (постачальниками) засобів вимірювальної техніки існує постійна необхідність удосконалення технічної та нормативної бази, що значно підвищить якість, ефективність та знизить собівартість робочого процесу.

В якості зразку запропонована методика калібрування частотомірів групи Ч3, принцип подачі характеристик засобів вимірювальної техніки у якій є таким, що самі засоби вимірювання показані через їхні метрологічні характеристики, які необхідні у роботі, що значно збільшує діапазон їх застосування та надає можливість міксувати засоби вимірювальної техніки за потребою: на заміну несправного, під час ремонту, з різних років та різних діапазонів, не прив’язуючись до фірми, марки та здійснювати застосування засобів вимірювальної техніки, що забезпечують вимірювання контрольованих параметрів з вказаною невизначеністю (похибкою).

Тобто, якщо, для прикладу, вказуємо генератор з максимально можливим діапазоном на уявному робочому місці, наприклад, з повними діапазонами частот від 0,1 Гц до 20 ГГц, потужності вихідного сигналу ± 30 дБмВт, та опорних частот (прецизійний генератор) із синусоїдальним сигналом у діапазоні 0,1 Гц – 400 МГц та із зовнішньою опорною частотою, наприклад, $\pm 5 \cdot 10^{-9}$ за рік, та вибираємо один генератор на всьому вказаному діапазоні або декілька, поділивши діапазон на частотні відрізки, з вказаною точністю, крім того, доцільно застосування одного сучасного засобу вимірювальної техніки на декількох робочих місцях.

Також для оновлення бази прецизійних генераторів було розглянуто можливість застосування генераторів сигналів з нижчою похибкою опорної частоти, при опційній можливості підвищення точності сигналу за рахунок роботи від стандарту частоти (рубідієвого або кварцового). При порівнянні економічної та технічної доцільності застосування даного методу для підвищення точності передачі сигналу, частіше за все вказує на те, що чим ширший діапазон вимірювань захоплений і вища точність виданого сигналу даного діапазону, тим вища і вартість приладу. Приладобудівні компанії засобів вимірювальної техніки від світових брендів (Keysight, Anritsu, Rohde&Schwarz, Tektronix, Siglent) є достатньо коштовними приладами, на ринку також з’явилися менш відомі, але з досить непоганими характеристиками та ціновою категорією (Precision Test Systems та ін.). Іноді, засіб вимірювальної техніки, що має досить гарні характеристики, та вартість, зняті з продажу, що збільшує час на пошуки.

Отже, модернізація робочих місць сучасними засобами вимірювальної техніки дозволяє зменшити масогабаритні показники робочих місць, здійснити автоматизацію процесу отримання, перетворення та обробки вимірювальної інформації під час проведення повірки, калібрування, зменшити похибку вимірювань, підвищити точність проведення вимірювань, завдяки багаторазовим вимірюванням, зменшити вплив випадкових факторів на результат вимірювання, значно зменшити час проведення повірних, калібрувальних робіт, зменшити енергозатратність робочих місць.

Після та під час модернізації робочих місць виникає необхідність створення нових або удосконалення вже існуючих методик для калібрування (повірки), у зв'язку з тим, що методики та технічні описи засобів вимірювальної техніки написані не державною мовою, та в них для калібрування (повірки) вказуються застарілі прилади, що ускладнює процес розуміння самого процесу повірки чи калібрування, а іноді і вимірювання, оскільки методичні матеріали при проведенні таких робіт мають бути місткими, інформативними, лаконічними за кожним визначеним типом вимірювання.

УДК 621.3

Третяк В.Ф., Коломійцев О.В., Осієвський С.В., Ковальчук І.М., Авдєєв В.Ф., Новикова О.О.

ОСОБЛИВОСТІ ЗАХИСТУ БАЗ ДАНИХ У ПІДГОТОВЦІ ТА ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ

В доповіді розглянуто тенденції розвитку баз даних (БД), які можуть впливати на підготовку та діяльність сил охорони правопорядку. Розкрито особливості захисту БД та надані пропозиції щодо захисту..

Сучасний розвиток технологій БД визначається рядом тенденцій, які можуть впливати на підготовку та діяльність сил охорони правопорядку. До основних тенденцій розвитку БД можливо віднести наступні:

– хмарні БД: зростання популярності хмарних рішень для зберігання та обробки даних, що дозволяє покращити масштабованість, доступність та забезпечити більшу гнучкість;

– розподілені бази даних (РБД): використання розподілених архітектур для забезпечення ефективності та високої доступності даних на різних георграфічно розподілених місцях;

– великі дані та аналітика: інтеграція БД з інструментами аналітики для обробки та вивчення великих обсягів даних, що дозволяє здійснювати більш деталізований аналіз;

– використання штучного інтелекту (AI) та машинного навчання (ML): застосування технологій штучного інтелекту для оптимізації роботи з БД (наприклад, для автоматичного оптимізованого запиту та покращення продуктивності);

– графові БД: розширення застосування графових БД для ефективного вирішення завдань, пов'язаних з моделюванням та аналізом взаємозв'язків між даними;

– технології контейнерів і оркестрація: використання контейнерів (наприклад, Docker) та оркестраційних систем (наприклад, Kubernetes) для спрощення розгортання та керування БД;

– розширена безпека: зосередження на покращенні засобів безпеки БД у відповідь на зростання загроз кібербезпеки;

– розвиток технологій реального часу: збільшення попиту на БД, які можуть обробляти та взаємодіяти з даними у режимі реального часу;

– blockchain у БД: використання технології блокчейн для забезпечення надійності, цілісності та безпеки даних.

Дані тенденції відображають рух галузі БД у напрямку більшої продуктивності, ефективності та забезпечення високого рівня безпеки та доступності даних.

Захист БД є важливою задачею, оскільки вони часто містять конфіденційну та цінну інформацію. До проблем захисту БД можливо включити наступні:

– несанкціонований доступ: атаки хакерів та несанкціоновані користувачі можуть

намагатися проникнути у систему, щоб отримати доступ до конфіденційної інформації або змінити дані;

– SQL-ін'єкції: атаки, спрямовані на виконання шкідливих SQL-запитів через вразливість вводу даних, що може призвести до витоку інформації або зміни структури БД;

– втрата даних: втрата даних може виникнути через технічні помилки, видалення даних користувачами або через кібератаки (регулярні резервні копії можуть допомогти відновити дані після таких втрат);

– вразливості програмного забезпечення: використання застарілих версій програмного забезпечення або виявлення нових вразливостей може призвести до атак та невірного виконання функцій;

– брак аудиту та моніторингу: відсутність систем аудиту та моніторингу може ускладнити виявлення аномальної активності та вразливостей у безпеці БД;

– недостатня аутентифікація та авторизація: слабкі системи аутентифікації та авторизації можуть дозволяти несанкціонованим користувачам отримувати доступ до системи або здійснювати неправомірні операції;

– фізична безпека: недостатня фізична безпека обладнання (серверів, зберігання даних) може призвести до фізичного доступу до обладнання та крадіжки даних;

– загрози внутрішніх користувачів: інсайдери, тобто внутрішні користувачі з доступом до системи, можуть стати джерелом загроз для безпеки, зокрема, якщо їх наміри нечесні;

– неякісне шифрування: шифрування даних може бути слабким або неправильно налаштованим, що робить його менш ефективним для захисту конфіденційності;

– соціальна інженерія: атаки, спрямовані на отримання доступу до системи через маніпулювання людьми (наприклад, отримання паролів або конфіденційної інформації).

Для вирішення перелічених проблем рекомендується використовувати комплексний підхід, який включає в себе технічні, організаційні та процесні заходи безпеки.

Захист баз даних є критичним аспектом забезпечення безпеки і конфіденційності інформації. До основних методів захисту БД можливо віднести наступні:

– аутентифікація та авторизація: аутентифікація включає в себе перевірку ідентичності користувача перед наданням доступу до БД;

– авторизація визначає рівень доступу користувача, тобто те, що він може робити у межах БД;

– шифрування даних: застосування шифрування даних у БД допомагає захистити конфіденційні інформаційні ресурси від несанкціонованого доступу;

– моніторинг і аудит: ведення журналів аудиту для реєстрації подій та дій у БД;

– регулярний моніторинг журналів аудиту для виявлення підозрілих або несанкціонованих активностей;

– фізична безпека: захист фізичного обладнання БД, включаючи сервери та зберігання даних, від несанкціонованого доступу або знищення;

– захист від вразливостей: регулярне виявлення та виправлення вразливостей програмного забезпечення БД;

– резервне копіювання і відновлення: регулярне створення резервних копій БД та їх конфігурацій;

– проведення тестів відновлення, щоб переконатися, що можливо відновити дані у разі втрати або пошкодження;

– керування правами доступу: детальна конфігурація прав доступу до конкретних таблиць, полів або операцій для кожного користувача;

– використання тунелювання та VPN: використання віртуальних приватних мереж (VPN) та тунелювання для захисту трафіку між додатками та БД.

Перераховані методи захисту БД часто використовуються у поєднанні для створення

комплексного підходу щодо безпеки даних. До основних систем та продуктів, що спрямовані на захист БД можливо виділити наступні:

– Oracle Advanced Security: включає різноманітні технології шифрування та аутентифікації для БД Oracle;

– Microsoft SQL Server Transparent Data Encryption (TDE): надає можливість шифрувати дані у покої БД на рівні файлів, що забезпечує захист від несанкціонованого доступу до даних на рівні носіїв;

– IBM Guardium: система моніторингу та захисту БД, яка виявляє та запобігає небезпеці для конфіденційності, цілісності та доступності даних;

– Symantec Data Loss Prevention (DLP): продукт, який допомагає виявляти і захищати конфіденційні дані, включаючи ті, що знаходяться у БД;

– McAfee Database Security: забезпечує контроль доступу, моніторинг активності користувачів та виявлення загроз для БД;

– Acunetix: засіб для виявлення та виправлення вразливостей в веб-додатках, включаючи ті, які можуть впливати на безпеку БД;

– Fortinet FortiDB: платформа для захисту БД, яка надає можливості моніторингу безпеки, аудиту та захисту від атак;

– DBShield: WAF (Web Application Firewall) для БД, який фільтрує та блокує SQL-ін'єкції та інші атаки на рівні БД;

– Imperva SecureSphere: рішення для захисту БД, яке включає моніторинг активності, захист від атак та управління доступом.

Розглянуті системи використовуються для різних аспектів захисту БД та можуть бути інтегровані у комплексний підхід до безпеки інформації.

Перспективні напрямки захисту БД включають в себе використання новітніх технологій та методів для підвищення рівня безпеки інформації, а саме:

– диференційований доступ: впровадження більш продуманих та гнучких систем авторизації, які дають можливість обмежити доступ до конкретних даних або операцій для різних користувачів;

– homomorphic Encryption: використання гомоморфного шифрування, яке дозволяє виконувати обчислення над зашифрованими даними без їх розшифрування, що підвищує конфіденційність;

– zero Trust Security: застосування концепції "нульового довір'я", яка передбачає, що навіть вже аутентифікованим користувачам потрібно постійно підтверджувати свою ідентичність та права для доступу до ресурсів;

– blockchain для безпеки даних: використання технології блокчейн для забезпечення недострокованої інтегрітети та відстеження змін у БД.

– детектори вразливостей у реальному часі: впровадження систем, які виявляють та реагують на вразливості у режимі реального часу, забезпечуючи швидку реакцію на потенційні загрози;

– розширені системи аудиту: розширення систем аудиту для забезпечення більш детального моніторингу активності користувачів та виявлення аномальних подій;

– використання штучного інтелекту у безпеці: застосування технологій штучного інтелекту для аналізу великих обсягів даних та виявлення аномальної або підозрілої активності;

– комплексні рішення забезпечення безпеки: використання інтегрованих рішень, які об'єднують технічні, організаційні та процесні заходи безпеки для створення комплексного підходу;

– захист від внутрішніх загроз: розробка систем, які ефективно виявляють та вирішують проблеми, що пов'язані з внутрішніми загрозами або нечесними діями персоналу;

– інтерактивні засоби навчання: застосування інтерактивних засобів навчання та

тренувань для персоналу, щоб підвищити рівень обізнаності та навичок у сфері кібербезпеки.

Таким чином, дані напрямки представляють сучасні технологічні та концептуальні підходи щодо захисту БД у підготовці та діяльності сил охорони правопорядку в умовах зростаючих загроз інформаційної безпеки.

Список використаних джерел

1. Коломійцев, О., Третяк, В., Воронін, В., Старцев, В., Пустоваров, В., Осієвський, С., ... & Рудаков, І. (2023). Роль та застосування систем баз даних у військовому управлінні та плануванні: аналіз основних аспектів. Scientific Collection «InterConf», (176), 247-255.

УДК 621.327:681.5

Тупиця І.М., Хмелевський С.І.

ТЕХНОЛОГІЯ КОДУВАННЯ ДАНИХ ПОВІТРЯНОЇ РОЗВІДКИ ДЛЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ

Досліджуються проблемні аспекти використання класичних методів кодування даних, що формуються бортовими оптикоелектронними системами повітряної розвідки безпілотних авіаційних систем. Для забезпечення необхідного рівня достовірності даних повітряної розвідки в умовах впливу помилок в лініях пересилання відеоданих запропоновано новий підхід - технологія компактного представлення даних повітряної розвідки, що реалізується за двохієрархічною схемою статистичного кодування.

Виклики сьогодення, пов’язані з широкомасштабним вторгненням на територію України військ противника, призвели до зростання ролі системи повітряної розвідки, як ключової компоненти своєчасного та всебічного забезпечення органів військового управління розвідувальними даними та ефективного управління підрозділами сил оборони.

На сьогоднішній день основним джерелом розвідувальної інформації є безпілотні авіаційні системи (БпАС), що надаються з перших днів війни країнами-партнерами та виробляються вітчизняними підприємствами. Проте використання як закордонних, так і вітчизняних зразків пов’язане з рядом проблемних факторів [1-3]:

- постійно зростаючі обсяги відеоданих, що формуються бортовими сенсорами оптикоелектронних систем повітряної розвідки безпілотних літальних апаратів (БпЛА) [1, 3];
- обмеження пропускної спроможності ліній пересилання відеоданих [2].

Зазначені фактори мають суттєвий вплив на оперативність доставки даних повітряної розвідки на станцію керування і контролю і, як наслідок, до кінцевого адресату. В свою чергу, для подолання дисбалансу між об’ємами даних повітряної розвідки та пропускною спроможністю ліній пересилання відеоданих активно використовуються компресійні технології. Для більш компактного представлення кодованих відеоданих активно удосконалюються етапи обробки відеозображень, реалізовані на базі платформи JPEG. Це пов’язано з тим фактом, що більшість сенсорів цільового спорядження БпЛА формують розвідувальну інформацію саме в цьому форматі стиснення даних. Проте основним недоліком використання алгоритмів зазначеного сімейства є низька стійкість кодованих відеоданих до помилок в лініях пересилання, що може призводити до суттєвого спотворення та руйнування відеоресурсу і, як наслідок, до неможливості подальшого дешифрування даних повітряної розвідки [4]. Таким чином, використання зазначених

алгоритмів в умовах впливу помилок в лініях пересилання відеоданих не дозволяє забезпечити необхідний рівень достовірності розвідувальної відеоінформації, що отримується з БпАС.

Для вирішення вищезазначеної проблеми пропонується технологія компактного представлення даних повітряної розвідки, що реалізується за двохієрархічною схемою статистичного кодування [5]. Відмінною рисою зазначеної технології є трансформація процесу статистичного кодування Хаффмана в двохетапну реалізацію з використанням маркерних роздільників. Це дозволяє забезпечити:

- необхідний рівень достовірності даних повітряної розвідки за рахунок локалізації впливу помилок;
- більш компактне представлення даних, що формуються бортовими сенсорами, за рахунок додаткового скорочення кодової надмірності, тобто формування маркерних роздільників у вигляді нерівномірних кодових конструкцій.

Список використаних джерел

1. Хмелевський С.І., Тупиця І.М., Махді Касім Аббуд, Мусієнко О.П., Пархоменко М.В., Боровенський Я.О. Розробка методу зовнішньої реструктуризації для підвищення ефективності кодування даних інформаційного ресурсу. *Системи обробки інформації*. 2021. № 3(166). С. 52-61. DOI: https://doi.org/10.30748/soi.2021.166.06.

2. Хмелевський С. І., Тупиця І. М., Кібіткін С. В., Королюк Н. О., Романюк А. О., Дзюба І. В. Створення моделі оцінки достовірності відеоданих для технології компресійного кодування в умовах дії помилок в каналі передачі даних. *Системи обробки інформації*. 2022. № 2 (169). С. 72-86. DOI: https://doi.org/10.30748/soi.2022.169.09.

3. Стасєв, Ю.В., Тупиця І.М., Пархоменко, М.В. Метод додаткового скорочення структурної надмірності кодового представлення відеоданих. *Вісник Вінницького політехнічного інституту.* 2022. №3 (162). С. 67–76. DOI: https://doi.org/10.31649/1997-9266-2022-162-3-67-76.

4. Тупиця І. М., Кібіткін С. О., Сухотеплий В. М., Непокритов Д. М., Конов Д. В. Метод реконструкції відеозображень для підвищення ефективності доставки в інфокомунікаційних системах аеросегмента. *Вісник Вінницького політехнічного інституту*. 2022. № 4 (163). С. 72–82. DOI: https://doi.org/10.31649/1997-9266-2022-163-4-72-82.

5. Karlov D., Tupitsya I., Parkhomenko M. Methodology of increasing the reliability of video information in infocommunication networks aerosegment. *Radio Electronics, Computer Science, Control*. 2022. No. 3. P. 120-132. DOI: https://doi.org/10.15588/1607-3274-2022-3-12.

УДК 004.056.53+ 004.8

Уманець М.С., Данилов А.Д.

