НАЦІОНАЛЬНА АКАДЕМІЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

КАФЕДРА ВІЙСЬКОВОГО ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ

НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО

КАФЕДРА ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЙИХ СИСТЕМ

Збірник тез науково-практичної конференції

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

27 лютого 2024 року

Харків-2024

Перспективи розвитку та застосування сучасних систем і засобів зв'язку в інтересах управління військами**:** Збірник тез науково-практичної конференції (Україна, м. Харків, 27 лютого 2024 року). – Х.: Національна академія Національної гвардії України, 2024. – 52с.

Організатори конференції:

Національна академія Національної гвардії України (м. Харків);

Національна академія Державної прикордонної служби України імені Богдана Хмельницького (м. Хмельницький).

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.

Заступник голови – І.С. Катеринчук, професор кафедри зв'язку та інформаційних систем Національної академії Державної прикордонної служби України імені Богдана Хмельницького, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, Заслужений працівник освіти.

Відповідальний секретар – О.О. Казіміров, доцент кафедри військового зв'язку та інформатизації командно-штабного факультету Національної академії Національної гвардії України, кандидат військових наук, доцент.

Члени організаційного комітету:

В.Т. Оленченко – начальник кафедри військового зв'язку та інформатизації Національної академії Національної гвардії України, кандидат технічних наук, доцент;

І.І. Чесановський – начальник кафедри зв'язку та інформаційних систем, кандидат технічних 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 355.415.1

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
Єманов В.В., перший заступник начальника Національної академії Національній гвардії України з навчальної та методичної роботи, доктор наук з державного управління, старший науковий співробітник

СЕРВІСИ ЗАБЕЗПЕЧЕННЯ КОМУНІКАЦІЙ ТАКТИЧНИХ СИСТЕМ ЗВ'ЯЗКУ ТА ІНФОРМАЦІЇ (CIS) ЗА ВИМОГАМИ КЕРІВНИХ ДОКУМЕНТІВ НАТО

Сучасні загрози звичайного та гібридного характеру, що постають перед країнами, які виділяють контингенти для участі в операціях НАТО, є одночасно симетричними та асиметричними. Такі загрози охоплюють різні виміри та фронти, вимагаючи підтримувати війська у стані готовності та забезпечувати швидку передислокацію передових підрозділів на великі відстані з метою стримування, гарантування безпеки, оборони або проведення наступальних дій для знищення загрози.

Забезпечення органів командування та управління належними системами зв'язку та інформації має допомогти командирам у виконанні поставлених завдань. Сучасні мережі, що розгортаються на підтримку проведення операцій, є доволі складними та вимагають від численної кількості функціональних сервісів та доменів різних країн-членів НАТО, підтримання взаємосумісності та спроможності забезпечувати командира розвідувальною інформацію для ухвалення належних рішень.

Згідно вимог керівних документах розглянуто перелік мінімально-необхідних сервісів CIS для забезпечення C4I підрозділів тактичної ланки, а також радіус дії згаданих сервісів з урахуванням бойового порядку (ORBAT) і структури командування та управління. Такий перелік має відображати практично досяжні вимоги для окремих країн та НАТО в цілому. До цього переліку входять сервіси за принципом «людина для людини» (H2H) (з урахуванням обмеженої здатності смуги пропускання), а також базові та функціональні сервіси.

Домен тактичної CIS (TACCIS) – це мережа (мережі), що розгортається на рівні від бригади (у разі розгортання) до найнижчого органу командування та управління наземними військами. Домен TACCIS забезпечує необхідні мережі для потреб сервісів H2H та C2. На даний момент, доступні сервіси для найменших підрозділів тактичної ланки не матимуть федеративності. Досягнення необхідного рівня взаємосумісності потребуватиме застосування принципів побудови взаємосумісності за силами та засобами. У разі потреби та за результатами аналізу вимог до обміну інформацією, від TACCIS може вимагатися забезпечення безперебійного споживання та поширення інформаційних продуктів з використанням федеративних сервісів.

Носії сервісів передачі даних на рівні батальйону/роти звикли споживати та передавати інформацію до вищого командування, оскільки суміжні та підпорядковані формування використовують бездротові вузькосмугові системи горизонтного або загоризонтного типу. Такі сервіси передачі даних відносяться до домену TACCIS. Тактичні радіостанції спроможні забезпечувати горизонтні / загоризонтні бездротові вузькосмугові сервіси. На даному рівні командування та управління переважають горизонтні тактичні радіостанції, що працюють в частотному діапазоні VHF та UHF. В свою чергу, використання загоризонтних систем передбачається за наявності складного рельєфу або недостатньої дальності роботи горизонтних систем. Розгорнуті підрозділи з батальйонним / ротним рівнем органу командування та управління мають залишатися гнучкими та мобільними. Саме тому, виникає потреба у забезпеченні сервісів H2H, а також сервісів для потреб командування та управління.

УДК. 372.862

Казіміров О.О., доцент кафедри Національної академії Національній гвардії України, кандидат військових наук, доцент
Ушаков В.А., старший викладач кафедри Національній гвардії України
Куртов А.І., завідувач кафедри Національного юридичного університету імені Ярослава Мудрого, кандидат технічних наук, доцент

ОГЛЯД СУЧАСНИХ ТА ПЕРСПЕКТИВНИХ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ ВІТЧИЗНЯНОГО ВИРОБНИЦТВА

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.

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.

В цих умовах, важливо теж мати на озброєнні сучасні та ефективні засоби РЕБ. В рамках військової допомого партнери України надають нам окремі зразки своїх засобів такого типу. Однак, актуальним являється удосконалення існуючих та розробка новітніх зразків систем та засобів радіоелектронної боротьби вітчизняними виробниками.

Основними виробниками такої техніки в Україні являються ГП СФВ “Укроборонекспорт” та АТ ХК “Укрспецтехніка”. Серед їх продукції є такі засоби РЕБ як: автоматизований комплекс радіозавад “МАНДАТ-Б1Э”; мобільний наземний комплекс радіопридушення ліній радіозв’язку і керування авіацією противника “ЛИМАН”; мобільний комплекс оптико-електронної протидії “КАШТАН-3М”; система придушення радіоліній керування діапазону частот 20–2 500 МГц “ГАРАНТ”; комплекс протидії БПЛА «АНКЛАВ».

Комплекс “МАНДАТ-Б1Э” призначений для придушення наземних каналів зв’язку з фіксованими робочими частотами будь-яких видів модуляції та стрибкоподібно змінюваними частотами у діапазонах КХ і УКХ за допомогою постановки прицільних за частотою і часом та загороджувальних завад.

Комплекс “ЛИМАН” призначений для придушення: каналів УКХ радіозв’язку і наведення, що використовуються для взаємодії екіпажів під час повітряної операції; каналів наведення літаків на повітряні та наземні цілі з повітряних і наземних пунктів керування; каналів передачі розвідувальних даних з літака на пункт керування; каналів наведення літаків на наземні цілі передовими авіанавідниками.

Комплекс“КАШТАН-3М” призначений для захисту важливих військових і цивільних наземних об’єктів або надводних кораблів від високоточної зброї (ракет, авіабомб і артилерійських снарядів), оснащеної напівактивними лазерними головками самонаведення.

Комплекс “ГАРАНТ” призначений для придушення різних радіотехнічних засобів, каналів радіозв’язку стаціонарних, мобільних і переносних радіостанцій, приймальних трактів радіотелефонів стільникових систем зв’язку, а також для захисту рухомих засобів (рухомих колон і одиночних транспортних засобів) та стаціонарних об’єктів шляхом запобігання радіокерованого підривання вибухових пристроїв (мін, фугасів тощо).

Комплекс “АНКЛАВ” призначений для створення завад для приймачів, що працюють на частотах навігаційних систем GLONASS та GPS. «АНКЛАВ» також може створювати завади для каналів управління та телеметрії, які використовуються у БПЛА та високоточному озброєнні.

Оснащення Збройних Сил України розглянутими вітчизняними системами та засобами радіоелектронної боротьби допоможе дезорганізувати систему бойового управління противника, а також захистити свої сили та засоби від його засобів вогневого ураження.

УДК 621.372.

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

ВОЛОКОННО-ОПТИЧНІ ТЕХНОЛОГІЇ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ ТА НАДІЙНОСТІ СТВОРЕННЯ СИГНАЛЬНИХ РУБЕЖІВ ОХОРОНИ ПЕРИМЕТРА

Цілі будь-якої охоронної системи полягають у ранньому виявленні небезпечної події, локалізації її місця, часу та характеру, сигналізації, ініціюванню заходів, що перешкоджають розвитку загрози проникнення, документуванню матеріалів для профілактики подібних подій у майбутньому. Цих цілей можна досягти лише комбінацією чи інтеграцією систем, заснованих на різних фізичних принципах.

Сучасні системи безпеки, що базуються на волоконно-оптичних технологіях, відіграють критично важливу роль у забезпеченні раннього виявлення загроз, що сприяє створенню надійних та ефективних систем охорони та контролю доступу.

Волоконно-оптичні системи ідеально підходять для сигнальних рубежів охорони периметра з низки причин:

1. Дальність передачі без втрат, що дозволяє створювати довгі периметри без необхідності встановлення додаткових підсилювачів сигналу.

2. Висока пропускна спроможність: забезпечує швидкий та надійний обмін інформацією між різними пристроями, такими як датчики, камери відеоспостереження та системи керування, що є критично важливим для забезпечення ефективної роботи сигнальних рубежів.

3. Стійкість до перешкод: мають високу стійкість до електромагнітних перешкод, радіочастотних впливів та інтерференції від інших пристроїв.

4. Компактність та безпека: мають малий розмір і легкість. Крім того, такі системи більш безпечні з точки зору конфіденційності інформації, що передається, так як вони не випромінюють електромагнітних сигналів і складніше піддаються перехопленню.

5. Інтеграція з іншими системами: легко інтегруються з системами безпеки, що дозволяє створити комплексну та уніфіковану систему охорони периметра.

6. Низька вартість експлуатації: системи мають тривалий термін служби та вимагають мінімальних витрат на обслуговування та ремонт.

У волоконно-оптичних охоронних системах використовують кілька методів реєстрації сигналів вторгнення:

- метод реєстрації спекл-структури;
- метод реєстрації міжмодової інтерференції;
- інтерференційний метод.

Аналіз наявної інформації дозволив розділити всі волоконно-оптичні охоронні системи, що існують на зарубіжному ринку, на підгрупи за способом їх застосування:

- системи для захисту еластичних огорож;
- системи для захисту жорстких огорож та стін;
- підземні системи з волоконно-оптичними кабелями;
- системи для захисту водних рубежів.

Використання волоконно-оптичних систем у системах безпеки державних установ та військових об'єктів надає надійні та безпечні засоби для виявлення та запобігання загрозам, а також забезпечує швидке та ефективне реагування на надзвичайні ситуації. Це відіграє важливу роль у забезпеченні національної безпеки та захисті важливих об'єктів.

УДК 621.396

Майборода І.М., доцент кафедри Національної академії Національної гвардії України, кандидат військових наук, доцент
Раєнко О.С., викладач кафедри Національної академії Національної гвардії України
Луньов О.Ю., заступник начальника Національної академії Національної гвардії України, кандидат військових наук

ДЕЯКІ АСПЕКТИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ MIMO У ВІЙСЬКОВИХ ЛІНІЯХ РАДІОЗВ'ЯЗКУ

Застосування технології MIMO у військових лініях радіозв'язку дозволяє вирішити два важливих завдання: підвищення швидкості передачі при використанні просторового мультиплексування; збільшення якості зв'язку за рахунок просторового, часового- та частотного кодування і (або) формування променів. Технологія MIMO (Multiple Input – Multiple Output) представляє собою метод просторового кодування сигналу, який дозволяє збільшити смугу пропускання каналу, в якому здійснюються передача та отримання даних за рахунок систем з декількох антен. Антенні елементи на передачі та прийомі розносять таким чином, щоб кореляція між сусідніми антенами була досить слабкою.

При різноманітних реалізаціях технології MIMO мається на увазі саме одночасна передача кількох незалежних повідомлень в одному фізичному каналі. MIMO застосовують багатоантенні системи, а саме: на передавальній стороні є N передавальних антен, а на приймальній стороні – M приймальних. Властивості MIMO-каналу, що з'єднує n-й передавальний елемент, з m-м приймальним елементом, описуються комплексними канальними коефіцієнтами h,n,m що утворюють канальну матрицю H розміру N × M. Їх значення випадково змінюються згодом через наявність багатопроменевого поширення сигналу. Практична реалізація антен MIMO може бути різною. Для військових радіозасобів необхідно поєднати високу ефективність при відносно невеликих розмірах, що може бути реалізовано з використанням панельних антен. Панельна антена MIMO може у прямому сенсі мати в одному корпусі два набори випромінюючих елементів ("патчів"). Прикладом можуть слугувати чотири патчі, що працюють з вертикальною поляризацією, а інші чотири – з горизонтальною. Тобто всього отримуємо вісім патчів, із двохпортовим (ортогональним) живленням. Наразі саме MIMO дозволяє передавати у 2 рази більше даних за той же часовий проміжок при варіанті 2x2 у наявній смузі частот. На жаль, на практиці максимальна швидкість передачі інформації складає 326 Мбіт/с, а не 400 Мбіт/с, як передбачає теоретичний розрахунок, якщо використовувати антенну реалізацію 4x4. Це напряму пов'язано із особливістю передачі даних через чотири антени. Для передачі опорних символів кожній із антен виділені певні ресурсні елементи. Ці елементи необхідні для оцінки каналів та організації когерентної демодуляції. У результаті 14,3% від усіх ресурсних елементів виділено на передачу опорних символів.

Таким чином, антени для систем MIMO не потребують великих матеріальних затрат на їх виготовлення, а проведений теоретичний аналіз показує, що на практиці їх застосування призводить до суттєвого збільшення пропускної спроможності каналів радіозв'язку. Виходячи із основних вимог до військових радіозасобів, це дасть змогу збільшити їх ефективність за рахунок використання антенних систем з відносно невеликими розмірами.

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., старший науковий співробітник науково-дослідного центру Національної академії Національної гвардії України, кандидат технічних наук, старший науковий співробітник
Башкатов Є.Г., начальник кафедри Національної академії Національної гвардії України кандидат військових наук, доцент,
Сидоренко І.І., доцент кафедри Національної академії Національної гвардії України, кандидат педагогічних наук, доцент

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ПРОГРАМНОГО ЗАСОБУ “КРОПИВА” ЩОДО ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ МЕРЕЖІ

Збройні Сили України (ЗСУ) та Національна гвардія України (НГУ) все більше відходить від старих радянських методів управління та опановує новітні розробки. 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. Так починаючи з 2018-го року у тестовому режимах, а з початку повномасштабного вторгнення російських військ в Україну в повному обсягу використовувались окремих інформаційних систем різного рівня – “Delta”, “Кропива”, “Віраж-планшет”, “GisArta” та інші. Всі перелічені системи працюють на тактичному рівні.

Для підрозділів НГУ при виконанні службово-бойових (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, а також управління боєм.

Бойова система управління тактичної ланки "Кропива" була випробувана в реальних бойових умовах. Бойова система управління тактичної ланки “Кропива” це програмне забезпечення на базі ГІС для створення інтелектуальних карт в поєднанні з пристроями та приладами, для планування, розрахунків та орієнтування на місцевості.

Програмний комплекс (ПК) “Кропива” працює на рівні батальйону (дивізіону), роти (батареї), взводу, окремої одиниці техніки та дає змогу автоматизувати окремі завдання з їх управління. Головна мета його використання є об’єднання оперативної інформації від засобів розвідки, управління та вогневого ураження в єдине інформаційне поле. За класифікацію, прийнятою у країнах НАТО ПК “Кропиву” можливо віднести до систем типу С2 (Command and Control).

Систему можна встановити на планшет, який працює на базі Android. При цьому для керування та передачі команд “Кропива” використовує короткохвильові та цифрові радіостанції, сумісні зі стандартами захищеного зв’язку військ НАТО. Також комплекс сумісний з іншими каналами зв’язку, включно із оптоволоконними та супутниковими мережами. Комплекс програмно-апаратних засобів відображення інформації та засобів передачі тактичних даних для реалізації конкретних функцій і завдань управління та розвідки створює автоматизоване робоче місце (АРМ) ПК “Кропива”.

Обмін оперативної тактичної обстановкою проводиться після обрання потрібних об’єктів, автоматичного формування сцени та передачі по сформованим каналам зв’язку одному або декільком користувачам зі переліку додатку “Тенета”. Можливі варіанти організації інформаційної мережі через закритий або відкритий канал Інтернету (зокрема використання месенджерів “Telegram” та “Signal”), через канал мобільного зв’язку GSM/CDMA шляхом обміну шифрованими SMS-повідомленнями, за допомогою мережі, утвореної з радіостанцій.

Для забезпечення обміну повідомленнями всі планшети абонентів мають бути об’єднані в єдину мережу та мати однаковий пароль шифрування даних. Для обміну інформацією в мережі підрозділу доцільно використовувати додаткове програмне забезпечення “OpenVPN for Android”, що забезпечує прихованість передачі даних.

УДК 621.315

Катунін А.М., викладач кафедри Національного університету цивільного захисту України, кандидат технічних наук, старший науковий співробітник
Кожушко Я.М., старший науковий співробітник Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, старший дослідник
Беспалько О.В. науковий співробітник Харківського національного університету Повітряних Сил імені Івана Кожедуба

УДОСКОНАЛЕННЯ МОДЕЛІ ОЦІНЮВАННЯ ТЕРМІНУ ЕКСПЛУАТАЦІЇ ІЗОЛЯЦІЇ КАБЕЛЬНИХ ВИРОБІВ ЗВ'ЯЗКУ

Темпи зростання ефективності систем зв'язку супроводжуються зростанням обсягів споживання електричної енергії, розвитком електричних мереж, збільшенням асортименту кабелів та проводів зв'язку. Внаслідок даного факту суттєво зростають вимоги до надійності функціонування визначених кабельних виробів.

На даний час відома значна кількість моделей, використання яких дозволяє зробити оцінювання ступеня зносу ізоляції та старіння кабельних виробів зв'язку. Основні моделі старіння ізоляції мають відповідні обмеження. Таким чином, доцільно запропонувати удосконалену модель для оцінювання терміну експлуатації ізоляції кабельних виробів зв'язку.

Для ефективного оцінювання ступеня зносу ізоляції відповідних кабельних виробів пропонується застосовувати комбіновану зворотньо ступеневу модель старіння, яка запропонована Арреніусом.

В свою чергу напруженість електричного поля в кабельних виробах безперервно змінюється внаслідок зміни напруги в електричних мережах (звичайно в межах 10% від номінального). Температура, при якої функціонують кабельні вироби, більш стабільна, однак її значення є також випадковою величиною.

