НАЦІОНАЛЬНА АКАДЕМІЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

КАФЕДРА ВІЙСЬКОВОГО ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ

Збірник тез науково-практичної конференції

ПЕРСПЕКТИВИ РОЗВИТКУ ТА ЗАСТОСУВАННЯ СУЧАСНИХ СИСТЕМ І ЗАСОБІВ ЗВ'ЯЗКУ В ІНТЕРЕСАХ УПРАВЛІННЯ ВІЙСЬКАМИ

26 лютого 2025 року

Харків-2025

Перспективи розвитку та застосування сучасних систем і засобів зв'язку в інтересах управління військами**:** Збірник тез науково-практичної конференції (Україна, м. Харків, 26 лютого 2025 року). – Х.: Національна академія Національної гвардії України, 2025. – 17с.

Організатор конференції:
Національна академія Національної гвардії України (м. Харків);

Організаційний комітет конференції:
Голова – І.М. Майборода, доцент кафедри військового зв'язку та інформатизації командно-штабного факультету Національної академії Національної гвардії України, кандидат військових наук, доцент.
Відповідальний секретар – О.О. Казіміров, доцент кафедри військового зв'язку та інформатизації командно-штабного факультету Національної академії Національної гвардії України, кандидат військових наук, доцент.

Адреса організаційного комітету: 61001, м. Харків, майдан Захисників України, 3, Національна академія Національної гвардії України, кафедра військового зв'язку та інформатизації.
Електронна адреса: Kaf4@ukr.net.

Тези доповідей опубліковано в авторській редакції, мовою оригіналу: **http://kinf.nangu.edu.ua**

УДК. 623.612

Власов К.В., старший викладач кафедри Національної академії Національній гвардії України
Новикова О.О., професор кафедри Національної академії Національній гвардії України, кандидат технічних наук, доцент

ОСОБЛИВОСТІ МЕТОДІВ БОЙОВОЇ ІДЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ СИГНАЛЬНИХ ЗАСОБІВ ЗВ'ЯЗКУ ЗА СТАНДАРТАМИ НАТО

З урахуванням досвіду ведення сучасних бойових дії та ростом значимості дій у сучасних війнах окремих зразків озброєння та військової техніки і суб'єктів збройної боротьби проблемними стають питання їх взаємного розпізнання на полі бою.

В країнах – учасницях НАТО питання розпізнання належності сил на полі бою або в районі операцій вирішується поєднанням процедур контролю, ситуативної поінформованості, застосуванням технічних засобів і проведенням ефективної підготовки.

Оскільки організація виконання цього завдання ускладняється при збільшенні відстані, складності рельєфу та зниженні видимості, основним засобом запобігання помилковій ідентифікації та знищенню один одного, особливо на рівні військової частини і вище, є використання ефективних заходів командування та управління.

Мета бойової ідентифікації полягає в тому, щоб на основі єдиних керівних документів, ефективної підготовки і дотримання правил ведення бойових дій досягти вдосконалення ситуативної поінформованості, а також методів, засобів і приладів розпізнавання з метою підвищення бойової ефективності і, як наслідок, зменшення випадків ураження своїх (взаємодіючих) військ.

Взаємна ідентифікація на полі бою здійснюється шляхом встановлення зв'язку (відповідно до АТР-3.2.2) і використання таких методів і процедур контролю: виконання обов'язків у бойовому просторі; використання систем автоматичного і ручного запиту та відповіді; організація підготовки особового складу; використання системи управління бойовим простором.

Ідентифікація та розпізнавання сил союзників здійснюється за допомогою таких засобів як: зовнішність особового складу та вид озброєння; динаміка дій; часові параметри; звукові характеристики; електронні випромінювання; інфрачервоний спектр; сигнали; відомості про дислокацію військ; наземні/повітряні панелі бойової ідентифікації.

Певні обмеження у застосуванні сигналів розпізнавання та ідентифікації, пов'язані з людським фактором і технічними несправностями. До таких обмежень відносяться: відсутність інформації в особового складу коаліційних військ щодо поточної відповіді на запит; вихід з ладу розпізнавального сигнального обладнання; відсутність належного рівня технічного обслуговування та чистоти; неспроможність дати правильну відповідь на запит не повинна розглядатися як доказ виявлення противника; можливість потрапляння сигналів до відома противника, відтак пристрої ідентифікації можуть бути ним імітовані; низька ефективність деяких методів як вдень, так і вночі, та за умов поганої видимості.

Крім вказаних вище, у процесі ідентифікації застосовуються також такі процедури та рекомендації: запити та відповіді повинні періодично змінюватися та повідомлятись лише за принципом необхідності; запити та відповіді не повинні використовуватися поза переднім краєм району бойових дій; у випадку фактичного або потенційного порушення безпеки слід використовувати альтернативні запити та відповіді, а також ідентифікаційні конфігурації; використання пасивних або активних пристроїв ідентифікації, що працюють в інфрачервоному спектрі, повинно розглядатися з урахуванням можливостей противника; для безпечності використання ідентифікаційні пристрої повинні залишатись прихованими від противника якомога довше; сили розвідки повинні відстежувати можливість застосування противником пристроїв бойової ідентифікації.

Ефективне розпізнавання взаємодіючих сил, що діють на полі бою, повинно ґрунтуватися на точному знанні військової форми, озброєння та бойових машин, що використовуються цими силами. Така обізнаність досягається методом постійних тренувань на всіх рівнях в усіх країнах

НАТО. Всі командири несуть відповідальність за належну підготовку особового складу до розпізнавання союзних сил та сил противника на полі бою.

Встановлення форми запитів і відповідей, а також комплектація засобів та пристроїв ідентифікації, які будуть використовуватися як для операцій, так і для навчання, входить до обов'язків командирів підрозділів. Командири несуть відповідальність за виконання директив вищого командування під час ведення спільних операцій. Рішення про конфігурацію ідентифікаційних засобів, вербальні та невербальні запити приймаються на найвищому рівні командування операцією і заздалегідь доводяться до відома підпорядкованим підрозділам. Сусіди і вище керівництво також повинні бути проінформовані про встановлені запити та протокольні відповіді.