ВИКОРИСТАННЯ ШУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КІБЕРРОЗВІДКИ

Поняття «Кіберрозвідка» доцільно розглядати як цілісний підхід до автоматизованого обміну розвідувальною інформацією про загрози, який сьогодні вважається однією з найперспективніших стратегій у сфері кібербезпеки, який виник у зв’язку з розвитком інформаційної війни та переходом бойових дій в кіберпростір. Її основна мета полягає у виявленні, аналізі та протидії цифровим загрозам безпеки, а також включає такі процеси, як збір, оцінка критичних даних і запуск наявної системи до того, як ці дані стануть загрозою. Кіберрозвідка дає змогу знаходити реальні рішення - забезпечувати проактивну кібербезпеку. Таким чином, можна бути готовим до можливих загроз і

вживати негайних заходів. Кіберзагрози можемо поділити на групи залежно від їхнього рівня, наведемо приклад такого поділу:

- стратегічна розвідка. Це розвіддані, що ідентифікують зловмисника через моніторинг установи. Включає мотиви, наміри та потенційні атаки, засновані на їхніх минулих діях;
- оперативна розвідка. Описує методи зловмисників, які аналізує команда SOC для вжиття заходів;
- тактична розвідка. Аналізує дані, що виявляють аномалії та шкідливі дії в системі, включно з IOC, IOA і TTP.

У роботі розглянуто алгоритми штучного інтелекту (далі ШІ), а також машинного навчання, які можуть активно застосовуватися силовими структурами під час кіберрозвідки для підвищення її ефективності та автоматизації роботи.

Одним з таких алгоритмів є моніторинг індикаторів компрометації (eng. Indicators of compromise (IOCs)**)**, що дає змогу ефективніше виявляти та реагувати на компрометацію системи безпеки. Збір і кореляція IOC у режимі реального часу дають змогу якнайшвидше виявляти інциденти безпеки, які могли залишитися непоміченими за допомогою інших інструментів, і надають необхідні ресурси для проведення криміналістичного аналізу інцидентів, а також автоматично оновлюють свої інструменти та політики безпеки, ґрунтуючись на попередньому досвіді [3], що є невід'ємною частиною процесу кіберрозвідки. Можна навести наступні приклади індикаторів компрометації:

- Mismatched Port-Application Traffic (невідповідність трафіку між портами та додатками);
- Web Traffic with Unhuman Behavior («нелюдська» поведінка веб-трафіку);
- Geographical Irregularities (географічні невідповідності).

Наступний розглянутий метод – це застосування ШІ Трансформерів. Застосування цієї методології - опрацювання природної мови (NLP) є корисним для аналізу комунікацій у рамках кіберрозвідки. Моделі Transformer чудово розпізнають складні шаблони та взаємозв'язки в даних, що робить їх ефективними у виявленні як відомих, так і нових кіберзагроз. Механізм самоконтролю дозволяє їм виявляти ледь помітні аномалії в даних. Трансформери можуть обробляти кілька типів даних одночасно, у режимі реального часу, наприклад, текст, зображення та числову інформацію. У кібербезпеці ця здатність є цінною для аналізу різноманітних джерел розвідданих про загрози.

Моделі Transformer є потужним доповненням до усього інструментарію кіберрозвідки, пропонуючи потенціал для покращення виявлення загроз, реагування на них та підвищення загальної ефективності та швидкості забезпечення безпеки.

Експерти з кібербезпеки здобувають величезну користь від впровадження алгоритмів, що можуть розпізнавати сигнатури атак, підозрілий трафік та вразливості коду без прямого втручання людини, і використовуючи отримані дані, будувати стратегії для прогнозування майбутніх кібератак та їх наслідків, визначення векторів загроз, ризиків та відповідних заходів щодо їх запобігання, саме для цього використовується - технологія баз знань (eng. The Security Knowledge DataBase). База знань відрізняється від знайомої нам бази даних тим, що містить не лише таблиці з числами, рядками, датами, але й об'єкти з вказівниками на інші об'єкти, які, в свою чергу, мають додаткові вказівники [1]. Зразкова архітектура наведена на рис. 1. Добрим прикладом представлення бази знань може слугувати об'єктна модель, структура – онтологія.

Під час аналізу впровадження або збільшення використання технологій на основі штучного інтелекту або машинного навчання у кіберрозвідці не можна оминути також деяких сумнівів щодо стовідсоткової безпеки застосування подібних методів саме у цій стратегії кібербезпеки, але на світовій арені все більше глобальних прикладів використання ШІ як спецслужбами так і самими зловмисниками.

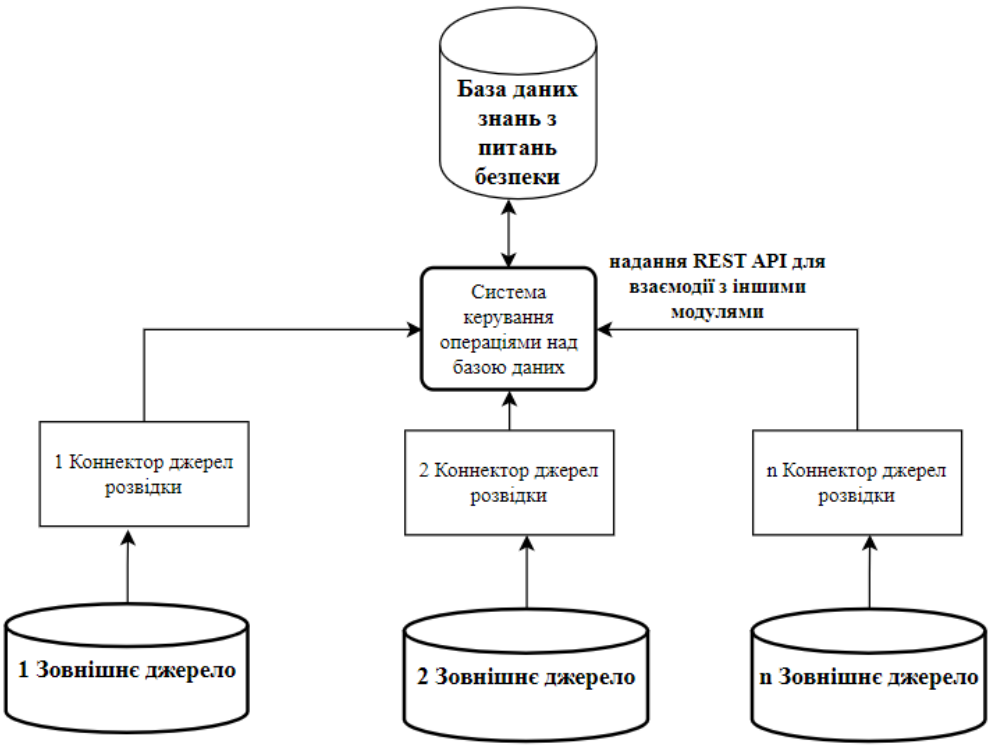


Рисунок 1 – Архітектура Бази Знань (The Security Knowledge DataBase)

Роб Джойс, директор з кібербезпеки АНБ (Агентство національної безпеки), виступив на Міжнародній конференції з кібербезпеки в Університеті Фордхем у Нью-Йорку, де заявив, що машинне навчання та штучний інтелект допомагають слідчим з кібербезпеки відстежувати цифрові вторгнення, які інакше було б дуже важко помітити. Він зазначив, що лідери кібербезпеки вже обговорювали зростаючі аспекти використання штучного інтелекту як хакерами, так і правоохоронними органами. Зокрема, китайські хакери націлені на транспортні мережі, трубопроводи і порти США, використовуючи приховані методи, які зливаються зі звичайною діяльністю в інфраструктурних мережах. За словами Джойса, ці методи є дійсно небезпечними, оскільки їхньою метою є дезорганізація суспільства, а не фінансова вигода чи шпигунство. Він додав, що хакери не використовують шкідливе програмне забезпечення, яке можуть виявити звичайні засоби безпеки [2].

Інструменти штучного інтелекту допомагають АНБ відстежувати операції, які використовують архітектурні недоліки, неправильні конфігурації або паролі за замовчуванням, щоб отримати доступ до мереж. "Машинне навчання, штучний інтелект і великі дані допомагають нам виявляти таку діяльність", - сказав Джойс, оскільки моделі краще виявляють аномальну поведінку нібито законних користувачів [2].

Отже, спираючись на світовий досвід, можна бути певними, що використання машинного навчання може дуже вдало розширити можливості кіберрозвідки шляхом автоматизації етапів про які йшла мова на початку роботи. Це може бути корисним, при наявній проблемі дефіциту спеціалістів у приватному секторі, особливо під час повномасштабної кіберзагрози, коли кожен фахівець і кожна хвилина це незамінна цінність для досягнення спільної мети.

Список використаних джерел

1. John Soldatos, James Philpot and Gabriele Giunta (eds.). (2020).Cyber-PhysicalThreat Intelligence for Critical Infrastructures Security. Boston–Delft: Now Publishers

2. Ribeiro A. Senior US cybersecurity official reveals use of AI to counter hackers targeting critical infrastructure - Industrial Cyber. *Industrial Cyber*.

URL: https://industrialcyber.co/critical-infrastructure/senior-us-cybersecurity-official-reveals-use-of-ai-to-counter-hackers-targeting-critical-infrastructure/ (дата звернення: 02.03.2024).

3. Decoding threats: understanding indicators of compromise (iocs) for robust cybersecurity. *NetWitness.com*. URL: https://www.netwitness.com/blog/indicators-of-compromise/ (дата звернення: 02.03.2024).

УДК 004.738

Ушаков В.А.

ОГЛЯД МОЖЛИВОГО ЗАСТОСУВАННЯ БАЗ ДАНИХ РЕЄСТРІВ UMTS ТА LTE ДЛЯ ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ, ПЕРЕМІЩЕННЯ ВІЙСЬКОВИХ ПІДРОЗДІЛІВ

Стрімкий розвиток мобільних мереж UMTS та LTE спричинив появу нових можливостей для визначення місцезнаходження та переміщення абонентів, включаючи військовослужбовців. Зловмисники з зовні шляхом несанкціонованого доступу або безпосередньо персонал мобільного оператора із злочинних спонукань можуть мати доступ до баз даних реєстрів UMTS та LTE, таких як HLR (Home Location Register), VLR (Visitor Location Register), EIR (Equipment Identity Register), HSS (Home Subscriber Server) для отримання інформації про абонентів, з метою подальшого її аналізу для визначення місць розташування та маршрутів переміщення військових підрозділів.

Актуальність цієї проблеми полягає в зростанні технічної та територіальної доступності мобільних технологій, розширенні асортименту користувацького обладнання (UE) що робить обладнання мобільних мереж загального користування все більш важливим джерелом інформації про користувачів, особливо про їх місцезнаходження. Це робить бази даних реєстрів UMTS та LTE найбільш вірогідними цілями в якості джерел даних для відстежувати пересування військових частин, підрозділів. Особливо важливим розгляд цього питання стає на фоні наявності статистичної інформації щодо застосування противником зброї далекого ураження по місцям скупчення особового складу.

Для розуміння цінності баз даних вищезгаданих реєстрів коротко наведу інформацію про їх основний вміст:

HLR (Home Location Register) – Опорний (домашній) Реєстр Місцезнаходження – це база даних, що містить всю адміністративну інформацію про кожного абонента разом з його останнім відомим місцезнаходженням. Таким чином, мережа може маршрутизувати виклики на відповідну базову станцію для MS. Коли користувач вмикає свій телефон, телефон реєструється в мережі, і з цього можна визначити, з якою BTS він спілкується, щоб вхідні дзвінки могли маршрутизуватися належним чином. Навіть коли телефон не активний (але увімкнений), він періодично перереєструється, щоб переконатися, що мережа (HLR) «знає» своє останнє положення. Вміст:

- містить інформацію про всіх абонентів, які зареєстровані в мережі UMTS;
- зберігає дані про IMSI, MSISDN, IMEI, тип аутентифікації, тарифний план, послуги, місцезнаходження абонента в мережі;
- використовується для аутентифікації абонентів, авторизації доступу до мережі, маршрутизації дзвінків та SMS, тарифікації послуг.

VLR (Visitor Location Register) – Гостьовий Реєстр Місцезнаходження - тимчасова база даних абонентів, які знаходяться в зоні дії певного MSC (Центр Мобільної Комутації)містить вибрану інформацію з HLR про UE користувачів, які знаходяться в роумінгу в мережі іншого оператора (т.з. - роумери). VLR зазвичай реалізується як невід'ємна частина MSC (Mobile Switching Center – Центр Комутації Мобільного Зв’язку). Вміст:

− містить інформацію про абонентів, які знаходяться в роумінгу в мережі іншого оператора, яка передана від HLR домашньої мережі;

− зберігає дані про IMSI, MSISDN, IMEI, місцезнаходження абонента в роумінговій мережі4

− використовується для маршрутизації дзвінків та SMS, тарифікації послуг в роумінгу.

EIR (Equipment Identity Register) - Реєстр Ідентифікації (абонентського) Обладнання. Цей реєстр містить інформацію про всі IMEI які використовуються в мережі, вирішує, чи може дане мобільне обладнання бути допущено до мережі. Кожне мобільне обладнання має номер, відомий як IMEI. Цей номер, міститься в обладнанні і перевіряється мережею при реєстрації. Залежно від інформації, яка міститься в EIR, обладнанню користувача (UE) може бути виділено один із трьох станів: дозволений доступ до мережі, заборонений доступ або контроль у разі проблем. Вміст:

− містить інформацію про всі IMEI, які використовуються в мережі UMTS/LTE;

− зберігає дані (в т.ч. місцезнаходження) про IMEI (активний/на контролі/ заблокований) за «білим», «сірим», «чорним» списками;

− використовується для запобігання крадіжкам, пошуку, відстежування UE, блокування несанкціонованого доступу до мережі (як правило на користь правоохоронних органів).

HSS (Home Subscriber Server) – Сервер Власних Абонентів в мережі LTE поєднує функції VLR, HLR, AUC мережі UMTS, крім того має вміст:

− централізований реєстр, який містить дані про всіх абонентів мережі UMTS/LTE;

− зберігає дані про IMSI, MSISDN, IMEI, тип аутентифікації, тарифний план, послуги, дані про роумінг, дані про сеанси зв'язку;

− використовується для аутентифікації абонентів, авторизації доступу до мережі, маршрутизації дзвінків та SMS, тарифікації послуг, управління мобільністю абонентів.

Висновки: вразливості в сотових мережах UMTS/LTE становлять значну загрозу для безпеки військових підрозділів, за умови активного використання мобільних пристроїв особовим складом, враховуючи те що інформація про ці пристрої потрапляє до вищезгаданих реєстрів всіх мобільних операторів, в зоні дії базових станцій яких знаходиться пристрій, незалежно від того є він зареєстрованим абонентом чи ні.

В разі успішної реалізації атак з метою доступу до даних реєстрів HLR, VLR, EIR, HSS, цілком можливе отримання необхідної інформації з метою подальшого аналізу для визначення місць розташування та переміщення військових частин, підрозділів с подальшим цілевказанням для засобів далекого враження противника.

Основним способом запобігання подібних загроз слід розглядати відхід від використання засобів публічних мобільних мереж військовослужбовцями в місцях розташування підрозділів та під час виконання завдань за призначенням в бік створення відомчої мобільної мережі фізично відділеної від публічних мобільних мереж.

УДК 621.396.6

Фик О.І.

РОЗРОБКА МЕТОДИКИ ПРОЕКТУВАННЯ ПЛОСКОГО РЕФЛЕКТОРА МІКРОПОЛОСКОВОЇ ВІДБИВАЮЧОЇ РЕШІТКИ ПЛОСКОЇ ДВОДЗЕРКАЛЬНОЇ АНТЕНИ КАССЕГРЕНА СУПУТНИКОВОЇ СИСТЕМИ ЗВ'ЯЗКУ

Основне і допоміжне дзеркала дводзеркальної антени Кассегрена (ДДзА) можна виконати у вигляді двох плоских відбиваючих антенних решіток, які складаються з набо-

ру мікрополоскових елементів (МПЕ). Оскільки до складу такої антени, окрім опромінювача, входить тільки дві решітки печатних елементів (одна розташована в плоскості випромінювача, друга (відбиваюча) у паралельні площині на фокусній відстані(F)), це забезпечує простоту її виробництва, низьку вартість, малі втрати, легкість і компактність конструкції у разі застосування у супутникових системах зв'язку .

Проаналізовано багато варіантів конструктивної реалізації цих антен для різних діапазонів частот і способів сканування променем антени. Проте їх спільною рисою є використання як елементів АР основного дзеркала мікрополоскових перевідбивачів прямокутної форми. В якості елементів відбиваючої антенної решітки (ВАР) основного рефлектора ДДзА використовувати мікрополоскові перевідбивачі складної форми, які є більш широкополосними і менш чутливими до погрішностей у виготовленні, а решітки з них також можуть виконувати функції достатньо широкополоскових твіст-рефлекторів. Однак, для проектування мікрополоскової відбиваючі решітки (МПВР) необхідно розробити чітку методику розрахунку розмірів МПЕ та всієї антеної решітки з урахуванням складної структури електромагнітної хвилі, яка відбивається від дифракційної МПВР.

