ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ ІМЕНІ ГЕРОЇВ КРУТ

Міжнародна науково-технічна конференція

Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку

КИЇВ - 2021

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ
ІМЕНІ ГЕРОЇВ КРУТ

І МІЖНАРОДНА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ

“Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку”

25 – 26 листопада 2021 року

(Доповіді та тези доповідей)

Київ – 2021

ББК
Ц4 (4Укр)39
П-768

У збірнику матеріалів першої міжнародної науково-технічної конференції опубліковано доповіді та тези доповідей вчених, науково-педагогічних та наукових працівників, докторантів, ад'юнктів, здобувачів, курсантів Військового інституту телекомунікацій та інформатизації імені Герої Крут та інших вищих навчальних закладів, представників промисловості в яких розглядаються пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення, застосування підрозділів, комплексів, засобів зв'язку та автоматизації в операції Об'єднаних сил. Метою конференції є аналіз стану та обмін досвідом з питань систем і технологій зв'язку, інформатизації та кібербезпеки з урахуванням досвіду застосування у Збройних Силах України.

ЗМІСТ

Доповіді

Тези

CONTENTS

д.т.н. Бараннік В.В. (ХНУ ім. В. Н. Каразіна)
к.т.н. Гуржій П.М. (ВІТІ ім. Героїв Крут)
Гаврилов Д. С. (ХНУРЕ)
Гуржій І.А. (ВІТІ ім. Героїв Крут)

МЕТОД ОБРОБКИ ВІДЕОЗОБРАЖЕННЯ З МОЖЛИВІСТЮ ЙОГО ЗАХИСТУ НА ЕТАПІ КВАНТУВАННЯ

,

Актуальність. У зв'язку зі збільшенням кількості мобільних пристроїв отримання, обробки, зберігання та передачі даних постійно зростає необхідність оперативно приймати обґрунтовані рішення. При цьому ефективність прийнятого рішення, дуже часто, залежить від проміжку часу за який його прийнято, та маєтенденцію к зменшенню. Тож, загострилось питання збереження доступності (оперативності) даних. В той же час, для якісного прийняття рішення отриманні дані мають мати необхідний рівень достовірності та конфіденційності. Застосування технологій обробки та кодування зображень може забезпечити зменшення обсягу відеозображень.

Постановка задачі. Провести є побудову методу обробки відеозображення з можливістю його обробки на етапі квантування з подальшим арифметичним кодуванням. Що дозволить при збереженні структурно – статистичної закономірності забезпечити необхідний рівень доступності, достовірності та конфіденційності при передачі відеоданих.

Основні положення. Рівень стиснення відеоданих є одним з ключових показників в процесі кодування. Але ж в останні роки з'являється потреба щодо забезпечення конфіденційності зображень та високої їх якості. Наприклад, такі технології розглядаються в працях [1 – 6]. В цьому напрямку існують різні підходи. А саме.

Перший підхід на основі використання стандартизованих криптографічних алгоритмів на різних етапах синтаксичного представлення відеозображень [2; 6; 7].

Другій підхід це з врахуванням механізмів переміщування декількох відеозображень, що викладається в працях [8 – 10]. Якщо процес перемішування стосується тільки окремих відеокадрів, тобто внутрішнього перемішування, то такий підхід розглядається в таких працях, як [11 – 12] – без градієнтних перетворень та [13 – 14] – у разі додаткового використання масок масштабування відео сегментів.

Найбільш розповсюджений варіант таких двох підходів це класична послідовна реалізація технологій компресії та захисту інформації, наприклад, що викладається в таких працях, як [12, 13]. Саме послідовна концепція стиснення та захисту відеоінформації з використанням методів JPEG реалізовані в працях [14], а з застосуванням методів JPEG 2000 в праці [15]. Їх різні реалізації наводяться відповідно в працях [12-16].