Даний аспект ніяк чином не враховувався в комбінованій моделі Арреніуса. Тому пропонується здійснювати аналіз залежності терміну експлуатації ізоляції кабелів та проводів зв'язку від напруженості електричного поля та температури із врахуванням того, що напруженість електричного поля та температуру є випадковими величинами.

В такому випадку запропонована модель оцінювання терміну експлуатації ізоляції кабельних виробів зв'язку буде являти собою адитивну функцію із постійними складові значень напруженості електричного поля та температури в точках розрахунку та випадковими складовими, які визначаються характерним законом розподілу та амплітудою коливань випадкової величини відповідно.

Таким чином, запропоноване удосконалення моделі можливо застосовувати на практиці для визначення термінів експлуатації ізоляції кабельних виробів, що досить широко застосовуються в системах зв'язку.

УДК 621.391

ЛитвинА.В., старший викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба
Олексіюк Д.П., курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба

ПРОПОЗИЦІЇ ЩОДО ПІДВИЩЕННЯ СТІЙКОСТІ СИСТЕМ НАЗЕМНОГО УКХ РАДІОЗВ'ЯЗКУ НА БАЗІ МОБІЛЬНИХ МЕРЕЖ КЛАСУ MANET

Під час відсічі повномасштабного вторгнення російської федерації на територію України активно застосовується системи наземного УКХ радіозв'язку побудовані на основі технологічних рішень стандарту DMR (Digital Mobile Radio – цифровий рухомий радіозв'язок). Переваги та недоліки таких систем добре відомі, та є характерними для систем, які

використовують фіксовані частоти радіозв’язку. В той же час значного розвитку в окремих родах військ набувають системи радіозв’язку на базі Mesh-мережа мобільних мереж класу MANET(MobileAd-HocNetworks). Для побудови мереж даного класу підрозділи Сил оборони України мають в своєму арсеналі УКХ радіостанції виробництва компанії L3 Harris (США), Aselsan (Турецька республіка) та радіостанції Himera G1 від української компанії Promin Aerospace.

На шляху створення української системи C4 ISR (Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance) доцільно використовувати такі мережі, як Mesh-мережі та MANET-мережі. Mesh-мережі - це бездротові мережі, в яких кожен вузол має можливість встановлення прямих з'єднань з іншими вузлами. Головною особливістю Mesh-мереж є велика міра стійкості, адже вони можуть працювати навіть при відмові окремих вузлів. MANET-мережі (MobileAd-hocNetwork) - це мережі бездротових комунікацій, в яких вузли мережі рухаються та змінюють своє місцезнаходження. Їх основною особливістю є динамічна топологія та обмежений ресурси вузлів. MANET-мережі складаються з мобільних та автономних вузлів без фіксованих інфраструктурних вузлів, тобто вони не потребують попереднього налаштування і можуть самостійно організовувати з'єднання між собою.

Однією з вимог до системи зв’язку є забезпечення стійкості цієї мережі, тобто можливість виконувати завдання в умовах впливу різноманітних факторів.

На основі аналізу протоколів маршрутизації Mesh-мереж та MANET-мереж, можна запропонувати такі способи підвищення стійкості систем радіозв’язку:

Використання гібридних протоколів: розробка та використання протоколів, що комбінують у собі переваги різних типів мереж (наприклад, протоколи, які поєднують маршрутизацію на основі проактивного та реактивного підходів), для забезпечення оптимального використання ресурсів та стійкості мережі.

Впровадження механізмів самовідновлення: реалізація алгоритмів та механізмів, які дозволяють мережі автоматично виявляти та усувати несправності або атаки, а також швидко відновлювати втрачені зв'язки та маршрути.

Удосконалення алгоритмів маршрутизації: розробка та вдосконалення алгоритмів маршрутизації з урахуванням специфіки мережі та її можливих проблем, таких як мобільність вузлів, втрати пакетів, затримки тощо.

Застосування технологій автоматичного сканування та оцінки середовища: використання додаткових датчиків та механізмів збору інформації про мережеве середовище для більш точного аналізу та прийняття відповідних рішень у реальному часі.

Таким чином, проведений аналіз мобільних мереж MANET та Mesh, які є перспективними до застосування в тактичній ланці управління військами, дозволив сформулювати основні способи покращення стійкості систем наземного УКХ радіозв'язку, що в свою чергу забезпечить підрозділи тактичної ланки управління військами всією необхідною для прийняття управлінських рішень інформацією в режимі реального часу, що значно підвищить бойову ефективність даних підрозділів.

УДК 623.624

Пічугін М.Ф., провідний науковий співробітник Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат військових наук, професор
Кожушко Я.М., старший науковий співробітник Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, старший дослідник
Іщенко Д.А., старший науковий співробітник Житомирського військового інституту, кандидат технічних наук, доцент
Кирилюк В.А., начальник науково-дослідної лабораторії Житомирського військового інституту, кандидат технічних наук, старший науковий співробітник
Клімішен О.О. старший викладач Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, старший науковий співробітник

ПІДХІД ДО ОЦІНЮВАННЯ НОСІЇВ СПРОМОЖНОСТЕЙ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ, НЕОБХІДНИХ ДЛЯ ВИКОНАННЯ ЗАВДАНЬ РАДІОЕЛЕКТРОННОГО ПОДАВЛЕННЯ

Розвиток та застосування сучасних систем і засобів зв’язку в інтересах управління військами йде пліч-о-пліч із протидією до них через розвиток радіоелектронної боротьби, важливість якої зростає у в сьому світі, як невід’ємної складової забезпечення сучасних бойових дій (БД). Набуття спроможності супровідної підтримки силами та засобами РЕБ з використанням спеціальних методів та характерних до них способів радіоелектронного подавлення, захисту та електронної (інформаційної) підтримки має зв'язок із практичними завданнями військ щодо перспективного розвитку ЗС України. Розвиток спроможностей здійснюється шляхом вдосконалення базових компонентів (складових): розвиток озброєння та військової техніки РЕБ; удосконалення доктрин, засад застосування; зміна організаційних структур; покращення системи відбору, навчання та мотивації персоналу. Раціональне розподілення зусиль за базовими складовими для набуття спроможностей з РЕБ є складним науково-практичним завданням, що потребує відповідного науково-методичного апарату його дослідження. Аналіз останніх досліджень та публікацій показав, що питання набуття спроможностей, планування сил і засобів, необхідних для виконання, завдань під час застосування військ (сил) за призначенням досить широко висвітлені в керівних і відкритих нормативних документів, але складність завдання потребує вирішення таких часткових завдань: аналізу можливих варіантів виконання завдань частин (підрозділів) РЕБ виду ЗС України в операціях (БД); розроблення методик (розрахункових задач) для визначення сил і засобів РЕБ виду ЗС України, необхідних для виконання завдань в операціях (БД); розроблення методики розрахунку вартості виконання завдань частинами (підрозділами) РЕБ виду ЗС України в операціях (БД); розроблення рекомендацій щодо порядку використання методик.

Планування РЕБ в операції (БД), у яких приймають участь військові частини (підрозділи) різних родів військ, обумовлює необхідність загального підходу до оцінювання носіїв спроможностей з РЕП, що належать до різних видів Збройних Сил. У доповіді надано підхід до оцінювання носіїв спроможностей з РЕБ, необхідних для виконання завдань в операціях (БД). Запропонований підхід є вдосконаленим у порівнянні з існуючими за рахунок врахування нових вимог до спроможностей за складовими РЕБ (боротьба з БПЛА, прикриття від радіокерованих вибухових пристроїв противника тощо). На відміну від відомого, він враховує нові підходи до планування (формування проектів концепції та програм розвитку) РЕБ на основі спроможностей, оцінювання відповідних проектів, що розробляються.

УДК 654.01

Душкін В.Д., доцент кафедри Національної академії Національної гвардії України, кандидат фізико-математичних наук, доцент
Глушко П.Г., курсант Національної академії Національної гвардії України
Федорчук І.І., курсант Національної академії Національної гвардії України

ЗАСТОСУВАННЯ ФРАКТАЛЬНИХ АНТЕН ДЛЯ ГЕОЛОКАЦІЇ ОКРЕМИХ ВІЙСЬКОВОСЛУЖБОВЦІВ

У опублікованому у 2022 році звіті інформаційно-аналітичний центру оборонних систем Defense Systems Information Analysis Center (DSIAC) сказано , що фрактальні радари існують уже 20 років і їх використання зараз лише набирає обертів через те, що противники США виявляють ознаки використання цієї технології.

Фрактальні антени мають кілька резонансів, на відміну від звичайних антен, що робить можливою роботу в декількох частотних діапазонах за допомогою однієї компактної антени. Цей тип антен широко використовується у цивільній сфері - бездротові мережі (протоколи Bluetooth, Wi--Fi, WiMAX, ZigBee), мобільний зв'язок (стандарти CDMA, GSM, DECT), мобільне телебачення (стандарти DVB-H і ISDB-H), системи супутникового позиціонування, радіочастотна ідентифікація та ін.

Унікальні властивості фрактальних антен знайшли своє застосування у військовій сфері. Можливість працювати на великій кількості частот у їх широкому діапазоні, динамічно переходити з однієї частоти на іншу за допомогою комп’ютерних алгоритмів робить фрактальні антени ефективними у здійсненні завадозахищенного радіозв’язку та радіелектронної боротьби. Використання фрактальнх антен у радіолокації дає переваги над антенами з неперервною апертурою, завдяки відсутності у діаграмі направленості бокових пелюстків, у порівнянні з радарами зі скінченною розрідженню апертурою, наприклад PAWS, має переваги у коефіцієнті підсилення потужності. Малі розміри та вага цього типу антен а також подібність фрактальних структур до природних об’єктів дозволяє ефективно маскувати їх, кріпити їх на їх на шоломи або бронежилети військовослужбовців, дозволяє встановлювати їх на безпілотні літальні апарати для здійснення трекінгу та управління ними.

Також розглядаються можливості використання фрактальних антен у системах пошуку та локалізації мобільних об’єктів, визначення несанкціонованих джерел радіовипромінювання при боротьбі з диверсійними групами та терористами.

В останнє десятиріччя одним з напрямків досліджень науковців було створення антен, стійких до згинання. Ці розробки мають перспективи використання як у цивільній так і військовій сфері. Зокрема проводиться розробка текстильних антен для визначення місцезнаходження окремих військовослужбовців. Для визначення місцезнаходження поранених потрібні антени, що зможуть працювати при пошкоджені частини їх геометричної структури. У цьому випадку має сенс розглядати періодичні структури з квазіфрактальною структурою періоду, сподіваючись що пошкодження частини електродинамічної структури при суттєвому багаторазовому повторенні елементів структури не позбавить можливості безперебійної роботи пристроїв. Практичні розробки цього класу антен є предметом дослідження науковців та науково-виробничих фірм.

УДК 177 +17.03 + 378

Козубцов І.М., професор кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, доктор педагогічних наук, старший науковий співробітник
Нестеров О.М., начальник кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, PhD
Пономарьов О.А., начальник факультету бойового застосування систем управління та зв'язку Військового інституту телекомунікацій та інформатизації ім. Героїв Крут

ДОСВІД ЗАСТОСУВАННЯ МЕТОДИКИ ВИПЕРЕДЖАЮЧОГО ВИКЛАДАННЯ КУРСАНТАМ ОКРЕМИХ НАВЧАЛЬНИХ ДИСЦИПЛІН КАФЕДРИ БОЙОВОГО ЗАСТОСУВАННЯ ПІДРОЗДІЛІВ ЗВ'ЯЗКУ В УМОВАХ ВОЄННОГО ЧАСУ

В умовах війни, вищі військові навчальні заклади (ВВНЗ) України функціонують в екстремальних умовах. Через часті та тривалі повітряні тривоги перед всіма учасниками освітнього процесу висувається ключове завдання продовжувати якісну підготовку курсантів – майбутніх офіцерів сектору безпеки та оборони. В результатів повітряних тривоги відбувається вимушене скорочення аудиторного часу (лекцій, практик / семінарів, лабораторних занять), що призводить до порушення логіки навчального процесу. В сучасних умовах головним пріоритетом завжди буде життя і здоров'я кожного учасника освітнього процесу. Тому найважливішою метою педагогічної діяльності в умовах війни – перетворення кожного ВВНЗ на територію безпеки.

Забезпечити якісну підготовку курсантів можливо за умов одночасно вимушеної особливої організації освітнього процесу у ВВНЗ та високої педагогічної майстерності науково-педагогічних працівників можливо із використанням методики випереджаючого викладання.

Обмеження накладаються при використанні методики за наявності у навчальному матеріалах інформації з обмеженим доступом.

Метою доповіді є висвітлення досвіду застосування методики випереджаючого викладання курсантам окремих навчальних дисциплін кафедри бойового застосування підрозділів зв'язку в умовах воєнного часу з головним пріоритетом якої життя і здоров'я кожного учасника освітнього процесу.

За розробленої раніше авторами методики, лекційний курс навчальної дисципліни завчасно видається курсантам на самостійне опрацювання поза аудиторією. Якщо це і раніше здійснювалось досвідченими майстрами педагогічної діяльності, то в умовах війни зростає усвідомленість курсантів перед майбутньою неминучою особистою відповідальністю за не набуття знань, що можуть призвести до трагічних наслідків. Така організація освітнього процесу є змішаним навчанням за технологією «випереджаючого навчання» або зарубіжним аналогом «перевернутий клас». На аудиторних заняттях лектору достатньо прокоментувати та/або відповісти на запитання курсантів, які до того часу вже з'являються.

Безумовно, що методика потребує подальшого удосконалення в напрямку проведення лабораторних, практичних занять із використання стаціонарного обладнання ВВНЗ. На допомогу цьому можуть прийти тренажери та або електронні лабораторні комплекси. Безумовно для покращення викладання і навчання необхідно використовувати допоміжні технології, наприклад, гейміфікацію, але потрібно слідкувати , щоб навчання через гру не перетворився в чисту гру.

Необхідно відзначити на якість відбору лектором основної та допоміжної навчальної літератури. Також існує потреба у розробці навчально-тренувальних карток за кожним зразком, що напри великий жаль не робиться на всіх кафедрах.

Таким чином, застосування дистанційної форми навчання та навчання на випередження дозволить не лише забезпечити виконання навчального плану з опанування освітньої компоненти, а й максимально забезпечити можливості здобувачів зі збереження життя і здоров'я в умовах війни.

УДК 177 +17.03 + 378

Нестеров О.М., начальник кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, доктор філософії
Козубцов І.М., професор кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, доктор педагогічних наук, старший науковий співробітник
Пуштарик О.С., викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут

ОСУЧАСНЕННЯ РУХОМИХ ЗАСОБІВ ФЕЛЬД'ЄГЕРСЬКО-ПОШТОВОГО ЗВ'ЯЗКУ ТА ОБРИС НОВИХ ФУНКЦІЙ

Результатами аналізу бойового досвіду застосування озброєння військової техніки та допоміжних підрозділів в умовах повномасштабної агресії і потреби високої маневреності підрозділів Збройних Сил України визначило концептуальні напрямки модернізації. Об'єктом нашого дослідження є рухомі засоби фельд'єгерсько-поштового зв'язку (ФПЗ).

Питання щодо заміни застарілих УАЗ-3151, УАЗ-452, ГАЗ-66 назріло уже давно. Даний факт засвідчує неефективність використання ФПЗ на базі автомобільної платформи УАЗ-3151, УАЗ-452, ГАЗ-66 через:

фінансово-економічних показників (перевитрати паливно-мастильних матеріалів на експлуатацію); низької мобільності (мала швидкість переміщення по автомобільним дорогам з твердим покриттям); відсутністю прихованого переміщення (по силуету типові для військової техніки);

використання морально застарілої техніки, ресурс яких давно вичерпано, а виробництво комплектуючих деталей в країні агресор.

Враховуючи вище зазначене, у потребі оновлення бази рухомих засобів ФПЗ в залежності від майбутньої концепції їх застосування розглядалася науковцями Військового інституту телекомунікацій та інформатизації ім. Героїв Крут ще в далекому 2011 році.

Нова концепція автоматизація визначила наукові установи з обґрунтування вибору рухомих засобів ФПЗ. На вирішення означених завдань виконувалась ряд науково-дослідних робіт (НДР). Однак з початком бойових дій на сході України зазначені НДР припинились або достроково завершили через переорієнтацію на більш пріоритетні напрямки та потреби.

І лише у 2018 році за рахунок коштів, спрямованих на розвиток озброєння та військової техніки Збройних Сил України, розпочалось часткове оновлення рухомих засоби ФПЗ.

Забезпечення новітніми рухомими засобами дасть можливість підвищити бойову спроможність військових частин, оперативність, надійність та безпеку системи зв'язку в цілому.

На підставі досвіду та потреб здійснимо осучаснення фельд'єгерсько-поштового зв'язку в залежності від концепції застосування, обрис рухомих засобів має забезпечувати функції: переміщення обладнання та членів екіпажу; телефонним зв'язком в русі та на стоянці; передачі даних; відпочинку членів екіпажу; перевезення поштових відправлень, кореспонденції в тому числі з грифом обмеження доступу; перевезення малогабаритних вантажів, спец-техніки; перевезення не заборонених речей військовослужбовців (особистих речей, бронежилетів, речового майна, з можливістю відтермінування доставки, або доставки у зазначений проміжок і термін).

Відповідно до обрису нових функцій та завдань вбачається три варіанти реалізації рухомих засобів ФПЗ:

1. «Високопрохідний» на базі броньованого вантажного автомобіля високої прохідності українського виробника ПАТ «АвтоКрАЗ».

2. «Швидкісний» на базах автомобілів іноземного виробництва (Volkswagen Crafter, Mercedes-Benz Sprinte, Ford Transit, Iveco Daily).

3. «Вантажний» для виконання функції вантажних перевезень.

УДК 177 +17.03 + 378

Ткач В.О., старший науковий співробітник Військового інституту телекомунікацій та інформатизації ім. Героїв Крут
Козубцов І.М., професор кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, доктор педагогічних наук, старший науковий співробітник
Самелюк В.П., старший науковий співробітник науково-дослідного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут

НАУКОВІ РОТИ, ЯК ДЖЕРЕЛО ТВОРЧИХ КАДРІВ ДЛЯ ВІЙСЬКОВО-НАУКОВОЇ ІННОВАЦІЇ

Потреба в зміцненні кадрового потенціалу військової науки в результаті повномасштабної гібридної агресії Збройних Сил Російської Федерації обумовлена пошуком інноваційних підходів до підвищення обороноздатності країни, пов'язаних з використанням сучасних досягнень науки і технологій. Система військової науки України з 24 лютого 2022 р., як і вся країна працює в екстремальних умовах. Особливістю цього періоду є необхідність поєднання виконання важливих науково-дослідних робіт, що беруть початок у довоєнний час і потребують свого логічного завершення та виконання пріоритетних актуальних оперативних завдань. Гібридний характер війн в чотирьох площинках (суші, морі, повітрі та кіберпросторі), посилення ролі інформаційної складової і нових технологічних рішень змушує переглядати підходи до військово-технічного забезпечення. На думку експертів у сфері військової економіки і озброєння, для адекватного швидкого виявлення військових загроз потрібне оснащення Збройних Сил України сучасними та перспективними зразками озброєнь, розробки і постачання у війська зразків нового покоління, заснованих на інноваційних технічних і технологічних рішеннях, створення принципово нових, нетрадиційних зразків, заснованих на використанні значних досягнень.