Під час проектування МПВР , як правило, доцільно користуватися припущенням про те, що розв'язання задачі дифракції плоскої хвилі на нескінченно довгій періодичній антенній решітці досить точно описує збудження МПВР полем первинного випромінювача. Спираючись на розв'язання цієї задачі, знаходимо залежності фаз відбитих полів від параметрів нескінченних антенних решіток із МПЕ, що збуджуються плоскими хвилями, а надалі користуємося ними в процесі проектування МПВР. Під час застосування цього наближення доводиться користуватися тими чи іншими обмеженнями, які залежать від типу досліджуваної МПВР. По-перше, ВАР (відбиваюча антенна решітка) повинна мати розміри, достатні для того, щоб розв'язання, яке маємо для нескінченної решітки, залишалося справедливим і для багатоелементних решіток кінцевих розмірів. По-друге, відношення F/D (фокусусна відстань та розмір випромінювача) також має бути досить великим, щоб електромагнітна хвиля (ЕМХ), що падає від випромінювача, у місцях розташування перевипромінювачів могла розглядатися як локально плоска. Тоді можна припустити, що кожен елемент у ВАР відбиває поле з такою ж фазою, як і в нескінченній АР. Ця модель дозволяє враховувати взаємозв'язки між елементами МПВР, а також дзеркальне відбиття від екрану. Насправді відбиваюча фокусуюча решітка містить елементи, які відрізняються або за розмірами, або за топологією. У той же час у вважаємо що печатні елементи відбиваючої решітки збуджуються уже майже плоскою хвилею тоді результати моделювання рефлектора періодичною решіткою МПЕ дасть вірогідний результат. Тобто, хвиля, що в цьому випадку падає від розміщеного поблизу рефлектора випромінювача, фронт якої відрізняється від плоского, може розглядатися, як сукупність декількох плоских хвиль, що падають на різні ділянки відбивача під різними кутами. У результаті кути відбиття хвиль на різних ділянках фазокоректуючого рефлектора є різними і, підбираючи відповідним чином фазові затримки, що вносяться перевипромінювачами-фазообертачами в поля хвиль, які відбиваються ними, можна добитися того, щоб загальний відбитий від решітки дифракційний промінь буде узгоджений.

У той же час у процесі проектування МПВР із частотним скануванням, що містить рупорний випромінювач і плоский рефлектор, який складається з квазіперіодичної печатної АР і є своєрідним варіантом зонної пластини Френеля, передбачається, що в деякій локальній ділянці цієї структури її відбиваючі властивості такі ж самі, як і в нескінченно протяжних відбиваючих решітках, на які падає плоска хвиля. Таким чином, функцію розподілу струму, наведеного на локальному елементі решіток, можна уявити, як функцію розподілу струму, наведеного на елементі, що входить до складу нескінченно протяжних решіток, які опромінюються плоскою хвилею. Період цих нескінчен-

но протяжних решіток дорівнює локальному періоду, а кут падіння плоскої хвилі дорівнює локальному куту падіння.

Наведені на печатних елементах решіток струми обчислюються з використанням теореми Флоке і методу моментів. Ці припущення допустимі, якщо по поверхні решіток її період міняється досить повільно і відстань між випромінювачем і рефлектором велика в порівнянні з довжиною хвилі. А оскільки локальні кути падіння і локальний період решіток все ж таки міняються вздовж поверхні рефлектора, то обчислення розподілу наведеного струму для кожного елемента решіток проводиться окремо в припущенні нескінченно протяжності решіток, період яких відповідає положенню цього елемента на поверхні рефлектора, для кута падіння плоскої хвилі, що дорівнює відповідному локальному куту падіння.

Таким чином, процес розсіювання хвиль на окремому МСЕ, навколо якого з усіх боків є елементи, які відрізняються за розмірами або за формою, приблизно може розглядатися, як процес відбиття хвиль від нескінченної АР, яка складається з однакових перевипромінювачів і тоді можна виділити такі етапи проектування плоского рефлектора на основі МПВР:

1. По відомим значенням робочої частоти, ширини смуги частот, втрат і передбачуваних витрат на виготовлення, вибирається матеріал підкладки АР.
2. Методом моментів розраховуються амплітуди і фази нулів, відбитих від нескінченно протяжних періодичних МПЕ як функції розмірів печатних елементів, довжин налаштувальних шлейфів або кутів повороту МПЕ.
3. Виходячи з умов забезпечення потрібної для фокусування або перетворення у вищий дифракційний порядок фазової затримки шляхом інтерполяції даних, що були отримані на попередньому етапі, визначаються необхідні розміри МПЕ, довжини налаштувальних шлейфів або кути повороту печатних перевипромінювачів.
4. Методами теорії антенних решіток розраховується діаграма спрямованості(ДС) решітки. При цьому амплітуда і фаза збудження кожного елемента АР знаходяться по відомій ДС окремого опромінювача методом геометричної оптики. Під час знаходження амплітуд і фаз полів, відбитих кожним із печатних елементів АР, для отримання більш точних результатів можна знову застосувати метод моментів.
5. Використовуючи відомі характеристики ДС випромінювача розраховуються ККД антени, а за ними визначаються ККД і КП МПВР.

Фіщук І.М., Поліщук А.М., Ликова І.В., Каляєв О.О.

МЕТОДИКА ДИСТАНЦІЙНОГО ТЕСТУВАННЯ ЗА УМОВ ЗАБЕЗПЕЧЕННЯ ВИСОКОГО РІВНЯ ПІДТРИМКИ САМОРЕГУЛЯЦІЇ

Рисами дистанційного навчання є інтерактива взаємодія у процесі навчання із відокремлення часу для самостійного освоєння матеріалу. Недоліками дистанційної освіти є потреба у надійному технічному оснащенні, переформатуванні окремих підходів та тем, покращення методичного забезпечення. Також дистанційне навчання підпадає під поняття про підтримку саморегуляції, що вказує на систему підтримки та стимулювання здатності особи або системи до самостійного контролю, регулювання та адаптації свого власного функціонування. У системі освіти Національної академії підтримка саморегуляції означає створення умов та ресурсів, які допомагають курсантам розвивати навички самоконтролю, планування, організації та метакогнітивних стратегій, це включає в себе надання курсантам інструментів для визначення своїх цілей та ефективного дистанційного самоконтролю.

Основною метою дистанційного навчання та тестування є стимулювання курсантів до самостійного навчання та контролю над своїми досягненнями, уникнення втручання

викладача. Застосування правильних підходів до мотивації курсантів для власного розвитку та самокритики у рівень їхніх знань призводить до підвищення рівня самомотивації до навчання, і це досягається без прямого впливу викладача.

Розроблено курс тестування по знанням озброєння і військової техніки, який включає викладення інформації про тактико технічні характеристики та правильність обслуговування техніки. На початку кожного тижня для всіх груп факультету надається інформація щодо тактико-технічних характеристик певного зразка озброєння, обраного представниками кафедри ракетних військ і артилерії. Цей вибір базується на основі аналізу якості освоєння матеріалу курсантами, які вивчають предмети кафедри. Ця інформація представлена лаконічно та графічно доконано для зручного засвоєння. Забезпечується максимальна стислість, щоб уникнути перевантаження курсантів та стимулювати їх до засвоєння цього матеріалу. Стиль подачі інформації використовується в формі гри, сприяючи високому ступеню прийнятності. Зазвичай тест включає в себе елементи, такі як тактико-технічні характеристики озброєння, його призначення, а в окремих випадках - будову окремих елементів чи загальну структуру.

Мета полягає в тому, щоб засвоєння матеріалу не витрачало більше 7-9 хвилин. Останній та найважливіший етап тестування відбувається у кінці тижня означений часом, визначеним керівництвом факультету як максимально прийнятний для участі в формі вікторини. Вікторина включає в себе від 5 до 15 питань із 3-4 варіантами відповідей. Керівництво факультету не має жодного впливу на кількісні показники курсантів, що беруть участь, оскільки участь у ній є добровільною. Основним психологічно ефективним елементом є відкритість результатів тестів. Кожен військовослужбовець факультету може оцінювати відповіді, що були надані, і переглядати, хто з колег та начальників які відповіді надавали. Це сприяє обговоренню результатів серед курсантів у їхніх соціальних групах, де може відбуватися як піднесення за вдалі відповіді, так і конструктивна критика за помилки. Відкритість тексту дозволяє створити атмосферу прозорості та чесності у формуванні результатів. Участь старших начальників у тестуванні підкреслює їхній авторитет та досвід, що стимулює курсантів до більш ефективного вивчення та освоєння навчального матеріалу. Відповідь на питання кожен військовослужбовець може надати тільки один раз та не може змінювати свій вибір.

Застосування курсу дистанційного тестування, в яких всі результати автоматизовані та недоступні для втручання створюють відчуття відкритості та справедливості серед курсантів. Кожен курсант розуміє, що вплив на результати тесту залежать виключно від його знань, що сприяє великому рівню довіри до представлених результатів. Системність проведення тестів та нагляд за їх результатами, допомагає командирам групи реагувати на курсантів, що потребують додаткової допомоги та надають необхідну підтримку. На рівні навчального курсу та факультету - це дозволяє контролювати та аналізувати результати, розробляти додаткові заходи, як спрямовані на додаткове засвоєння матеріалу та консультації, щоб допомогти курсантам наздогнати відставання у засвоєнні матеріалу. Головна концепція не примушувати курсантів до проходження тесту а створити передумови формування його власного бажання до перевірки свого рівня знань.

УДК 372.853

Флорін О.П.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ВІРТУАЛЬНИХ ЛАБОРАТОРІЙ З ЕЛЕКТРОТЕХНІКИ ТА ЕЛЕКТРОНІКИ ЯК КОМПОНЕНТІВ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

В сучасному світі інформаційно-комунікаційні технології (ІКТ) визначають новий рівень розвитку підготовки фахівців. Застосування цих технологій в освітньому процесі не лише трансформує традиційні методи навчання, але і відкриває безмежні можливості для підвищення якості, доступності та інноваційності освіти.

ІКТ дарують можливість створювати гнучкі та ефективні системи навчання. Дистанційне навчання, он-лайн-ресурси та віртуальні платформи роблять освіту доступною для всіх, незалежно від місця проживання. Це відкриває нові горизонти для розвитку освіти в умовах глобалізації.

Вивчення технічних дисциплін, в яких, розглядається будова, принцип дії та особливості застосування складних радіоелектронних пристроїв неможливе без наявності широкої номенклатури навчально-лабораторної бази (НЛБ). Однак, стрімкий розвиток науки і технологій, а також проблеми соціально економічного характеру в Україні обмежують її виробництво та впровадження в освітній процес.

Суттєвого загострення означені проблеми набули, спочатку під час пандемії COVID-19, а потім з початком повномасштабної агресії російської федерації, коли заняття вимушено були переведені у дистанційний та он-лайн формат[1-2].

Віртуальні лабораторії та симулятори з електротехніки та електроніки - це програмно-апаратні комплекси, що надають можливість виконання експериментів, аналізу та моделювання різноманітних електричних та електронних систем без необхідності використання фізичних пристроїв та обладнання. Основна мета їх використання полягає в навчанні, дослідженні та проектуванні різноманітних електричних та електронних систем.

Характеристика віртуальних лабораторій і симуляторів включає такі аспекти:

1. Демонстрація концепцій. Віртуальні лабораторії надають можливість демонструвати основні та складні концепції електротехніки та електроніки через візуалізацію та інтерактивні експерименти.

2. Симуляція реальних умов. Ці інструменти можуть імітувати реальні умови роботи електричних та електронних систем, такі як коливання, перенапруги, шуми тощо.

3. Моделювання систем. Віртуальні лабораторії дозволяють створювати моделі різноманітних систем для аналізу їх функціонування та взаємодії компонентів.

4. Тестування та налагодження. Завдяки симуляціям можна проводити тестування та налагодження електричних та електронних пристроїв без ризику пошкодження реального обладнання.

5. Прототипування. Віртуальні лабораторії надають можливість створювати та тестувати прототипи електричних та електронних пристроїв без необхідності фізичного виготовлення.

6. Оптимізація проектів. За допомогою симуляцій можна виконувати оптимізацію параметрів систем для досягнення кращої ефективності та продуктивності.

7. Дослідження нових технологій. Віртуальні лабораторії дозволяють вченим та дослідникам вивчати нові технології та методи електротехніки та електроніки в контрольованому середовищі.

8. Моделювання складних систем. За допомогою симуляцій можна вивчати взаємодію складних систем та прогнозувати їхнє поведінку в різних умовах.

9. Верифікація та тестування продуктів. Віртуальні лабораторії дозволяють виробникам перевіряти та тестувати продукцію перед випуском на ринок, що зменшує ризик виникнення дефектів.

10. Оптимізація виробничих процесів. Використання симуляторів дозволяє підвищувати ефективність виробничих процесів та зменшувати витрати на тестування та налагодження обладнання.

Окрім науки та виробництва віртуальні лабораторії та симулятори з електротехніки та електроніки є невід'ємною частиною сучасної вищої освіти в галузі інженерії, електроніки, комп'ютерних наук та інших технічних дисциплін. Вони надають студентам можливість вивчати, відпрацьовувати та експериментувати з різноманітними концепціями та технологіями без необхідності великих витрат на обладнання та матеріали.

Віртуальні лабораторії та симулятори стали важливою складовою сучасного освітнього процесу, що допомагає підвищувати якість навчання та підготовку кваліфікованих фахівців.

Розглянемо кілька конкретних програмних продуктів з функціями віртуальних лабораторій та симуляторів з електроніки, які широко використовуються у вищій освіті.

1. *LTspice* - це безкоштовний програмний продукт для моделювання та аналізу електронних схем, розроблений компанією Linear Technology (тепер Analog Devices). LTspice є популярним інструментом для вивчення аналогових та цифрових електронних схем у вищій освіті [3]. Він постачається з бібліотекою моделей SPICE від Analog Devices , Linear Technology , Maxim Integrated та сторонніх джерел.

Він дозволяє студентам експериментувати з різними типами компонентів та параметрами схем для отримання глибшого розуміння їхньої роботи.

2. Cadence PSpice - (англ. *Personal Simulation Program with Integrated Circuit Emphasis*) програма симуляції аналогових схем і цифрової логіки, описаної мовою SPICE, яка призначена для персональних комп'ютерів для моделювання та аналізу аналогових та цифрових схем [4]. PSpice є популярним інструментом для навчання електроніці та дизайну схем у вищій освіті. Він надає широкий спектр функцій для симуляції різноманітних електронних схем та дозволяє студентам отримувати практичні навички у проектуванні та аналізі схем.

3. CircuitLab - це он-лайн сервіс для моделювання та аналізу електронних схем. Він має інтуїтивно зрозумілий інтерфейс та багато функцій для створення та симуляції схем [5]. CircuitLab є популярним інструментом для навчання електроніці в університетах та коледжах. Він надає студентам можливість легко створювати та аналізувати електронні схеми у віртуальному середовищі.

4. Simulink - це інтерактивний інструмент, середовище моделювання та симуляції для систем динамічного та статичного характеру. Воно використовується для моделювання електронних, керуючих та інших складних систем [6]. Розроблене компанією The MathWorks. Дає можливість будувати графічні блок-діаграми, імітувати динамічні системи, досліджувати працездатність систем і вдосконалювати проекти.

Simulink повністю інтегрований з MATLAB, що забезпечує швидкий доступ до широкого спектра інструментів аналізу і проектування. Simulink широко використовується в університетах для навчання студентів моделюванню та симуляції систем у реальному часі. Він дозволяє створювати складні математичні моделі та аналізувати їх поведінку.

5. TINA Design Suite - це потужний, але доступний розробник схем та програмний пакет для дизайну друкованих плат для аналізу, проектування та тестування в режимі реального часу аналогових, цифрових, IBIS, HDL, MCU та змішаних електронних схем [7]. Ви також можете проаналізувати SMPS, зв'язок та оптоелектронні схеми; генерувати та налагоджувати код MCU за допомогою вбудованого інструменту блок-схеми; і перевірити застосування мікроконтролера в змішаному середовищі. Оф-лайн ліцензії TINA включають безкоштовні приватні он-лайн ліцензії на один рік.

6. NI Multisim та його он-лайн версія ***NI Multisim Live*** - це програмне забезпечення для моделювання електронних схем, що дозволяє студентам створювати, аналізувати та симулювати електричні та електронні схеми [8]. Multisim надає можливість використовувати інтерактивні та реалістичні симуляції для вивчення різноманітних електронних концепцій та принципів. Він широко використовується в університетах для навчання електроніці та проектування схем.

Ці програмні продукти представляють лише частину ринку віртуальних лабораторій та симуляторів з електроніки, які використовуються у вищій освіті. Кожен з них має свої особливості та переваги, і вони можуть використовуватися для різних цілей навчання та досліджень у галузі електроніки.

Список використаних джерел

1. Султанова Л.Ю., Желуденко М.О. Вплив пандемії COVID-19 на розвиток освітніх систем у глобальному, європейському та національному вимірах. Освіта дорослих: теорія, досвід, перспективи. 2020. Вип. 2 (18).

2. Організація освіти в умовах війни: рекомендації міжнародних організацій. *О.Локшина, О.Глушко, А.Джурило та ін.*. URL: https://uej.undip.org.ua/index.php/journal/article/view/593/537. (дата звернення 08.02.2024).

3. LTSpice. ANALOG DEVICES. URL: https://www.analog.com/en/designcenter/design-tools-and-calculators/ ltspice-simulator.html (дата звернення 08.02.2024).

4. Personal Simulation Program with Integrated Circuit Emphasis. URL:https://www.cadence.com/en_US/home/tools/pcb-design-and-analysis/analog-mixed-signal-simulation/ pspice.html (дата звернення 08.02.2024).

5. CircuitLab URL:https://www.circuitlab.com/ (дата звернення 08.02.2024).

6. Simulink is for Model-Based Design URL:https://ch.mathworks.com/products/simulink.html (дата звернення 08.02.2024).

7. CIRCUIT SIMULATOR FOR ANALOG, DIGITAL, MCU AND RF CIRCUITS. URL:https://www.tina.com/ (дата звернення 08.02.2024).

8. Офіційний сайт компанії NI. [Електронний ресурс]. https://www.ni.com/en/shop/electronic-test-instrumentation/application-software-for-electronic-test-and-instrumentation-category/what-is-multisim.html/. (дата звернення 08.02.2024).

Фтемов Ю.О., Мельник Р.М.

ОПТИМІЗАЦІЯ ПРОЦЕСУ ПЛАНУВАННЯ ЗАХОДІВ ІНЖЕНЕРНОЇ ПІДТРИМКИ МОБІЛЬНОСТІ ВІЙСЬК (СИЛ)

Враховуючи особливості сучасної ведення збройної боротьби, визначається основне протиріччя у сфері управління військами: зростаючі обсяги інформації "протистоять" обмеженому часу, доступному для її збору, обробки та передачі командувачу (командиру). Органи управління повинні оптимізувати цей процес для раціонального та обґрунтованого прийняття рішень.

