

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА



ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

XX Міжнародної науково-практичної конференції

**«Військова освіта і наука:
сьогодення та майбутнє»**

29 листопада 2024 року

Київ – 2024

Військова освіта і наука: сьогодення та майбутнє : зб. тез доповідей XX Міжнародної науково-практичної конференції, м. Київ, 29 листопада 2024 р. Київ : Військовий інститут Київського національного університету імені Тараса Шевченка, 2024. 532 с.

Рекомендовано до друку Вченою радою Військового інституту Київського національного університету імені Тараса Шевченка
(*протокол від 21.11.2024 № 3*).

Редакційна колегія:

Сіроштан О.О., п-к, **Попков Б.О.**, п-к, к.військ.н., с.н.с., **Лойшин А.А.**, п-к, д-р філософії, **Пампуха І.В.**, п-к, к.т.н., доц., **Гончарук Л.М.**, п-к, к.філол.н., **Сафін О.Д.**, прац. ЗСУ, д.психол.н., проф., **Мась Н.М.**, п-к, к.психол.н., **Коропатнік І.М.**, п-к, д.ю.н., проф., **Рижиков В.С.**, прац. ЗСУ, д.пед.н., проф.

У збірнику тез доповідей друкуються матеріали виступів наукових і науково-педагогічних працівників, курсантів (студентів) Військового інституту Київського національного університету імені Тараса Шевченка та інших вищих військових та закладів вищої освіти України.

У публікаціях розглядаються: технічні проблеми озброєння і військової техніки та технології подвійного призначення; актуальні проблеми лінгвістичного забезпечення Збройних Сил України; актуальні питання військової психології та соціальної роботи; інформаційна та психологічна боротьба у військовій сфері; інформаційно-медійне забезпечення МОУ та ЗСУ в умовах правового режиму воєнного стану; фінанси; актуальні проблеми військового права в умовах воєнного стану; актуальні проблеми геопросторової підтримки військ в умовах ведення російсько-української війни; наукові проблеми воєнної політології та морально-психологічного впливу; аналіз бойового застосування частин (підрозділів) Сухопутних військ Збройних Сил України у сучасному загальновійськовому бою (тактичних діях)

© Військовий інститут Київського національного університету імені Тараса Шевченка

Зміст

СЕКЦІЯ 1 ТЕХНІЧНІ ПРОБЛЕМИ ОЗБРОЄННЯ І ВІЙСЬКОВОЇ ТЕХНІКИ ТА ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ	26
Banzak H.V., Zherebtsova L.N., Todorov M.F., Lisetskaya M.A., Sotnikov Y.O. Development and research of methods for optimizing the maintenance processes of military equipment	26
Banzak H.V., Chelnokov A.S., Fedotov V.V. Development of a reliability model for a complex technical object of military equipment	27
Banzak H.V., Vetrov S.V., Strelchenko K.V. Development of a simulation statistical model of the process of technical maintenance of military equipment	28
Banzak O.V., Zherebtsova L.N., Dovgan I.O. Development of a portable digital gamma-ray spectrometer for radiation survey in field conditions	29
Banzak O.V., Zherebtsova L.N., Ovchinnikov A.I., Golub M.S. Gamma radiation detection unit based on cdznte sensor for radiation and technological control systems of a nuclear power plant	30
Lienkov S.V., Banzak O.V., Kotov S.A. Detector modeling for radiation monitoring systems	31
Анікін В.А., Нігловський О.О., Сотніков Є.О., Рикун К.В. Система безпечових настанов малого комерційного офісного приміщення	32
Анікін В.А., Розгон І.Д., Федорчук М.І. Система захисту програмного комплексу фінансового документообігу з вебархітектурою	33
Анікін В.А., Коцюк М.М., Калій К.В., Селюкова Т.В. Система запобігання інформаційним витокам комп'ютеризованого робочого місця	34
Барабаш А.В., Олексюк Д.А., Ратушняк М.В. Збільшення цінності цифрового електронного підпису застосуванням особових атрибутів	35
Басистий В.А., Чешун О.В., Чешун В.М. Застосування одноплатних мікрокомп'ютерів для підвищення стійкості інтернету речей до DDOS атак.	36
Бельська О.А. Черних Ю.О. Цілі використання в САУ управліннь надмірної розмірності	37
Вишковський Д.П., Гурман І.В., Сотніков Є.О. Штучний інтелект у протидії фішинговим атакам в сфері банківської справи	39
Джулій В.М., Ленков С.В., Купчик Н.С., Чорненко С.В. Проблеми інформаційної безпеки в інформаційно-телекомунікаційних мережах	40
Джулій В.М., Мірошніченко О.В., Томусяк А.В., Горбатюк Н.І. Протоколи програмного розподілу секретної інформації між абонентами IP – телефонії	41
Джулій В.М., Селюков О.В., Заставна Я.В., Чешун Д.В. Методи та засоби захисту від загрозливих програм	42
Жиров Г.Б., Зозуля А.А. Програмний застосунок для розрахунку енергетичного потенціалу радіолінії «Космічний апарат – наземна станція»	43