Рішення цих завдань неможливо без збереження і розвитку кадрового потенціалу наукових шкіл в науково-дослідних інститутах і ВВНЗ. Кадровий потенціал зазвичай характеризується такими узагальненими показниками: частка працівників з вченими ступенями, побічно характеризує продуктивність і якість виконуваної наукової роботи; укомплектованість кадрами, як співвідношення зайнятих наукових посад до загального штатного числа наукових посад, що характеризує можливості наукової організації по збалансованому розподілу праці та повноцінного виконання співробітниками своїх обов'язків; середній вік співробітників, як непрямий індикатор інноваційної спрямованості наукової організації, оскільки науковці молодого і середнього віку з великою часткою ймовірності володіють сучасними знаннями і високою адаптивністю до мінливих умов глобального інформаційного середовища.

В цілях збереження і розвитку наукового потенціалу необхідно залучати високо мотивованих, наповнених ентузіазмом молодих військових і цивільних громадян після закінчення закладів освіти та забезпечувати їх професійний ріст. Дане завдання щодо військовослужбовців вирішується шляхом підготовки кадрів за програмами аспірантури, ад'юнктури та докторантури, їх подальше працевлаштування здійснюються в рамках закритої системи організацій Міністерства оборони. Рівень оплати наукової праці на офіцерських посадах і можливості самореалізації зумовлюють привабливість наукової кар'єри для офіцерів.

Стимулювання перспективних випускників цивільних закладів освіти для роботи у військових наукових установах на посадах цивільного персоналу видається більш складною задачею. Всезростаючий розрив між грошовим забезпеченням офіцерів та цивільними у наукових відділах відгукується. Проте себе чудово зарекомендувало військово-цивільне співробітництво саме з небайдужих фахівців ІТ галузі (Кібер Армія, Stop Russian Channel MRIYA) для виконання широкого спектру завдань із запобігання кібератак Російської Федерації в об’єкти критичної інформаційної інфраструктури України. І доречи, це є ефективний розподіл людського ресурсу за мобілізацією.

УДК 004.08

Хмелевський С.І., начальник кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент
Хмелевська О.О., провідний науковий співробітник наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, старший науковий співробітник

МЕТОДИЧНІ ОСНОВИ ТЕСТУВАННЯ СКЛАДНИХ ПРОГРАМНИХ КОМПЛЕКСІВ

Для виявлення та усунення помилок та дефектів усі етапи розробки та супроводу програмного продукту необхідно підтримувати методами та засобами верифікації та систематичного автоматизованого тестування якості для вимірювання його рівня та визначення реальних характеристик програм з метою виявлення та усунення дефектів.

На етапах розробки програмного продукту доцільно застосовувати різні методи, зразки та види тестування, кожен з яких орієнтований на виявлення, локалізацію чи діагностику певних типів дефектів. Непередбачуваність конкретних дефектів і помилок у програмах призводить до доцільності послідовного методичного аналізу можливості прояву будь-якого типу помилок та до необхідності їх виключення на ранніх етапах розробки при мінімальних витратах. Результати тестування та вимірювання значень показників якості повинні порівнюватися з вимогами технічного завдання або специфікацій для визначення ступеня відповідності висунутим вимогам. Для тестування необхідні досить повні зразки, такі як сукупність вимог технічного завдання та їх поетапна декомпозиція в специфікаціях. Планування тестування необхідно поділити на три групи даних: про цикли у програмі; про маршрути виконання програми; про предикати, що визначають маршрути виконання програми та межі областей зміни змінних. Для виділення маршрутів тестування розробник повинен зазначити критерій, яким слід формувати маршрути. Крім того, він має визначити стратегію для складання впорядкованого списку маршрутів, за яким слід планувати послідовність тестування. В результаті складається список маршрутів, упорядкованих за обраною стратегією. За цими маршрутами розраховується повна кількість тестів та сумарна складність тестування структури програми відповідно до обраного критерію виділення маршрутів. Можливе коригування планів. За отриманими співвідношеннями між змінними в предикатах можуть бути побудовані межі областей зміни змінних для кожного з маршрутів та програми в цілому. Автоматичний розрахунок та впорядкування інформації про характеристики програми, а також відображення відомостей у компактній та наочній формі, дозволяє зробити процес тестування ефективним та економічним. Ряд особливостей тестування складних програм відрізняє процес від традиційного методу, що використовується для перевірки апаратури та інших технічних систем. З цієї позиції основними особливостями процесу тестування програмних комплексів є:

відсутність повністю визначеного достовірного еталона-програми, якому повинні точно відповідати всі результати тестування програми, що перевіряються;

висока складність комплексів програм та принципова неможливість побудови і використання повних комплектів тестових наборів, достатніх для вичерпної перевірки якості та надійності функціонування програмного продукту;

відносно невисокий ступінь формалізації, критеріїв якості результатів тестування та досягнення при цьому коректності, безпеки та надійності функціонування об'єктів випробувань.

УДК 316.774

Головань О.В., науковий співробітник Інституту радіофізики та електроніки Національної академії наук України

ПРОГРАМНО-КЕРОВАНІ АНТЕНИ В СИСТЕМАХ МЕТЕОРНОГО ЗВ'ЯЗКУ

Системи метеорного радіозв'язку (СМР) можуть використовуватись в інтересах Міністерства Оборони та дипломатичних представництв, а також для організації радіозв'язку в зонах стихійних лих, важкодоступних та віддалених районах. Вони можуть бути малобюджетною альтернативою супутниковим системам зв'язку. Їх застосування суттєво ускладнює пеленгацію місць розміщення абонентів мережі.

Побудова СМР нової генерації передбачає підвищення пропускної спроможності, перешкодозахищеності та скритності функціонування системи, а також скорочення часу очікування з'єднання.

Вибір топології мережі метеорного радіозв'язку забезпечує необхідне покриття і можливість одночасного доступу абонентських станцій (АС) до декількох базових станцій (БС), що скорочує час очікування появи іонізованих слідів метеороїдів, що мають точку дзеркального відбиття і, відповідно, збільшує пропускну здатність системи.

Оскільки БС є найбільш критичним елементом мережі метеорного радіозв'язку, необхідно передбачити можливість її додаткового захисту від навмисних і ненавмисних перешкод. Ця можливість може бути реалізована на основі використання програмно-керованих антен, що забезпечують необхідне покриття та адаптацію до умов функціонування системи, що змінюються. При використанні адаптивних антенних решіток (АФАР) існує можливість програмного формування «нулів» діаграм спрямованості (ДС) у напрямі джерел перешкод. Для цього можуть застосовуватись додаткові (компенсаційні) антени, розташовані поблизу основної антени БС.

Істотно скоротити час очікування з'єднання та збільшити пропускну здатність СМР дозволить використання на АС антени з керованою (або комутованою) ДС. При заданому географічному положенні БС, наведення антен АС на «гарячі зони», де поява відповідних метеорних слідів найбільш ймовірно, вимагають урахування сезонного та добового розподілу радіантів спорадичних метеороїдів для кожної АС із зазначеними координатами.

Для помірних широт північної півкулі позитивний ефект від наведення антен АС спостерігається, якщо виконуються такі рекомендації:

• на трасах, що йдуть переважно зі сходу на захід, антени БС та АС необхідно спрямовувати так, щоб головні осі ДС перетиналися на північ від траси з 00.00 до 12.00 годин місцевого часу та на південь з 12.00 до 24.00 годин;

• на трасах, що йдуть переважно з півночі на південь, антени БС та АС мають бути спрямовані з 18.00 до 06.00 місцевого часу на захід від напрямку траси та з 06.00 до 18.00 години на схід.

Точне наведення антен на «гарячі зони» потребує розробки спеціального програмного забезпечення. Основні алгоритми і розрахункові співвідношення, необхідні для його виконання, наведені в монографії "Transmission of information using meteor radio channels", що готується до друку.

УДК 621.396.6

Фик О.І., професор кафедри Національної академії Національної гвардії України, доктор технічних наук, професор
Воронін О.І., старший викладач кафедри Національної академії Національної гвардії України

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ НАДПРОВІДНОГО ПРИСТРОЮ ДЛЯ ЗАХИСТУ СИСТЕМИ УПРАВЛІННЯ І ЗВ'ЯЗКУ ВІД УРАЖЕННЯ ЕЛЕКТРОМАГНІТНИМ ІМПУЛЬСОМ ЯДЕРНОГО ВИБУХУ

Найбільш небезпечний для радіоелектронної апаратури систем управління та зв'язку (СУЗ) є ЕМІ висотного ядерного вибуху, що має малу тривалість імпульсу ($t_i \approx 100\ 10^{-9} - 200\ 10^{-9}$ с) і фронту ($t_ф \approx 5\ 10^{-9}$ с), значною амплітудою напруженості електричного та магнітного поля ($E_m \approx 50\ 10^3$ В/м, $H_m \approx 130$ А/м) і здатний поширюватися на великі відстані.

У випадку при впливі ЕМІ висотного ядерного вибуху на РЕА СУЗ спостерігаються: пробої p-n-переходів у напівпровідникових приборів; пробої вакуумних та газонаповнених проміжків; розплавлення та обриви струмоведучих доріжок, місць паяння, (зварювання) проводів через термо- та електродинамічні напруження.

Використання конструктивних методів захисту не виключає можливості проникнення ЕМІ висотного ядерного вибуху через антенно-фідерні пристрої (АФУ). Для обмеження значних по амплітуді струмів і напруг, що виникають під дією ЕМІ в АФУ, часто застосовують різного типу захисні пристрої. До них відносяться газорозрядні прилади, варистори, стабілітрони і обмежувальні діоди. Однак дослідження показали, що вони не здатні захистити РЕА СУЗ від проникнення ЕМІ через антенно-фідерні пристрої, якщо тривалість імпульсу менше десятків наносекунд. Це зумовлено порівняно повільними фізичними процесами, що визначають час перемикання існуючих захисних пристроїв.

Зараз багато публікацій присвячених можливості створення захисного пристрою на основі високотемпературного надпровідника (ВТНП). Пропонується конструкція захисного пристрою у вигляді полоскової лінії передачі, являючи собою провідник стрічкового типу і прямокутного перерізу (тонка ВТНП-плівка), виконаний з високотемпературного надпровідника і розташований на діелектричній підкладці. При прийомі корисних сигналів, полосковий провідник знаходиться у надпровідному стані. Однак, у разі прийомом антени потужного електромагнітного випромінювання струм, що протікає у фідерному тракті, руйнує надпровідність полоскового провідника (фазовий S-N перехід) і переводить його в змішаний і згодом в не надпровідний (нормальний) стан, тим самим, збільшуючи його хвильовий опір на три порядки, викликаючи неузгодженість лінії передачі. Тривалість такого фазового S-N переходу визначає швидкодію надпровідного захисного пристрою (за різними експериментальними даними оцінюється від от 10^{-9} до 10^{-15} с) і залежить від конструктивних параметрів надпровідника і характеристик вхідного сигналу.

Пропонується обрати несиметричний вібратор з надпровідним захисним пристроєм. Для високотемпературного надпровідника були прийняті такі основні конструктивні параметри: довжина 0.25 м, площа перерізу $S = 4 \times 10^{-12}$ м^2 та питомий опір $\rho = 16.4 \times 10^{-7}$ Ом м.

Якщо оцінити кількість теплоти, що виділяється на штатному захисному пристрої(розрядники, pin-діоди) при дії ЕМІ ядерного наземного вибуху можна дійти невтішного висновку, що накопиченої теплоти, що виділяється на навантаженні рамкової антени достатньо щоб пройти крізь захист і порушити працездатність РЕА СУЗ незалежно від площі витка антени. Однак, застосування запропонованого надпровідного захисного пристрою (несиметричний вібратор з надпровідним захисним пристроєм) дозволяє ефективно захистити апаратуру систем зв'язку, знижуючи кількість теплоти, що виділяється на навантаженні нижче порогового значення (пороговий енергетичний рівень 10^{-7}-10^{-12}Дж). При цьому основна енергія ЕМІ виділяється на надпровідному захисному елементі пристрою, а решта віддзеркалюється назад у простір.

Треба відзначити, що вплив сигналу ЕМІ висотного ядерного вибуху на надпровідний захисний пристрій супроводжується високою швидкістю введення струму, при якій надпровідник втрачає стабільний надпровідний стан і переходить за одиниці наносекунд у нормальний (непровідний) тобто

без урахування інерційних (одиниці мікросекунд) теплових процесів. Порівняно малі значення енергії (менше одиниці мікроджоулів), необхідні для руйнування надпровідності захисного пристрою за одиниці наносекунд переключають надпровідник в змішаний і непровідний стан. А більша частина потужного сигналу, яка не приймала участь в переключенні надпровідника, поглинається надпровідником (поки це теоретично не пояснено) і віддзеркалюється від вже непровідного захисного пристрою назад у простір. Тобто убезпечуються чутливі напівпровідникові елементи приймального тракту від електромагнітного руйнування.

УДК 681. 323

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

СУЧАСНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ У НАВЧАЛЬНОМУ СЕРЕДОВИЩІ ЗАКЛАДУ ВІЙСЬКОВОЇ ОСВІТИ

Кіберборотьба та протидія кіберзагрозам в інформаційній сфері розглядається сучасним суспільством будь-якої країни як один із найважливіших пріоритетів безпеки, вагомий чинник у розвитку військового, соціального, економічного та інших секторів. Концептуально розроблення ефективних засобів кібербезпеки Української держави та, зокрема, Збройних сил та Національної гвардії України, передбачено в низці законодавчих документів, що націлені на розвиток спроможностей сил оборони України.

Подальша інтеграція в європейські структури безпеки та міжнародне оборонне співробітництво передбачають: державну підтримку оснащення Збройних сил, Національної гвардії України та інших складових сил оборони новим високотехнологічним озброєнням, військовою та спеціальною технікою; розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту й кібероборони під час підготовки та ведення всеохопної оборони України; набуття повноправного членства України в НАТО.

Освіта, зокрема професійна, повинна сприяти розвитку навичок критичного мислення, цифрової грамотності і навичок кіберзахисту. Нині дедалі більшої значущості набуває створення безпечного інформаційно-освітнього середовища закладів освіти різного рівня та профілю, що здійснюють підготовку фахівців і підвищення їхньої кваліфікації за різними спеціальностями.

Важливим завданням сьогодення є необхідність створення надійної системи кібернетичної безпеки. Тобто напряму, який пов'язаний із захистом цифрової інформації, операційних систем, комп'ютерних мереж, серверів, баз даних тощо від несанкціонованого втручання сторонніх осіб. Отже, ми виокремили основні кіберзагрози у сфері освіти: порушення конфіденційності, цілісності, доступності інформаційних ресурсів, що обробляються (передаються, зберігаються] у закладах освіти, злам баз даних працівників освіти, знищення вірусами баз даних, порушення безпеки режиму функціонування документообігу, порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних і технологічних систем. Проблемою є використання недостовірної, ненаукової інформації або дезінформації з мережі Інтернет під час підготовки та/або проведення навчальних занять, відсутність захисту відомостей з електронної пошти, використання інтернет-ресурсів з відкритих джерел і засобів електронних комунікацій. Отже, для України залишається актуальною низка проблемних питань, вирішення яких потребуватиме часу та зусиль як з боку держави, так і сектору безпеки й оборони. Від ефективності їх вирішення залежить, якою мірою українське суспільство зможе відповісти на сучасні кібербезпекові виклики.

УДК 004.716

Флорін О.П., доцент кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент
Пасічник А.В., старший викладач кафедри Національної академії Національної гвардії України

ЗАХОДИ БЕЗПЕКИ ПРИ ЕКСПЛУАТАЦІЇ ТЕРМІНАЛІВ STARLINK

Виконання бойових завдань з захисту територіальної цілісності України висуває підвищені вимоги до організації високошвидкісного захищеного зв'язку та передачі даних.

Використання глобальної супутникової системи Starlink є одним з варіантів вирішення зазначеної проблеми. Однак, термінали Starlink, у випадку їх виявлення, можуть стати мішенню для засобів ураження супротивника. Тому розгляд демаскуючих ознак та способів їх усунення є актуальною задачею. Розглянемо варіанти прихованого застосування обладнання Starlink з урахуванням візуального, радіоелектронного та інфрачервоного маскування.

Візуальне маскування. В комплект обладнання Starlink входить приймально-передавальна антена з розмірами від 50 см в довжину, що доволі легко виявляються засобами фото-відео-розвідки. Для забезпечення прихованості слід використовувати засоби маскування (сітка, тканина тощо). Крім того доцільно розміщувати термінал якнайдалі від місця використання використовуючи адаптер PoE, до якого можна під’єднати до 100 метрів кабелю витої пари для організації віддаленого робочого місця оператора.

Радіомаскування. Діаграма спрямованості антени терміналу Starlink окрім головного променя містить і додаткові бічні пелюстки, що відноситься до демаскуючих ознак і дає можливість виявити станцію та визначити геолокацію конкретного терміналу. У випадку розміщення антени в такому положенні, в якому фізичні перешкоди або рельєф місцевості блокуватимуть горизонтальні радіочастотні сигнали є можливість суттєво знизити радіоелектронну помітність терміналу. Під час відсутності сеансу зв’язку необхідно, вимикати живлення, для запобігання передачі радіочастотної енергії через особливості функціонування терміналу. Також, при можливості, слід якомога частіше змінювати місце розташування терміналу для ускладнення його геолокації.

Комплект Starlink можна використовувати як точку доступу до Інтернету за технологією Wi-Fi, сигнал якого, на відкритій місцевості може розповсюджуватись на значну відстань і може бути виявлений. Для боротьби з такими проявами Wi-Fi роутер слід розташовувати всередині металевого корпуса техніки (наприклад, бронеоб’єкта або причепа кунга) або заглиблених приміщеннях чи окопах, що значно ослабляють радіовипромінювання.

Комплектний Wi-Fi роутер від Starlink при роботі передає унікальний ідентифікатор (MAC-адресу), який вказує на виробника обладнання. Тому замість роутера Starlink, що йде в комплекті, слід використовувати роутер будь-якого іншого поширеного виробника. Це дозволить приховати факт застосування обладнання Starlink.