УДК. 372.862

Казіміров О.О., доцент кафедри Національної академії Національній гвардії України, кандидат військових наук, доцент

Онипченко П.М., провідний науковий співробітник Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат педагогічних наук, доцент

СУЧАСНІ ПОГЛЯДИ НА МЕТОДИКУ ОПАНУВАННЯ КУРСАНТАМИ ПРАКТИЧНИК НАВИЧОК ІЗ ВІЙСЬКОВО-СПЕЦІАЛЬНИХ ДИСЦИПЛІН

З блоку військово-спеціальних дисциплін однією з дисциплін, які викликають у курсантів труднощі під час навчання являється дисципліна "Робота на кінцевих засобах зв'язку" (РКЗЗ). Головним практичним результатів вивчення цієї дисципліни являється опанування курсантами прийому на слух знаків азбуки Морзе для ведення інформаційного обміну в слуховому радіотелеграфному режимі.

Але, як показує досвід викладання цієї військово-спеціальної дисципліни, опанування прийому знаків азбуки Морзе завжди викликало труднощі у переважної більшості курсантів. Однією з головних причин являється відсутність належного професійного відбору під час набору групи зв'язківців.

Тим не менш, аналіз показує, що за 15 років викладання дисципліни РКЗЗ 80% курсантів достатньо легко вдалося опанувати прийом. У решти 20% були істотні труднощі і насамперед через низьку мотивацію до вивчення азбуки Морзе. Спробував швидко навчитись - не вдалося, а у інших швидко виходить. Впав в розпач, опустив руки та перестав займатися. На виправдання курсанти говорили: " - Мені ведмідь на вухо наступив, я не чую", "- Я хотів навчатись на іншій спеціальності", "-Азбука зараз ніде не використовується ".

Щоб спонукати курсантів навчатись приходилось:

наводити особистий досвід в опануванні прийому азбуки Морзе;

розповідати про випадки, в яких знання азбуки Морзе допомагало не тільки виконати бойове завдання але й врятувати життя військовослужбовців (за досвідом збройної агресії росії проти України);

інформувати слухачів про застосування азбука Морзе у збройних силах держав-членів НАТО.

Окрім цього постійно приходиться звертати увагу на те, що вивчення азбуки Морзе - це тренування мозку людини на швидкість опрацювання інформації.

Щоб підвищити мотивацію курсантів у вивченні азбуки Морзе довелося впровадити у навчання ігрові методи навчання. На першому етапі проводиться прийом контрольного тексту та визначаються ті, хто прийняв контрольний текст взагалі без помилок. Надалі ці курсанти в парах змагаються між собою біля дошки (до першої помилки) та визначається кращий з них. На другому етапі відбувається змагання з викладачем біля дошки. Курсантам цікаво - вони бачать вживу, а що сам вміє викладач.

Курсантам такі методи навчання цікаві і вони чекають наступних занять (звісно чекають ті, у кого добре виходить з прийомом). Вони бачать свої результати у порівнянні з іншими та хочуть бути кращими, деяким соромно що вони в групі останні у навчанні.

Втілення в навчальний процес подібних ігрових методів викличе зацікавленість курсантів, допоможе їм у навчанні, підвищить якість та успішність навчання.

Де ще можуть використовуватись такі ігрові методи навчання? Наприклад, під час проведення практичних занять на техніці. Хто швидше запрограмує чи налаштує радіостанцію, хто першим увійде у зв'язок, хто скоріше виконає норматив та т.і.

УДК 372.862

Лазарев В.Д., старший викладач кафедри Національної академії Національної гвардії України
Ткаченко К.Н. доктор філософії, заступник начальника кафедри Національної Академії національної гвардії України.

ПІДВИЩЕННЯ ГНУЧКОСТІ ТА ОПЕРАТИВНОСТІ УПРАВЛІННЯ ЧАСТИНАМИ НГУ ЗА ДОПОМОГОЮ ІНТЕРКОМУНІКАЦІЙНОЇ СИСТЕМИ ІНТЕРКОМ RF-7800I ВИРОБНИЦТВА КОМПАНІЇ HARRIS

На озброєння НГУ надходить система інтерком Harris RF-7800I. Це сучасна, гнучка, багатофункціональна цифрова система внутрішнього зв'язку для бронетехніки та інших транспортних засобів, в яку інтегруються автомобільні радіостанції Harris та засоби зв'язку інших виробників

При якісному налаштуванні відповідно до потреб бойового управління, Harris RF-7800I дозволяє значно покращити координацію екіпажу бойової машини та підвищити її бойові можливості. Крім бойових машин, системи інтерком можуть встановлюватись на командно-штабних машинах та командних пунктах.

Система інтерком Harris RF-7800I має гнучку модульну структуру. Ядро системи - центральний блок, який містить промисловий комп'ютер. До нього за допомогою системи кабелів під'єднуються блоки екіпажу з різним набором функцій: від клавішно-дисплейного блоку управління до простих трикнопкових абонентських блоків. До блоків членів екіпажу підключаються гарнітури з активним шумоподавленням та комп'ютери, оснащені послідовним портом. Також до центрального блоку під'єднуються радіостанції бойової машини та гучномовець.

Органи управління системою - функції клавіш, дії поворотного перемикача, значення піктограм на дисплеї тощо - налаштовуються згідно з набором підключеного обладнання та завдань екіпажу бойової машини, щоб максимально спростити бойове управління.

Система інтерком для транспортних засобів Harris RF-7800I складається з центрального блоку, блоків екіпажу, допоміжних блоків, з'єднувальних кабелів та системи електроживлення. Функції системи визначаються конкретним набором блоків, встановлених на об'єкті, і підключеними до них радіостанціями та зовнішніми лініями, а також конфігураційним файлом.

В командно-штабних машинах та на стаціонарних командних пунктах, як правило, монтуються системи на основі центрального блоку RF-7800I-CU100. В них, зокрема, входять два блоки управління RF-7800I-KD400 та блок телефонії, до якого може бути підключена стаціонарна зовнішня телефонна лінія. Також центральний блок інтеркому може бути підключений до зовнішнього IP-каналу через роз'єм Ethernet. Блок виклику встановлюється на робочому місці військового начальника, в інтересах якого працює КШМ або пункт управління. Блок дистанційного підключення через польовий кабель може в цьому випадку використовуватись для організації радіовиносу.