Аналізуючи ведення локальних війн і збройних конфліктів останніх років, слід зазначити, що відбуваються значні зміни в теорії інженерної підтримки сучасних бойових дій. Чільне місце при цьому займає створення, перш за все, ефективної системи інженерної підтримки мобільності військ (сил). Однак, питанням автоматизованого управління, а особливо плануванню заходів інженерної підтримки мобільності військ (сил), у загальній системі, належної уваги не приділено.

Одним із варіантів вирішення зазначеного вище є створення спеціалізованого програмного забезпечення (СПЗ) для планування цих заходів. Іншими словами –

програмного продукту, який в подальшому повинен стати невід'ємною складовою єдиної автоматизованої системи управління військами.

З метою забезпечення успішного функціонування програмного продукту створюється багаторівнева база даних до якої входять: часові показники, основні завдання (заходи) інженерної підтримки, детальні відомості про сили, засоби, як противника, так і про свої війська тощо.

Загальний алгоритм роботи СПЗ являє собою ряд взаємопов'язаних деталізованих інструкцій, що реалізують процес обчислення, який, починаючи з початкового стану, відбувається через послідовність логічних станів та завершується кінцевим. Перехід з попереднього до наступного стану не обов'язково детермінований – деякі алгоритми можуть містити елементи випадковості.

При введені інформації (завдань, окремих заходів), для прикладу з мобільності підрозділів: кінцевим результатом обчислення є формування висновку щодо можливостей (спроможностей) своїх підрозділів виконати визначене бойове завдання.

Важливим етапом формування вихідних даних є цифрове відображення на дисплеї планшета (ПЕОМ) детальної обстановки, що склалася, відомостей про противника та свої війська, особливо про їх інженерні заходи. Далі, відповідно до замислу (рішення) загальновійськового командира, на цифровій карті (схемі) виводяться задані напрямки пересування своїх підрозділів та ін.

У подальшому основним завданням органу управління є оцінювання ефективності створеної противником системи інженерних загороджень, яка формується шляхом нанесення на цифрову карту по елементах різноманітних інженерних загороджень і перешкод з урахуванням "доступності" для дій своїх військ. Програма дає можливість при збільшенні (зменшенні) форми об'єкта, отримувати відомості про його протяжність, глибину, ймовірність ураження, час затримання тощо. При цьому оператором обов'язково задаються такі відомості як: ймовірний ефект загородження, тип боєприпасів, спосіб виконання завдання, сили, засоби механізації, умови виконання та ін.

Результатом опрацювання наведених вище даних є надання пропозицій щодо спроможності підрозділу виконати визначене завдання, потреба у додатковому оснащенні засобами, пропонується схема подолання загородження (перешкод) для досягнення заданого ефекту, а також за даними інженерної розвідки визначаються щільність загороджень їх координати, які у свою чергу доповнюють базу даних програми, з можливістю передачі інформації до вищих штабів, а також внесення змін (доповнень) у ході виконання завдань в умовах реального часу тощо.

Необхідно зазначити, що в ході передачі даних з одного рівня до основної бази даних, оператором вводяться умови ведення бою (операції) з обов'язковим врахуванням різноманітних коефіцієнтів, серед яких чільне місце займає "коефіцієнт реальності", який враховує поступове зменшення можливостей своїх підрозділів. Після чого на інтерфейс користувача виводиться інформація про витрату засобів інженерного озброєння, майна, визначається потреба у машинорейсах, пальному тощо.

Результатом обробки даних на завершальному етапі, є формування ряду пропозицій, які надаються на затвердження старшому командиру (начальнику).

Також, у разі виявлення обмежених можливостей підрозділів з виконання завдань по подоланню створених противником загороджень (перешкод) на визначеному напрямку, передбачено функцію щодо додаткового залучення необхідних сил і засобів старшого начальника. При підтвердженні запиту, вони вносяться до загальної бази даних.

Після затвердження командиром пропозицій, наданих начальником інженерної служби (відділу групи), здійснюється їх доведення до підпорядкованих підрозділів через систему засобів комунікації. Тому питання оперативності та своєчасності вироблення рішення, доведення до підрозділів, уточнення і врахування інтенсивності змін будуть запорукою успішності ведення бойових дій військ (сил).

Таким чином, впровадження рекомендацій щодо розроблення СПЗ, дозволить скоротити час на проведення розрахунків до 25%, а також підвищить кількість можливих варіантів подолання загороджень і перешкод на напрямках пересування військ (сил).

Одним із подальших напрямків проведення досліджень є системний захист передачі інформації в інформаційно-комунікаційній мережі в умовах реального часу та вдосконалення СПЗ на основі використанням штучного інтелекту тощо.

УДК 008.04

Хмелевська О.О., Хмелевський С.І., Івахненко Т.О.

ВЕРИФІКАЦІЯ І ТЕСТУВАННЯ СКЛАДНИХ ПРОГРАМНИХ КОМПЛЕКСІВ

Одним з найважливіших елементів організації динамічної верифікації та тестування є оцінювання трудовитрат і часу, необхідні їх виконання. Витрати на динамічне тестування складних комплексів програм можуть становити істотну частину. Важливо, щоб тестування проводило достатня кількість фахівців і мали достатньо часу на якісне виконання завдань. Обмеження реальних ресурсів на верифікацію та тестування часто визначають досяжну якість динамічних програмних продуктів.

Для програми динамічного тестування може бути визначений власний життєвий цикл розробки, який включає планування стратегій і цілей, визначення вимог до тестів, їх аналіз, проектування та кодування. Група тестування має створювати спеціальні інструменти – генератори динамічних тестів, які автоматично створюють тести. Автоматизація тестування повинна забезпечувати людині, які здійснює тестування можливість спроектувати та розробити на основі вихідних вимог до комплексу програм повний комплект тестових сценаріїв, а потім із невеликими витратами повторювати динамічні тестові сценарії для виявлення та усунення помилок.

Витрати, необхідні автоматизації генерації тестів, зазвичай більше витрат за ручне написання тестів. При припущенні, що виконувати автоматизовані тести у випробуваннях або з метою технічного обслуговування системи може мати сенс побудувати спеціалізований стаціонарний випробувальний стенд генерації динамічних тестів, який може використовуватися весь період, доки підтримується та розвивається програмний комплекс.

Важливим аспектом організації динамічного тестування складного програмного продукту є рішення, в якому обсязі тестування достатньо і коли необхідно завершити процес тестування. Прийняття рішення про закінчення тестування включає аналіз та облік вартості та ризиків, пов'язаних з потенційними збоями та порушеннями надійності функціонування динамічного програмного засобу, що тестується. Водночас вартість самого тестування також є одним із обмежень, на основі яких приймається рішення про продовження тих чи інших пов'язаних з проектом робіт (зокрема, тестування) або їх припинення.

Для забезпечення високої якості складних комплексів програм реального часу потрібні відповідні проблемно-орієнтовані інтегровані системи автоматизації динамічного тестування, здатні досить повно замінити випробування програм із реальними об'єктами довкілля. При цьому висока вартість і ризик випробувань з реальними об'єктами майже завжди виправдовують значні витрати на такі інтегровані системи, якщо чекають випробування критичних програм з високими вимогами до якості функціонування програмних комплексів, з тривалим життєвим циклом і безліччю версій, що розвиваються. При необхідності такі генератори можуть швидко створювати тестові дані, наприклад, для проведення тестування навантаження.

Інструментальні засоби автоматизації процесів динамічного тестування та випробувань складних комплексів програм реального часу мають забезпечувати:

– визначення та формування динамічних тестів – реалізацію процесу тестування розробником: введення тестових наборів; генерацію тестових даних; введення очікуваних, еталонних результатів;

– виконання ділянки комплексу програм, що тестується між контрольними точками, для якого засіб тестування може перехопити операторське введення (клавіатури, миші і т.п.) і для якого дані можуть бути відредаговані і включені в наступні тестові сценарії;

– управління тестами та ділянкою програми, для якого засіб тестування може автоматично виконувати тестові набори;

– аналіз та обробку тестових результатів – можливість засобу тестування автоматично аналізувати тестові результати: порівняння очікуваних та реальних результатів, порівняння файлів, статистичну обробку результатів;

– аналіз покриття тестами вихідних вимог до програмного продукту виявлення функцій: які були виконані; процедур, які були викликані; даних сегментів коду; тимчасові характеристики функціонування програми, що випробовується; не було звернень;

– аналіз продуктивності комплексу програм, що він виконується: завантаження центрального процесора; завантаження пам'яті; звернення до специфікованих елементів даних;

– моделювання довкілля – підтримку процесу тестування з допомогою моделі динамічної імітації даних для програмного комплексу із зовнішніх апаратних компонентів системи.

Методи динамічного тестування з виконанням контрольованого комплексу програм більшою чи меншою мірою орієнтовані на виявлення помилок певних типів, переважно у структурі комплексу програм і реалізованих маршрутах обробки інформації. Методи тестування потоків даних орієнтуються на виявлення помилок в обчислювальній частини програм та у процесах перетворення різної інформації.

Така орієнтація дозволяє впорядковувати послідовність пріоритетного застосування методів з метою усунення, перш за все, помилок, що найбільше відображаються на коректності виконання програм, а також зосереджуватись на методах, що дозволяють вирішувати приватні завдання досягнення необхідної їх якості та відповідності вимогам за мінімальних витратах.

УДК 004.8

Ховрат А.В., Кобзєв В.Г.

ВИЯВЛЕННЯ СФАБРИКОВАНОЇ ТЕКСТОВОЇ ІНФОРМАЦІЇ В СОЦІАЛЬНО ОРІЄНТОВАНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ НЕЙРОМЕРЕЖ

Розвиток технологій генерації та видозміни оригінальних даних зумовив поширення проблеми фальсифікації інформації. Особливо гостро питання стоїть щодо текстових повідомлень, які важко перевірити. Під час соціально-політичної нестабільності обсяг подібних даних зростає і здатен призводити до поглиблення кризи чи загострення психологічного стану населення, ризиків його здоров'ю та життю. Особливо це стосується систем, які ставлять за мету розширення соціальних зв'язків, так звані соціально орієнтовані системи. Частина користувачів подібних застосунків за звичайних умов здатні самостійно за допомогою критичного мислення виявляти сфабриковані дані, але у випадку інформаційного перенасичення, що супроводжує надзвичайні ситуації, це стає доволі проблематичним завданням. Як приклад подібної ситуації можна згадати фейко-

ві фотографії, пов'язані з пандемією COVID-19 [1], чи величезну кількість підтверджених фактів фальсифікації новин під час вторгнення російської федерації на територію України [2], що використовувалися для приховування фактів порушення законів ведення війни армією рф чи дискредитації Збройних Сил України.

Створення моделей, що використовують сучасні засади інтелектуального аналізу даних, та таких, що зможуть швидко і точно виявляти факт підробки, дозволить зменшити вплив подібної інформації на зазначені системи, зокрема соціальні мережі, і пом'якшити супроводжувані ризики. Існуючі рішення, у більшості випадків, базуються або на штучному інтелекті, або на імовірнісних моделях. Останні дозволяють здійснювати аналіз історичних даних для побудови ймовірнісної сітки, за допомогою якої відбувається класифікація вихідної інформації. У випадках простого сортування текстових даних на предмет спаму подібні алгоритми здатні забезпечити високу точність, але у ситуаціях зі структурно складними даними або необхідністю врахування поточного контексту вони не дають потрібний результат [3].

Тому доцільно зупинитися на моделях, що базуються на штучному інтелекті, зокрема згорткових та рекурентних нейромережах, і перевірити ефективність їх застосування для виявлення факту підробки україномовних та російськомовних текстів. При цьому додатково необхідно розглянути алгоритми передобробки даних задля врахування контексту і засоби паралелізації запропонованих підходів.

Етап передобробки даних, окрім базових стадій очистки та фільтрації цільових наборів текстової інформації, має враховувати дві наступні складові:

– внутрішній контекст подання даних;
– зовнішнє інформаційне поле.

У соціальних мережах, які є прикладом соціально орієнтованих систем, видозміна інформації може слугувати формою гумору, а не бути спрямованою на маніпуляцію. У таких випадках відбувається хибнопозитивне маркування через внутрішній контекст подання даних. Для перевірки цього можна скористатися аналізом коментарів та реакцій, що супроводжують ту чи іншу новину. Оцінка їх емоційного забарвлення дає можливість пом'якшити проблему некоректної класифікації. Однак треба розуміти, що це не дозволить уникнути ситуацій, коли використовуються так звані «боти» –замасковані під людей програми або ж інші люди, що мають на меті розповсюдження дезінформації. Аналіз і врахування їх реакцій може змінити рішення класифікатору на хибнонегативне. Задля цього необхідно додатково розглядати зовнішнє інформаційне поле – агреговані історичні дані з «умовно перевірених» джерел.

Зазначена вище практика, дозволяє зменшити описані ризики, однак ґрунтується на припущенні, що існують такі бази знань, які не містять сфабрикованих даних. І хоча це твердження є помилковим, застосування агрегаційного підходу та методу експертної оцінки щодо визначення 100 найбільш достовірних джерел даних, дозволяє суттєво зменшити ймовірність хибнонегативного сприйняття.

Задля оптимізації часу роботи створених алгоритмів, доцільно перетворити зазначені складові в числовий вигляд і подавати на вхід як додаткові змінні. На цьому шляху використовується базовий ланцюжок контент аналізу: розподіл текстів на токени, їх лематизації та стемінг, видалення слів без лексичного навантаження і, зрештою, знаходження частотно-полярної характеристики на основі BM 25. Реакції та використані небуквенні вирази (зокрема смайли) було вирішено розподілити на групи за допомогою колеса емоцій Роберта Платчіка [4] і врахувати як корегуюче значення при визначенні частотно-полярної характеристики.

Аналіз запропонованих моделей класифікації почнемо з рекурентних нейромереж. Найпростіша нейромережа складається з декількох прихованих шарів, які працюють послідовно, опрацьовуючи результати попереднього шару. Зазначену особливість прийнято називати короткстроковою пам'яттю по аналогії з людським мозком. Така "короткостроковість" пояснюється збереженням результату лише попереднього кроку. Вра-

ховуючи зазначене, можна постулювати, що описана модель має два суттєвих недоліки – неможливість врахування довгострокового контексту та обмеженість у напрямку аналізу. З урахуванням того факту, що цільовими даними є текст, а також поліморфність української мови, найпростіша модель буде малоефективною.

Задля подолання окреслених недоліків доцільно обрати двонаправлену рекурентну нейромережу з довгостроковою пам'яттю (BiLSTM). Сутність цієї архітектури полягає у використанні двох різнонаправлених мереж, які містять у собі перетворення даних за допомогою сігма-функції та гіперболічного тангенсу, забезпечуючи таким чином обмеженість вихідного результату.

Після проведення детального аналізу та крос-валідації з'ясовані наступні значення гіперпараметрів моделі нейромережі:

– кількість прихованих шарів: зазвичай цей параметр встановлюється на рівні 2, оскільки кількість ситуацій, у яких продуктивність покращується за допомогою збільшення цього показника, є обмеженою. Крос-валідація дала аналогічний результат;

– розмір пакету: обробка кожного запису окремо може призвести до перенавчання, аби уникнути цього, дані розглядаються пакетно. При аналізі цього параметра встановлено, що оптимальним значенням є 50 записів;

– обрізання градієнту: специфічний параметр, який дозволяє уникнути проблем зникаючого та вибухового градієнтів, обрізаючи їх при подібних ситуаціях. Оскільки обрана модель BiLSTM, цей параметр є непотрібним;

– швидкість навчання: якщо значення занизьке, то навчання більш надійне, але оптимізація займе багато часу оскільки кроки до мінімуму функції втрат невеликі. Якщо навпаки швидкість занадто висока, то навчання може не збігатися або навіть розбігатися. Шляхом дослідження встановлено значення, що дорівнює 0.002.

Архітектура згорткової нейромережі (CNN) не має ані короткострокової, ані довгострокової пам'яті, натомість контекст враховується за допомогою згорток, що редукують розмірність тексту. І хоча подібний підхід не є настільки всеохоплюючим як у випадку BiLSTM, він не має недоліків, що притаманні найпростішій рекурентній мережі. Гіперпараметри такої нейромережі визначено наступним чином:

– розмір фільтра: після проведення кросс-валідації встановлено, що для обраного випадку найкращим буде 3-вимірний фільтр розмірності 3×3×3;

– кількість дескрипторів: цей параметр регулюються через розмір фільтру та відповідає останньому значенню розмірності, у нашому випадку – 3;

– глибина мережі: параметр визначається кількістю використаних фільтрів і зазвичай теж має бути не меншим за кількість дексрипторів. Крос-валідація показала, що оптимальним значенням є 3;

– розмір ядра: встановлено оптимальне значення, що дорівнює 4;

– розмір кроку при розгляді: виходячи із рекомендацій, які вказують на небажаність використання кроку більше 3, визначено оптимальне значення, що дорівнює 1. При такому кроці, параметр додавання неістотних нулів не застосовуватиметься.

З метою експериментальної перевірки ефективності, після аналізу результатів експертного оцінювання, встановлені наступні критерії для лінійної адитивної згортки з ваговими коефіцієнтами і максимізаційним ступенем оптимізації:

– економія часу класифікації з коефіцієнтом важливості 4 (вага 0.16);
– економія часу навчання з коефіцієнтом важливості 3 (вага 0.12);
– точність класифікації з коефіцієнтом важливості 10 (вага 0.4);
– ступінь врахування екзогенних змінних з коефіцієнтом важливості 8 (вага 0.32).

У якості цільових вибірок використані два набори новин щодо повномасштабного вторгнення російської федерації на територію України [5, 6]. Результати проведеного експерименту, приведені до єдиного принципу оптимізації та нормалізовані, наведені у таблиці 1.