Маскування від інфрачервоного випромінювання. В терміналі Starlink передбачено спеціальна функція захисту від налипання снігу та зледеніння антени шляхом її підігріву. В той же час підвищена температура, навіть при застосуванні маскувальної сітки є потужною демаскувальною ознакою в інфрачервоному діапазоні, і сучасні засоби розвідки з використанням тепловізорів дозволяють їх виявити. Для приховання обладнання слід в застосунку Starlink вимкнути опцію Snow Melt, (підігрів від снігу), завдяки цьому зменшиться теплове випромінювання і помітність для тепловізорів.

Таким чином, виконання визначених рекомендацій дозволить суттєво зменшити вірогідність виявлення супротивником застосування терміналів Starlink і як наслідок зберегти особовий склад та забезпечити виконання завдань.

УДК 621.39

Василишин В.І., начальник кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, доктор технічних наук, професор

Лучен О.І., курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба

Василишин К.В., аспірант Харківського національного університету радіоелектроніки

АНАЛІЗ ШЛЯХІВ ВДОСКОНАЛЕННЯ LINK-16

На сьогоднішній день в країнах-членах NATO з метою забезпечення управління військами (C2 - Command and Control) активного застосування знаходять тактичні мережі обміну даних TADIL (Tactical Digital Information Link). Прикладом таких мереж яких є Link 16, визначеної в STANAG 5516 Ed.4. Забезпечення множинного доступу користувачів в такій системі здійснюється з використанням часового розподілу каналів TDMA (Time Division Multiple Access).

В межах багатофункціональної системи розподілу інформації (MIDS-Multifunctional Information Distribution System) Link 16 визначений одним з цифрових сервісів, який забезпечує передачу зображень, мовної інформації та повідомлень. Окрім TDMA в такій мережі використовується технологія псевдовипадкової перебудови робочої частоти (ППРЧ), яка забезпечує завадозахищеність мережі. Остання знайшла широке застосування в радіостанціях L3Harris, Aselsan та інших. Відомі приклади використання такої технології в радіостанціях рф та в деяких вітчизняних радіостанціях.

Аналіз технічної літератури щодо Link-16 вказує на те, що дана мережа не повністю задовольняє вимогам до швидкості передачі даних, а саме передачі відеозображень високої чіткості, що є актуальним для ряду військових додатків. Тому актуальним є пошук шляхів щодо підвищення швидкості передачі даних в Link-16 з урахуванням наявної технології ППРЧ та сучасних комунікаційних технологій. Одним із підходів щодо вирішення такого завдання для інших комунікаційних систем є використання сучасних комунікаційних технологій, а саме ортогонального дискретного частотного мультиплексування (OFDM) та інших. Відомі приклади комбінованого використання технологій OFDM та ППРЧ для цифрових систем зв'язку.

Серед дослідників такого завдання слід вказати В. Слюсаря, який запропонував варіант удосконаленого способу передачі даних на основі комбінування технологій ППРЧ і OFDM на фізичному рівні протоколу Link-16. В цьому випадку стрибок за частотою здійснюється одночасно для всіх піднесучих із сукупності піднесучих, що формується. При цьому рознесення піднесучих у відповідності до принципів OFDM зберігають ортогональним. Стрибок за частотою може здійснюватися на певний (довільний) інтервал, який визначається у відповідності до варіанту алгоритму зміни (перебудови) частоти.

З метою порівняльного аналізу системи передавання інформації з ППРЧ та такої ж системи з додатковим використанням OFDM було проведене імітаційне моделювання. Швидкість псевдовипадкової перебудови частоти обиралася близькою до швидкості, що використана в Link-16. Число піднесучих приймалося рівним 12. Стрибки за частотою здійснювалися відносно центральної частоти сукупності піднесучих та виконувалися умови ортогональності піднесучих за частотою. Результати моделювання підтверджують підвищення швидкості передачі інформації при комбінованому використанні двох технологій.

До напрямків подальших досліджень слід віднести використання відомих модифікацій технології OFDM, кодування пакету даних, що формується при використанні OFDM, сучасних підходів по вдосконаленню класичних варіантів ППРЧ (а саме, врахування стану каналу зв'язку, величини імовірності бітової помилки і т.д.) та відомих варіантів ППРЧ, що використовуються в засобах радіозв'язку.

УДК 621.396.946:004.722.45

Коломійцев О.В., професор кафедри Національного технічного університету «Харківський політехнічний інститут», доктор технічних наук, професор, Заслужений винахідник України
Цебрюк І.В., доцент кафедри Національної академії національної гвардії України, кандидат технічних наук, доцент, полковник
Рудаков І.С., аспірант кафедри Національного технічного університету «Харківський політехнічний інститут»
Бєсова А.О., студентка кафедри Національного технічного університету «Харківський політехнічний інститут»
Коломійцев В.О., студент кафедри Національного технічного університету «Харківський політехнічний інститут»

ПРОПОЗИЦІЇ ЩОДО ПІДВИЩЕННЯ БЕЗПЕКИ ПОЛЬОТІВ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В МІСЬКОМУ СЕРЕДОВИЩЕ

Згідно з визначенням Міжнародної асоціації безпілотних систем (UVS International), дрони є родовою конструкцією літака, яка працює без людського пілота на борту. Тому, безпілотне повітряне судно (безпілотний літальний апарат (БпЛА)) – це повітряне судно, що призначене для виконання польоту без пілота на борту, керування польотом якого і контроль за яким здійснюються за допомогою спеціальної станції керування, що розташована поза повітряним судном. До основних переваг БпЛА можна віднести їх порівняну дешевизну, швидкість розгортання та мобільність, що дає змогу вирішувати проблеми різного роду та характеру як у цивільній, так і у військовій сферах.

Сучасний розвиток інформаційних технологій призвів також до суттєвого підвищення якості цифрових камер та їх роздільної здатності. Тому, одним із напрямків щодо застосування БпЛА – є моніторинг міського середовища, де БпЛА використовуються для завдань, виконання яких пілотованою технікою (авіацією) з різних причин не доцільно. До таких завдань можна віднести наступні: моніторинг міської забудови (будівництво, стан будівель тощо) і пожежної небезпеки, термінова доставка вантажу у важко доступні місця та транспортування постраждалих тощо. Використання БпЛА дозволяє здійснювати швидкій збір даних, дає можливість виконувати зйомку у важко доступних і небезпечних місцях повністю у автоматизованому режимі тощо. В комплексі з БпЛА встановлене спеціальне програмне забезпечення, за допомогою якого виконується обробка отриманих в результаті зйомки даних, створюються 3D моделі, здійснюється підрахунок об’ємів, площ тощо. Однак, використання великої кількості та різних типів БпЛА, що керуються як дистанційно за командами оператора, так і автоматизовано за програмою, підвищує рівень небезпеки польотів. Таким чином, розробка пропозицій щодо підвищення безпеки польотів БПЛА в міському середовищі – є актуальною науковою задачею.

В доповіді розглянути типи БпЛА, що використовуються для моніторингу міського середовища, а також їх основні засоби щодо застосування (поодиноке, групове та змішане). Висвітлено основні задачі, які пов’язані з БпЛА – розгортання і керування групою (роєм) БпЛА, а також – передача даних (інформації) та втрата контролю над БпЛА (системи навігації та зв’язку). Представлено аналіз сучасних підходів і тенденцій щодо розвитку бортових систем навігації (БСН). Доведено, що основним шляхом підвищення функціональної ефективності БСН є надання їм властивості автономності шляхом застосуванням інтелектуальних технологій аналізу даних на основі машинного навчання та розпізнавання образів. Показано, що більшість задач також можна вирішити за допомогою технологій штучного інтелекту, а саме машинного навчання (Machine Learning, ML).

Таким чином, використання технологій штучного інтелекту дасть змогу покращити якість системи навігації і зв’язку як між БпЛА, так і БпЛА з операторами (пунктами дистанційного керування (наземними станціями керування)) тощо, а тим самим – підвищити безпеку польотів БПЛА у міському середовищі.

УДК 623.441/443

Коломійцев О.В., професор кафедри Національного технічного університету «Харківський політехнічний інститут», доктор технічних наук, професор, Заслужений винахідник України
Третяк В.Ф., науковий співробітник наукового центру Повітряних Сил Харківського Національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент, старший науковий співробітник
Цебрюк І.В., доцент кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент, полковник
Рибальченко А.О., аспірантка кафедри Національного технічного університету «Харківський політехнічний інститут»
Любченко О.В., аспірант кафедри Національного технічного університету «Харківський політехнічний інститут»

ПРОПОЗИЦІЇ ЩОДО ВІДСІКАННЯ БЕЗПЕРСПЕКТИВНИХ ВАРІАНТІВ ДЛЯ ЗАДАЧ ЦІЛОЧИСЕЛЬНОГО ЛІНІЙНОГО ПРОГРАМУВАННЯ З БУЛЕВИМИ ЗМІННИМИ

Відомо, що в автоматизованих інформаційно-управляючих системах (АІУС) одне із головних місць займають бази даних (БД), від якості побудови котрих залежить ефективність інформаційних систем (різного призначення), що розробляються. Для підвищення продуктивності розподілених додатків, що працюють з БД, необхідні ефективні методи проектування розподілених БД (РБД) та оптимізації їх структури.

Одним із недоліків АІУС є зниження продуктивності розподілених додатків при зростанні навантаження (збільшення кількості користувачів), накопиченні інформації за тривалий час, а також висока фрагментація збережених даних, яка характерна для транзакційних систем (ТС). Такий недолік є критичним для ринку OLTP-рішень, які призначені для введення, структурного зберігання та обробки інформації (даних) у режимі реального часу. Також, у них суттєво обмежені можливості виконання таких функцій, як формування бухгалтерської та аналітичної звітності в різних розрізах та з різною глибиною деталізації. Існуючим вирішенням даної проблематики є те, що компанії, які надають послуги, змушені купувати дороге обладнання, проводити його налаштування та постійно користуватися послугами високооплачуваних фахівців.

Таким чином, як базову архітектуру при розробці білінгових OLTP-систем пропонується використовувати хмарну технологію, яка дозволить замінити великі капітальні витрати на реалізацію даної системи операційними. Основна ідея даного підходу полягає у перенесенні обчислень, обробки та зберіганні даних значною мірою з персональних комп'ютерів (ПК) на сервери мережі Інтернет. Отже, актуальним завданням є оптимальне розподілення даних у хмарі, що дозволить значно скоротити витрати та підвищити швидкість роботи OLTP-системи.

В доповіді показано, що у більшості випадків OLTP-системи будуються без урахування критеріїв ефективності та з великим запасом масштабування. Висвітлено проблематику оптимізації структури РБД для хмарних OLTP-систем. Розглянуто мережу з довільною топологією (хмара), яка з'єднує вузли (сервери) і локальну обчислювальну мережу з регулярною структурою, усі ПК яких мають доступ до цієї мережі з довільною топологією, де БД розподілена по вузлах хмари. Запропоновано метод відсікання безперспективних варіантів для задач цілочисельного лінійного програмування з булевими змінними з використанням рангового підходу. В основу методу покладено множину стратегій, застосування яких до узагальненої процедури приведе до розробки алгоритмів рішення даної задачі, що дозволить отримати різні модифікації процедури залежно від комбінацій використовуваних правил відсікання безперспективних шляхів у множинах на основі застосування принципу оптимізації за напрямком.

УДК 623.746.2

Споришев К.О., докторант докторантури та ад'юнктури Національної академії Національної гвардії України, кандидат технічних наук, доцент
Самойленко В. М., ад'юнкт докторантури та ад'юнктури Національної академії Національної гвардії України

МЕТОД ПОЗИЦІЮВАННЯ БПЛА В УМОВАХ ВІДСУТНОСТІ GPS СИГНАЛУ ШЛЯХОМ ПОРІВЯННЯ ПОТОЧНОГО ТА ЕТАЛОННОГО ЗОБРАЖЕННЯ У ВЕКТОРНИХ ФОРМАТАХ

В умовах сучасної війни Україні проти російської агресії використання безпілотних літальних апаратів (БпЛА) у військовій сфері набуває особливої актуальності. БпЛА стали невід'ємною частиною сучасних бойових дій, про що свідчить Указ Президента України №51/2024 «Про нарощування спроможностей сил оборони».

Ефективність їх використання безпосередньо залежить від точності та надійності систем навігації, що робить розробку та удосконалення таких систем одним із ключових напрямків у підвищенні бойових можливостей. Традиційно сучасні методи навігації БпЛА стикаються з рядом викликів: перешкоди для GPS-навігації, висока динаміка, необхідність у прихованому переміщенні та високі вимоги до точності та швидкості реакції є основними проблемами, які потребують розв'язання. Як правило, навігація автономних БпЛА здійснюється за допомогою систем бортової інерційної навігаційної системи (БІНС) сумісно із системами GPS або оптико-електронною системою навігації, що дозволяє забезпечити високу точність позиціонування. Однак, в умовах бойових дій сигнали GPS можуть бути заглушені, що робить таку навігацію ненадійною.

Сучасні автономні БпЛА, що працюють на основі оптико-електронної системи навігації, використовують растрові зображення. Існуючі методи мають обмежену масштабованість і їх якість погіршується при збільшенні, що ускладнює точне порівняння з еталонними зображеннями. Це вимагає значного об'єму пам'яті для зберігання високодеталізованих зображень, і їх якість сильно залежить від умов зйомки, що може спотворити дані при порівнянні. Втрата важливих деталей при зменшенні якості зображень та зміни умов зйомки (освітлення, погодні умови, час доби, сезонні зміни, перспектива зйомки) може ускладнити автономне порівняння зображень.

Одним із методів вирішення цієї проблеми є використання методів порівняння векторних зображень. Зокрема, акцент робиться на методах порівняння рядків розмітки формату SVG. Розробка методу позиціонування БПЛА в умовах відсутності GPS-сигналу базується на порівнянні поточного та еталонного зображень у векторних форматах. Такий підхід передбачає аналіз рядків формату SVG, що дозволяє порівнювати рядки поточного векторного зображення з еталонними векторними картами.

Основою методу є створення або використання вже існуючих векторних карт місцевості у форматі SVG. Ці карти відображають ландшафт, будівлі та інші об'єкти як векторні графіки, що дозволяє зберігати високу точність деталей при будь-якому масштабі. Векторні карти формують базу даних для подальшого порівняння із зображеннями, отриманими від БпЛА. Наступний крок полягає у перетворенні або аналізі зображень, отриманих з БпЛА, для їх подальшого порівняння з векторними картами. Це включає перетворення поточних зображень у векторний формат. Ключовим моментом є порівняння рядків отриманих векторних зображень з базовими векторними картами. Цей процес включає аналіз структурних та геометричних відмінностей між зображеннями, що дозволяє визначити точне місцеположення БпЛА відносно відомих об'єктів на карті.

Розроблення методу порівняння векторних зображень у форматі SVG дозволить зменшити час обробки порівняння поточного зображення з еталонним, що дозволить підвищити точність за рахунок збільшення перебору зображень.

УДК 623.6

Нікора І.В., викладач Харківського національного університету Повітряних Сил імені Івана Кожедуба
Говорун І.О., слухач факультету Харківського національного університету Повітряних Сил імені Івана Кожедуба

ПЕРЕВАГИ СХЕМИ ЛОКАЛЬНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ «MESH-ПРОТОКОЛУ» ДЛЯ АВТОМАТИЗАЦІЇ ПЕРЕДАЧІ ДАННИХ НА ПУНКТІ УПРАВЛІННЯ

В умовах російсько-української війни, особливо під час застосування противником засобів повітряного нападу, швидкість яких іноді досягає 5-6 махів, критично важливо швидко прийняти рішення та передати команди управління підпорядкованим нижче підрозділам ЗРВ, Авіації та РЕБ.

Одним з запропонованим методом вирішення проблеми швидкості передачі інформації є використання протоколу MESH – Wi – Fi. Як приклад бездротової мережі користувачі з бездротовим доступом можуть працювати ефективніше, ніж їхні колеги, що використовують дротові комп’ютерні мережі.

В даний час технологія бездротової мережі Wi – Fi є найбільш зручною для ситуацій, що вимагають швидкості та оперативності для користувача, а також простоти в користуванні та налаштуванні пристрою. Базовий спосіб фізичного підключення через дротову мережу може забирати багато часу, а також, крім цього створює проблеми для забезпечення підрозділів, що розташовані у сільській та гірський місцевості, або взагалі на важкодоступній місцевості.

Найбільш ефективно “MESH – Wi – Fi” показує себе коли його використовують мобільні вогневі групи або підрозділи на рухомих засобах що забезпечують охорону повітряного простору держави та знищують засоби повітряного нападу противника. Під’єднані до одної мережі такі підрозділи мають змогу отримувати команди управління набато швидше ніж якби вони фізично підключались до пристрою передачі інформації, що забезпечував зв’язок з командним пунктом управління.

Ось чому MESH–мережі є такою технологією, яка використовує прості, недорогі бездротові маршрутизатори, встановлені в будинках, для побудови бездротових мереж на основі громади без необхідності будь–якої фіксованої існуючої інфраструктури. Через що є актуальною для вивчення.

УДК 004.93

Стасєв Ю.В., професор кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, доктор технічних наук, професор
Гончаренко К.Г., слухач факультету Харківського національного університету Повітряних Сил імені Івана Кожедуба

МЕТОД ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ СКАНУВАННЯ РАЙДУЖНОЇ ОБОЛОНКИ ОКА

Забезпечення надійного захисту інформації в інформаційних системах від зростаючої загрози кібератак на сьогодення є однією з актуальних проблем, що потребує невідкладного її вирішення та вимагає багатостороннього підходу, включаючи надійні заходи кібербезпеки, регулярну оцінку ризиків та навчання користувачів з питань кібербезпеки. Вирішуючи цю проблему, основна увага була зосереджена на вдосконаленні методу автентифікації, спрямованому на ефективність обчислень, надійність, перевірку та мінімальний рівень помилкових спрацьовувань. Важливо, щоб захист і безпека інформації були комплексними, включаючи різноманітні захисні заходи, такі як апаратне, програмне забезпечення, фізичні та організаційні засоби захисту, що значно підвищить рівень безпеки інформаційних систем.

В доповіді авторами показано, що найбільш вразливими є системи, які використовують однофакторну автентифікацію на основі паролю. У цьому контексті інтерес розробників систем автентифікації спрямовано на біометрічні методи захисту. Зростаюча важливість біометрічних методів зумовлена вразливістю традиційних систем безпеки, яка часто призводить до частих порушень безпеки. Для визначення ефективності біометричних систем контролю доступу було прийнято математичну структуру, яка базується на оцінці двох ймовірнісних параметрів: помилка хибного доступу (ПХД) та помилка хибної відмови (ПХВ). Точка, в якій лінії перетинаються має назву: рівна частота помилок. Коли кількість помилкових прийомів зменшується, кількість помилкових відхилень зростатиме, і навпаки. Важливо зазначити, що на ПХВ і ПХД можуть впливати різні фактори, такі як якість біометричних даних, тип використовуваної біометричної модальності, процедура зіставлення та поріг безпеки, встановлений системою. Розроблено методику оцінки бажаного рівня безпеки та точності біометричної системи.