В пунктах управління можуть використовуватись конфігурації інтеркому з декількома центральними блоками, з'єднаними у локальну мережу; в таких конфігураціях може взаємодіяти велика кількість блоків екіпажу. Аналогічну конфігурацію можна створити, об'єднуючі центральні блоки командно-штабних машин, які входять в склад мобільного пункту управління.

Система інтерком Наггіs RF-7800I тільки починає застосовуватись в підрозділах НГУ. Її функціональність найбільше розкривається при застосуванні в командно-штабних машинах, які експлуатує більш підготований персонал, і на яких встановлено дві або більше радіостанцій. Розгорнуто систему інтерком на деяких стаціонарних пунктах управління вищої ланки.

УДК 004.8: 004.056

Наконечний В.С., професор кафедри Київського національного університету ім. Тараса Шевченка, доктор технічних наук, професор
Побережний А.А., науковий співробітник науково-дослідної лабораторії Національної академії Національної гвардії України

ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМИ БЕЗПЕКИ

У сучасному світі підвищення стійкості інформаційних систем до кіберзагроз є актуальною задачею, що має першочергове значення для організацій, які взаємодіють між собою та використовують інформаційні ресурси. Зараз можна спостерігати зростання атак на дані, ресурси та критичну інфраструктуру. В умовах постійної еволюції мережевих загроз, виявлення та протидія кіберзагрозам є перспективним напрямком. Однією з найважливіших областей застосування штучного інтелекту (ШІ) є кібербезпека. Тут його роль набуває критичного значення: алгоритми машинного навчання аналізують величезні обсяги даних, сприяючи виявленню аномалій у мережевому трафіку та ідентифікації потенційно небезпечних вразливостей. Засоби на основі ШІ стають ефективним інструментом, який дозволяє автоматизувати процеси виявлення та реагування на загрози кібербезпеки.

Умови найефективнішого впровадження ШІ в систему безпеки:

1. Використовувати високоякісні дані.

Ефективність ШІ в кібербезпеці значною мірою залежить від якості даних, які використовуються для навчання алгоритмів машинного навчання. Щоб забезпечити максимальну точність і ефективність інструментів безпеки на основі ШІ, слід використовувати лише якісні джерела даних і забезпечити надійну стратегію керування даними.

Це включає збір даних із різноманітних джерел, регулярне оновлення та підтримку наборів даних.

2. Людський контроль.

Хоча ШІ пропонує значні переваги у сфері протидії кібератакам, важливо пам’ятати, що це не ідеальне рішення. Людський контроль залишається вирішальним для забезпечення ефективного та відповідального використання інструментів на основі ШІ.

Фахівці з безпеки повинні продовжувати відігравати активну роль у моніторингу та управлінні інструментами безпеки на основі ШІ, забезпечуючи їх належну роботу та приймаючи обґрунтовані рішення щодо того, як реагувати на потенційні загрози.

Незважаючи на те, що ШІ в значній мірі покращує ефективність безпеки, існує декілька проблем, які можуть виникнути при його використанні. Ризики використання ШІ в кібербезпеці:

1. Упередженість і дискримінація в процесі прийняття рішень.

Упереджене прийняття рішень в системах ШІ може виникати з різних причин, таких як неякісні набори даних, використання алгоритмів, яким бракує необхідної об’єктивності.

Якщо належним чином не контролювати роботу ШІ, то його упередження можуть призвести до дискримінаційних рішень щодо певних груп або окремих осіб і мати значні наслідки для організації.

Наприклад, рішення, прийняте системою ШІ на основі упереджених вхідних даних, може призвести до помилкових спрацьовувань і заблокувати законним користувачам доступ до систем компанії, що призведе до втрати продуктивності або клієнтів.

2. Відсутність зрозумілості та прозорості.

Алгоритми, які використовуються для прийняття рішень щодо загроз безпеці, не завжди прозорі. Іноді буває дуже важко інтерпретувати дії ШІ, через це не зрозуміло, чому були прийняті саме ці рішення.

Таке непорозуміння може призвести до неправильних рішень, які можуть мати серйозні наслідки для безпеки організації.

Обробляючи та аналізуючи величезні обсяги даних, ШІ дозволяє досить швидко реагувати на нові загрози, мінімізуючи вплив потенційних порушень та значно підвищуючи захист організацій у цифровому середовищі. Використання ШІ в кібербезпеці не тільки підвищує загальну стійкість, але й дає можливість організаціям швидко адаптуватися в постійно мінливому ландшафті безпеки. Але потрібно пам'ятати, що неконтрольоване та неправильне використання ШІ також може призводити до небажаних наслідків.

УДК 623.618:623.644

Горєлишев С.А., провідний науковий співробітник науково-дослідного центру Національної академії Національної гвардії України, кандидат технічних наук, доцент
Баулін Д.С., провідний науковий співробітник науково-дослідного центру Національної академії Національної гвардії України, кандидат технічних наук, старший науковий співробітник
Іванченко А.О., доцент кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент
Іванець Г.В., старший науковий співробітник науково-дослідної лабораторії Харківського Національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент

КОМПЛЕКСНЕ ВИКОРІСТАННЯ ПРОГРАМНИХ ЗАСОБІВ "КРОПИВА", "ДЕЛЬТА", "ВІРАЖ" ПРИ ВИКОНАННІ БОЙОВИХ ЗАВДАНЬ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Характер сучасної війни майже не дозволяє в чистому вигляді використовувати класичні підходи до організації взаємодії в рамках виконання бойових завдань підрозділами НГУ. Разом з тим, при виконанні бойових завдань часто не приділяється потрібної уваги таким факторам сучасного збройного конфлікту як мобільне та інтернет покриття, наявність різноманітних, часто не підпорядкованих командуванню груп розвідки, доступність планшетних комп'ютерів зі спеціалізованим програмним забезпеченням типу "Кропива", "Дельта" та "Віраж-планшет" та інших технології. Саме тому необхідно узагальнити підхід з організації управління та обміну інформацією в рамках виконання бойових завдань без прив'язки до існуючих формальних посадових інструкцій, а з точки зору практичних порад в рамках фактичних ролей та обов'язків.

Вже зараз перед силовими структурами поставлено завдання впровадження сучасних автоматизованих систем управління (АСУ) підрозділами, які згодом будуть зв'язані в загальновійськову Єдину автоматизовану систему управління Збройних Сил. На жаль у нашій країни на озброєнні таких систем не існує. Але бачимо що розвиток форм і способів ведення бойових дій в Україні супроводжується відповідним розвитком АСУ військами і зброєю та появою низки програмних додатків, які є її елементами.