Захаров В.В., Чешун В.М. Технологія HONEYNET в захисті корпоративної інформації від кіберзагроз.....	44
Каменяр М.Л., Пивовар О.С. Моделювання впливу системних завад на хаотичний канал зв'язку.....	45
Кириленко І.В. Використання інноваційних технологій для покращення логістики у Збройних Силах України під час війни.....	46
Мельник М.М., Чешун В.М., Чешун Д.В. Розподіл задач цифрової криміналістики на основі мережевої моделі OSI.....	47
Мостовий С.В., Жмурик І.М. Основні кіберзагрози в IOT та методи їх запобігання.....	48
Муляр І.В., Гловюк В.С., Зацепін К.О., Чернов С.В. Використання моделі GPT для автоматизації тестування IOT-пристроїв.....	49
Муляр І.В., Зейлик Р.Ю., Житнік Р.Л., Футорний Р.В. Аналіз підходів до побудови системи сканування хостів і портів для аналізу вразливостей мережі з вебінтерфейсом, збереження та обробкою даних.....	50
Муляр І.В., Сиротенко Д.А., Шкребета В.С. Способи захисту від фішингу через QR-коди.....	51
Савельєв С.В., Кириленко І.В. Ефективність управління логістичними процесами у сфері речового забезпечення військових частин України.....	52
Слободянюк А.С., Пивовар О.С., Ленков С.В. Оптимізація взаємодії технологій IoT та LoRaWAN.....	53
Стецюк М.В., Панько Р. Кіберетика та право: етичні питання у кіберпросторі, проблеми зламів, кібершпигунства, вплив на права і свободи людини.....	54
Хмельовський В.Р., Бойцун Д.О., Кльоц Ю.П. Підвищення рівня захищеності даних користувача при реплікації через NFC.....	55
Toliupa S. Koval M. Analysis of cyber threats and cloud security risks.....	56
Гахович С.В. Модель SIEM-системи з підсистемою підтримки прийняття рішення.....	57
Канчуга М.К., Ковба М.В., Дуфанець І.Б. Пікапи у військовому застосуванні.....	59
Коваль М.О. Карпенко А.О. Військові операції в сфері електромагнітного спектру (ЕМС).....	60
Кравченко І.О. Адаптивні стеганографічні системи як інструмент підвищення інформаційної безпеки в умовах кіберзагроз.....	61
Кравченко О.І. Заходи безпеки бездротових сенсорних мереж військового призначення, при функціонування в умовах заводової обстановки та кібервпливу.....	62
Kulaha Y. TOPic: future threats and challenges for blockchain technologies.....	64
Кулько А.А., Толюпа С.В. Побудова інтелектуальної системи протидії.....	

Таким чином, ефективність управління логістичними процесами у сфері речового забезпечення військових частин України відіграє вирішальну роль у забезпеченні боєздатності армії. Впровадження сучасних методів управління, зокрема ERP-систем та автоматизованих складів, значно покращує процеси забезпечення, скорочує час на доставку матеріальних ресурсів та підвищує ефективність використання наявних ресурсів. Однак для досягнення максимальних результатів необхідно розв'язувати питання фінансування та підготовки кадрів, а також адаптувати логістичні системи до умов війни.

Слободянюк А.С. (ХмНУ)
к.т.н., доц. Пивовар О.С. (ХмНУ)
д.т.н., проф. Ленков С.В. (ВІКНУ)

ОПТИМІЗАЦІЯ ВЗАЄМОДІЇ ТЕХНОЛОГІЙ IoT та LoRaWAN

На даний час різноманітні Інтернет технології широко застосовуються як для цивільних, так і для військових потреб. Необхідність економії електричної енергії стала повсякденною необхідністю і парадигма застосування глобальних мереж низького енергоспоживання LPWAN в діючих стандартах передачі різноманітних даних потребує глибокого дослідження в рамках організації конкуренції із іншими існуючими стандартами передачі даних.

Саме в цьому контексті концепція технології LoRaWAN дозволяє отримати позитивні результати, через забезпечення дещо вищої пропускнуєї спроможності та часу подвійного оберту (ping) без суттєвого збільшення складності системного забезпечення керування доступом.

Докладне моделювання поширення сигналів LoRa на системному рівні, що враховує реалістичний сценарій розташування мережевих вузлів для інтеграції в IoT дозволяє провести оцінку доцільності розробки модулів, що поєднують в собі найкращі риси IoT та LoRa.