Встановлено, що при реалізації біометричних систем максимально допустимі значення ПХД знаходиться в діапазоні від 10^{-3} до 10^{-6} , а в системах з великою кількістю користувачі і високим рівнем безпеки допустимі значення – до 10^{-9}. При цьому значення ПХВ, коливається від 0,025 до 0,01, а в системах з великою кількістю користувачів це значення не повинно перевищувати 0,001–0,0001.

Авторами доводиться, що перспективним є використання методу двофакторної автентифікації на основі сканування райдужної оболонки ока (РОО) та пароля. Унікальність візерунків райдужки додає рівень безпеки, який важко відтворити. На відміну від паролів, які можна забути, сканування РОО за своєю суттю пов’язане з особою та забезпечує надійний біометричний ідентифікатор, що ускладнює задачу противникам видати себе за дійсних користувачів системи.

Авторами обґрунтовано необхідність застосування двохфакторного методу автентифікації, а також, доведено, що впровадження даного методу значно посилить захист інформації, ефективно захистить систему від різних кіберзагроз і знизить ризик викрадення даних противником на 2-3 порядки. Крім того, включення сканування РОО разом із автентифікацією за допомогою пароля може створити додатковий рівень безпеки.

УДК 004.22

Королюк Н.О., професор кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент
Зенова Є.С., слухач факультету Харківського національного університету Повітряних Сил імені Івана Кожедуба

ОСОБЛИВОСТІ ПЛАНУВАННЯ РОЗВІДУВАЛЬНОГО ПОЛЬОТУ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ

Аналіз досвіду ведення бойових дій на території України свідчить, що вдосконалення розвідки, зокрема, повітряної, у теперішній час є одним з важливих завдань у процесі створення ефективної системи розвідки Збройних Сил України відповідно до стандартів НАТО. Планування повітряної розвідки за допомогою безпілотного літального апарату є складним завданням, що потребує проведення складних розрахунків для побудови маршрутів. У цьому контексті необхідно врахувати різноманітні чинники: характер майбутнього бою; умови проведення розвідки; вплив зовнішнього середовища (метеоумови, рельєф) на дальність польоту безпілотного літального апарату; вплив системи протиповітряної оборони противника тощо.

Наявність великих потенційних можливостей безпілотного літального апарату не гарантує досягнення заданої ефективності розвідки. Її підвищення може бути досягнуто шляхом інтелектуального прогнозування поведінки противника, врахуванням впливу факторів зовнішнього середовища, знань і досвіду операторів під час управління безпілотним літальним апаратом. Досвід бойового застосування безпілотним літальним апаратом у ході виконання розвідувальних завдань виявив проблемні питання у прийнятті обґрунтованого рішення щодо вибору набору параметрів для здійснення польоту і побудови доцільного маршруту

Таким чином, динамічність і швидкоплинність бойових дій, невизначеність обстановки, часові обмеження вимагають підвищення рівня автоматизації вирішення завдань даного класу. Але автоматизація процесу вибору доцільного маршруту для виконання розвідувального завдання безпілотним літальним апаратом ускладнюється необхідністю врахування досвіду з їх застосування особами, які приймають рішення. Це обумовлює доцільність удосконалення спеціального математичного та програмного забезпечення шляхом формалізації власних знань, досвіду бойової роботи особами, які приймають рішення.

УДК 004.056

Шило С.Г., доцент кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент
Зільник М.О., слухач факультету Харківського національного університету Повітряних Сил імені Івана Кожедуба
Зільник С.Д., курсовий офіцер факультету Харківського національного університету Повітряних Сил імені Івана Кожедуба

КРИПТОСТІЙКА ФУНКЦІЯ ГЕШУВАННЯ ДЛЯ ПІДВИЩЕННЯ РІВНЯ ЦІЛІСНОСТІ ДАНИХ В КОМУНІКАЦІЙНІЙ СИСТЕМІ ПОВІТРЯНИХ СИЛ

Під час збройної агресії рф проти України безпека інформаційних ресурсів потребує надійного захисту. Однією з основних вимог до забезпечення інформаційної безпеки є цілісність інформації. Реалізація цієї вимоги на практиці, дозволяє забезпечити процес передачі конфіденційних даних без втручання, спотворення та розкрадання їх з боку зловмисників. У зв'язку з цим актуальним постає питання стосовно забезпечення гарантованої цілісності комунікаційних мереж спеціального призначення.

До найбільш ефективних шляхів вирішення вищезазначеного питання відноситься використання геш-функцій, що включають в себе множину логічних і математичних операцій. Геш-функції можна поділити на безліч алгоритмів, які відрізняються один від одного за своїми розмірами, кількістю ітерацій, безпекою, швидкістю і довжиною, але в підсумку кожна з них виконує поставлене перед нею завдання.

Незважаючи на широке застосування методів гешування на сучасному етапі розвитку комунікаційних систем, для них притаманні деякі недоліки. До основних слід віднести високу алгоритмічну складність, яка вимагає підвищені вимоги до обчислювальних потужностей. Це пов'язано з тим, що процес формування типової геш-функції включає в себе велику кількість складних математичних конструкцій.

Тому важливим є пошук нових підходів до формування геш-функцій з точки зору можливості практичної реалізації властивостей, які вони демонструють. У сучасних комунікаційних системах для підвищення рівня інформаційної безпеки, з точки зору забезпечення цілісності інформаційних ресурсів, широко використовується методика розпаралелювання геш-функцій, у якості прикладу можна навести використання SHA та MD5. Сутність цієї методики полягає у розбитті певним оптимальним способом вхідного повідомлення на частини, які обчислюються паралельно.

Застосування такого підходу до геш-функції "Купина" передбачає розбиття блоків інформації на складові однакової довжини. Відмінними рисами цього підходу є швидкість обчислень та використання більшої кількості аргументів функції. Це дозволяє досягнути потрібних значень показників ефективності, оскільки виникає можливість маніпулювати окремими аргументами в процесі формування геш-функцій, а в підсумку проводити більш швидкі перетворення з незначними вихідними спотвореннями, які не впливають суттєво на якість процесу забезпечення цілісності даних в комунікаційних систем.

УДК 004.056.53

Стасєв Ю.В., професор кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, доктор технічних наук, професор

Козюберда К.В., слухач магістратури Харківського національного університету Повітряних Сил імені Івана Кожедуба

АНАЛІЗ МЕТОДІВ СТЕГАНОГРАФІЧНОГО ПЕРЕТВОРЕННЯ В КОНТЕЙНЕРАХ ДЛЯ ПЕРЕДАЧІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Існуючі методи стеганографії, які використовують в якості контейнера цифрове зображення, за типом використовуваної надлишковості діляться на групи, які враховують психовізуальну, структурну, ймовірносно-статистичну і комбінаторну надлишковість. Стеганографічне вбудовування, на основі психовізуальної надлишковості викликане нечутливістю зорової системи людини до деяких видів спотворень цифрового зображення та може використовуватись для передачі конфіденційної інформації. Авторами пропонується розглянути найбільш відомі та вживані методи такі як : метод заміни молодших біт, широкосмугові методи та статистичні методи.

Проаналізовано, що класичним методом є метод заміни молодших біт (LSB-метод). Він базується на тому, що молодші розряди графічних, аудіо і відео форматів, які несуть мало інформації і їх зміна практично не позначається на якості переданого зображення або звуку. Це дає можливість використання їх для кодування конфіденційної інформації.

Суть широкосмугових методів полягає в розширенні смуги частот сигналу, до ширини спектру, значно більшої ніж це необхідно для передачі реальної інформації. Для розширення діапазону існують два способи: метод прямого розширення спектру, за допомогою псевдо–випадкової послідовності, і метод стрибкоподібного переналаштування частоти. При цьому корисна інформація розподіляється по всьому діапазону, тому при втраті сигналу в деяких смугах частот в інших смугах залишається достатньо інформації для її відновлення.

Відомо, що статистичні методи приховують інформацію шляхом зміни деяких статистичних властивостей зображення. Даний метод забезпечує високу стійкість до операцій цифрової обробки, та важкість виявлення прихованих даних без відповідного секретного ключа.

Таким чином авторами зроблено висновки, що надійність методів заміни в просторовій області залежить від рівня частотних спотворень контейнера. Разом з тим вони забезпечують високу швидкодію і значний обсяг вбудованих даних, тому їх доцільно використовувати при передачі повідомлень як в основний так і в резервний спосіб обміну конфіденційної інформації.

Методи, що діють в частотній області є стійкішими до спотворень та операцій цифрової обробки, але можуть приховати менший об’єм даних. Наявність секретного ключа у широкосмугових та статистичних методах, що використовують псевдовипадкове кодування, підвищує їх надійність. А розподіл прихованих біт по всьому контейнері зумовлює високу стійкість до випадкових та умисних спотворень, що враховується при побудові цифрових водних знаків.

УДК 621.396.99

Стасєв Ю.В., професор кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, доктор технічних наук, професор

Козюберда М.Р., слухач Харківського національного університету Повітряних Сил імені Івана Кожедуба

Непокритов Д.М., доцент кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

БЕЗПЕКА ІНФОРМАЦІЇ КАНАЛУ УПРАВЛІННЯ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ

Безпілотні літальні апарати (БПЛА) стали невід'ємною складовою сучасних бойових дій та операцій. Їх застосування зменшує ризик втрати особового складу та техніки, підвищує шанси виконання завдання розвідки та знищення противника. Але це можливо за умови забезпечення безпеки інформації, що передається каналом управління БПЛА з необхідною ймовірністю.

Рішення проблеми безпеки інформації, що передається в системах зв'язку та управління, пов'язане з проблемами імітостійкості та перешкодозахищеності. Досліди показують, що ці проблеми вирішуються окремо один від одного. Авторами розглядається актуальні напрямки забезпечення імітостійкості каналу управління безпілотним літальним апаратом. Приводяться результати аналізу методів побудови складних сигналів та визначено один з перспективних напрямків досягнення даної мети за допомогою алгоритмів іміто-захищеності на дискретному рівні та на рівні складних сигналів. Визначено, що при реалізації динамічного режиму функціонування досягається виграш на 4-5 порядків у порівнянні з характеристичними послідовностями й на 5-6 порядків у порівнянні з лінійними рекурентними послідовностями максимального періоду. В основі даного методу лежить формування складних сигналів, в якому досягається потрібного рівня імовірності нав'язування хибної команди управління. Запропоновано ефективні алгоритми застосування складних сигналів, які дозволяють підвищити імітостійкість і перешкодозахищеність радіосистем управління й зв'язку на фізичному рівні.

Проблема перешкодозахищеності вирішується за рахунок збільшення енергетичних ресурсів каналу управління, або за рахунок застосування на фізичному рівні складних сигналів з частотною надлишковістю. Показано, що необхідний рівень імітостійкості та ймовірність прийому/передачі інформації в системах управління можливо досягти за допомогою реалізації динамічної передачі сигналів, при якій відповідне "інформаційне повідомлення – сигнал управління" змінюється в часі за псевдовипадковим законом.

Реалізація режиму динамічної зміни сигналів дозволяє на фізичному рівні вирішити проблему захисту від несанкціонованого доступу до каналу управління, а також забезпечити достатню скритність змісту повідомлення, що передається. Крім того, реалізація режиму динамічної передачі сигналів забезпечує активну систему імітозахисту, при якій імітовані сигнали отримані абонентом визначається як перешкода.

Показано, що для забезпечення необхідних імовірно-часових характеристик радіолінії управління необхідно прийняти цілий комплекс заходів, спрямованих на досягнення заданих значень імітостійкості каналу управління, а також забезпечити необхідний доступ переданих по каналу інформації та команд управління об'єктами, що запобігає витік інформації і обмежує доступ до енергетичних ресурсів суміщеної радіолінії.

УДК 004.91

Басараб О.К., викладач кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького, кандидат технічних наук, доцент

ЩОДО РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АВТОМАТИЗАЦІЇ СТВОРЕННЯ КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

В Державній прикордонній службі України, як і в будь-якому правоохоронному органі держави інтенсивно створюються, та функціонують інформаційно-комунікаційні системи спеціального призначення. В таких системах циркулює інформація з обмеженим доступом. До прикладу, інформаційно-комунікаційна система прикордонного контролю «Гарт-1» містить конфіденційну інформацію, а саме: персональні дані осіб, що перетинають державний кордон, інформацію щодо осіб яким заборонено в'їзд, або тимчасово обмежений виїзд з України, інформацію, щодо осіб, відносно яких отримані доручення правоохоронних органів, індекс доручення тощо. Така інформація має бути захищена від несанкціонованого доступу, тому обробляється на об'єктах інформаційної діяльності, на яких розгорнуті та застосовуються комплексні системи захисту інформації, одним з основних елементів яких є комплекс технічного захисту інформації. І це є обов'язковою умовою для обробки інформації з обмеженим доступом.

Водночас, створення комплексної систем захисту інформації та комплексу технічного захисту інформації – це складні процеси, які вимагають від виконавця не тільки знань та вмінь визначити напрямки та засоби захисту інформації на об'єктах інформаційної діяльності (далі – ОІД), але й розробити та опрацювати чималу кількість супутньої документації, що визначена керівними документами.

Виходячи з аналізу документів, що розробляються під час створення комплексної системи захисту інформації, в цілому, та комплексу технічного захисту інформації, зокрема, а також враховуючи те, що розробкою можуть займатися різні підрозділи, цілком ймовірна ситуація, коли моделі загроз та порушника, а також деякі інші документи на один об'єкт інформаційної діяльності можуть давати різні показники та/або результати проведених досліджень. Така ситуація неприпустима, коли справа стосується охорони державної таємниці або іншої конфіденційної інформації, що підлягає захисту з боку держави.

Для вирішення даної проблеми нами запропоновано розробка програмного забезпечення, яке автоматизує процес документального супроводу створення комплексної системи захисту інформації та комплексу технічного захисту інформації. Ідея розробки даного програмного забезпечення полягає в тому, що авторський програмний продукт надає можливість вносити результати вивчення зовнішнього середовища, в якому функціонує об'єкт інформаційної діяльності, обстеження безпосередньо самого об'єкту, результати аналізу та вивчення основних та допоміжних технічних засобів, що встановлено на об'єктах інформаційної діяльності, результати спеціальних досліджень на наявність технічних каналів витоку інформації та інша інформація, яка потрібна для розробки пакету документів на створення комплексної системи захисту інформації та комплексу технічного захисту інформації. Водночас, в програмному забезпеченні створені шаблони формалізованих документів, які входять в зазначений пакет документації. В результаті роботи, програма на основі формалізованих шаблонів створює документи на конкретний обраний об'єкт інформаційної діяльності з використанням раніше внесених результатів обстежень, аналізів, досліджень тощо.

В перспективі, застосування системи управління базою даних MySQL дозволить наростити програмне забезпечення та розширити його можливості з точки зору використання в мережевому просторі з декількох клієнтських автоматизованих робочих місць.

УДК 004.75

Бабарика А. О., доцент кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького, доктор філософії
Катеринчук І. С., професор кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького, доктор технічних наук, професор

ДОСЛІДЖЕННЯ КОНЦЕПЦІЙ ХМАРНИХ ТА ПОСТХМАРНИХ ОБЧИСЛЕНЬ КОНЦЕПЦІЙ ЯК ОСНОВИ ДЛЯ РОЗБУДОВИ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

Рівень розвитку технологій призвів до того, що сучасні системи відеоспостереження розглядаються не як окремо розгорнуті замкнуті системи, які виконують лише функцію перегляду обстановки з камер відеоспостереження та фіксацію цих даних на носії інформації.

Сучасні інтелектуальні системи відеоспостереження розглядаються як складні системи, які не обмежуються територіально, є обчислювальними системами, які не лише фіксують інформацію з камер відеоспостереження, але і мають змогу проводити аналіз цієї інформації.

Ключовим напрямком розвитку інтелектуальних систем відеоспостереження стала концепція розвитку розумних міст та інтернету речей. Ряд наукових досліджень присвячено проблематиці комплексного застосування різнорідних технологій для вирішення задач вищевказаних концепцій. Одним з проблемних питань є вдосконалення технологій розподіленої обробки даних.

Концепція інтернету речей має вагомий вплив на технології побудови інтелектуальних систем відеоспостереження. Розгорнуті системи відеоспостереження Державної прикордонної служби України (ДПСУ) дають можливість здійснювати спостереження за визначеними об’єктами в режимі реального часу, здійснювати запис інформації з камер відеоспостереження у випадку виявлення руху в секторі огляду, цілодобовий запис чи за визначеним розкладом, пошук відеофайлів у відеоархіві за датою та часом події по визначеному відеоканалу.

В умовах сьогодення відбувається поступова модернізація розгорнутих систем відеоспостереження. В результаті проведених заходів поступово впроваджуються алгоритми відеоаналітики (виявлення рухомих об’єктів, виявлення задимлених ділянок, виявлення підозрілої активності, ідентифікація осіб за зображенням обличчя тощо).

Системи відеоспостереження ДПСУ широко впроваджуються при охороні протяжних ділянок кордону, при цьому активно застосовуються як нерухомі так і рухомі камери відеоспостереження (PTZ). Спостереження за ділянками кордону здійснюється і з використанням безпілотних літальних апаратів. При модернізації існуючих систем відеоспостереження постає ряд проблемних напрямків, одним з яких є необхідність обробки великих обсягів інформації з територіально розподілених датчиків. Такими датчиками можна розглядати як окремі камери відеоспостереження, БПЛА, так і окремі сегменти системи.

Вирішення вказаних напрямків потребує дослідження існуючих технологій розподілених обчислень. Застосування хмарних технологій у системах відеоспостереження ДПСУ дасть змогу вирішити проблему гнучкості та масштабованості систем.

Також, завдяки хмарним сервісам, визначені користувачі можуть отримати доступ до відеопотоку з будь-якого пристрою з доступом до відомчої Інтранет мережі ДПСУ, що дозволяє віддалено контролювати об'єкти спостереження.

Хмарні рішення забезпечують автоматичне резервне копіювання даних, захист від втрати інформації та доступ до неї в разі виникнення непередбачених ситуацій (наприклад, збоїв в системі).

Застосування хмарних технологій дозволяє використовувати потужні алгоритми машинного навчання та штучного інтелекту для аналізу відеопотоків у реальному часі, що поліпшує можливості виявлення подій та вирішення проблем безпеки.

Проблеми, що постали перед інтелектуальними системами відеоспостереження на сучасному етапі частково вирішуються використанням хмарних архітектур побудови таких систем. Проте такі архітектури також мають певні недоліки. Для їх усунення дослідники вдало імплементували таке рішення як FOG обчислення. Системи, побудовані по цій архітектурі

відповідають вимогам масштабованості, безпеки, пропускної здатності та швидкості обробки даних. При цьому, системи відеоспостереження функціонують не як самостійні системи, а інтегруються до більш складних комплексних систем, таких як розумні міста та комплексних систем безпеки. Для зменшення затримок в обчисленнях та підвищення рівня автономності систем дослідниками було розроблено концепції Edge, та Mist обчислень.