Таблиця 1 – Експериментальні результати аналізу новин двома типами нейромереж

Тип нейромережі	Економія часу класифікації	Економія часу навчання	Нормалізована точність	Врахування зовнішнього впливу
CNN	1.00	0.17	0.94	1
BiLSTM	0.93	0.00	0.96	1

Висновки: 1) архітектура BiLSTM є більш ефективною моделлю за CNN, при цьому результати точності та швидкодії доводять доцільність її використання на практиці задля виявлення факту фальсифікації текстів; 2) така архітектура нейромереж може бути випробувана для опрацювання більш широкого кола текстової інформації.

Список використаних джерел

1. The impact of fake news on social media and its influence on health during the COVID-19 pandemic: a systematic review / Y. M. Rocha et al. Journal of Public Health. 2023. Vol. 31. P. 1007–1016.

2. Internet platforms as alternative sources of information during the Russian-Ukrainian war / K. Horska et al. Amazonia Investiga. 2023. Vol. 12, no. 62. P. 353–360.

3. Yakovlev S., Khovrat A., Kobziev V. Using Parallelized Neural Networks to Detect Falsified Audio Information in Socially Oriented Systems. X International Scientific Conference "Information Technology and Implementation" (IT&I-2023): Conference Proceedings, Kyiv, 20–21 November 2023. 2024. P. 220–238.

4. Kumar P., Vardhan M. Plutchik Wheel of Emotion and Machine Learning-Based Hybrid Sentiment Analysis for the Hindi Language with Minimum Dependency on High Computation Resources. SN Computer Science. 2023. Vol. 4. 797.

5. DS-Pr1nce. War in Ukraine: Russian social network discussions. Kaggle. URL: https://www.kaggle.com/datasets/ustyk5/war-in-ukraine-russian-social-network-discussions (date of access: 20.02.2024).

6. Zepopo. Ukrainian news. Kaggle. URL: https://www.kaggle.com/datasets/zepopo/ukrainian -fake-and-true-news (date of access: 20.02.2024).

УДК 658.012.2

Чала О.В, Богатов Є.О.

РОЗРОБКА ПРЕДСТАВЛЕННЯ БІЗНЕС-ПРОЦЕСУ ДЛЯ ПЕРШОГО РІВНЯ ЗРІЛОСТІ ПРОЦЕСНОГО УПРАВЛІННЯ

Запропоновано опис бізнес-процесу для першого рівня зрілості процесного управління. Дане представлення містить статичну і динамічну складові, які визначають структурні елементи процесу та їх взаємозв'язок на рівнях даних, процедур та знань. Представлення орієнтовано на автоматизоване формування моделі бізнес-процесу методами process mining при переході від функціонального до процесного управління.

Останні роки спостерігається стале зростання кількості підприємств, що впроваджують та успішно використовують процесний підхід до управління [4]. Альтернативою процесному підходу на сьогодні лишається використання функціонально-орієнтованого підходу, який має ряд переваг: вузьку спеціалізацію кожної організаційної одиниці; спроможність функціонування таких одиниць незалежно одна від одної; легкість управління, оскільки кожен відділ має свого керівника, через якого проходять

всі організаційні зв'язки; наявність чітко визначених ролей. Всі ці переваги є запорукою успішного функціонування порівняно малих вузько фахових організацій. Але по мірі зростання організації на перший план виходять гнучкість процесів підприємства, швидкість прийняття рішень, стандартизація робіт, можливість їх планування, масштабування та моніторингу. Реалізація цих вимог є вкрай складною задачею для функціонально орієнтованих підприємств. Все це створює підґрунтя для побудови моделей бізнес-процесів (БП) та подальшого переходу до першого рівня зрілості процесно-орієнтованого управління.

Такий перехід відбувається шляхом побудови моделей бізнес процесів «as-is» та подальшого удосконалення отриманих моделей, з тим, щоб отримати моделі «to be». Для побудови процесних моделей «as-is» використовуються методи Process mining [2]. В якості вхідних даних використовуються логи (журнали подій) [3]. Основна увага в Process mining приділяється побудові моделей поточних бізнес-процесів підприємства. На основі даних, зібраних під час виконання бізнес-процесів генеруються графові моделі, які дозволяють побудувати прототипи бізнес-процесів з метою їх подальшого використання при побудові удосконалених моделей «to-be» [4]. Зростання популярності цієї технології та відкритість коду програмних інструментів виконання інтелектуального аналізу процесів призвела до розробки та впровадження великої кількості підходів до аналізу логів подій та БП. Розроблені на сьогодні підходи дозволяють відобразити найрізноманітніші аспекти бізнес-процесів, що обмежені лише наявними даними про БП. Однак існуючі підходи не дають можливість побудувати модель бізнес-процесу в умовах неповноти даних щодо послідовності виконання робіт такого процесу.

Запропоновано розширений опис бізнес процесу, котрий охоплює його статистичні та динамічні властивості, а також враховує рівні зрілості процесного управління з метою формування моделі бізнес-процес при відсутності знань щодо порядку виконання процедур.

Запропоноване представлення бізнес-процесу містить такі складові: рівень даних, рівень процедур процесу та рівень знань БП. На рівні даних окремо виділені множини даних та елементи організаційної структури підприємства. Рівень даних представлений через сукупність об'єктів, атрибутів об'єктів, дані або припустимі значення атрибутів, та правила їх обробки. Правила обробки об'єктів представлені у логу у вигляді подій, оскільки подія містить інформацію про атрибути об'єктів та їх значення, а також дію, що призвела до становлення даних значень. Це визначає подію як джерело формування знань, та представляє правило обробки об'єктів у вигляді «дія - атрибут». Таке представлення процесів властиве підприємствам першого рівня процесного управління. Інформація про події міститься у логах. Результат процедури в таких логах представлений набором значень атрибутів об'єктів, що були отримані внаслідок виконання певної дії. Окремо визначений в моделі організаційний рівень також оперує об'єктами, але з тією відмінністю, що вони мають додаткові атрибути «роль» та «виконавець». Це виокремлення було зроблене з метою виділення організаційного аспекту як окремого аспекту БП, що дозволяє відобразити взаємодію певних ролей, виконавців. Наявність рівня даних у моделі є критичною для аналізу процесів систем першого та другого рівнів процесного управління, через їх орієнтованість на окремих виконавців.

Рівень послідовності процедур представлений через множину процедур як варіант виконання БП, та множину правил, що накладаються на послідовність їх виконання в межах певного процесу. Перехід між станами може супроводжуватися зміною об'єктів, що використовуються в межах визначеної процедури при виконанні сукупності визначених дій. Цей рівень є властивим підприємствам другого рівня зрілості процесів та вище.

Рівень знань являє собою сукупність бізнес-правил на виконання БП, які визначають межі процесу та умови його виконання. Джерелом таких знань можуть виступати внутрішні політики підприємства, результати інтерв'ювання виконавців, наявність сталих

послідовностей виконання робіт, вимоги технологічного процесу виробництва. Використання знань про процес властиве підприємствам третього рівня зрілості процесів та вище. Підприємства з рівнем зрілості вищим за третій, як правило, не доповнюють модель БП новими артефактами, але активно використовують наявні для моніторингу та контролю бізнес-процесів підприємства, а також для стратегічного планування подальших дій.

Кожен з визначених у моделі рівнів дозволяє виконати поступове уточнення вимог до виконання БП, та визначає зв'язок між моделлю БП та логами подій, що генеруються в результаті його виконання.

Відмінність запропонованого представлення бізнес-процесу полягає в тому, що попередні моделі розглядали БП як статичну структуру, а опис динамічної складової процесу був обмежений включенням правил послідовності виконання процедур. Окрім того запропоноване представлення дозволяє розглядати обмежений перелік рівнів в залежності від рівня зрілості процесів підприємства.

Список використаних джерел

1. Aalst W. M. P. v. d. Process Mining: Data Science in Action. Springer, 2016. 467 p.

2. Aalst W. v. d. Using Process Mining to Bridge the Gap between BI and BPM. Computer. 2011. Vol. 44, no. 12. P. 77–80. URL: https://doi.org/10.1109/mc.2011.384 (date of access: 03.03.2024).

3. Caeldries F., Hammer M., Champy J. Reengineering the Corporation: A Manifesto for Business Revolution. The Academy of Management Review. 1994. Vol. 19, no. 3. P. 595. URL: https://doi.org/10.2307/258943 (date of access: 03.03.2024).

4. Process Mining Handbook / ed. by W. M. P. van der Aalst, J. Carmona. Cham : Springer International Publishing, 2022. URL: https://doi.org/10.1007/978-3-031-08848-3 (date of access: 03.03.2024).

УДК 004.5:004.6

Чала О.В, Євдокимов Б.С.

АНАЛІЗ ЗНАННЯ-ОРІЄНТОВАНИХ МЕТОДІВ ПОБУДОВИ РЕКОМЕНДАЦІЙ В ІТ-ПРОЕКТАХ ІНДИВІДУАЛЬНОГО СТРАХУВАННЯ

Запропоновано підхід до побудови рекомендацій з використанням темпоральних знань. Останні визначають упорядкованість у часі подій вибору товарів та послуг в рекомендаційній системі. Підхід дає можливість врахувати зміни у потребах користувачів, в тому числі в проектах індивідуального страхування.

Рекомендаційні системи аналізують дії користувача, визначають його потреби та формують пропозиції щодо товарів та послуг з урахуванням визначених потреб. Використання рекомендацій у індивідуальному страхуванні дає можливість у автоматизованому режимі підібрати страховий поліс згідно потреб користувача. Однією із важливих задач щодо побудови рекомендованого списку послуг є задача динамічної побудови рекомендацій з урахуванням змін у контексті вибору користувача. Динамічна побудова рекомендацій передбачає зміну умов вибору та потреб користувачів в реальному часі. Основною її метою є надання користувачам актуальних і персоналізованих рекомендацій з урахуванням їхнього поведінкового змінюваного контексту.

Вирішення даної задачі передбачає використання гібридних методів побудови рекомендацій. Такі методи зазвичай включають колаборативну фільтрацію та додаткову обробку вхідних даних та результатів. Тобто формується послідовність методів відбору

вхідних даних, колаборативної фільтрації та відбору або упорядкування отриманих за результатами фільтрації рекомендацій. Однак існуючі гібридні методи орієнтовані в першу чергу на використання інформації про відомих користувачів. Відсутність даних для нових користувачів спотворює такі рекомендації[1].

В роботі пропонується підхід, який враховує темпоральну упорядкованість даних як щодо поточного користувача (послідовність взаємодії з інтерфейсом рекомендаційної системи), так і щодо інших користувачів (темпорально упорядкована інформація про вибір користувачів).

Запропонований підхід передбачає порівняння темпоральних упорядкованостей для цільового користувача, для інших користувачів і відбір предметів для рекомендацій на основі схожості цих упорядкованостей. В практичному плані підхід дає можливість побудувати рекомендації для нових користувачів, які тільки починають взаємодіяти з рекомендаційною системою, або ж при зміні потреб та вподобань користувачів[2].

Динамічна побудова рекомендацій відкриває перед страховими компаніями безліч можливостей. Її здатність адаптуватися до змін у поведінковому контексті користувача дозволяє надавати персоналізовані рекомендації, що перетворює взаємодію між страхувальниками та клієнтами у більш ефективний та задовільний процес. Крім того, динамічні рекомендації сприяють оптимізації процесу прийняття рішень в страховій сфері, забезпечуючи ефективнішу роботу страхових агентів та зменшення часу, потрібного для вибору найбільш вигідних умов страхування. Це сприяє підвищенню задоволення клієнтів та зменшенню витрат на виробництво.

Список використаних джерел

1. Бурк, Р. (2002). Гібридні системи рекомендацій: огляд та експерименти. User Modeling and User-Adapted Interaction, 12(4), 331-370.

2. Констан, Д. А., & Рідл, Дж. (2012). Системи рекомендацій: від алгоритмів до користувацького досвіду. User Modeling and User-Adapted Interaction, 22(1-2), 101-123.

УДК 004.8:004.9

Чалий С.Ф, Дементʼєв А.М.

ІНТЕРПРЕТОВАНЕ ПРЕДСТАВЛЕННЯ ПРОЦЕСУ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ПОБУДОВІ ПОЯСНЕНЬ В ІНТЕЛЕКТУАЛЬНІЙ СИСТЕМІ

Запропоновано представлення спрощеного процесу прийняття рішень в інтелектуальній системі, що містить ймовірнісні куазальні залежності. Такий опис процесу може бути безпосередньо інтерпретований при формуванні пояснення в інтелектуальній системі.

Стрімке зростання кількості інтелектуальних систем у військовій, банківській, медичній, сферах свідчить про нові можливості оперативного прийняття та імплементації рішень, що забезпечує використання таких систем [1]. Зокрема, в США проводяться дослідження щодо розробки безпечного та етичного ШІ для військових застосувань [2]. Базовою умовою імплементації запропонованих інтелектуальною системою рішень є довіра користувачів. Для забезпечення цієї умови розробляються самопояснювальні інтелектуальні системи. Така система здатна представити причини отриманого результату. Ключова ідея існуючих підходів до побудови пояснень полягає у формуванні ключових залежностей процесу прийняття рішень в інтелектуальній системі на основі доступних вхідних, вихідних і проміжних даних. Однак такі залежності визначають лише поверхневі знання і не дають можливість визначити механізм прийняття рішень.

Деталізація процесу прийняття рішень потребує створення його спрощеної інтерпретованої моделі, що і свідчить про актуальність теми даного дослідження.

Для вирішення вказаної проблеми пропонується сформувати інтерпретоване представлення процесу прийняття рішень на основі дерева рішень. Вибір даного представлення обумовлено тим, що дерево рішень містить залежності r_j^i, які є прозорими для користувача в сенсі відображення причинно-наслідкових зв'язків між d_i – вхідними/ проміжними й d_j – результуючими даними процесу прийняття рішення. Такі причинно-наслідкові зв'язки є ймовірнісними, тобто кожна залежність $d_i \to d_j$ характеризується ймовірністю p_j^i: $r_j^i : d_i \overset{p_j^i}{\to} d_j$. Прохід по дереву дає можливість інтерпретувати пояснення Π у вигляді послідовності каузальних залежностей як спрощеної моделі процесу прийняття рішення, представленого даними d_J: $\Pi = \left\langle r_j^1 .... r_J^{J-1} \right\rangle$. В якості вхідних даних для побудови інтерпретованого представлення використовуються логи інтелектуальної системи.

Розроблене представлення дає можливість отримати пояснення із заданим ступенем деталізації у відповідності до кваліфікації користувача інтелектуальної системи.

Список використаних джерел

1. Artificial Intelligence Index Report 2023 [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf.

2. Vergun D. U.S. Endorses Responsible AI Measures for Global Militaries [Електронний ресурс] / David Vergun. – 2023. – Режим доступу до ресурсу: https://www.defense.gov/News/News-Stories/Article/Article/3597093/us-endorses-responsible-ai-measures-for-global-militaries/.

УДК 004.8:004.9

Чалий С.Ф, Єрохін Д.О.

ОЦІНКА ПОЯСНЕНЬ КОРИСТУВАЧАМИ З ВИКОРИСТАННЯМ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ПРОЦЕСІВ

Сучасні інтелектуальні системи використовують складні алгоритми прийняття рішень, які є неявними, непрозорими для користувача внаслідок технологічних або юридичних обмежень. Для обґрунтування процесу прийняття рішень в таких системах і подальшого їх ефективного використання використовуються пояснення. Стрімкий розвиток методів побудови пояснень за останні роки пов’язаний із формуванням та реалізацією програми пояснювального штучного інтелекту (ПШІ) [1]. Методи ПШІ передбачають формування пояснень з урахуванням особливостей даного процесу або у відповідності до ментальної моделі користувача інтелектуальної інформаційної системи. Методи першої групи враховують зв'язок між вхідними даними та рішенням системи, або ж зв'язок між доступними для спостереження діями та отриманим рішенням. Методи другої групи базуються на дослідженнях у сфері психології та орієнтовані на побудову пояснень з урахуванням особливостей когнітивного процесу, зокрема на основі порівняння інформації щодо об'єктів, які сприймає людина. Таким чином, методи першої та другої групи формують пояснення у різних аспектах – внутрішнього механізму прийняття рішень та використання отриманих рішень. Однак для ефективного форму-

вання пояснень доцільно інтегрувати обидва аспекти. Зазначене свідчить про актуальність теми дослідження.

Таки інтеграція дає можливість виконати оцінку пояснень і може бути виконана на основі підходу After-Action Review, який широко використовується в армії США [2]. Підхід передбачає аналіз виконаних військових операцій. Аналіз може бути проведений на основі як суб'єктивних даних, представлених інформацією від виконавців, так і об'єктивних даних, представлених доступними записами про виконані дії.

Для вирішення задачі оцінки пояснень на основі об'єктивних даних про дії в інтелектуальних системах з використанням After-Action Review доцільно використати методи інтелектуального аналізу процесів (process mining). Ці методи використовують журнали подій для формування моделі процесу прийняття рішення. Журнал містить записи у вигляді подій про доступні для спостереження дії даного процесу. Побудова моделі дає можливість користувачеві зіставити пояснення із отриманим результатом та доступною для спостереження послідовністю дій процесу прийняття рішення.

Запропонований підхід до оцінки пояснень містить такі етапи. По-перше, формується підмножина журналу подій, що відображає суттєві для пояснення дані. По-друге, встановлюються залежності між подіями (послідовні у часі події, незалежні подій, паралельні події, тощо) з використанням методу Alpha-miner. По-третє, відбираються залежності, суттєві для пояснення. Таким є залежності, що містить події із значеннями атрибутів, що були використані в поясненні. В четвертих, формується набір можливих залежностей між діями та рішенням системи. В-п'ятих, отримані альтернативні залежності та основне пояснення оцінюються користувачем системи з точки зору обґрунтованості отриманого рішення та упорядковуються.

Отримана оцінка пояснення у порівнянні з можливим альтернативами створює умови для уточнення пояснення з тим, щоб воно відповідало сприйняттю користувача за обмежень щодо відповідності процесу прийняття рішення.