Для підрозділів НГУ при виконанні бойових задач пропонується використовувати функціональні можливості ПК "Кропива" при вирішенні задач орієнтування на місцевості, виконання топогеодезичних розрахунків, нанесення тактичної обстановки та обмін цією інформацією між користувачам, об'єднання оперативної інформації від засобів розвідки, управління та вогневого ураження в єдине інформаційне поле, а також управління боєм.

Інформаційно-комунікаційні системи "Інтеграційна платформа "Дельта"" дає змогу забезпечення підрозділів НГУ найбільшою базою розвідувальних відомостей та актуальними перевіреними даними про ворога, а також координацію дій сил оборони. На жаль на даному етапі розвитку інформаційного забезпечення повноцінна синхронізація ПК "Кропива" та ІП

“Дельта” не можлива, але експорт-імпорт даних з однієї системи в іншу необхідно робити у ручному режимі. Зробити це можливо за допомогою встановленню в ПК “Кропива” режиму роботи з новими сценами “Сцена v2.0” і “Тенета Групи”. В 2.0 версії сцени всі об’єкти прив’язані до сцен: елементи БП, треки, маяки, корегування, тактика, метео і проч. В 2.0 сцени можуть бути двох типів: локальні (внутрішні або приватні) – сцена до якої має доступ тільки користувач цього пристрою та групові (зі спільним доступом) – сцена яка автоматично створюється відповідно до групи в “Тенета Групи”. В груповій сцені всі зміни автоматично синхронізуються з усіма учасниками групи.

Система “Віраж-планшет” забезпечує автоматизацію найбільш складних і трудомістких задач збору, обробки, відображення, аналізу даних спостереження та видачі інформації оповіщення про повітряну (надводну) обстановку, а також підтримки прийняття рішення командирів шляхом проведення оперативно-тактичних розрахунків.

Можливі варіанти організації інформаційної мережі між даними програмними засобами через закритий або відкритий канал Інтернету, через канал мобільного зв’язку GSM/CDMA шляхом обміну SMS-повідомленнями, за допомогою мережі, утвореної з радіостанцій.

УДК 623.55.02

Малюк В.Г., доцент кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент
Лазарев В.Д., старший викладач кафедри Національної академії Національної гвардії України

ПРОГРАМНИЙ ЗАСІБ ГЕНЕРАЦІЇ ГРУП КЛЮЧІВ ШИФРУВАННЯ ДЛЯ ЗАСОБІВ МОБІЛЬНОГО РАДІОЗВ’ЯЗКУ

Сучасні засоби радіорозвідки забезпечують з високою ефективністю сканування, перехоплення сигналів, їх пеленгування та аналіз, на основі чого виконується оцінка дій та намірів супротивника. Це робить надзвичайно актуальною проблемою зниження ефективності радіорозвідки шляхом застосування ключів шифрування та автентифікації для засобів мобільного радіозв’язку, які використовуються у формуваннях Національної гвардії України.

Програмне забезпечення широко використовуваних радіостанцій Motorola та Harris дозволяє активувати/деактивувати функції базового або покращеного шифрування, додати/видалити ключі шифрування, встановити ID ключа, назву (псевдонім) ключа та ввести відповідне значення ключа. Ключ шифрування для цих радіостанцій представляє собою послідовність довжиною у 10, 32 або 64 літер у шістнадцятирічній системі. Засоби для створення таких ключів шифрування наразі слабо представлені на ринку програмних продуктів. Існуючі онлайн-сервіси дозволяють створювати окремі екземпляри ключів і не надають можливості перевірки одержаних ключів на унікальність. Для прискорення та покращення якості процесу створення таких ключів існує потреба у розробці автоматизованого процесу генерації унікальних ключів шифрування у будь-якій кількості.

У середовищі програмування Delphi для ОС Windows розроблено комп’ютерну програму для генерації груп унікальних ключів шифрування. Алгоритм генерації ключів містить такі основні блоки: визначення кількості ключів у групі; генерація ключа шифрування визначеної довжини як випадкової послідовності літер із визначеної базової множини; перевірка поточного варіанту ключа на унікальність у складі групи, що створюється; виведення значень одержаної групи ключів шифрування на екран; збереження результатів роботи у файлі; перевірка збережених груп ключів на унікальність.

Використання даної програми дозволяє як спростити процес генерації ключів шифрування так і покращити його якість, гарантуючи унікальність одержаних ключів у складі групи.

УДК 623

Іванець Г.В., старший науковий співробітник науково-дослідної лабораторії Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент
Горєлишев С.А., провідний науковий співробітник науково-дослідного центру Національної академії Національної гвардії України, кандидат технічних наук, доцент
Іванець М.Г., провідний науковий співробітник – провідний інженер-випробувач науково-дослідного відділу Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки, кандидат технічних наук, старший дослідник
Воїнов В.В., заступник начальника факультету з навчальної та наукової роботи Харківського національного університету Повітряних Сил імені Івана Кожедуба**,** кандидат технічних наук, доцент

ПОРІВНЯЛЬНИЙ АНАЛІЗ СПОСОБІВ ПОШАРОВОЇ АПРОКСИМАЦІЇ СФЕРИЧНИХ ЛІНЗ ЛЮНЕБЕРГА

Останнім часом у супутниковому зв’язку та комунікаційних системах для підсилення сигналу та зменшення перешкод використовуються лінзові антені, зокрема на базі лінз Люнеберга. Завдяки фокусування електромагнітної хвилі в певних точках на своїй поверхні або всередині лінза Люнеберга є важливим елементом у високотехнологічних системах зв’язку, радіолокації та навігації. Виготовлення лінз Люнеберга із плавною зміною діелектричної проникливості вздовж її радіусу досить складна задача. На практиці переходять до ступінчатої апроксимації закону зміни діелектричної проникливості за допомогою багатошарової конструкції. В межах одного шару такої конструкції діелектрична проникливість постійна. Чим тонший шар і більше їх кількість, тим точніша апроксимація і ближчі характеристики реальної лінзи до характеристик ідеальної із плавною зміною діелектричної проникності. Як показує практика, найбільшою технологічністю володіють 6-8 шарові лінзи. Розрізняють наступні способи розбиття лінзи на шари: рівномірне розбиття за показником заломлення; рівномірне розбиття лінзи за діелектричною проникністю; рівномірне розбиття лінзи по радіусу.