Тому, враховуючи широкі можливості хмарних та постхмарних концепцій, актуальною задачею є проведення їх порівняльного дослідження з метою подальшого застосування при розбудові інтелектуальних систем відеоспостереження ДПСУ.

УДК 621.39

Городиський Р. О., старший викладач кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького
Ваврічен О. А., старший викладач кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького

ЗАХИСТ ІНФОРМАЦІЇ В СУЧАСНИХ ЗАСОБАХ РАДІОЗВ'ЯЗКУ

За останні роки система захисту інформації, яка передається радіозв'язком у всьому світі зазнала значних змін. На теперішній час, вона передбачає як проектування та розробку нових методів захисту інформації в сучасних засобах радіозв'язку, так і вдосконалення та модернізацію існуючих. На початку гібридної війни на сході України та на момент повномасштабного вторгнення росії в Україну, Збройні сили України були оснащені застарілими засобами радіозв'язку, які виявилися неефективними в умовах бойових дій та застосовувалися відомі ворогу методи захисту інформації, що передавалися саме такими засобами зв'язку. Однак, часу на розробку нової техніки радіозв'язку не було в Україні, тому Збройні сили України були оснащені цивільним телекомунікаційним обладнанням, яке зарекомендувало себе, але ще не відповідало високого стандартам захисту інформації які передаються засобами радіозв'язку. Наприклад, використання цивільних засобів радіозв'язку в складних погодних умовах перешкоджало передавати інформацію без її перехоплення ворогом, не було можливість протидії застосування засобів радіоелектронної боротьби та радіоелектронної розвідки противника. Незважаючи на ці недоліки, технології передачі даних радіозв'язком, які використовують комерційні компанії, широко використовуються у військовій сфері діяльності. При цьому, згодом, за допомогою західних партнерів Україні почали надавати сучасні і модифіковані засоби радіозв'язку, які відповідають високим стандартам захисту інформації, яка буде передаватися такими приладами.

Одним з ефективних шляхів забезпечення завадозахищеності сучасних засобів радіозв'язку в умовах впливу навмисних або ненавмисних завад є застосування сигналів з розширеним спектром: шумоподібних сигналів, сигналів з псевдовипадковим переналаштуванням робочих частот, псевдовипадковим переналаштуванням часу і їх комбінацій.

Однією з основних характеристик систем радіозв'язку є завадозахищеність, складовими якої є завадостійкість і скритність.

Підходами щодо захисту інформації під час передачі по відкритим каналам зв'язку для запобігання перехоплення інформації, її пошкодження є комбінування методів (засобів) криптографічного та стеганографічного захисту інформації.

Найбільш поширеними і в більшості випадків ефективними є криптографічні методи та засоби захисту інформації - це методи шифрування, кодування або іншого перетворення інформації, в результаті якого її вміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення.

На теперішній час в Україні активно використовують комплексну систему захисту інформації (далі - КСЗІ) - це взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Невід'ємною складовою є радіоелектронний захист, який організовується і здійснюється для захисту своїх радіоелектронних засобів від розвідки, вогневого і радіоелектронного впливу противника, від взаємних завад. Заходи охоплюють, насамперед, всі види маскування випромінювань радіоелектронних засобів від радіорозвідки противника, захист від радіоперешкод і захист від ураження самонавідною зброєю противника.

Найбільше застосування для захисту від навмисних завад отримали сигнали із псевдовипадковою перебудовою робочої частоти (далі - ППРЧ). Технологія ППРЧ знайшла своє застосування майже у всіх сучасних військових засобах радіо-зв'язку різних виробників, таких як: «Harris» (до 1000 стр/с), «Aselsan» (до 1600 стр/с), «Elbit» (понад 200 стр/с).

Технічний захист інформації в сучасних засобах радіозв'язку є надзвичайно важливим, а особливо під час правового режиму воєнного стану, який діє в Україні з 24 лютого 2022 року, під час якого наша держава стикається з серйозними загрозами і викликами для своєї безпеки, та територіальної цілісності. У таких умовах правильне управління інформацією та її захист є ключовим елементом успішного забезпечення національної безпеки.

Отже на сьогодні забезпечення захисту інформації в засобах радіозв'язку це використання сукупності організаційно-правових заходів, інженерно-технічних, криптографічних та програмно-апаратних засобів.

УДК 621.391

Мул Д.А., доцент кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького, кандидат технічних наук, доцент
Прокопенко Є.В., заступник начальника зв'язку та інформаційних систем Національної академії Державної прикордонної служби України імені Богдана Хмельницького, кандидат технічних наук, доцент

ВПЛИВ КІБЕРАТАК НА ФУНКЦІОНУВАННЯ СУПУТНИКОВОГО ЗВ'ЯЗКУ

Супутниковий зв'язок є невід'ємною частиною системи зв'язку підрозділів Сил оборони України.

Більшість систем супутникового зв'язку має у своєму складі три складові частини: космічний сегмент; наземний сегмент; користувацький сегмент.

Космічний сегмент представляє собою один або декілька супутників-ретрансляторів. Також космічний сегмент може представляти собою сузір'я супутників-ретрансляторів.

Наземний сегмент представляє собою сукупність декількох елементів серед яких можна відзначити: центр запуску космічних об'єктів; центр управління супутниковими угрупуваннями; центр управління зв'язком; наземні станції (шлюзові станції).

Користувацький сегмент представляє собою сукупність комунікаційного обладнання, яке використовується безпосередньо користувачами системи супутникового зв'язку. Саме наземні станції здійснюють інтеграцію системи супутникового зв'язку з наземними комунікаційними системами і ресурсами.

Виходячи з аналізу принципів побудови більшості систем супутникового зв'язку, слід зауважити, що найбільш ймовірним для виникнення кіберзагроз сегментом цих систем є наземній сегмент і в-першу чергу наземні (шлюзові) станції.

У ніч з 23 на 24 лютого 2022 року російська військова розвідка провела операцію проти американської компанії Viasat, яка надає високошвидкісний широкосмуговий супутниковий доступ комерційним і військовим замовникам. Десятки тисяч терміналів компанії були пошкоджені. Українські військові використовували їх як резервний зв'язок, а головною метою російської операції було позбавити їх зв'язку – що підтвердили у спільній заяві ЄС, Великої Британії та США.

Кібератаки можуть мати значний вплив на функціонування супутникового зв'язку через кілька механізмів:

переривання сервісу (downtime). Кібератаки можуть спричинити переривання у роботі супутникових систем, що призведе до припинення зв'язку на певний час. Це може відбутися через заборону доступу до ключових систем керування супутниками або внаслідок пошкодження програмного забезпечення, яке керує супутниковими пристроями;

підробка даних (data manipulation). Кібератаки можуть змінювати або викрадати дані, які передаються через супутниковий зв'язок. Це може призвести до недостовірності або порушення конфіденційності інформації, що передається через цю систему;

відмова в обслуговуванні (denial of service - DoS). Кібератаки можуть спрямовуватися на перевантаження супутникових систем запитами, що призводить до їхнього відмову в обслуговуванні для законних користувачів;

видалене відключення (remote disablement). У разі успішної атаки зловмисники можуть намагатися відключити або пошкодити супутникові системи з віддаленої точки, що може призвести до тимчасового або постійного припинення їх роботи;

фізичні атаки через кіберкомпоненти. Оскільки супутникові системи використовують комп'ютери і мережеве з'єднання, їх можна атакувати через вразливості в програмному забезпеченні або фізично.

Ці види кібератак можуть мати серйозні наслідки для супутникового зв'язку, включаючи припинення роботи систем, втрату даних, порушення конфіденційності та інші негативні наслідки.

УДК: 004.056

Прокопенко Є. В., заступник начальника кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького, кандидат технічних наук, доцент
Мул Д. А., доцент кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького, кандидат технічних наук, доцент

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ПЛАНУВАННІ ПОЛІТИКИ БЕЗПЕКИ ДЛЯ ІНФОРМАЦІЇ ЩО ЦИРКУЛЮЄ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

В сучасному світі, де інформаційні технології швидко розвиваються, забезпечення безпеки інформації стає надзвичайно важливим завданням для державних органів, зокрема для прикордонних служб. Державна прикордонна служба України, як ключовий гравець у забезпеченні національної безпеки, має активно долучатись до впровадження технології штучного інтелекту в свої інформаційні системи з метою покращення планування політики безпеки для обробки та захисту інформації, що циркулює в їхніх системах.

Штучний інтелект дозволятиме Державній прикордонній службі здійснювати більш ефективний та точний аналіз інформації, отриманої з різних джерел, що допомагає вчасно реагувати на потенційні загрози та ризики. Ось кілька ключових аспектів застосування технологій штучного інтелекту в цьому контексті:

Аналітика даних та прогнозування. За допомогою алгоритмів машинного навчання та аналізу великого обсягу даних, інформаційна система прикордонної служби може виявляти патерни, тенденції та аномалії, що вказують на можливі загрози для безпеки. Це дозволяє приймати управлінські рішення на основі об'єктивних даних та прогнозувати можливі інциденти заздалегідь.

Виявлення та реагування на кіберзагрози. Штучний інтелект використовується для виявлення аномальних або підозрілих дій у мережі, які можуть вказувати на кібератаку або спробу несанкціонованого доступу. Це дозволяє реагувати негайно та уникнути серйозних наслідків для безпеки інформації та інфраструктури.

Моніторинг та управління ризиками. Інтелектуальні системи аналізують різноманітні джерела даних для ідентифікації потенційних загроз та оцінки рівня ризику. Це допомагає

розробляти стратегії управління ризиками та приймати превентивні заходи для зменшення імовірності інцидентів.

Забезпечення конфіденційності та інтегрітету даних. Технології штучного інтелекту використовуються для шифрування даних, контролю доступу та виявлення недостовірних або змінених даних, що допомагає забезпечити конфіденційність інформації та запобігти її порушенню.

Автоматизоване прийняття рішень. Інтелектуальні системи можуть бути налаштовані для автоматичного прийняття рішень на основі заданих правил та алгоритмів. Це дозволяє реагувати на загрози в реальному часі без затримок, що може врятувати час та ресурси.

Загалом, застосування технологій штучного інтелекту в плануванні політики безпеки для інформації, що циркулює в інформаційній системі Державної прикордонної служби України, є важливим кроком у напрямку покращення безпеки країни. Ці технології допомагають виявляти, аналізувати та реагувати на загрози швидко та ефективно, забезпечуючи захист національних інтересів. Важливо запроваджувати такі технологій з метою зміцнення безпекових заходів та забезпечення стабільності країни в умовах сучасних викликів і загроз.

УДК 005.2

Стрельбіцький М.А., викладач кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького, доктор технічних наук, професор

КОНЦЕПЦІЯ ОБРОБКИ «АГРЕГОВАНОЇ» ІНФОРМАЦІЇ

Аналіз керівних документів, які класифікують інформацію з обмеженим доступом, показав дозволив сегрегувати пункти класифікаторів на дві групи: перша група – які визначають ступінь обмеження доступу на підставі тільки змісту; друга група – такі, ступінь обмеження доступу яких збільшується в залежності від кількості інформації. В сучасних умовах рівень використання засобів автоматизованої обробки інформації з обмеженим доступом постійно зростає. Вищенаведене створює передумови до порушення конфіденційності інформації з обмеженим доступом які підпадають під правила другої групи класифікаторів. Причому, варто зауважити, що в інформаційно-комунікаційних системах при обробці такої інформації вимоги політики безпеки дотримуються. Вищенаведена обставина порушення конфіденційності інформації з обмеженим доступом стає можливою за умови збільшення кількості інформації другої групи класифікаторів, що в свою чергу призводить до неконтрольованого підвищення рівня обмеження доступу. Така ситуація притаманна окремим категоріям інформації у якої ступінь обмеження доступу підвищується залежно від її кількості. Для множин інформації такого типу пропонується дати визначення «агрегованої інформації».

Як приклад можна навести Звід відомостей, що становлять державну таємницю. Аналіз цього керівного документу показав наявність інформації «агрегованого» типу у кожному із розділів цього керівного документу. Наведемо умови порушення безпеки інформації, рівень конфіденційності якої залежить від кількості інформації. В структурі сучасних інформаційно-комунікаційних систем як правило присутній центральний вузол зберігання даних. Таким чином, постійне накопичення кількості інформації другої групи призведе до підвищення ступеня обмеження доступу, який може бути вищий за дозволений. Така обставина передбачає наявність двох можливих каналів прихованого витоку інформації з вузлів мережі без порушення встановленої політики безпеки інформаційно-комунікаційної системи. Перший канал – при проходженні інформації через вузол системи та другий – при тимчасовому зберіганні інформації на вузлі інформаційно-комунікаційної системи. З метою уникнення загрози конфіденційності інформації з обмеженим доступом пропонується запровадити такі протоколи обміну між вузлами інформаційно-комунікаційних систем, які б унеможливили теоретичну здатність до формування «критичного» обсягу такої сукупності інформації другого типу. Концептуально протокол обміну «агрегованої» інформації між вузлами мережі повинен передбачати використання контейнерів «агрегованої» інформації, які контролювали та забезпечували

формування інформації з вищим рівнем доступу на захищеному вузлі інформаційно-комунікаційної системи. Функціонал протоколу повинен складатись із трьох основних етапів: перший – формування контейнеру «агрегованої» інформації із визначенням кількості складових та адреси захищеного вузла фінального збереження даних; другий – заповнення контейнеру із контролем кількості даних; третій – фінальна збірка контейнера на захищеному вузлі інформаційно-комунікаційної системи. Ключовою ознакою розробленого протоколу обміну «агрегованої» інформації є виключення можливості формування блоку даних на вузлах інформаційно-комунікаційної системи рівень захищеності яких не відповідає рівню обмеження доступу об’єднаної («агрегованої») інформації.

УДК 621.396
Рачок Р.В., професор кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького, доктор технічних наук, професор
Хоптинський Р.П., доцент кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького, кандидат технічних наук

ЕКСПЕРИМЕНТАЛЬНЕ ВИЗНАЧЕННЯ ЙМОВІРНОСТІ НАЯВНОСТІ ЗВ'ЯЗКУ МІЖ ВУЗЛАМИ СЕНСОРНОЇ РАДІОМЕРЕЖІ

При охороні кордону в умовах сьогодення надзвичайно важливим є використання сучасних інженерних засобів і систем у яких застосовуються різноманітні датчики (датчики руху, сейсмічні датчики, камери спостереження тощо). Для отримання інформації від них можуть, зокрема, використовуватись сенсорні радіомережі. На сьогодні існує значна кількість різноманітних радіомодулів (наприклад NRF24L01) які можливо застосувати при побудові сенсорних радіомереж. Ці модулі достатньо зручно інтегруються з сучасними мікроконтролерами і можуть бути використані в конструкції різноманітного кінцевого обладнання. Однак при побудові сенсорних радіомереж надзвичайно важливо забезпечити їх подальше ефективне функціонування. В цьому контексті необхідно врахувати на якій максимальній дальності між вузлами сенсорної радіомережі буде забезпечуватись надійна передача даних.

Якщо використовувати детерміновану модель, з урахуванням потужності передавача, відомих характеристик антен і чутливості приймача можливо було би оцінити наявність або відсутність радіозв’язку в залежності від відстані між вузлами аналітично. Однак є значна кількість стохастичних факторів, які інколи суттєво можуть вплинути на досліджуваний процес. До них, зокрема, можна віднести: зміни погодних умов, вплив випадкового рельєфу місцевості, вплив перешкод та інші фактори. Тому пропонується методика експериментального визначення ймовірності наявності зв'язку між вузлами сенсорної радіомережі. В цій методиці комплекс усіх факторів, що впливають на дальність радіозв’язку, враховується опосередковано в ході статистичних випробовувань. Пропонується реалізувати передачу тестових повідомлень між вузлами радіомережі з контролем їх прийому. На невеликій відстані, звичайно, усі тестові повідомлення будуть прийняті. При збільшенням відстані до декого (наперед невідомого) значення кількість прийнятих повідомлень почне знижуватись (у дослідженні використовувалась передача у кожній серії 100 тестових повідомлень). Коли це зниження досягне критичного значення, відстань при якій це стається фіксується. Такі дослідження повторюються значну кількість разів в умовах впливу стохастичних факторів. На основі отриманої множини значень відстаней формується аналітичний вираз для обчислення ймовірності наявності зв’язку між вузлами сенсорної радіомережі в залежності від відстані між ними. Використання цього співвідношення дозволить в подальшому проводити раціональну побудову сенсорної радіомережі.

УДК 004.004.896

Табенський С.М., старший викладач кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького
Кожушко В.Ю., курсант факультету Національної академії Державної прикордонної служби України імені Богдана Хмельницького

ПОРІВНЯЛЬНИЙ АНАЛІЗ ІНСТРУМЕНТІВ МАШИННОГО НАВЧАННЯ МОДЕЛЕЙ ДЛЯ ВИРІШЕННЯ ЗАДАЧ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ОБ'ЄКТІВ

Автоматичне розпізнавання об'єктів є важливою задачею в області комп'ютерного зору, знань про відео та обробки зображень. Розпізнавання об'єктів відіграє ключову роль в широкому спектрі застосувань, включаючи автономні автомобілі, безпеку та багато іншого. Особливо активно ця технологія почала використовуватись, як метод автоматичного визначення цілей у воєнній сфері, з початком використання безпілотних літальних апаратів в якості засобів ураження та розвідки.

Завдяки зростанню доступності обчислювальних ресурсів та розвитку нових алгоритмів машинного навчання, виникає багато нових методів та безкоштовних інструментів для розв'язання цієї задачі.

TensorFlow є однією з найпопулярніших бібліотек машинного навчання, розробленою компанією Google. Вона надає гнучкість та широкий набір функцій для розробки та навчання різних моделей машинного навчання.

Серед переваг даного інструменту є гнучкість, що передбачає широкий набір інструментів для побудови різноманітних моделей машинного навчання та глибокого навчання, включаючи конволюційні нейронні мережі (CNN), рекурентні нейронні мережі (RNN) та автокодувальні мережі.

Проте використання цього інструменту передбачає ряд недоліків, а саме: складність, порівняно низька швидкодія та довгий час навчання на великих наборах даних.

PyTorch - це бібліотека машинного навчання розроблена компанією Facebook, яка спеціалізується на побудові та навчанні нейронних мереж. Вона відома своєю динамічною обчислювальною графікою, що робить розробку моделей зручною та інтуїтивно зрозумілою.