Список використаних джерел

1. Explainable Artificial Intelligence: Exploring XAI Techniques in Military Deep Learning Applications / L.Luotsinen, D. Oskarsson, P. Svenmarck, U. Bolin. – Sweden, 2019.

2. Scott C. Implementing after-action review systems in organizations / C. Scott, A. Dunn. – North Carolina, USA, 2015.

УДК 004.8:004.9

Чалий С.Ф, Кравченко Р.В.

ОПИС СТАНІВ ПОЯСНЕННЯ В ІНТЕЛЕКТУАЛЬНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ З ВИКОРИСТАННЯМ ТЕМПОРАЛЬНИХ ЗАЛЕЖНОСТЕЙ

Запропоновано темпорально упорядковане представлення станів процесу пояснення в системі штучного інтелекту. Дане представлення дає можливість використати зміни стану інтелектуальної системи з часом для побудови пояснення, що дає можливість врахувати зовнішні впливи на таку систему.

Сучасні інтелектуальні інформаційні системи орієнтовані на вирішення складних завдань, пов'язаних із знаходженням залежностей у великих масивах даних, зокрема виявленням зовнішніх утручань та загроз, в тому числі у сфері кібербезпеки. Моделі роботи таких систем формуються з використанням алгоритмів машинного навчання і тому є закритими від користувачів. При використанні рішення такої системи користувач має впевнитись, що отриманий результат не є наслідком скритих упередженості у да-

них. Для вирішення цієї задачі системи штучного інтелекту доповнюються можливостями пояснення [1].

Однак існуючі підходи до побудови пояснень орієнтовані на наперед визначені процеси прийняття рішень в інтелектуальній системі і не враховують зовнішні впливи, які можуть привести до змін в таких процесах. Прикладом таких утручань є атаки в рекомендаційних системах, які спотворюють рейтинги запропонованих позицій і, в підсумку, спотворюють рекомендації. Довіра до таких спотворених рекомендацій може привести до некоректних рішень користувача. Таким чином, при побудові пояснень необхідно враховувати можливі зміни у процесі прийняття рішень. Тому задача темпорального опису процесу пояснення, що відображає процес прийняття рішень в інтелектуальній системі, є актуальною задачею.

Темпоральні залежності задають відносну упорядкованість станів або дій процесу у часі. Така упорядкованість задається для пар станів [2]. Тоді процес пояснення може бути описаний у загальному вигляді для $j-$реалізації через темпоральні правила виду $s_{j,i} \to s_{j,i+n} : t_{j,i} < t_{j,i+n}$, що пов'язують пари станів $s_{j,i}, s_{j,i+n}$, які виникли у моменти $t_{j,i}$, $t_{j,i+n}$ відповідно. Вказані правила узагальнюються для відомих реалізацій пояснення L_j. Кожен стан характеризується множиною змінних $c_{j,i}^k$, що визначають причини виконання дій процесу прийняття рішення та мають значення $v_{j,i}^{k,l}$. Відповідно, темпоральні правила можуть бути деталізовані у вигляді залежностей між значеннями цих змінних: $\left(c_{j,i}^k, v_{j,i}^{k,l}\right) \to \left(c_{j,i+n}^k, v_{j,i+n}^{k,l}\right)$. Кожен варіант процесу пояснення, що формується з цих правил, складається з послідовностей таких пар $\left(c_{j,i}^k, v_{j,i}^{k,l}\right)$, зміна значень яких враховує зовнішні впливи на процес прийняття рішення. Вибір послідовності для пояснення виконується в залежності від властивостей отриманого рішення.

Список використаних джерел

1. . Gunning and D. Aha, “DARPA’s Explainable Artificial Intelligence (XAI) Program,” AI Magazine, vol. 40, no. 2, pp. 44–58, Jun. 2019, doi: https://doi.org/10.1609/aimag.v40i2.2850.

2. Chala, O. (2018). Models of temporal dependencies for a probabilistic knowledge base. Econtechmod. An International Quarterly Journal, 7(3), 53-58.

УДК 004.8:004.9

Чалий С.Ф, Лещинський В.О.

КОМБІНОВАНА ОЦІНКА ПОЯСНЕНЬ В СИСТЕМАХ ШТУЧНОГО ІНТЕЛЕКТУ

Запропоновано комбінований підхід до оцінки пояснень, який включає оцінку відповідності пояснення як процесу прийняття рішення, так і знанням щодо використання отриманого в інтелектуальній системі рішення. Оцінка щодо відповідності пояснення процесу прийняття рішення базується на використанні показників чутливості, коректності та складності пояснення. Оцінка відповідності пояснення знанням щодо використання результату базується на узгодженості знань щодо предметної області. Запропонований підхід дає можливість відбирати одне із можливих пояснень згідно його відповідності поточному екземпляру процесу прийняття рішення в системі штучного інтелекту, а також з урахуванням потреб користувача.

Дослідження в галузі психології пізнання свідчать, що людина сприймає нові знання лише після їх обґрунтування. Таке обґрунтування зазвичай надається в формі пояснень. Пояснення, як правило, відображають у графічному, текстовому, формальному вигляді причинно-наслідкові залежності між даними, подіями та діями, які були використані для представлення нових знань [1].

Пояснення в системах штучного інтелекту надають можливість користувачеві впевнитись у коректності та практичній корисності отриманого результату, оскільки такі системі зазвичай використовують моделі, що є незрозумілими, «непрозорими» для людини-користувача [2]. Непрозорість є наслідком різних принципів формування рішень інтелектуальною системою та людиною. Людина використовує обмежений об'єм даних, пов'язаних причинно-наслідковими залежностями, тоді як сучасні інтелектуальні системи оперують великими об’ємами даних із латентними залежностями. Відповідно, наявність упередженості в даних приводить до помилкових рішень та не може бути виявлено безпосередньо, без пояснень.

Зазначене свідчить про важливість вирішення задач формування та подальшої оцінки пояснення з тим, щоб надати тлумачення, що робить прозорим процес прийняття рішення та є зрозумілим для користувача.

Сучасні підходи до побудови пояснення базуються на формуванні залежностей між вхідними та проміжними даними системи штучного інтелекту, а також отриманим результатом. Окремий напрямок досліджень у даній сфері пов'язаний із формуванням ментальної моделі користувача [3]. Така модель використовується для того, щоб сформувати пояснення згідно вимог та рівня знань користувача.

Існуючі підходи передбачають, що оцінка пояснення виконується окремо для процесу пояснення, а також окремо у аспекті сприйняття користувачем.

Оскільки пояснення можна розглядати як узагальнений та спрощений опис процесу прийняття рішення в інтелектуальній системі, який містить лише ключові залежності, то при оцінці тлумачення важливо врахувати відхилення пояснення внаслідок змін у вхідних даних та відповідність пояснення реальному процесу формування результату [4]. В цілому оцінка відповідності пояснення процесу прийняття рішення враховує явні знання щодо системи штучного інтелекту.

Оцінка відповідності пояснення знанням користувача враховує можливість практичного використання пояснення, а також результату інтелектуальної системи. Традиційно дана оцінка виконується на основі анкетування користувачів. Однак таке анкетування виявляє лише явні знання клієнтів і не враховує неявні знання, оскільки останні не можуть бути виражені в вербальній формі.

Зазначене протиріччя свідчить про актуальність розробки комбінованого підходу до оцінки пояснення, який би враховував його відповідність процесу прийняття рішення та узгодженість із знаннями щодо предметної області, включаючи неявні знання.

Запропонований підхід використовує таку інформацію: вхідні дані інтелектуальної системи; доступні дані логу системи; дані щодо області використання отриманих результатів.

Слід зазначити, що лог (або журнал подій) інтелектуальної системи може бути отриманий при наявності підсистеми моніторингу. Події відображають доступні для спостереження дій і тому можуть бути використані для пояснення. Дані щодо використання отриманих результатів можуть містити текстовий опис предметної області.

Підхід містить такі етапи.

Етап 1. Оцінка чутливості пояснення.

На даному етапі використовується оцінка в рамках теорії можливостей, тобто оцінюється можливість використання поточної залежності для пояснення.

Етап 2. Оцінка коректності пояснення.

На даному етапі використовується бінарна оцінка щодо відповідності пояснення процесу прийняття рішення.

Етап 3. Оцінка складності пояснення.

На поточному етапі складність оцінюється через кількість значень змінних, які будуть використані для пояснення. В подальшому коректні пояснення упорядковуються за значенням складності.

Етап 4. Оцінка відповідності пояснення знанням щодо предметної області.

Дана оцінка виконується на основі векторного пошуку у базі знань, що містить текстовий опис предметної області. Такий пошук дає можливість визначити семантичну узгодженість текстових значень змінних, що використовуються для пояснення, та слів з опису предметної області. На даному етапі у процесі пошуку враховується неявна складова знань.

Етап 5. Відбір підмножини пояснень, що відповідають знанням про предметну область та упорядкування їх за складністю.

Запропонований підхід дає можливість із множини альтернативних тлумачень підібрати пояснення, яке відповідає знанням про предметну область та має меншу складність, що забезпечує можливість адаптації пояснення до потреб користувача.

Список використаних джерел

1. Miller T. (2019), “Explanation in artificial intelligence: Insights from the social sciences”, Artificial Intelligence, vol. 267, pp.1-38, DOI: https://doi.org/10.1016/j.artint.2018.07.007

2. Gunning and D. Aha, “DARPA’s Explainable Artificial Intelligence (XAI) Program,” AI Magazine, vol. 40, no. 2, pp. 44–58, Jun. 2019, doi: https://doi.org/10.1609/aimag.v40i2.2850.

3. Чалий, С., & Лещинська, І. (2023). Концептуальна ментальна модель пояснення в системі штучного інтелекту. Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, (1 (9), 70–75. https://doi.org/10.20998/2079-0023.2023.01.11

4. Chalyi, Sergii & Leshchynskyi, Volodymyr. (2023). Інформаційна технологія оцінки пояснень в інтелектуальній інформаційній системі. Системи управління, навігації та зв’язку. Збірник наукових праць. 4. 120-124. 10.26906/SUNZ.2023.4.120.

УДК 621.396

Чесановський І.І., Волощук Є.В.

АНАЛІЗ ТИПОВИХ КОНСТРУКЦІЙ ВИНОСНИХ УКХ АНТЕН ДЛЯ МАЛОПОТУЖНИХ РАДІОСТАНЦІЙ

Досвід ведення бойових дій виявив ряд слабких місць в системі організації зв’язку, особливо в польових умовах. Як виявилось, наявні портативні засоби радіозв’язку, при їх використанні з підземних укриттів, бліндажів, тощо не забезпечують достатньої дальності та якості зв’язку. Вирішення проблеми шляхом під’єднання антени через додатковий фідер унеможливлювалось відсутністю виносних конструкцій антен, сумісних з даним типом радіостанцій та неможливість їх під’єднання до портативних засобів зв’язку через особливості побудови антено-фідерного пристрою портативної радіостанції.

В результаті радіоаматорських експериментів з радіостанціями та різними антено-фідерними рішеннями було вироблено ряд конструктивних рішень, що частково вирішували дану проблему. Аналіз таких рішень показав, що найбільшого розповсюдження дістали конструкції виносних антен, виготовлених з відрізку коаксіального кабелю з використанням противісів (антена «павук») або коаксіальні симетричні вібраторні ан-

тени з використанням фільтрів індуктивних фільтрів-пробок. Проте, в більшості випадків, як і очікувалось такі конструкції антено-фідерних пристроїв недостатньо узгоджені з прийомо-передавачем радіостанції, що призводить до значних втрат в лінії передачі і як наслідок, низької якості та малої дальності зв'язку.

Було проведено ряд експериментів з даними конструкціями антен, що розраховувались під конкретні матеріали для конкретних умов застосування та з заданими параметрами коаксіальної лінії передачі з метою встановлення відповідності їх характеристик прогнозованим. Як виявилось в результаті лабораторного дослідження отриманих конструкцій антен, їхні характеристики значно відрізняються від прогнозованих що обумовлюється цілою низкою причин починаючи від невідповідності заявлених характеристик матеріалів і закінчуючи недосконалістю самої конструкції в частині сполучення симетричної лінії передачі та несиметричного входу (виходу) прийомопередавача. Як показали результати вимірювань, значення коефіцієнта стоячих хвиль (КСВ) може сягати значень від 3 до 5 в більшій частині робочої смуги частот, що є абсолютно неприйнятним. Особливої уваги заслуговують антени що будуються на основі фільтрів пробок з коаксіального кабелю. Як показали результати вимірювань, для УКХ діапазону частот, побудувати ефективний фільтр-пробку (з опором порядку сотень або тисяч Ом) шляхом намотування відрізка коаксіального кабелю неможливо. Крім того, наявність такої коаксіальної конструкції вносить значну нерівномірність в АЧХ АФП (в межах 2-3 за значенням КСВ в точці підключення до радіостанції), що також негативно впливає на характеристики радіосистеми в цілому.

Таким чином, виготовлення ефективних конструкцій виносних антен та використання симетричних ліній передачі електромагнітної енергії для підключення їх до портативних радіостанцій може бути застосовано за виконання ряду вимог, а саме: вибору правильної комбінації конструкції антени, лінії передачі та схеми підключення; застосування вимірювального приладу (векторного аналізатора, вимірювача КСВ, тощо) при налаштуванні АФП та урахування умов застосування АФП.

УДК 004.8-378

Шамшин О.П.

ОНЛАЙН-ПЛАТФОРМА ДЛЯ РІШЕННЯ І ПЕРЕВІРКИ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ФІЗИЧНИХ ЗАВДАНЬ

У цій роботі ми розглянемо архітектуру онлайн-платформи вирішення та перевірки на основі штучного інтелекту фізичних завдань, її ключові компоненти та принципи роботи. Ми також обговоримо потенційні вигоди від використання такої системи та виклики, з якими вона може зіткнутися, а також запропонуємо рекомендації щодо її розробки та впровадження.

Уміння вирішувати завдання з фізики грає ключову роль в освітньому процесі, оскільки сприяє досягненню кількох важливих цілей [1]. По-перше, студенти бачать, як теоретичні знання застосовуються на практиці, що робить їхнє навчання більш усвідомленим і змінює їхнє ставлення до навчання. По-друге, це розвиває їхнє логічне мислення, допомагає конкретизувати отримані знання та пов'язує теоретичний матеріал з його практичним застосуванням. У процесі вирішення фізичних завдань (ФЗ) студенти розвивають також низку особистісних якостей, включаючи розумові здібності, творче мислення, логіку, кмітливість, спостережливість, самостійність та акуратність.

Використання комп'ютера під час вирішення завдань часто призводить до того, що моделі студента, використовувані у навчальних системах, не відповідають їх реальному

психологічному та інтелектуальному стану, що може призвести до зменшення інтересу до навчання та дослідницької активності [2]. Для успішного навчання необхідно, щоб педагог рефлексував на процесі навчання, включаючи вибір методів вирішення завдань, контроль за діяльністю учнів, вибір навчальних впливів та побудову моделей учнів. Це може бути реалізовано через ієрархічну структуру правил або інструкцій, що визначають стратегію навчання, включаючи правила вирішення завдань, метаправила, правила навчальних впливів та правила поводження з правилами. Складність завдання в навчанні залежить від багатьох факторів, включаючи заплутаність завдання, мотивацію та підготовленість студента. Комп'ютерне навчання трансформує ці проблеми на "розмір кроку" - кількість можливих помилок на кожному етапі і час з їхньої рішення, що можна порівняти з принципом "один крок у навчанні може означати сто кроків у розвитку".

Створення онлайн-платформи для вирішення та перевірки ФЗ можна розділити на дві частини: перша – це програма рішення ФЗ, що включає розробку інтерфейсу, що відповідає класичному виду запису розв’язання ФЗ: умова завдання, «Дано» - короткий запис умови з переведенням величин у СІ, «Знайти » - запис величин, які шукаються в задачі, «Рішення» - поле для запису рішення, «Набір формул» - меню, що випадає, з формулами даного розділу, теми заняття, «Довідкові значення» - меню, що випадає, значень фізичних констант і довідкових значень, меню «Дії», що включає кнопки «Рішення рівняння», «Заміна (підстановка)», «Додати поле (формулу)», «Спростити», «Рахувати», «Рисувати», «Перевірити». Основна складність першої частини – це можливість запису математичних рівнянь у формі LaTeX, перетворення цих рівнянь та фронтенд розробка клієнтської частини. Друга частина включає бекенд розробку, основна складність якої пов'язана з організацією адекватної системи перевірки розв'язання задачі – реакція на натискання кнопки «Перевірити», порівняння з кроками розв'язання задачі, записаними в базі даних.

Використання способу перевірки, що застосовується, наприклад, при проведенні ЗНО, коли перевіряється збіг чисельного значення шуканої величини, отриманий студентом або абітурієнтом, з відповіддю перевіряючого не є інформативним і не дозволяє виявити помилки, що з'являються під час вирішення завдання. Використання варіантів відповідей завдання зводиться до лотереї і найчастіше вирішується перебором можливих відповідей. Можливі випадки, коли у тестах немає правильної відповіді, і, як приклад, можна назвати завдання на парадокс обертання монети американського тесту SAT 1982 року.

Зазначимо, що перевірка запису умови завдання, відповіді, величин, які потрібно знайти, розмірності всіх фізичних величин, що використовуються у рішенні, не є такою складною проблемою порівняно з перевіркою ходу рішення та його аналізом, у зв'язку з тим, що, по-перше, можливі різні способи розв'язання задачі. По-друге, навіть якщо завдання і перевірка використовують той самий спосіб вирішення, все одно можливі різні кроки рішення, послідовності знаходження чи вираження невідомих величин. Відомо, що студенти молодших курсів часто при вирішенні ФЗ використовують шкільні покрокові підстановки, при яких замінюється по одній змінній у виразі, а не кілька одразу. Кожна заміна - це нова рівність, в якій знак дорівнює входить один раз. Тоді як у виші мається на увазі запис рівності в один рядок з багаторазовим використанням знака дорівнює. По-третє, можливі різні спрощення виразів, скорочення, угруповання, порядок яких у вирішенні та перевірці може не співпадати, використовуватись або не використовуватись. По-четверте, відома теорема Річардсона, згідно з якою неможливо визначити, чи ідентичні два символьні вирази в цілому, однак у багатьох випадках можна порівняти два вирази, щоб перевірити, чи представляють вони один і той же математичний об'єкт. При цьому можливі два корисні способи порівняння символічних виразів: структурна та математична рівність.