Суть рівномірного розбиття лінзи на шари за показником заломлення. Залежність показника заломлення від радіуса ділиться на рівні частини за показником заломлення. Знаходяться відповідні радіуси шарів відповідно до кількості шарів. Кожний шар розбивається по радіусу на дві рівні частини та передбачається що вони мають постійне значення показника заломлення відповідних меж шару. Показник заломлення усього шару розраховується як середнє значення меж в кожному шарі лінзи. В результаті одержимо рівномірне розбиття лінзи за показником заломлення.

Суть рівномірного розбиття лінзи на шари за діелектричною проникністю. Залежність діелектричної проникності від радіуса ділиться на рівні частини по значенню діелектричної проникності. Знаходяться відповідні радіуси шарів. Кожний шар розбивається на дві рівні частини та передбачається що вони мають постійне значення діелектричної проникності відповідних меж шару. Діелектрична проникність усього шару розраховується як середнє значення меж в кожному шарі лінзи. В результаті одержимо рівномірне розбиття лінзи за діелектричною проникністю.

Суть рівномірного розбиття лінзи на шари по радіусу. Сферична лінза розбивається на шари однакової товщини. Діелектрична проникність усього шару розраховується як середнє значення меж в кожному шарі лінзи. В результаті одержимо рівномірне розбиття по радіусу.

Чим ближче закон розподілу діелектричної проникності наближається до неперервного, тим менше характеристики багатошарової лінзи відрізняються від ідеальної. В якості критерію ефективності наближення ступінчатої апроксимації закону зміни діелектричної проникності до теоретичного вибрано середню абсолютну похибку наближення. Проведені дослідження показали, що при створенні багатошарової сферичної лінзи максимальне приближення реальних характеристик до ідеального закону забезпечує рівномірне її розбиття на шари по радіусу. Так, наприклад, для шестишарової сферичної лінзи абсолютна похибка наближення діелектричної проникності до теоретичного значення при розбитті лінзи за показником заломлення складає 6,8%, за діелектричною проникністю – 7,1%, а за радіусом – 6,6%.

УДК 654.1

Рижов Є.В., начальник науково-дослідного відділу Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, старший дослідник
Давіденко С.В., провідний науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент
Заєць Я.Г., старший науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, старший дослідник

ДОСВІД ЗАСТОСУВАННЯ LTE (4G) СИСТЕМИ ЗВ'ЯЗКУ В ІНТЕРЕСАХ СИЛ ОБОРОНИ УКРАЇНИ

З метою підвищення стійкості системи управління з'єднань, частин та підрозділів Сил оборони України, робочою групою офіцерів зв'язку було проведено дослідження щодо функціонування власної LTE системи зв'язку, яка була розгорнута на обладнанні одного з національних операторів, що було ним передано одній з військових частин Сил оборони України.

За результатами дослідження були визначені ключові аспекти та фактори, які впливають на роботу системи LTE зв'язку в умовах ведення бойових дій (операцій) в межах усієї смуги відповідальності. Основними особливостями побудови та функціонування розгорнутої LTE системи зв'язку на базі військової частини є наступні.

На початковому етапі були обладнані нові та/або відновлено функціонування існуючих базових станцій мобільного зв'язку.

Завдяки програмним засобам управління і моніторингу станцій мобільного зв'язку вдалося організувати використання відбудованого сегменту мобільної мережі в інтересах підрозділів військової частини, що знаходяться в межах покриття сегменту, в районах проведення бойових дій.

Надані оператором SIM карти запрограмовані таким чином, що надають найвищий пріоритет доступу до частотного ресурсу та пропускної здатності згаданого сегменту мережі, завдяки чому у відповідальних за адміністрування фахівців з'являється можливість забезпечувати роботу сегменту, як в інтересах сил оборони, так і цивільного населення.

Базова станція сегменту комплектується декількома радіомодулями, які дозволяють забезпечити одночасну роботу в частотних діапазонах від 700 МГц до 2100 МГц, і, таким чином, здійснювати резервування частотного ресурсу на випадок впливу засобів радіоелектронної боротьби (РЕБ) з боку противника.

Стійкість роботи системи забезпечується шляхом резервування. Для цього було створено декілька кілець ліній базових станцій покриття, які перекриваються та розраховані таким чином, що навіть одночасна втрата декількох базових станцій не призводить до виходу з ладу LTE систему зв'язку та втрати зв'язку з підрозділами.

За результатами дослідження, проведеного засобами моніторингу кінцевих пристроїв, підтверджено, що система дозволяє виконувати маневр частотами в широкій смузі частот, що ускладнює радіоелектронне подавлення з боку засобів РЕБ противника.

Основною перевагою LTE системи зв'язку є доступність і низька вартість кінцевих пристроїв абонентів. Розгорнутий сегмент забезпечує стабільне покриття LTE системи зв'язку в межах усієї смуги відповідальності, що дозволяє організувати зв'язок між підрозділами Сил оборони України та створює транспортне середовище передачі даних.

Досвід використання LTE технологій для забезпечення зв'язку у військовій частині оцінюється позитивно. Доцільно здійснювати заходи щодо впровадження (масштабування) зазначеного досвіду при організації системи зв'язку з'єднань, частин та підрозділів Сил оборони України.

УДК 654.1

Рижов Є.В., начальник науково-дослідного відділу Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, старший дослідник
Давіденко С.В., провідний науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент
Заєць Я.Г., старший науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, старший дослідник

ВДОСКОНАЛЕННЯ РАДІОЕЛЕКТРОННИХ СИСТЕМ КОМУНІКАЦІЇ ТА РОЗВИТОК АЛЬТЕРНАТИВНИХ ТЕХНОЛОГІЙ ЗВ'ЯЗКУ

В умовах повномасштабної війни противник ефективно перехоплює та давить засобами радіоелектронної боротьби канали зв'язку Сил Оборони, що створює критичні виклики для виконання бойових завдань та координації підрозділів СОУ. В цих умовах, забезпечення завадозахищеного і безпечного зв'язку стає одним з пріоритетних напрямків вдосконалення системи управління військами та зброєю.