Головна особливість PyTorch - це його динамічна графіка обчислень. Відмінність полягає в тому, що у PyTorch граф обчислень формується безпосередньо під час виконання програми, що дозволяє змінювати структуру графа та відлагоджувати моделі у реальному часі. Ця особливість забезпечує більшу гнучкість та зручність при розробці та експериментах з нейронними мережами, оскільки розробники можуть легко маніпулювати обчислювальним графом, додаючи, видаляючи або змінюючи операції та шари моделі під час виконання.

Проте одним з основних недоліків PyTorch може бути його обмежена масштабованість у великих обчислювальних кластерах порівняно з іншими інструментами.

Teachable Machine - це безкоштовний онлайн-інструмент для машинного навчання, розроблений командою Google Creative Lab. Він призначений для створення моделей штучного інтелекту без необхідності в програмуванні або використання складних алгоритмів.

Teachable Machine надає можливість користувачам створювати моделі машинного навчання, які можуть класифікувати об'єкти на основі відео-, аудіо- або зображень, а також захоплювати деякі рухи. Він базується на технологіях машинного навчання, зокрема на нейронних мережах, але забезпечує простий та інтуїтивно зрозумілий інтерфейс для звичайних користувачів. Проте він характеризується обмеженим функціоналом та гнучкістю.

Окрім розглянутих інструментів є ряд інших технічних рішень для розв'язання задачі автоматичного розпізнавання об'єктів, серед яких Clarifai, Lobe, Keras та інші.

Проте вибір конкретного інструменту залежить від багатьох факторів, включаючи характеристики проекту, доступні ресурси, рівень користувача та власні уподобання.

УДК 654.01

Пархоменко М.В., доцент кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук
Черкасов В.С., слухач Харківського національного університету Повітряних Сил імені Івана Кожедуба
Коцур А.А., слухач Харківського національного університету Повітряних Сил імені Івана Кожедуба

АНАЛІЗ СУЧАСНИХ КРИПТОГРАФІЧНИХ ХЕШ-ФУНКЦІЙ ДЛЯ ЗАХИСТУ ДАНИХ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ МЕРЕЖІ ПОВІТРЯНИХ СИЛ

Необхідність розгляду та аналізу існуючих механізмів криптографічного захисту даних в інформаційно-комунікаційній мережі Повітряних Сил і їхньої вразливості перед сучасними атаками стає надзвичайно актуальною в контексті постійного розвитку технологій та зростаючої складності кіберзагроз. Особливу увагу потрібно звернути на особливості військового середовища, де інформаційна безпека є визначальним фактором для успішного виконання завдань. Урахування специфіки військового середовища, зокрема вимог до швидкості реакції та надійності, у процесі розробки та впровадження криптографічних заходів захисту є критично важливим. Підвищення рівня свідомості серед персоналу щодо кіберзагроз і відповідних заходів безпеки також має велике значення для успішного функціонування інформаційної системи Повітряних Сил.

Проведено більш глибокий аналіз існуючих криптографічних хеш-функцій, розроблених різними країнами, "Купина" (Україна), "SM3" (Китай) та "SHA-2" (США). Розглянуто ключові аспекти, що включають в себе використані алгоритми шифрування, системи ідентифікації та автентифікації, а також методи управління ключами. Зокрема, розглядається ефективність застосування симетричного та асиметричного шифрування в контексті інформаційної безпеки.

У результаті проведеного дослідження, виявлені основні закономірності і тенденції у сфері криптографічного захисту даних в інформаційно-комунікаційній мережі Повітряних Сил. "Купина" відзначається великими довжинами хеш-значень та високою швидкістю обчислення, що робить її привабливою для вимогливих застосувань. В той же час, "SM3" є важливим стандартом для китайських потреб та має розподільчу стійкість. "SHA-2" виявилася універсальною та широко визнаною хеш-функцією з різними розмірами хеш-значень. Ці результати об'єднані в консолідовані висновки, які вказують на шляхи подальших досліджень та вдосконалення систем криптографічного захисту даних в інформаційно-комунікаційній мережі Повітряних Сил.

УДК 654.01

Балакірева С.М., провідний науковий співробітник Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук
Нікора І.В., викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба
Богдановський В.В., слухач Харківського національного університету Повітряних Сил імені Івана Кожедуба

ДОСЛІДЖЕННЯ МОДЕЛЕЙ ОЦІНКИ ПРОПУСКНОЇ ЗДАТНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ ПОВІТРЯНИХ СИЛ В УМОВАХ КІБЕРНЕТИЧНОГО ВПЛИВУ ПРОТИВНИКА

В сучасному світі інформаційно-комунікаційні мережі стають ключовим елементом забезпечення ефективності та надійності зв'язку в Повітряних Силах. Зростаюча загроза кібернетичних атак вимагає постійного вдосконалення моделей оцінки пропускної здатності цих

мереж. Дослідження в цій області виявляється надзвичайно важливим для забезпечення безпеки та ефективності діяльності Повітряних Сил у сучасних умовах. З метою забезпечення оптимального функціонування та захисту від кібернетичних загроз, дослідження моделей оцінки пропускної здатності інформаційно-комунікаційних мереж в Повітряних Силах виходить на передовий план. Ці дослідження спрямовані на розробку та вдосконалення методів виявлення, аналізу та реагування на кібернетичні загрози, що дозволить забезпечити безпеку, стійкість та неперервність зв'язку в умовах інтенсивного кібернетичного впливу противника. Важливим елементом дослідження є визначення моделей пропускної здатності, які дозволяють оцінити максимально можливе навантаження, яке мережа може передати в умовах кібернетичного нападу.

Загальну пропускну здатність мережі доцільно визначати як середню кількість інформації, переданої між усіма вузлами мережі в одиницю часу. У випадку розподілу мережі на сегменти або підмережі загальна пропускна здатність мережі дорівнює сумі пропускних спроможностей підмереж, пропускної здатності міжсегментних або міжмережевих зв'язків. Ця метрика є ключовою для визначення ефективності та продуктивності мережі, оскільки вона відображає загальну можливість передачі даних, яка є вирішальною для забезпечення потреб користувачів у швидкому та надійному зв'язку. У випадку, коли мережа розподілена на сегменти або підмережі, загальна пропускна здатність мережі обчислюється як сума пропускних спроможностей цих підмереж. Це означає, що загальна пропускна здатність мережі визначається не лише внутрішньою пропускною здатністю окремих сегментів, а також пропускною здатністю міжсегментних або міжмережевих зв'язків. Такий підхід дозволяє врахувати взаємозв'язок між окремими частинами мережі та враховувати їхню взаємодію в процесі передачі даних.

Отже, для оптимізації пропускної здатності мережі Повітряних Сил пропонується використовувати модель розподілу ресурсів. Ця модель спрямована на ефективне використання доступних ресурсів мережі, таких як пропускна здатність сегментів та міжсегментних зв'язків, з метою підвищення швидкості передачі інформації між вузлами мережі за одиницю часу. Використання цієї моделі дозволить ефективно керувати ресурсами мережі, враховуючи їхні обмеження та вимоги до пропускної здатності. Це, у свою чергу, сприятиме підвищенню продуктивності та надійності зв'язку в Повітряних Силах, що є важливим чинником для забезпечення успішного виконання завдань в сучасних умовах.

УДК 654.01

Королюк Н.О., професор кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент.
Дзюба І.В., старший науковий співробітник науково-дослідної лабораторії Харківського національного університету Повітряних Сил імені Івана Кожедуба
Скринник Б.О., слухач Харківського національного університету Повітряних Сил імені Івана Кожедуба

РОЗРОБКА МЕТОДУ ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ДІЯЛЬНОСТІ ОСІБ, ЩО ПРИЙМАЮТЬ РІШЕННЯ ПРИ УПРАВЛІННІ ЛІТАЛЬНИМИ ПОВІТРЯНИМИ АПАРАТАМИ

В сучасному світі, де швидкість прийняття рішень може мати вирішальне значення, особливо в управлінні літальними повітряними апаратами, розробка ефективних методів підвищення оперативності діяльності осіб, що приймають рішення, стає актуальною проблемою. Необхідність швидких та точних рішень в цій області постійно зростає з введенням нових технологій та розвитком автоматизованих систем.

На даний момент установлені на сучасних літаках системи навігації, бомбометання й пуску ракет, наявність достатньої кількості наземних технічних засобів забезпечення літаководіння й управління польотами в сполученні з відмінною теоретичною й практичною штурманською

підготовкою льотного складу дозволяють виконувати бойові (польотні) завдання з високим ступенем точності, надійності й безпеки в будь-яких умовах повітряної, метеорологічної й тактичної обстановки.

Одним з найбільш важливих вимог, пропонованих до льотної роботи, є її безпека. Основні положення по забезпеченню безпеки польотів викладені у відповідних розділах документів, що регламентують льотну роботу в авіаційних частинах.

Розглядається вплив розроблених методів на інформаційне забезпечення тренажерного комплексу. Показано, що тренажер, який використовує інтелектуальну систему, дозволяє отримати більш адекватні результати порівняно із системами, що використовують традиційні аналітичні моделі та алгоритми керування. У висновку слід зазначити, що розроблений метод підвищення оперативності діяльності осіб, що приймають рішення при управлінні літальними повітряними апаратами (ЛПА), є важливим і актуальним кроком у розвитку авіаційної безпеки та ефективності управління.

Шляхом поєднання передових технологій штучного інтелекту, оптимізації процесу прийняття рішень та підвищення кваліфікації персоналу, цей метод сприяє забезпеченню швидкості, точності та ефективності управління ЛПА. Впровадження розробленого методу може допомогти знизити ризики та збільшити безпеку польотів, підвищуючи рівень професійної підготовки персоналу та забезпечуючи оперативний реагування на будь-які ситуації в повітряному просторі. Такий підхід до управління ЛПА є важливим для подальшого розвитку авіаційної індустрії та забезпечення безпеки польотів як на місцевому, так і на міжнародному рівнях. Пропонується розробити метод оцінки ефективності підготовки операторів, обґрунтувати рекомендації щодо вдосконалення процесів тренажерної підготовки офіцерів бойового управління, оцінити витрати на реалізацію запропонованих методів, розробку та модифікацію спеціального програмного забезпечення тренажеру.

Першин О.В., старший викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба
Хміль О.А., слухач Харківського національного університету Повітряних Сил імені Івана Кожедуба
Осадчук О.М., слухач Харківського національного університету Повітряних Сил імені Івана Кожедуба

ПОБУДОВА АДАПТИВНОЇ СИСТЕМИ РОЗПІЗНАВАННЯ ТА ПРОГНОЗУВАННЯ КІБЕРЗАГРОЗ НА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНУ МЕРЕЖУ ПОВІТРЯНИХ СИЛ

Побудова адаптивної системи розпізнавання та прогнозування кіберзагроз на інформаційно-комунікаційну мережу Повітряних Сил є актуальною задачею в умовах сучасних збройних конфліктів. З метою забезпечення безпеки інформації та захисту від кібератак потрібне розроблення та впровадження систем, які здатні адаптуватися до нових загроз та швидко реагувати на них.

У процесі побудови адаптивної системи розпізнавання та прогнозування кіберзагроз необхідно враховувати досвід сучасних збройних конфліктів та аналізувати інформацію про кіберзагрози з різних джерел, включаючи відкриті джерела та соціальні мережі. Для цього можна використовувати методи машинного навчання та штучного інтелекту.

Загалом, побудова адаптивної системи розпізнавання та прогнозування кіберзагроз на інформаційно-комунікаційну мережу Повітряних Сил є важливою задачею, яка забезпечить більш високий рівень безпеки інформації та захисту від кібератак в умовах сучасних збройних конфліктів.

В процесі побудови такої системи, велика увага повинна бути приділена використанню методів машинного навчання та штучного інтелекту, які дозволяють ефективно обробляти

великі обсяги даних та виявляти нові, раніше невідомі загрози. Адаптивність системи до змін у кіберзагрозах важлива для того, щоб ефективно реагувати на нові кібератаки.

Окрім того, розробка алгоритмів та моделей для прогнозування кіберзагроз та їх класифікації стає ключовим елементом системи. Ці алгоритми мають бути не тільки точними, але й гнучкими, щоб швидко адаптуватися до змін у кіберзагрозах та вдосконалюватися з часом.

Побудова адаптивної системи розпізнавання та прогнозування кіберзагроз на інформаційно-комунікаційну мережу Повітряних Сил є невід'ємною частиною стратегії кібербезпеки в умовах сучасних збройних конфліктів. Ця система забезпечить вищий рівень безпеки інформації та ефективний захист від кібератак, що є важливим для успішного функціонування і виконання завдань Повітряних Сил в сучасному кіберпросторі.

Побудовано систему інтелектуального виявлення атак яка дозволяє створити адаптивний механізм самонавчання системи розпізнавання аномалій, загроз та кібератак у критично важливих інформаційних системах.

УДК 654.01

Королюк Н.О., професор кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент

Яровий А.С., слухач Харківського національного університету Повітряних Сил імені Івана Кожедуба

ОСОБЛИВОСТІ МЕТОДУ ЕФЕКТИВНОГО УПРАВЛІННЯ ЛІТАЛЬНИМИ ПОВІТРЯНИМИ АПАРАТАМИ З ВИКОРИСТАННЯМ СУЧАСНИХ СИСТЕМ І ЗАСОБІВ ЗВ'ЯЗКУ ПРИ УПРАВЛІННІ ВІЙСЬКОВИМИ ОПЕРАЦІЯМИ

В сучасному світі, де швидкість, точність та координація є вирішальними факторами успішного ведення військових операцій, методи управління літальними повітряними апаратами знаходяться на передньому краї інноваційних технологій. Особливості ефективного управління виникають в контексті використання сучасних систем і засобів зв'язку, що дозволяють забезпечити оперативність, невловимість та безпеку у керуванні ареальними платформами під час військових операцій.

Передові технології забезпечують високу швидкість передачі інформації та зв'язку між командним центром та літальними апаратами, що робить можливим оперативне реагування на зміни в обстановці на полі бою. Сучасні системи керування дозволяють забезпечити точність в управлінні апаратами, що є критично важливим у місіях з високим ступенем складності та ризику. Надзвичайна увага приділяється також забезпеченню безпеки зв'язку інформації, що передається між управляючими пунктами та літальними апаратами. Шифрування та інші заходи забезпечення конфіденційності дозволяють уникнути несанкціонованого доступу до важливих даних та запобігти можливим кібератакам. У сучасній воєнній доктрині ефективне управління літальними повітряними апаратами відіграє вирішальну роль у забезпеченні успішної ведення військових операцій. Це вимагає впровадження передових систем і засобів зв'язку, які забезпечують оперативність, точність та безпеку у керуванні ареальними платформами в умовах складних бойових ситуацій.

Використання сучасних технологій, таких як штучний інтелект та алгоритми машинного навчання, сприяє автоматизації процесів управління, підвищує ефективність дій та забезпечує оптимальне використання літальних апаратів у військових операціях, отже для дослідження ефективності управління літальними повітряними апаратами в контексті військових операцій пропонується використовувати метод адаптивного розподілу задач для автоматизації вирішення оперативних і технологічних завдань у системі автоматизованого управління з використанням сучасних систем і засобів зв'язку.

УДК 621.391

Чечуй О.В., доцент кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент
Мельников О.К., магістр заочної форми навчання Харківського національного університету Повітряних Сил імені Івана Кожедуба

ШЛЯХИ УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ БПЛА ПРИ ПОБУДОВІ РАДІОМЕРЕЖ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ЗА КРИТЕРІЄМ ІНФОРМАЦІЙНОЇ ЗВ'ЯЗНОСТІ

Досвід ведення бойових дій ЗС України при відбитті збройної агресії рф вказує на широке застосування безпілотних літальних апаратів (БпЛА) для вирішення бойових завдань різного роду. Однією із типових задач, які покладаються на БпЛА, є забезпечення управління військами при веденні бойових дій шляхом побудови радіомереж тактичної ланки із застосуванням ретрансляторів на базі БпЛА. Основними технічними вимогами до радіомереж тактичної ланки управління, можна визначити:

– інтеграція всіх видів трафіка (мова, дані, відео, відеоконференція);
– повна мобільність всіх абонентів і елементів мережі;
– забезпечення заданої якості обслуговування користувачів (QoS) на значних географічних територіях в умовах застосування як звичайної, так і ядерної, біологічної та хімічної зброї;
– гарантована засекреченість усіх видів інформації;
– мінімальна участь людини в питаннях планування й ведення зв'язку.

Сучасні світові підходи до побудови систем управління військами обумовлюють застосування безпроводових самоорганізуючих мереж зв'язку з використанням БпЛА (Flying Ad-hoc networks).

Особливості застосування мереж БпЛА полягають у наступному:

– вплив ефекту Допплера на якість каналів зв'язку в само організованих мережах БпЛА. Це пов'язано з тим, що вузли такої мережі можуть мати високу швидкість руху як відносно землі, так і відносно один одного;
– діючі вузли можуть відключатися, а нові вузли – приєднуватись до мережі під час виконання завдання;
– топологія мережі схильна до швидких і частих змін, і, як наслідок, до таких же змін підпадають маршрути доставки відеоданих і зображень від джерела (камери на борту БпЛА) до одержувача (наземної станції).

Запропоновано удосконалена функціональна модель системи оперативного управління мережею БпЛА, де за рахунок застосування підсистеми управління топологією мережі зв'язку досягається оптимальне рішення за критерієм інформаційної зв'язності. Математично модель управління топологією мережі представлена у вигляді ненаправленого зваженого графу, де у якості ваги використовується значення відстані та пропускної спроможності між вузлами мережі.

Оптимальна топологія мережі зв'язку враховує мінімум використовуваного апаратного ресурсу, мінімальну кількістю БпЛА при заданих умовах дій противника (район ведення бойових дій, застосування супротивником засобів РЕБ з урахуванням типу завад та методів впливу на БпЛА), мінімізацію довжини маршрутів БпЛА та максимальну продуктивність обміну інформації в мережі. Особливістю запропонованого алгоритму оптимальної топології управління мережею БпЛА слід визначити, додаткове врахування розрахункових значень часу польоту БпЛА в залежності від погодних умов (пори року) та дій засобів РЕБ противника.

Запропонований алгоритм оптимальної топології управління мережею БпЛА дозволяє вирішувати задачі із забезпечення зв'язком військ (сил), та забезпечить підвищення показників мобільності та стійкості системи зв'язку ЗС України.

УДК 004.056

Равлюк В. В., викладач кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького
Ваврічен О. А., старший викладач кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького

ПЕРСПЕКТИВНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ДЕРЖПРИКОРДОНСЛУЖБИ УКРАЇНИ

В сучасному світі інформаційні технології є невід'ємною складовою будь-якої сфери діяльності. Завдяки швидкому розвитку технологій збільшується не лише кількість, але й значущість цифрової інформації. Проте разом із зростанням цінності інформації зростає й загроза її втрати або пошкодження в результаті несанкціонованого доступу. Необхідність комплексних та інноваційних підходів до захисту інформації стає надзвичайно важливим як в умовах постійного світового зростання кіберзагроз та ризиків втрати даних, так і зі сторони кіберзлочинної путінської росії. Інноваційні підходи до захисту інформації поряд із традиційними у комплексі дозволять не лише ефективно захищати важливу інформацію від різноманітних загроз, але і залишатися на крок попереду у непередбачуваному цифровому просторі.