Поточні методи перевірки розв'язання фізичних завдань поділяють на ручну та автоматизовану. Ручна перевірка характеризується трудомісткістю і тривалістю процесу, схильна до людського чинника і не забезпечує миттєвий зворотний зв'язок. Системи автоматизованої перевірки порівнюють відповідь користувача з еталонною, можуть використовуватися для перевірки простих завдань, але не можуть перевірити завдання, що вимагають складних міркувань і не можуть надати докладні пояснення помилок, що ускладнює навчання.

Інтеграція генеративних моделей штучного інтелекту (ШІ) у вирішення фізичних завдань привернула значну увагу протягом останніх п’ятнадцяті місяців. Можна відзначити, що процес використовування ШІ в розв’язанні ФЗ, застосування його як асистента та довідника при цьому доволі широко освітлюється в літературі, наприклад [3], але можливість використовувати ШІ при оцінюванні розв’язання ФЗ майже не розглядалася.

Використання ШІ у перевірці фізичних завдань приносить безліч переваг. Дозволяє автоматизувати процес перевірки та, таким чином, знижує необхідність ручної роботи та прискорює процес оцінки. Системи ШІ здатні аналізувати великі обсяги даних із високою точністю. Вони можуть виявляти навіть дрібні помилки чи неточності. ШІ не схильний до суб'єктивних упереджень. Він оцінює завдання на основі фактів та правил, що забезпечує більш об'єктивну оцінку. Системи ШІ характеризуються масштабованістю, можуть обробляти велику кількість завдань одночасно. Це особливо корисно у разі великих навчальних потоків, коли кількість студентів перевищує 40 – 50 осіб, або під час проведення масових контрольних робіт, екзаменів. ШІ може адаптуватися до унікальних потреб користувачів. Наприклад, він може надавати індивідуальні рекомендації для кожного студента, можлива організація підказок по ходу розв'язання задачі, спливаючих контекстних підказок до величин, що входять до фізичних законів, організація системи списків формул, що належать до розділу фізики, за яким проводиться практичне заняття. Наприклад, у механіці це будуть заняття з кінематики та динаміки поступального та обертального руху, законів збереження імпульсу та енергії, механічної роботи. Число формул у списку на одне заняття варіюється в межах 20 - 60 і залежить від того, скільки розділів поєднує те чи інше заняття.

Завдяки ШІ можна скоротити час, який викладачі витрачають на перевірку завдань. Це дозволяє їм більше часу приділяти навчанню та консультації студентів, знижує психологічне навантаження на викладача, зменшує зорове навантаження, пов'язане як з безперервним перебуванням за екраном ноутбука, так і з постійною необхідністю дешифрації, декодування почерку студентів, який через відсутність практики письма часто перетворюється у нечитаний набір символів. Спроби розпізнати окремі рішення задач студентами за допомогою Google Gemini призводять до його відповіді: «На жаль, зображення, яке ви надіслали, не несе інформації, необхідної для перевірки завдання.»

Системи ШІ можуть навчатися нових даних і постійно поліпшуватися. Це дозволяє їм бути актуальними та адаптуватися до змін у навчальних матеріалах.

Загалом використання ШІ у вирішенні та перевірці фізичних завдань сприяє підвищенню ефективності, точності та якості освіти.

У даній роботі ми розглядаємо основні проблеми створення та впровадження в учбовий процес онлайн-платформи самостійного розв’язання ФЗ з можливістю оцінювання як окремого кроку розв’язання, так і виставлення підсумкової оцінки, з можливістю використання штучного інтелекту на різних етапах рішення, а особливо при перевірки задачі, досліджуємо складні взаємозв'язки між штучним інтелектом та процесом прийняття рішень студентами, звертаючи увагу на когнітивні та емоційні аспекти, які важливо враховувати при використанні штучного інтелекту для вирішення фізичних завдань. Ми також розглядаємо педагогічні наслідки впровадження штучного інтелекту в освітній процес з фізики та наголошуємо на важливості підтримки збалансованого підходу, який сприяє розвитку критичного мислення, творчості та етичних міркувань.

При старанній роботі над цими аспектами ми можемо використати потенціал штучного інтелекту для розширення можливостей вирішення завдань, зберігаючи при цьому незаперечну цінність людського інтелекту та досвіду у наукових дослідженнях.

Список використаних джерел

1. Shamshin A. Development and use of the program of automatic problem solving when conducting practical classes in physics at the university //*ScienceRise: Pedagogical Education.* 2021. 5(44). С. 23 – 29. https://doi.org/10.15587/2519-4984.2021.241236.

2. Шамшин О.П. Психолого-педагогічні проблеми комп'ютеризації розв'язку задач з фізики в технічному ЗВО // *Перспективи та інновації науки. Серія «Педагогіка».* 2022. №13(18). С. 516 – 528. *https://doi.org/10.52058/2786-4952-2022-13(18)-516-528.*

3. Шамшин О.П. Психолого-педагогічні проблеми використання штучного інтелекту при розв'язання фізичних задач //*ScienceRise: Pedagogical Education*. 2023. №5(56). С. 4 - 10. https://doi.org/10.15587/2519-4984.2023.292760.

УДК 621.396:623.1/.7

Швидкий А.В., Галицький О.Ф., Кукобко С.В.

УДОСКОНАЛЕННЯ РОБОТИ БАГАТОКАНАЛЬНОЇ СТАНЦІЇ НАВЕДЕННЯ РАКЕТ ЗЕНІТНОГО РАКЕТНОГО КОМПЛЕКСУ С-300В1 ПРИ ВИЯВЛЕННІ ТА СУПРОВОДЖЕНІ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Результати аналізу сучасних безпілотних літальних апаратів (БПЛА), методів виявлення та супроводження цілей, що рухаються на малих висотах з низькою швидкістю виявили необхідність з'ясування спроможностей існуючих вогневих засобів протиповітряної оборони по боротьбі з ними [1-13].

За результатами проведених досліджень приймального пристрою багатоканальної станції наведення ракет (БСНР) встановлено наступне. Приймальний пристрій сигналів ІІТ забезпечує когерентну обробку сигналів на проміжній частоті в межах посилки з ціллю оптимізації відношення сигнал-шум на вході приймального пристрою, перетворює інформацію в форму, зручну для візуальної індикації і роботи пристрою автоматичної обробки виявлених сигналів. Передбачена можливість роботи з системою некогерентного цифрового накопичення інформації від восьми зондувань. Використовується також в режимі автосупроводження для організації сторожових стробів по дальності і швидкості. Приймальний пристрій супроводження є складовою частиною приймальної системи БСНР, служить для обробки радіолокаційних сигналів типу ІІТ з ціллю отримання сигналів похибки по первинних координатам. Принцип роботи приймального пристрою супроводження полягає в квазіоптимальній обробці вхідних сигналів і виділення сигналів похибки первинних координат. З ціллю збільшення комплексної роздільної здатності по швидкості здійснюється вагова обробка вхідних сигналів. Збільшення динамічного діапазону приймального пристрою супроводження здійснюється шляхом обробки сигналів на чотирьох проміжних частотах. Нормування сигналів похибки проводиться за допомогою двох пов'язаних між собою систем дискретного автоматичного регулювання підсилення.

Пропозиції щодо удосконалення виявлення та супроводження БПЛА БСНР базувалось на наступному:

а) поточна реалізація компенсації дзеркального каналу за допомогою НВЧ фільтру призводить до втрати 2 дБ енергії корисного сигналу;

б) запропонована схема компенсації позбавлена вказаних недоліків.

в) реалізація запропонованого рішення дозволить збільшити ймовірність виконання завдань за призначенням зенітною ракетною батареєю за рахунок збільшення дальності виявлення та, як наслідок, додаткового часу, що з'являється.

Список використаних джерел

1. Асавалюк А.В. Похибки визначення повного вектора швидкості в єдиній прямокутній системі координат системою оглядових станцій радіолокації с різною точністю / А.В. Асавалюк, С.В. Герасимов, Є.С. Рощупкін // Системи озброєння і військова техніка. – 2017. – № 2. – С. 53-56. http://nbuv.gov.ua/UJRN/soivt_2017_2_13

2. Джус, В., Гайбадулов, Б., Калугін, Д., Титаренко, Р., & Кукобко, С. (2021). Вплив похибок топоприв'язки та орієнтування радіотехнічних засобів контролю повітряного простору на оцінки координатної інформації, що видаються ними. Наукові праці Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки, (8), 31-43. https://doi.org/10.37701/DNDIVSOVT.8.2021.04

3. Кукобко С.В. Оцінювання радіолокаційної помітності безпілотних літальних апаратів як цілей для засобів радіолокації протиповітряної оборони Сухопутних військ / С.В. Кукобко, Є.С. Рощупкін // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXVII міжнародної науково-практичної конференції MicroCAD-2019, 15–17 травня 2019 р.: у 5 ч. Ч. V. / за ред. проф. Сокола Є.І. – Харків: НТУ "ХПІ". – С. 99.

4. Herasimov S.V. Assessment of possibilities of detection and tracking of drones the system of radiolocation stations of antiaircraft defense / S.V. Herasimov, S.V. Kukobko, E.S. Roshchupkin, A.E. Roshchupkina// Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXVIII міжнародної науково-практичної конференції MicroCAD-2020, 28-30 жовтня 2020 р.: у 5 ч. Ч. V. / за ред. проф. Сокола Є.І. – Харків: НТУ "ХПІ". – С. 270.

5. S. Herasimov, E. Roshchupkin, V. Kutsenko, S. Riazantsev and Yu. Nastishin, Statistical analysis of harmonic signals for testing of Electronic Devices, International Journal of Emerging Trends in Engineering Research, vol.8, is. 7, 2020, p.p. 3791-3798, https://doi.org/10.30534/ijeter/2020/143872020

6. Кукобко С.В., Рощупкін Є.С. (2022). Моделювання системи технічного обслуговування безпілотних літальних апаратів. Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2022): тези доповідей XII Міжнародної науково-практичної конференції, Чернігів

7. Герасимов С.В. Синтез вимірювальних сигналів для визначення технічного стану систем автоматичного управління / С.В. Герасимов, С.В. Кукобко, Є.С. Рощупкін, О.О. Расстригін // Озброєння та військова техніка. – 2016. – № 4. – С. 32-36. http://nbuv.gov.ua/UJRN/ovt_2016_4_7

8. Герасимов, С.В., Гречка, А.В., Рощупкин, Е.С., Рощупкина, А.Е., & Кукобко, С.В. (2020). Адаптивный метод технической диагностики системы разнесенных радиотехнических устройств. Azərbaycan dövlət dəniz akademiyasının elmi əsərləri (ISSN 2220-1025), 2, 129–137. https://doi.org/10.5281/zenodo.5035853

9. Tymchenko, S., Kaplun, Y., Roshchupkin, E., Kukobko, S. (2023). Substantiation of Time Distribution Law for Modeling the Activity of Automated Control System Operator. In: Shkarlet, S., et al. Mathematical Modeling and Simulation of Systems. MODS 2022. Lecture Notes in Networks and Systems, vol 667. Springer, Cham. https://doi.org/10.1007/978-3-031-30251-0_9

10. Кукобко, С.В., Ветошкін, О.Г., Рощупкін, Є.С., & Джус, В.В. (2020, July 1). Автоматизове технічне обслуговування рознесених електронних інформаційних систем. Математичне та імітаційне моделювання систем (МОДС 2020), Чернігів: ЧНТУ. https://doi.org/10.5281/zenodo.5067687

11. Dzhus, V., Roshchupkin, Y., Kukobko, S., Herasymov, S., Drob, N., & Trofymova, M. Estimation of noise radiance point sources multichannel direction finding systems resolution by linear prediction method. Sistemi obrobki ìnformacìï. 2021. № 4(167). С. 19-26. https://doi.org/10.30748/soi.2021.167.02

12. Герасимов С.В. Підвищення боєготовності зенітних ракетних військ шляхом оптимальної закупівлі комплектуючих виробів зенітних ракетних комплексів / С.В. Герасимов, Д.М. Ізосімов, Є.С. Рощупкін, В.В. Старцев // Системи озброєння і військова техніка. – 2010. – № 1(21). – С. 55-59. http://nbuv.gov.ua/UJRN/soivt_2010_1_13

13. Кукобко С.В. Структура спеціального математичного забезпечення імітації повітряної обстановки в підсистемі тренажу АСУ спеціального призначення / С.В. Кукобко, М.А. Павленко, Є.С. Рощупкін // Системи озброєння і військова техніка. – 2008. – № 2. – С. 44-48. http://nbuv.gov.ua/UJRN/soivt_2008_2_16

Шкамета О.С.

ДОСЛІДЖЕННЯ МЕТОДІВ АНОТУВАННЯ З ВИКОРИСТАННЯМ МОВНИХ МОДЕЛЕЙ В ІТ-ПРОЕКТАХ ЕЛЕКТРОННОГО АРХІВУВАННЯ

Запропоновано підхід до анотування текстів з використанням мовних моделей та векторного пошуку в базі знань, що містить опис предметної області.

Системи штучного інтелекту, що базуються на використанні нейронних мереж, забезпечили принципово нові можливості у сфері обробки природної мови. Великі мовні моделі (Large Language Models – LLM) забезпечують можливість автоматизованого анотування великих обсягів документів, що значно спрощує процес архівування інформації та підвищує його ефективність. Традиційно використовуються такі підходи до анотування, як класифікація, розмічання семантики, тощо [1]. Використання LLM, а також локальних мовних моделей в реальних ІТ-проектах електронного архівування дає можливість підвищити точність та швидкість вказаних підходів. Тим самим компанії, які використовують LLM, можуть заощадити час і матеріальні витрати на електронне архівування, а також уникнути людських помилок. Проведені дослідження доводять, що використання глибоких нейронних мереж значно підвищує швидкість анотування документів у порівнянні з традиційними методами [2].

Основним викликом у покращенні технології анотування з використанням великих та локальних мовних моделей є проблема налаштування нейронних мереж для досягнення оптимальних результатів при використанні міток класифікації, ключових слів та семантичної розмітки. Друга задача полягає у включенні до складу ІТ-проекту електронного архівування локальних мовних моделей з тим, щоб створити єдину інтелектуальну систему.

Для вирішення вказаних задач зазвичай пропонується збільшити обсяг навчальних даних для підвищення точності мовної моделі [3]. Однак такий підхід потребує суттєвих обчислювальних ресурсів. В якості альтернативного підходу на основі використання локальної мовної моделі пропонується реалізувати перетворення тексту з використанням векторного пошуку у базі знань відповідної тематики. Такий семантичний пошук дає можливість виділити ключові елементи тексту для анотування і в подальшому поєднати текст по ключовим словам з використанням мовної моделі.

Запропонований підхід дає можливість знизити витрати на підготовку моделі та на анотування і створює умови для побудови інтелектуальної системи із вбудованою підсистемою автоматизованого архівування.

Список використаних джерел:

1. Сміт М., Грейстоун, П., Шин Ц. (2020). Покращення ефективності архівування за допомогою глибоких нейронних мереж. Журнал електронного архівування, 123-135.
2. Шульженко І.П. (2021). Оптимізація систем анотування на базі нейронних мереж. Матеріали конференції з обробки природної мови, 45-50.
3. Кравець Л.С., Неклеса А.Ф., Авраменко О.О. (2022). Нейронні мережі та анотування: виклики та перспективи. Журнал технологій та інформаційних систем, 15, 78-89.

УДК 621.391

Штомпель М.А., Приходько С.І.

БІОІНСПІРОВАНЕ ДЕКОДУВАННЯ АЛГЕБРАЇЧНИХ ЗГОРТКОВИХ КОДІВ

Перехід до новітніх радіотехнологій та складна завадова обстановка призводить до необхідності забезпечення заданої якості надання сучасних послуг електронних комунікацій. Важливим критерієм якості обслуговування користувачів є достовірність передавання інформації. У значній кількості технологій радіозв'язку для вирішення цієї задачі застосовуються згорткові завадостійкі коди. Окремим класом даних кодів є алгебраїчні згорткові коди, побудовані на основі недвійкових блокових кодів, зокрема, кодів Ріда-Соломона. М'яке декодування даних кодів дозволяє підвищити ефективність їх застосування у сучасних системах радіозв'язку шляхом використання наявних досягнень у теорії оптимізації, теорії алгоритмів, обчислювальної біології та інших напрямах.

У роботі представлено підхід до м'якого декодування алгебраїчних згорткових кодів з використанням біоінспірованих оптимізаційних процедур, що складається з наступних етапів.

Етап 1. Формування жорсткого рішення та обчислення синдрому для прийнятої послідовності.

На даному етапі прийнятий сигнал перетворюється у двійкову послідовність та визначається відповідний синдром для заданої перевірочної матриці алгебраїчного згорткового коду. Якщо отриманий синдром не дорівнює нулю, то здійснюється перехід до наступного етапу.

Етап 2. Розміщення елементів прийнятої послідовності за зменшенням їх надійності та формування найбільш надійного базису.

На цьому етапі здійснюється упорядкування елементів прийнятої послідовності з урахуванням наявної м'якої інформації, отриманої з каналу зв'язку, та застосовуються відповідні перестановки для знаходження найбільш надійного базису породжувальної матриці алгебраїчного згорткового коду.

Етап 3. Біоінспірований пошук переданої кодової послідовності.

Даний етап передбачає формування початкової популяції пробних інформаційних послідовностей, що використовуються для знаходження можливих кодових послідовностей шляхом їх множення на найбільш надійний базис породжувальної матриці алгебраїчного згорткового коду. Далі відбувається оцінювання отриманих кодових послідовностей на основі обраної фітнес-функції та формування наступного покоління популяції пробних інформаційних послідовностей з використанням обраної біоінспірованої процедури. Даний біоінспірований пошук здійснюється ітеративно та завершується після досягнення максимальної кількості ітерацій, в результаті чого знаходиться найбільш імовірна пробна кодова послідовність.