Сучасні засоби РЕБ здатні створювати радіоперешкоди та перехоплювати повідомлення на відстані більш як 30 км від лінії бойового зіткнення (ЛБЗ), що дозволяє ефективно блокувати інфокомунікаційну складову системи управління наших ЗС і ускладнює виявлення та ураження ворожих пунктів придушення та розвідки.

Зважаючи на це необхідно розвивати технології супутникового зв'язку, когнітивного радіо, оптоволоконного передавання даних, лазерних комунікацій, 5G та 6G технологій передавання даних, безпілотних ретрансляційних систем.

В тактичній ланці управління своєчасність, достовірність та безпеку інфокомунікацій можливо підняти за рахунок впровадження радіозасобів на сучасних принципах.

MESH та MANET радіомережі забезпечують динамічну маршрутизацію та самоорганізацію вузлів, що підвищує стійкість зв'язку. Завдяки можливості автоматичного підключення вузлів мережа залишається працездатною навіть при втраті окремих елементів. Це робить їх ефективними в умовах відсутності стаціонарних базових станцій і при активному впливі РЕБ, оскільки мережі автоматично обирають оптимальні маршрути передачі даних.

Основними вимогами до засобів радіозв'язку є захист від перешкод, швидка адаптація до умов і шифрування даних. Використання протоколів з псевдовипадковим переналаштуванням робочих частот (ППРЧ) дозволяє уникнути придушення сигналу.

Сучасний цифровий радіозв'язок неможливо уявити без застосування стійких алгоритмів шифрування таких як AES, який забезпечує захист інформації, що передається від розвідки противника.

Хімера Юкрейн постачає до ЗС України сучасні тактичні радіостанції HIMERA G1 Pro L, які мають низьку вихідну потужність, ППРЧ, шифрування AES-256 та застосовують технологію MANET. Радіостанції тестували в умовам пересіченої місцевості, де вони показали стабільні результати в режимі «точка-точка» на дистанції до 6 км та до 13 км з використанням функції ретрансляції, в тому числі із додатком ситуаційної обізнаності ComBat Vision 4 для обміну тактичними даними по радіо каналу між двома групами.

Таким чином застосування сучасних технологій радіокомунікацій дозволяє суттєво покращити ситуацію з обміном усіма видами інформації на полі бою.

УДК 623.612
Флорін О.П., доцент кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент.

ВИЗНАЧЕННЯ ШЛЯХІВ ЗАХИСТУ МЕРЕЖ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Проблема захисту систем військового радіозв'язку є комплексною, оскільки залежить від здатності засобів радіозв'язку протистояти засобам радіоелектронної розвідки противника, а також від здатності засобів радіозв'язку виконувати своє функціональне завдання з заданою якістю в умовах впливу навмисних завад.

Перша задача забезпечує розвідзахищеність засобів радіозв'язку, які приймають участь у радіообміні. При проведенні заходів щодо забезпечення скритності виключається або ускладнюється визначення противником призначення, типу, приналежності, місця розташування, тактико-технічних характеристик і параметрів сигналів засобів радіозв'язку, призначення та місце розташування обслуговуваних ними об'єктів. Скритність засобів радіозв'язку досягається виконанням заходів щодо маскування, і в першу чергу з радіоелектронного маскування.

Останнім часом широке застосування знайшли пристрої Hi-Tech: засоби радіозв'язку, обробки інформації, навігації, Wi-Fi камери, тепловізори, безпілотні літальні апарати невеликих розмірів тощо. Ці пристрої є засобами подвійного призначення і породжують масу проблем збройним силам і силам охорони правопорядку, до яких відноситься Національна гвардія України.

Аналіз наслідків радіоелектронного протиборства під час відсічі збройної агресії російської федерації показав можливості використання радіоелектронних засобів Hi-Tech в умовах інформаційного протиборства, коли ведуться радіоелектронна розвідка та радіопротидія, застосовуються радіомаскування та захист від спеціальних завад. Це дозволяє визначити доцільність створення просторово-розподілених систем розвідки і постановки завад, їх структуру, види і характеристики завад, що випромінюються малогабаритними модулями.

Друга задача забезпечує надійність функціонування засобів радіозв'язку. На озброєнні розвинених у воєнному відношенні країн світу стоять сучасні мобільні засоби та системи радіорозвідки, які спроможні з високою ефективністю виконувати сканування, перехоплення, аналіз, класифікацію та моніторинг радіопередач противника. Це робить надзвичайно актуальною проблемою зниження ефективності цих засобів і систем шляхом зниження енергетичних показників систем радіозв'язку засобів Hi-Tech в умовах інформаційного протиборства.

Радіоелектронне придушення, що є складовою частиною радіоелектронної боротьби, являє собою комплекс заходів і дій, що проводяться військами (силами) в бою і операції з дезорганізації або зниження ефективності дії радіоелектронних засобів противника шляхом впливу на них електромагнітним випромінюванням. Одним із завдань радіоелектронного придушення є постановка навмисних завад, що дозволяє одночасно виконати завдання з блокування доступу до радіообміну та порушення цілісності повідомлень.

Застосування стандартних засобів захисту від навмисних завад для потреб військ (сил), як показує аналіз дій у зоні відсічі збройної агресії російської федерації, більшою частиною неможливо через особливості ведення бойових дій та застосуванням противником сучасних засобів радіопридушення. Забезпечення роботи радіомереж в умовах радіопридушення потребує вдосконалення наукових методів і технічних рішень щодо підвищення завадостійкості. На практиці часто використовують комбіновані методи захисту.

Відмітимо, що одним з можливих шляхів вирішення завдання забезпечення завадозахищеного радіозв'язку для існуючих засобів радіообміну є виростанням принципів отримання енергетичної переваги за рахунок розробки спеціально створених антен з заданими діаграмами спрямованості, що здатні адаптуватись до умов електромагнітної обстановки в зоні застосування мобільної компоненти тактичної ланки управління Національної гвардії України.