Державною прикордонною службою України як і іншими державними органами у сфері національної безпеки і оборони постійно здійснюється захист відкритої інформації та інформації з обмеженим доступом за традиційними технологіями захисту. Розглянемо традиційні технології захисту інформації прикордонним відомством.

Шифрування даних є одним із основних засобів захисту інформації. Використання сучасних алгоритмів шифрування дозволяє надійно захистити дані від несанкціонованого доступу. Зокрема, симетричне та асиметричне шифрування, таке як RSA або ECC, забезпечують надійний захист.

Системи аутентифікації та авторизації використовуються для контролю доступу до інформації. Використання багаторівневих систем аутентифікації разом із механізмами двофакторної аутентифікації дозволяє забезпечити високий рівень безпеки.

Системи моніторингу та аналізу поведінки користувачів дозволяють вчасно виявляти відхилення від звичайної поведінки, що може свідчити про несанкціонований доступ до системи. Використання штучного інтелекту, в перспективі, надало б можливість цим системам забезпечувати більш точне виявлення аномалій.

Антивірусний захист який є ключовою складовою систем безпеки в сучасних інформаційно-комунікаційних системах. Він призначений для виявлення, блокування та видалення шкідливих програм, таких як віруси, троянські програми, черви та інші загрози, які можуть завдати шкоди інформації та функціонуванню інформаційно – комунікаційних системи.

Мережеві екрани, також відомі як firewall – це система безпеки, яка контролює та фільтрує мережевий трафік, що надходить на електронно-обчислювальні машини або мережу. Він блокує несанкціонований доступ та захищає від атак зловмисників.

Застосування традиційних технологій захисту інформації супроводжується наступними обов’язковими аспектами.

Використання ліцензійного програмного забезпечення із обов’язковим регулярним оновлення цього програмного забезпечення. Забезпечення актуальності всього програмного забезпечення в системі, включаючи операційну систему, додатки та антивірусне програмне забезпечення, є важливою складовою захисту службової інформації для усіх складових сектору безпеки і оборони України.

Навчання користувачів щодо безпеки інформації та правильних процедур роботи з нею може значно зменшити ризик втрати даних через людські помилки (фактори) або соціально-інженерні атаки.

Регулярне створення резервних копій даних є важливим заходом для забезпечення можливості відновлення інформації у випадку її втрати або пошкодження. Воно допомагає забезпечити надійність та доступність інформації, а також відновлення даних у випадку втрати

через різні причини, такі як випадкове видалення, кібератаки, технічні збої, техногенні або природні катастрофи.

Застосування традиційних технологій захисту інформації поряд із вище зазначеними обов'язковими елементами захисту не є вичерпними технологіями та потребують застосування перспективних або новітніх технології захисту інформації в інформаційно – комунікаційних системах.

Перш за все, це застосування штучного інтелекту та машинне навчання для прогнозування та запобігання кібератак.

Штучний інтелект та машинне навчання стають дедалі більш важливими інструментами для прогнозування та запобігання кібератак. Ці технології можуть допомогти аналітикам з кібербезпеки виявляти та блокувати загрози швидше та ефективніше, ніж це можливо за допомогою традиційних методів.

До переваг використання штучного інтелекту та машинного навчання відносять: швидкість, точність та автоматизація.

Штучний інтелект та машинне навчання можуть обробляти великі обсяги даних значно швидше, ніж люди. Це дозволяє їм виявляти загрози на ранніх стадіях, перш ніж вони завдадуть якоїсь шкоди.

Штучний інтелект та машинне навчання можуть бути навчені на багатьох різних типах даних, що дозволяє їм більш точно виявляти загрози.

Також штучний інтелект та машинне навчання можуть автоматизувати багато завдань з кібербезпеки, що звільняє час аналітикам для роботи над більш складними завданнями.

Застосування штучного інтелекту має великий потенціал для покращення технологій захисту інформації. Ці технології можуть допомогти аналітикам з кібербезпеки виявляти та блокувати загрози швидше та ефективніше, ніж це можливо за допомогою традиційних методів.

Наступним є застосування блокчейну для забезпечення цілісності та конфіденційності даних.

Блокчейн – це децентралізована система реєстрації транзакцій, яка забезпечує високий рівень цілісності та конфіденційності даних.

Перевагами використання блокчейна для забезпечення цілісності та конфіденційності даних є: цілісність, конфіденційність, прозорість та децентралізація.

Під цілісністю даних, розуміється те, що дані в блокчейні не можна змінити без відома та згоди всіх учасників мережі. Це робить його дуже стійким до фальсифікацій та шахрайства.

Конфіденційність даних в блокчейні реалізується їх шифруванням, щоб захистити від несанкціонованого доступу.

Всі транзакції в блокчейні є публічними та доступними для перегляду всіма учасниками мережі, чим забезпечується їх прозорість.

Децентралізація блокчейну характеризує відсутність контролю жодною зі сторін, що робить його більш стійким до маніпуляцій із ним.

Отже, блокчейн є потужним інструментом для забезпечення цілісності та конфіденційності даних, зокрема у сферах національної безпеки, фінансів, логістики, медицини та інших, де важлива безпека інформації.

Наступним інноваційним методом є квантове шифрування.

Квантове шифрування - це передова технологія, яка використовує принципи квантової механіки для забезпечення надійного захисту даних від атак, включаючи ті, які можуть бути виконані за допомогою квантових комп'ютерів. Ця технологія стійка до атак з боку квантових комп'ютерів, які становлять загрозу для традиційних методів шифрування. Деякі переваги використання квантового шифрування.

Стійкість до квантових атак. Квантове шифрування використовує квантові властивості світла, які роблять його неможливим для зламу за допомогою квантових комп'ютерів.

Безпечна передача даних. Квантове шифрування може використовуватися для безпечної передачі даних по незахищеним каналам зв'язку.

Отже, квантове шифрування надає потужний інструмент для захисту даних від атак з боку квантових комп'ютерів та інших сучасних загроз кібербезпеки.

Ще однією перспективною стратегією захисту інформації є застосування концепції Zero Trust Security (захист на основі недовіри).

Zero Trust Security – це модель кібербезпеки, яка відходить від традиційного периметрового підходу "довіряй всім внутрішнім пристроям і блокуй всі зовнішні". Замість цього, Zero Trust Security передбачає, що не можна довіряти нікому і нічому в мережі, включно з внутрішніми користувачами та пристроями, і кожен доступ повинен бути постійно перевірений і авторизований.

Деякі ключові аспекти стратегії Zero Trust Security: мінімальний привілей, який передбачає надання користувачам лише мінімальний набір дозволів, необхідних для виконання конкретних завдань. Безперервна оцінка ризиків, що передбачає постійну оцінку рівнів доступу на основі факторів, таких як ідентифікація користувача, пристрій, місце розташування, час доби та активність. Мікросегментація – передбачає розділення мережі на менші зони і надання доступу лише до необхідних ресурсів. А також захист даних, який передбачає, що дані повинні бути шифровані як у «стані спокою, так і в русі», щоб забезпечити конфіденційність та цілісність даних.

Загалом, стратегія Zero Trust Security створює відокремлене середовище безпеки, де доступ до ресурсів мережі надається лише на основі об'єктивної перевірки та аутентифікації, забезпечуючи високий рівень захисту від внутрішніх та зовнішніх загроз.

Таким чином, забезпечення надійного захисту інформації традиційно передбачає впровадження комплексної системи захисту інформації, що включає традиційні та новітні технології, регулярне оновлення програмного забезпечення та систем захисту інформації, систематичне навчання персоналу з питань кібербезпеки, а також створення культури кібербезпеки в організації.

Захист інформації – це постійний процес, який потребує постійного вдосконалення.

Впровадження новітніх технологій та кращих вітчизняних та світових практик дозволить забезпечити ефективний захист інформації в інформаційно-комунікаційних системах.

Для вдосконалення захисту інформації, необхідно поряд із традиційними технологіями захисту інформації, акцентувати свою увагу на новітніх технологіях захисту інформації, таких як штучний інтелект, машинне навчання, блокчейн та квантове шифрування, а також стратегія Zero Trust Security як перспективного напрямку розвитку сфери захисту інформації.

Незмінною рекомендацією щодо вдосконалення захисту інформації є важливість саме комплексного підходу до захисту інформації з використанням традиційних та інноваційних технологій забезпечення кібербезпеки, що є ключовим для забезпечення безпеки інформаційно-комунікаційних систем.

УДК 621.311

Чесановський І. І., начальник кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького, кандидат технічних наук, доцент

ЗАСТОСУВАННЯ СИСТЕМ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ В ЗАДАЧАХ ДОСЛІДЖЕННЯ ЕЛЕКТРОМАГНІТНИХ СТРУКТУР

Ефективною альтернативою навчальним лабораторіям стала низка віртуальних інструментів, які дають змогу не тільки проводити експерименти і окремі вимірювання, а і детально візуалізують процеси в середині і зовні електродинамічних структур, що значно підвищує ефективність лабораторної практики як в освітньому процесі так і в наукових дослідженнях. Широкий спектр сучасних інструментів імітаційного моделювання радіотехнічних задач включає велику кількість різних за призначенням, обчислювальною і математичною основою систем, що в поєднанні з стрімко зростаючою доступністю та обчислювальною потужністю комп’ютерів дають змогу не тільки проводити розрахунки будь-якої складності а і враховувати великі набори зовнішніх і внутрішніх умов. Така гнучкість, оперативність а в деяких випадках і достовірність є недоступною для натурного лабораторного експерименту, особливо в задачах дослідження НВЧ і випромінюючих структур, що виводить

системи імітаційного моделювання в даній галузі на позицію основного інструменту лабораторних досліджень.

В даній доповіді пропонується порівняльна оцінка сучасних систем імітаційного моделювання електродинамічних структур з узагальненням чисельних методів що використовуються в них. Окреслено загальні перспективи віртуалізації лабораторної частини навчання в галузі антен та пристроїв НВЧ з урахуванням власного досвіду та існуючих тенденцій.

Для вирішення задачі електромагнітного поля існують різні підходи. Один з них - аналітичний розв’язок, який точний, але можливий лише для простих структур. Інший - чисельний розв’язок, який наближений, але може застосовуватися для будь-яких структур. Незважаючи на обмежену точність, саме чисельні методи використовуються в системах імітаційного і математичного моделювання, оскільки, в більшості задач лабораторних досліджень цього цілком достатньо. Основними методами розв’язку рівнянь Максвела, що широко використовуються в системах імітаційного і математичного моделювання електродинамічних структур, є: чисельний розв’язок диференційних рівнянь і розв’язок інтегральних рівнянь в частотній або часовій області; аналітичний розв'язок в S-площині, аналітичний інтегральний операторний розв’язок, аналітичний метод геометричної симетрії, аналітичний диференційно-геометричний синтез, аналітичний просторово-часовий розв'язок та аналітичні топологічні методи.

Сучасні системи імітаційного моделювання базуються на числових методах розв'язку задач, які мають різні підходи до пошуку розв'язків, дозволяють аналізувати пристрої різної складності як у частотній, так і в часовій або просторовій областях. Хоча всі без винятку програми електродинамічного моделювання мають свою практичну спрямованість, в них інтегруються додаткові засоби візуалізації результатів, для отримання яких більш зручними є певні методи. При цьому, обчислювальне ядро системи будується на методі чисельного аналізу, який є найбільш ефективним для класу задач, для розв’язку яких розробляється система.

Для підтвердження цього, варто розглянути функціональні можливості сучасних програм моделювання НВЧ структур і антен.

FEKO (FEldberechnung bei Korpern mit beliebiger Oberflache) призначена для проведення розрахунку електромагнітного поля тіл довільної форми. Дана система, завдяки своїй зручності та широкому спектру задач, що вирішуються знайшла широкого застосування в лабораторних практикумах з дисциплін, що спрямованні на вивчення НВЧ техніки і антен.

ANSYS HFSS (High Frequency System Simulator). Пакет програм для тривимірного електромагнітного моделювання і розробки високочастотних радіоелектронних і антенних пристроїв. Однією з вагомих переваг даної програми, є можливість використання різних плагінів-конструкторів, що значно спрощує процес створення моделей.

μWave Wizard поєднує в собі гнучкість 2D/3D методу скінченних елементів з швидкістю і точністю традиційних методів узгодження мод. Простий процес складання складних НВЧ-структур з використанням основних блоків виключає необхідність створення повної 3D моделі всієї структури і прискорює процес проектування.

MMANA (Macato Mori Antenna Analyzer). За допомогою MMANA можливі розрахунки і аналіз антен, реалізованих як довільний набір тонких проводів заданого діаметру. За допомогою програми можна здійснювати автоматичну оптимізацію антени, гнучко налаштовуючи $Z_{вх}$, КСХ, підсилення, тощо.

Sonnet Suites. Пакет програм Sonnet Suites призначений для електромагнітного моделювання планарних НВЧ структур: смужкових і мікросмужкових ліній, копланарних хвилеводів, одно- і багатошарових друкованих плат, а також антен.

CST MICROWEVE STUDIO (CST MWS). Призначена для чисельного моделювання тривимірних високочастотних пристроїв (антен, фільтрів, відгалужувачів, планарних багатошарових структур).

AWR Microwave Office. Представляє собою універсальну систему моделювання всіх видів радіочастотних і НВЧ пристроїв, починаючи від складних НВЧ вузлів і закінчуючи інтегральними НВЧ мікросхемами.

Antenna Magus. Містить велику базу даних по більш ніж 250 видах антенних і фідерних пристроїв, що розроблені по заданих параметрах підсилення, смуги пропускання і ширини діаграми спрямованості, причому для того або іншого параметра синтезується оптимальна конфігурація обраного виду пристрою.

Electromagnetic Professional (EMPro). Програмна платформа електромагнітного тривимірного моделювання призначена для аналізу об'ємних електромагнітних ефектів різних електронних компонентів, включаючи корпуси високошвидкісних і високочастотних мікросхем, з'єднувальні лінії, антени, внутрішньосхемні і зовнішні пасивні елементи, з'єднання друкованих плат.

XGtd. Призначена для високочастотного електромагнітного моделювання полів дальньої зони і параметрів розсіювання, аналізу електромагнітних випромінювань і перешкод, властивостей поглинаючих матеріалів на електрично-великих об'єктах. Програма дає змогу візуалізувати електромагнітні характеристики в 2D і 3D.

EDF-EME. Програмне середовище електромагнітного моделювання кораблів. Оперує тривимірною моделлю корабля. Дає змогу виконувати розрахунки не тільки електромагнітної обстановки і рівнів електромагнітної сумісності радіоелектронних засобів, але й проводити оцінку електромагнітної безпеки промислових і біологічних об'єктів.

Optenni Lab. Спеціалізоване програмне забезпечення, призначене для автоматичного синтезу кіл узгодження НВЧ пристроїв, оцінки максимально допустимої смуги робочих частот антен і розрахунків гіршого випадку розв'язки між декількома антенами в системі.

Це далеко не повний перелік програм електродинамічного моделювання, оскільки існує ще велика кількість вузькоспеціалізованих систем побудованих на основі різних чисельних методів, в тому числі і не розглянутих в доповіді. На сьогоднішній день, спектр середовищ моделювання охоплює всі практичні задачі електродинамічного аналізу, в тому числі і задачі навчального характеру.

УДК 621.311.6

Площик А. С., викладач кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького.

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ЕНЕРГОЕФЕКТИВНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ АВТОНОМІЇ ЕЛЕКТРОННИХ СИСТЕМ У СИЛОВИХ СТРУКТУРАХ

В сучасному світі, де силові структури відіграють важливу роль в забезпеченні національної безпеки та виконанні завдань оборони, питання енергоефективності та автономії електронних систем стають все більш актуальними.

Очевидно, що застосування використання енергоефективних технологій дозволяє зменшити споживання електроенергії в складових Сил безпеки та оборони України. Впровадження енергоефективних рішень дозволить в довготривалій перспективі зменшити витрати на електроживлення силових структур.

Першою та важливою перспективою використання альтернативних джерел живлення є зменшення залежності від енергетичних ресурсів.

У прикордонній службі України можливі до застосування різноманітні альтернативні джерела живлення, спрямовані на забезпечення незалежності від традиційних системах електроживлення та підвищення стійкості енергозабезпечення.

Розглянемо різновидів альтернативних джерел живлення в прикордонній службі.

Перш за все варто відмітити сонячні електростанції. Актуальним та доцільним є використання сонячних панелей для збору сонячної енергії та конвертації її в електроенергію. Перспективи застосування є досить суттєві, а саме: екологічно чиста, стійка до погодних умов, можливість автономного енергозабезпечення.

Вітроенергетика не так поширена у використанні в межах наших територіях в силу географії вітрів. Проте, як додатковий спосіб акумуляції енергії, використання вітрогенераторів

для виробництва електроенергії за рахунок вітрового потоку можливий та рентабельний. На противагу екологічній чистоті системи, наявність великого потенціалу у вітряних регіонах та автономність основним недоліком є нестача вітрових потужностей. Тому для повноцінної заміни варто застосовувати вітрові генератори в парі із системами сонячних батарей.

Як додатковий спосіб акумуляції електроенергії також варте уваги застосування мікрогідроелектростанцій. За основу береться використання потоків води для генерації електроенергії на малих гідроелектростанціях. Перевагою використання є екологічно безпечне, діє за наявності водних ресурсів та має низькі експлуатаційні витрати.

При часовій нерівномірності вироблення електроенергії за допомогою альтернативних джерел живлення значна економія традиційних енергоносіїв може бути досягнута шляхом акумуляції енергії, яка виробляється в періоди її мінімального поживання. Постає гостра необхідність мати системи, що запасають енергію, при експлуатації установок з нерегулярним виробленням протягом доби або триваліших періодів – вітрових станцій, сонячних батарей, гідроелектростанцій. Гідроакумулюючі станції, дозволяють повернути в енергосистему в години пік до 70% енергії, накопиченої в години мінімуму споживання, проте їх будівництво доцільне в місцевостях з гористим рельєфом. Установка вітрових станції потребує детальнішого вивчення для оптимального місця розташування.

Загальною перспективою використання енергоефективних технологій у силових структурах є не лише забезпечення надійності та стійкості електронних систем, але і сприяння сталому розвитку та відновленню природних ресурсів.. Підсумовуючи, варто зазначити, що застосування енергоефективних технологій може призвести до скорочення залежності силових структур від енергетичних ресурсів.

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