Етап 4. Формування оцінки переданої кодової послідовності на основі зворотного перетворення.

На даному етапі знаходиться оцінка двійкової переданої кодової послідовності шляхом застосування зворотних перестановок на основі найбільш надійного базису породжувальної матриці алгебраїчного згорткового коду.

За результатами проведених досліджень для обраних моделей каналу зв'язку визначено, що запропонований метод м'якого декодування алгебраїчних згорткових кодів дозволяє підвищити енергетичну ефективність даних кодів та має прийнятну обчислювальну складність. Таким чином, представлений метод декодування доцільно використовувати у новітніх системах радіозв'язку.

Shubina G., Shevchenko O.

GENERAL CHARACTERISTICS OF INTELLIGENT WIRELESS TELECOMMUNICATION SYSTEMS

The report notes that the development of wireless technologies has made it possible to fully license and distribute all existing frequency bands. Therefore, in today's environment, the introduction of new services is becoming increasingly difficult, and in some cases impossible. To address this situation, the IEEE 802.22 WRAN standard is currently being used, which opens up new opportunities for efficient and optimal use of the radio frequency spectrum. The IEEE 802.22 WRAN (Wireless Regional Area Network) standard is a wireless standard that was developed to create wireless access networks of a regional and local nature. The main purpose of the standard was its application in the unused or free parts of the radio frequency spectrum that were previously used for television broadcasting, i.e. the spectrum in the frequency range of 54 to 862 MHz. Even its name - "Wireless Regional Area Network" - indicates its regional purpose for the implementation of wireless communications, where the creation of wired infrastructure was difficult to access or even impossible or impractical.

Яровий В.С.

ЗАБЕЗПЕЧЕННЯ РЕЗЕРВНОГО ЕЛЕКТРОЖИВЛЕННЯ ЗА ДОПОМОГОЮ ГІБРИДНИХ СОНЯЧНИХ СТАНЦІЙ В УМОВАХ ВОЄННОГО СТАНУ

Війна в Україні поставила нові виклики перед енергетичною інфраструктурою. Російські ворожі атаки на українську енергетику призвели до необхідності мати резервне джерело енергопостачання і на рівні інфраструктурних об'єктів, і на рівні забезпечення електронних комунікаційних систем Сил оборони .

Ефективне застосування резервних джерел дозволить знизити сьогоденні ризики. Рішення щодо підвищення енергетичної безпеки повинні враховувати функціонування всіх складових енергосистеми та специфіки кожного з видів діяльності у сфері енергетики.

Тому слід відзначити один із варіантів резервування системи електроживлення електронних комунікаційних систем – за допомогою гібридних сонячних станцій

Перевагами такого резервування є:

– набагато безпечніша (в порівнянні з паливними генераторами) експлуатація;

– відсутність шуму (може бути невеликий шум від вентилятора системи охолодження);

– відсутність рухомих частин і відповідно більш надійна експлуатація;

– суттєве зменшення споживання в літній період;

– дешевша в порівнянні з паливними генераторами електроенергія (на рівні вартості енергії з мережі);

– в сонячні дні значно збільшується тривалість резервування – можна працювати без зовнішнього джерела;

– на цивільних об’єктах є потенціал щодо продажу надлишків генерації в зовнішню мережу.

Незважаючи на переваги, існують і певні недоліки такого резервування, а це:

– неможливість забезпечення повного резервування в зимовий період;

– потреба в порівняно великих капіталовкладеннях;

– необхідність наявності місця під розміщення сонячних панелей.

При використанні такого виду резервування необхідно врахувати наступне:

– використовувати лише гібридні інвертори, що можуть працювати від сонця, батарей чи електромережі, а головне працюватимуть під час відключення зовнішньої електромережі. Більш дешеві мережеві інвертори після відключення електропостачання просто вимкнуться, навіть якщо сонця буде достатньо;

– забезпечувати підключення в розрив з електромережею через двохпозиційний вимикач для виключення можливості подачі мережевої напруги на інвертор і вихід його з ладу;

– вибирати потужність інвертора і батареї на 50–100% більшою ніж середня потужність споживачів (для забезпечення робочого струму в найбільш ефективних діапазонах);

– для підключення батарей використовувати кабелі достатнього перерізу;

– за умови необхідності запуску від інверторів насосів без частотних перетворювачів (особливо це стосується свердловин) – передбачати 2–3 кратний запас по потужності на “пускові струми”;

– за можливості використовувати пристрої з таймерами заряджання для включення заряджання в періоди, коли мережа не перевантажена іншими пристроями (програмується в гібридному інверторі);

– підключати до інвертора лише критичних споживачів, бо через використання потужних споживачів, дуже швидко розряджатимуться акумулятори;

– можливість нарощування ємності акумуляторів;

– необхідність використання системи на базі LiFePo4 акумуляторів, які безпечніші, довговічніші за свинцеві та можуть швидко заряджатися.

В той же час заборонено підключати генератори в мережу через систему “вилка – вилка”, так як це є причиною аварій, загорянь і виходу з ладу обладнання, а також використання систем резервування зі свинцевими акумуляторами в закритих погано вентильованих приміщеннях.

Таким чином використання електроживлення за допомогою гібридних сонячних станцій є одним із варіантів забезпечення електронних комунікаційних систем резервним електроживленням, але внаслідок демаскуючої ознаки сонячних панелей, є більш доцільним в пунктах постійної дислокації, а також у мирний час.

УДК 539.3

Яровий Г.Г., Васильєв А.Ю., Баулін Д.С., Ткачук Г.В., Шаталов О.Є.

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ СТІЙКОСТІ БОЙОВИХ БРОНЬОВАНИХ МАШИН ПРИ ЗДІЙСНЕННІ ПОСТРІЛІВ ІЗ ВЛАСНОГО ОЗБРОЄННЯ

Запропоновано математична та чисельна моделі системи "бойовий модуль – бронекорпус – система підресорювання – непідресорені елементи – ґрунт» на дію реактивних сил віддачі. Це дозволить при обмеженої тривалості проведення розрахунків з заданої точністю розраховувати такі показники як поперечна та повздовжня статична стійкість бойових машин, що впливають на спроможності бойових броньованих машин при здійсненні пострілів із власного озброєння.

Питання впливу додаткового бронезахисту на підвищення маси бронетехніки, зміщення центру мас та відповідно вплив на стійкість броньованих бойових машин, у тому числі і при виконанні вогневих завдань є на даний час актуальними. Одним із важливих показників, які впливають на спроможності бойових броньованих машин при здійсненні пострілів із власного озброєння, є поперечна та повздовжня статична стійкість бойових машин [1].

Тут слід враховувати, наприклад, і розташування осі цапф малокаліберних автоматичних гармат, якими оснащені їхні бойові модулі, і калібр озброєння, який значним чином визначає рівень реактивних сил віддачі при стрільбі, і кути стрільби, з одного боку, відносного власного корпусу машини, а з іншого, – відносно горизонту.

Окрім того, одним із додаткових важливих визначальних чинників є вплив розташування бойової машини на місцевості, що диктує її статичну номінальну просторову орієнтацію [2]. Ще одним важливим чинником, який також раніше не враховувався, є динамічний характер дії реактивних сил віддачі. Дійсно, на відміну від урахування тільки статичних складових діючих на корпус броньованої машини сил, урахування динамічних складових потенційно змінює реакцію системи "бойовий модуль – бронекорпус – система підресорювання – непідресорені елементи – ґрунт» на дію реактивних сил віддачі. Відбувається перерозподіл динамічних реакцій опорних елементів на ґрунті, а відтак – і характеристики стійкості бойової машини [3].

В основу математичного моделювання покладено метод скінченних елементів. Для цього використовувалися комп'ютерне проектування та моделювання образів досліджуваних об'єктів на базі обчислювальних логічних алгоритмів CAE-модуля ANSYS [3,4]. Математична модель легко броньованих бойових машин складається з таких елементів, як бойовий модуль, бронекорпус, система підресорювання, колісна база. Бойовий модуль та бронекорпус складається з набору тривимірних плоских поверхонь, обмежених набором прямолінійних і криволінійних кромок. У загальному випадку кромки можуть бути або вільними – у цьому разі вони описують геометрію отворів у бронепластині, або належати кільком поверхням одночасно (зазвичай двом), у цьому разі кромка найчастіше є зварним швом між різними "проекціями" (бронепластини).

Для моделювання поведінки означеної динамічної системи із урахуванням перелічених нових чинників на основі рівнянь Лагранжа 2-го роду розроблені математична та чисельна моделі.

Чисельне моделювання проводилось на основі таких припущень:

– аеродинамічний рух снаряда в середині ствола не розглядається;

– розглядається процес одиночного пострілу;

– властивості матеріалу розглядаються як монолітні, ізотропні з однорідною структурою.

За допомогою цих моделей виконані відповідні дослідження реакції бойової машини на здійснення пострілів із озброєння бойового модуля.

Список використаних джерел

1. Наукові основи створення спеціального шасі з комбінованою енергетичною установкою для колісної техніки Національної гвардії України: остаточний звіт про НДР (“Шасі-К”) М.А. Подригало, Д.С. Баулін, О.О. Морозов, та інші № держреєстрації 0121U107478. Харків : НАНГУ 2023. С. 185.

2. Манжура С.А. Багатошарові броньовані структури для забезпечення захисту особового складу і військової техніки [Текст]: монографія / С.А. Манжура, Д.С. Баулін, С.А. Горєлишев, М.А. Ткачук, А.Ю. та інші – Х.: Національна акад. НГУ, 2023. – 335 с

3. Математическое представление построения трехмерных тактических диаграмм с учетом движения и изменения ориентации корпуса бронированной машины в пространстве / О.Е. Шаталов, А.Ю. Ларин, А.Ю. Васильев, А.В. Мартыненко, А.Н. Ткачук, А.В. Грабовский. Вестник НТУ “ХПИ”. Машинознавство та САПР. 2005. № 5. С. 152-161.

4. Пономарев Е.П., Васильев А.Ю. К вопросу о проведении многовариантного анализа напряженно-деформированного анализа корпуса МТ-ЛБ// Механіка та машинобудування. – 2005.– №1. – с.289-294.

ЗМІСТ

АБЕТКОВИЙ ПОКАЖЧИК АВТОРІВ ПУБЛІКАЦІЙ

Військова частина А 3444, м. Черкаси

Іванов Б.В.	- провідний науковий співробітник	***27***

Військовий інститут Київського національного університету імені Тараса Шевченка

Кубявка М.Б.	- кандидат технічних наук, начальний науково-дослідного відділу	***200***
Пирогов К.О.	- науковий співробітник	***200***
Черних Ю.О.	- кандидат технічних наук, доцент, провідний науковий співробітник	***200***

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут , м. Київ

Андрущенко В.М.	- головний науковий співробітник науково-дослідного управління наукового центру зв'язку та інформатизації	***158***
Бескровний О.І.	- кандидат технічних наук, доцент, доцент кафедри	***155***
Бондаренко О.Є.	- начальник науково-дослідного відділу - заступник начальника науково-дослідного управління наукового центру зв’язку та інформатизації	***273, 275***
Бондаренко Т.В.	- старший науковий співробітник наукового центру зв’язку та інформатизації	***320***
Бригадир С.П.	- старший науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру зв’язку та інформатизації	***273***
Вороная С.М.	- науковий співробітник науково-дослідного відділу наукового центру зв’язку та інформатизації	***40***
Гетьман А.В.	- старший науковий співробітник науково дослідного відділу науково-дослідного управління наукового центру зв’язку та інформатизації	***273, 275***
Глобін А.В.		***111***
Живило Є.О.	- доцент кафедри	***98***
Івченко М.М.		***111***
Карабань О.В.		***111***
Козубцов І.М.	- доктор педагогічних наук, кандидат технічних наук, старший науковий співробітник, професор кафедри	***40, 155, 266, 298***
Козубцова Л.М.	- кандидат технічних наук, доцент, завідувач кафедри	***155***
Комаров В.О.	- кандидат технічних наук	***206***
Куцаєв П.В.	- молодший науковий співробітник науково-дослідної лабораторії науково-дослідного управління наукового центру зв’язку та інформатизації	***277***
Мальцева І.Р.	- старший науковий співробітник науково-дослідної лабораторії науково-дослідного управління наукового центру зв’язку та інформатизації	***226***
Мартинюк В.В.	- провідний науковий співробітник науково-дослідної лабораторії науково-дослідного управління наукового центру зв’язку та інформатизації	***226***
Логвіненко Н.М.	- кандидат педагогічних наук, доцент, доцент кафедри	***298***
Нестеров О.М.	- кандидат військових наук, начальник кафедри	***266***
Овсянніков В.В.	- кандидат технічних наук, провідний науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру зв’язку та інформатизації	***226***
Ольшанський В.В.	- доцент кафедри	***266***
Паламарчук Н.А.	- начальник науково-дослідної лабораторії науково-дослідного управління наукового центру зв’язку та інформатизації	***277***
Паламарчук С.А.	- начальник науково-дослідного управління наукового центру зв’язку та інформатизації	***226***
Побережець Т.В.	- лабораторії науково-дослідного управління наукового центру зв’язку та інформатизації	***277***
Пономарьов О.А.	- начальник факультету	***266***
Прохорський С.І.	- науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру зв’язку та інформатизації	***273, 275***
Процюк Ю.О.	- провідний науковий співробітник науково-дослідної лабораторії науково-дослідного управління наукового центру	***277***

Інститут радіофізики та електроніки імені О.Я. Усикова НАН України, м. Харків

Holovan O.	- науковий співробітник	***68***
(Головань О.В.)		
Кудряшов В.Є.	- кандидат технічних наук, с.н.с., провідний науковий співробітник	***203***

Луцький національний технічний університет

Ліщина В.О.	- кандидат технічних наук, доцент, завідувач кафедри	***155***

Науково-дослідний центр гуманітарних проблем Збройних Сил України, м. Київ

Приходько Ю.І.	- кандидат педагогічних наук, доцент, провідний науковий співробітник	***144***

Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький

Бабарика А.О.	- доктор філософії	***134, 316***
Басараб О.К.	- кандидат технічних наук, доцент, викладач кафедри	***16***
Вавpічен О.А.	- старший викладач кафедри	***30, 75, 280***
Волощук Є.В.	- курсант	***362***
Городиський Р.О.	- старший викладач кафедри	***30, 75***
Катеринчук І.С.	- доктор технічних наук, професор, професор кафедри	***134***
Кожушко В.Ю.		***316***
Лазоренко О.В.	- кандидат психологічних наук, доцент	***316***
Мул Д.А.	- кандидат технічних наук, доцент, доцент кафедри	***239, 271***
Площик А.С.	- викладач кафедри	***262***
Прокопенко Є.В.	- кандидат технічних наук, доцент, заступник начальника кафедри	***239, 271***
Равлюк В.В.	- викладач кафедри	***280***
Радіон Н.В.	- курсант	***16***
Рачок Р.В.	- доктор технічних наук, професор, професор кафедри	***286***
Стрельбіцький М.А.	- доктор технічних наук, професор, викладач кафедри	***314***
Табенський С.М.	- старший викладач кафедри	***316***
Хоптинський Р.П.	- кандидат технічних наук, доцент кафедри	***286***
Чесановський І.І.	- кандидат технічних наук, доцент, начальник кафедри	***362***

Національна академія Національної гвардії України, м. Харків

Алфімова Л.Д.	- кандидат хімічних наук, доцент, завідувачка кафедри	***7***
Баулін Д.С.	- кандидат технічних наук, с.н.с., провідний науковий співробітник науково-дослідної лабораторії Науково-дослідного центру	***370***
Бордунова К.І.	- старший інженер Центру імітаційного моделювання	***27, 206***
Vlasov K.	- старший викладач кафедри	***39***
(***Власов К.В.)***		
Горєлишев С.А.	- кандидат технічних наук, доцент, провідний науковий співробітник науково-дослідної лабораторії Науково-дослідного центру	***70***
Глушко П.Г.	- курсант	***91***
Глущенко М.О.	- старший викладач кафедри	***64***
Душкін В.Д.	- кандидат фізико-математичних наук, доцент, доцент кафедри	***7, 91***
Єльчанінов О.Д.	- кандидат технічних наук, доцент, доцент кафедри	***302***
Iokhov O.	- доктор технічних наук, професор, начальник Центру імітаційного моделювання	***115, 116, 117***
(Іохов О.Ю.)		
Казіміров О.О.	- кандидат військових наук, доцент, доцент кафедри	***119***
Константинов С.О.	- науковий співробітник Центру імітаційного моделювання	***138***
Лазарев В.Д.	- старший викладач кафедри	***216***
Майборода І.М.	- кандидат військових наук, доцент, доцент кафедри	***223***
Малюк В.Г.	- кандидат технічних наук, доцент, доцент кафедри	***224***
Манько А.В.	- ад'юнкт	***115***
Новикова О.О.	- кандидат технічних наук, доцент, професор кафедри	***94, 161, 334***
Оленченко В.Т.	- кандидат технічних наук, доцент, начальник кафедри	***242***
Пасічник А.В.	- викладач кафедри	***86***
Раєнко О.С.	- викладач кафедри	***283***

Для нотаток

For notes

Наукове видання

Міжнародна науково-практична конференція

“ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ ТА ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ”

Збірник тез доповідей

Відповідальний за випуск *О. Ю. Іохов*

В авторській редакції.
Упорядник: *О. О. Новикова*
Комп’ютерна верстка: *О. О. Новикова*

Формат 60х84/16. Ум. друк. арк. 9,62. Тираж 30 пр. Зам. № 39.

Видавець і виготовлювач Національна академія Національної гвардії України
Майдан Захисників України, 3, м. Харків, 61001.
Свідоцтво суб’єкта видавничої справи ДК № 4794 від. 24.11.2014 р.