Розроблена та досліджена модель програмно-апаратної реалізації удосконаленого методу оптимізації конвергенції компонентів IoT та LoRaWAN на базі програмного забезпечення Network Simulator (DES) із згенерованим модулем Loga та проведено ряд експериментальних досліджень.

Сценарій для побудови моделі - міська забудова радіусом близько 7 км, що охоплюється шлюзом таким чином, щоб кінцеві пристрої також обслуговувались суміжними шлюзами діючими в рамках глобальної гексагональної сітки. Шлюзами так що вся територія все ще покривалася одним шлюзом, де кінцеві пристрої охоплюють глобальною гексагональною сіткою. В рамках такої моделі великий відсоток вузлів та кінцевих споживачів IoT попадають в зону радіотіні. В рамках позаміської пласкої місцевості це відповідає радіусу горизонту огляду людини.

Дослідження під час моделювання показало, що для досягнення надійності обслуговування абонентів понад 95% шлюзи LoRaWAN мають бути розгорнуті таким чином, щоб кожен шлюз забезпечував радіус покриття близько 1,3км. Розроблений модуль симуляції дозволяє проводити оцінку

параметрів мережі Loga в рамках обслуговування пристроїв IoT на заданій території із заданою якістю на рівнях MAC та PHY та по відношенню до типової схеми ALOHA забезпечує просту доступність масштабування та покращений рівень надійності висхідного зв'язку із коефіцієнтом втрати пакетів в найгіршому випадку не більше 3%.

доктор філософії Стецюк М.В. (ХмНУ)
Панько Р. (ХмНУ)

КІБЕРЕТИКА ТА ПРАВО: ЕТИЧНІ ПИТАННЯ У КІБЕРПРОСТОРИ, ПРОБЛЕМИ ЗЛАМІВ, КІБЕРШПИГУНСТВА, ВПЛИВ НА ПРАВА І СВОБОДИ ЛЮДИНИ

Проблема зламів та прав людини: Кіберінструменти на зразок шпигунських програм, як-от Pegasus, можуть перетворити смартфон на засіб для 24-годинного спостереження, що порушує приватність користувачів і часто використовується не за призначенням, наприклад, для утисків активістів і журналістів. Це вимагає встановлення жорстких міжнародних обмежень на продаж та використання таких технологій.

Етичні принципи у кібервійнах: Міждержавні кібератаки часто мають серйозні наслідки, однак їх регулювання досі залишається недосконалим. Професор Маріаросарія Таддео підкреслює необхідність пропорційного та відповідального підходу до кібернападів, зокрема відокремлення цільових військових об'єктів від цивільних у кіберпросторі. Крім того, існує потреба в нових етичних та правових рамкових документах, щоб врахувати унікальні ризики, пов'язані з кіберопераціями.

Приватність та цифровий моніторинг: За даними ООН, зростаюча кількість цифрових технологій для моніторингу, включаючи розпізнавання облич та аналіз соціальних мереж, підривають право на приватність і часто порушують права людини. Це вимагає запровадження контролю над застосуванням біометричних технологій та масового збору даних, а також прозорості державних програм спостереження.

Наслідки цифрового стеження для демократії: Використання шпигунського ПЗ та інших засобів масового спостереження підриває основи демократії, адже вони здатні обмежувати свободу слова та зменшувати плюралізм думок. Згідно з ООН, цифрове стеження часто виходить за межі своєї заявленої мети – боротьби з тероризмом – і стає інструментом контролю за журналістами, правозахисниками та опозиційними політиками, що робить його загрозою для прав людини.

Етичні стандарти для військових кібероперацій: Професор Маріаросарія Таддео підкреслює необхідність узгодження міжнародних етичних принципів для кібероперацій, зокрема на основі Міжнародного гуманітарного права. Ці принципи включають пропорційність дій, чітке розмежування військових і цивільних цілей, а також необхідність обмеження масштабів атаки, щоб мінімізувати побічний збиток і уникнути непоправних наслідків для цивільних.

Наукове видання



ТЕЗИ ДОПОВІДЕЙ

XX Міжнародної науково-практичної конференції

«Військова освіта і наука: сьогодення та майбутнє»

Тексти тез представлено у авторській редакції. Автори несуть повну відповідальність за зміст, добір, точність наведених фактів, цитат, власних імен, дат та інших відомостей.

Збір, технічне редагування та комп'ютерна верстка – Бадрук О.О.
Оригінал-макет та обкладинка – Халіманенко С.М.

Підписано до друку 21.11.2024. Формат 60x84/16.
Гарнітура Times. Папір офсетний. Друк ризограф. Тираж 10.
Умов. друк. аркушів 18. Заказ № 41-16.

Надруковано в навчальному картографічному комплексі ВІКНУ
03189, Київ, вул. Юлії Здановської, 81
521-32-89