УДК 621.391

Чечуй О.В., доцент кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент
Трофімова Ю.О., магістр очної форми навчання Харківського національного університету Повітряних Сил імені Івана Кожедуба

УДОСКОНАЛЕНА МОДЕЛЬ СИСТЕМИ ОПЕРАТИВНОГО УПРАВЛІННЯ МЕРЕЖЕЮ ПОВІТРЯНИХ РЕТРАНСЛЯТОРІВ З ВИЗНАЧЕННЯМ ТОПОЛОГІЇ РАДІОМЕРЕЖІ ЗА КРИТЕРІЄМ ІНФОРМАЦІЙНОЇ ЗВ'ЯЗНОСТІ

Досвід ведення бойових дій ЗС України за час повномасштабного вторгнення та відбиття збройної агресії рф вказує на широке застосування повітряних платформ (ПП) для забезпечення успішного виконання бойових завдань підрозділами ЗС України. ПП можуть застосовуватись для забезпечення управління підрозділами ЗС України при веденні бойових дій шляхом побудови радіомереж із застосуванням ретрансляторів на базі безпілотних літальних апаратів (БпЛА) або аероплатформ, що дозволяє підвищити стійкість зв'язку в процесі обміну інформацією між абонентами мережі. Застосування сучасних цифрових радіостанцій надає можливість побудови безпроводових самоорганізуючих мереж зв'язку Flying Ad-hoc networks (FANET) з використанням ПП, що дозволяє, у свою чергу, підвищити ефективність їх використання. Крім того, сучасні системи FANET обумовлюють застосування рою відповідної кількості літальних апаратів, які мають взаємодіяти у залежності від виду бойових завдань та забезпечувати зв'язність мережі з урахуванням застосування противником засобів радіоелектронної боротьби (РЕБ).

Запропоновано удосконалена функціональна модель системи оперативного управління мережею повітряних ретрансляторів, яка враховує кількість БпЛА та аероплатформ, висоти їх польоту (зону покриття, дальність радіозв'язку), а також район ведення бойових дій та дозволяє визначити оптимальну топологію мережі радіозв'язку за критерієм інформаційної зв'язності. Модель оперативного управління топологією мережі представлена у вигляді ненаправленого зваженого графу, де у якості ваги використовується значення відстані та пропускної спроможності між вузлами мережі, які змінюються у залежності від інтегральної оцінки показників якості радіозв'язку під впливом засобів РЕБ противника. Особливістю запропонованої моделі слід визначити, додаткове врахування характеристик ПП, часу їх перебування в польоті, висот та швидкостей переміщення.

Запропонована модель системи оперативного управління мережею повітряних ретрансляторів дозволяє вирішувати задачі із забезпечення управління підрозділами ЗС України та підвищити показники стійкості системи зв'язку ЗС України.

.

УДК 621.396

Майборода І.М., доцент кафедри Національної академії Національній гвардії України, кандидат військових наук, доцент

ЗАСТОСУВАННЯ КВАДРИФІЛЯРНИХ АНТЕН ДЛЯ ЗАХИСТУ ЗАСОБІВ ТА СИСТЕМ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Ведення бойових дій в сучасних умовах неможливо представити без всебічного та практично безперервного застосування засобів та систем радіоелектронної боротьби (РЕБ), головними завданнями яких є виявлення засобів спостереження противника, їх дезорієнтування і захист своїх радіоелектронних систем від ворожого впливу. Як показав досвід застосування засобів РЕБ в тактичній ланці управління під час постійних штурмових дій зі сторони російських агресорів, пріоритетним визначається захист особового складу, об'єктів та

обладнання від впливу ворожих безпілотних літальних апаратів і так званих «окопних» засобів РЕБ противника.

Одним із надійних рішень, якому довіряють військові експерти, що забезпечує найвищий рівень захисту своїх систем РЕБ, є застосування квадрифілярних антен. Ці антени з унікальною конструкцією забезпечують купольний захист, що не дозволяє ворожим безпілотникам обійти нашу оборону зверху, значно підвищуючи ефективність протидії. Завдяки круговій поляризації, вони ефективно працюють як з горизонтально, так і з вертикально поляризованими сигналами, гарантуючи їх ефективну роботу у будь-яких умовах.

Хоча квадрифілярні антени можуть мати трохи меншу дистанцію придушення у порівнянні з колінеарними аналогами, вони надають незаперечну перевагу – створення справжнього “електромагнітного купола”, що забезпечує всебічний захист нашої техніки та обслуговуючого персоналу. Компактна конструкція дозволяє уникати перешкод, таких як гілки дерев, і витримує потужність до 100 Вт, що робить ці антени надзвичайно надійними навіть у складних умовах. Квадрифілярні антени працюють в широкому діапазоні частот від 700 до 1050 МГц, забезпечуючи значне підсилення в 2 дБі та високий коефіцієнт стоячої хвилі в межах 1,3-1,6, що дозволяє легко адаптувати їх до різних потреб засобів та систем РЕБ.

Таким чином, вибираючи квадрифілярні антени для наших систем РЕБ, можна отримати універсальне рішення, що поєднує міцність, надійність і ефективність застосування.

УДК 355.424
Глущенко М.О., старший викладач Національної академії Національної гвардії України.
Малюк В.Г., доцент кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент.

РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ЗАСОБІВ РАДІОЗВЯЗКУ ВІД ВОГНЕВОГО УРАЖЕННЯ ПРОТИВНИКА

Основними завданнями радіоелектронної радіорозвідки (РЕР) противника є виявлення штабів і командних пунктів, скупчення техніки та особового складу, перехоплення інформації під час радіообміну, фіксація, пеленгація та ідентифікація джерел сигналів, фіксація роботи розвідувальних груп, виявлення груп керуючих БПЛА, виявлення контрбатарейних радарів, портативних радіолокаційних станцій. За різними оцінками, засобами РЕР отримуються 80-90 % первинної інформації.

Практика роботи фронтових зв’язківців показує, що дальність пеленгації визначення місцезнаходження військовослужбовців із засобами зв’язку фронтовими пеленгаторами противника складає від 2 до 50 км.

Пеленгатори радіорозвідки противника ніколи не стоять на «нулі», як правило, їх розміщення вибирається не ближче ніж 10 км від лінії фронту. Залежно від типу пеленгатора та особливостей його встановлення точність визначення позицій радіозасобів складає від 200 м до 500 м, залежно від відстані до лінії фронту.

Для зменшення ймовірності виявлення джерел радіовипромінювання, вогневого ураження військовослужбовців та засобів зв’язку пропонується ряд заходів:

вивчити з особовим складом базові правила радіообміну;

для передавання критично важливої інформації віддавати перевагу дротовим засобам зв’язку;

використовувати режим роботи засобів радіозв’язку на мінімальній потужності та широкосмугові сигнали;

використовувати спрямовані антени у напрямку на кореспондента;

встановлювати металеві відбивачі (екрани) зі сторони антени в напрямку противника;

не встановлювати радіостанції, ретранслятори та антени поруч з пунктами управління та місцями розташування особового складу;

організовувати взаємодію із сусідніми підрозділами, підрозділами розвідки для обміну інформацією щодо застосування противником засобів вогневого ураження та РЕБ;

організовувати постійний радіомоніторинг бойової та електромагнітної обстановки на лінії зіткнення (у зоні відповідальності);

використовувати природні та штучні перешкоди поширенню радіохвиль (рельєф місцевості, будівлі тощо);

уникати скупчення на невеликій території великої кількості одночасно включених мобільних телефонів, радіостанцій або одночасно працюючих передавачів пультів від дронів;

не використовувати телефон як точку доступу WI-FI і не роздавати Інтернет іншим;

для коротких повідомлень, або тих, що часто повторюються, використовуйте "псевдо-морзянку" (поєднання коротких та/або довгих натискань тангенти) без передачі «голосу»;

для розпізнавання в ефірі "свій-чужий" необхідно використовувати таблицю сигналів управління для підрозділів тактичної ланки управління;

в умовах лісу рекомендується використовувати діапазон VHF, в умовах міста – UHF;

у разі виявлення впливу засобів РЕБ противника на систему зв'язку необхідно проаналізувати робочий спектр завад, їх характер та перейти на інші робочі частоти (наприклад, на частоти, які знаходяться поза межами або на краю спектра завади) та/або змінити поляризацію сигналу.

Дотримання правил користування засобами зв'язку і ведення радіообміну, максимальне скорочення часу виходу в ефір, використання коротких сигналів і команд, а також дублюючих каналів зв'язку, способів та прийомів маскування дасть можливість підвищити захист військослужбовців і засобів радіозв'язку від вогневого уражання противника.

УДК: 355.45

Смирнов О.Г., старший викладач кафедри Національної академії Національної гвардії України

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ РОЗРОБЦІ ТЕСТОВИХ ЗАВДАНЬ

Сучасний розвиток інформаційних технологій значно впливає на освітній процес, зокрема на методи оцінювання знань. Штучний інтелект (ШІ) відкриває нові можливості для автоматизації створення тестових завдань, адаптації їх до рівня знань студентів і підвищення об'єктивності оцінювання.

Метою цього дослідження є аналіз можливостей та перспектив використання ШІ у розробці тестових завдань, що дозволить підвищити якість тестування, зробити його більш персоналізованим та об'єктивним.

Однією з ключових можливостей ШІ є автоматична генерація тестових завдань на основі навчального матеріалу. Алгоритми обробки природної мови дозволяють аналізувати великі обсяги текстової інформації та формувати питання різних типів, таких як:

питання з вибором правильної відповіді;

відкриті питання;

питання на відповідність;

завдання на заповнення пропусків.

Автоматичне формування тестів дозволяє значно скоротити час, який витрачається на підготовку контрольних заходів, а також забезпечує стандартизованість питань.

Одним із головних переваг використання ШІ у тестуванні є адаптивність. Система може змінювати складність питань у режимі реального часу залежно від рівня знань студента. Це дає змогу:

індивідуалізувати процес оцінювання;

визначати слабкі місця у знаннях студента;

забезпечувати більш точну оцінку рівня підготовки.

Такі системи вже успішно застосовуються у міжнародних стандартизованих тестах, таких як GRE, GMAT, TOEFL.

ШІ може не лише перевіряти правильність відповідей, а й аналізувати відповіді на відкриті питання, використовуючи методи обробки природної мови. Це дозволяє оцінювати не лише фактологічні знання, але й логіку мислення студента, що є важливим аспектом якісного навчання.

Традиційні методи тестування можуть містити суб'єктивний фактор через людський вплив на оцінку відповідей. Використання ШІ мінімізує цей ризик, оскільки оцінювання здійснюється автоматизовано, за чітко визначеними критеріями. Це особливо важливо при перевірці тестів великої кількості студентів.

Незважаючи на значні переваги, використання ШІ у тестуванні має певні виклики, серед яких:

якість згенерованих тестових завдань – ШІ потребує високоякісних навчальних матеріалів, щоб створювати коректні та змістовні питання;

етичні аспекти – існує ризик надмірної автоматизації процесу навчання, що може зменшити роль викладача у формуванні критичного мислення студентів;

технічні обмеження – не всі навчальні заклади мають необхідні ресурси для впровадження таких систем.

Запропонований підхід до використання ШІ у розробці тестових завдань має наукову новизну завдяки:

автоматизованій генерації тестових питань на основі аналізу навчальних матеріалів із застосуванням алгоритмів обробки природної мови;

використанню адаптивного тестування, що дозволяє персоналізувати процес оцінювання відповідно до рівня знань студентів;

застосуванню методів машинного навчання для аналізу відповідей на відкриті питання, що сприяє об’єктивному оцінюванню не лише фактологічних знань, а й критичного мислення студентів;

інтеграції ШІ у навчальні платформи для автоматичного вдосконалення тестових матеріалів на основі результатів тестування.

Застосування ШІ у розробці тестових завдань є перспективним напрямом розвитку освіти, що сприяє підвищенню ефективності оцінювання знань, забезпеченню індивідуального підходу та зменшенню впливу людського фактору. Проте подальші дослідження повинні бути спрямовані на вдосконалення алгоритмів адаптивного тестування, інтеграцію ШІ у навчальні платформи та розв’язання етичних і технічних викликів.

ЗМІСТ

НАУКОВЕ ВИДАННЯ

ПЕРСПЕКТИВИ РОЗВИТКУ ТА ЗАСТОСУВАННЯ СУЧАСНИХ СИСТЕМ І ЗАСОБІВ ЗВ'ЯЗКУ В ІНТЕРЕСАХ УПРАВЛІННЯ ВІЙСЬКАМИ

Збірник тез науково-практичної конференції

(українською мовою)

Друкується в авторській редакції

Кафедра військового зв'язку та інформатизації командно-штабного факультету
Національної академії Національної гвардії України
61001, м. Харків, пл. Захисників України, 3