Третій підхід щодо захисту інформації в системах компресії полягає у її прихованні. Тут використовуються особливості відеозображень перш за все обумовлені їх аналоговою природою походження. Приклади таких методів розглядаються та досліджуються в працях [13-16].

В теж час загальний недолік таких методів полягає у тому що не повній мірі враховується захист саме ключової інформації відеозображень. Отже це призводить до виникнення втрат інформації, значних часових затримок на обробку або до зменшення величини коефіцієнта стиснення. От-же, існує проблематика забезпечення необхідного рівня доступності, достовірності та конфіденційності даних в системах обміну інформацією. За основу пропонується використовувати алгоритм JPEG у зв'язку з широкою популярністю та ефективністю робити.

В багатьох роботах описано методи, які базуються на JPEG - платформі. Дослідження публікацій вказало на актуальність науково-прикладної задачі забезпечення необхідного рівня доступності, достовірності та конфіденційності даних в системах обміну інформацією Для вирішення цієї задачі пропонується використовувати селективний підхід. Під селективної обробкою розуміємо процес виявлення і подальшу обробку значущих складових

відеокадру в процесі його кодування і побудови формату. Переваги селективного методу на етапі колірного перетворення полягають в наступному: не потрібно додатково витрачати час на виявлення значимої інформації в складовій по яскравості так, як вся компонента яскравості вважається значимою і виділена в ході колірного перетворення; у разі потреби забезпечення конфіденційності зображення необхідним є вилучання компоненти по яскравості з процесу обробки алгоритмом на основі JPEG-платформи, що збільшить рівень достовірності. В свою чергу, час на обробку цієї компоненти буде прямувати до нуля.

Недоліки селективного методу на етапі колірного перетворення полягають в наступному : у разі потреби забезпечення конфіденційності зображення, об'єм вихідних даних після селективної обробки збільшиться у порівнянні з об'ємом вихідних даних після алгоритму на основі JPEG – платформи. При цьому, об'єм, колірних компонент після селективної обробки залишається без змін.

Таким чином, середній час доведення компоненти яскравості значно більший за середній час на доведення хроматичних компонент: відсутня оцінка блоків компоненти яскравості на предмет значимості. Таким чином, має місце надлишковий вплив на всю компоненту яскравості, замість впливу лише на блоки інтересу; можливість отримання несанкціонованим користувачем значимої інформації при аналізі колірних.

Переваги методу селективної обробки Баранніка – Комолова:

- основна енергетика міститься в низькочастотних компонентах, що дозволяє при обробці лише низькочастотних компонентах зруйнувати основні візуальні ознаки об'єктів зображення, замість впливу на всю трансформанту;

- визначення низькочастотних компонент як значимих з подальшою обробкою має незначний вплив на вихідний об'єм даних;

- зменшення частки надлишкової обробки даних. Це відбувається за рахунок наявності системи класифікації блоків по рівню насиченості (слабо, середьо, сильнонасичений). Це дозволяє дозовано визначити кількість низькочастотних елементів трансформанти, які є значимими і потребують подальшої обробки.

Недоліки методу селективної обробки Баранніка – Комолова: збільшення часу на обробку трансформанти на етапі dct. За рахунок складного математичного апарату та наявності класифікації блоків за рівнем насиченості; відсутня чітка границя між низькими і середніми частотами. Це ускладнює процес виявлення значимих компонент і відноситься до всіх подібних методів. Основним недоліком перших двох етапів є руйнування структурно – статистичної закономірності трансформанти. Часткове усунення недоліків перших двох етапів можливе на третьому етапі обробки.

Розроблено метод обробки відеозображення з можливістю його захисту на етапі квантування з подальшим арифметичним кодуванням. Що дозволить при збереженні структурно – статистичної закономірності виконати поставлені вимоги. Забезпечення необхідного рівня доступності пов'язане зі зменшенням об'єму відеозображення на 30% у порівнянні з вихідним об'ємом. При цьому, забезпечення необхідного рівня достовірності підтверджується оцінкою пікового відношення сигнал/шум для авторизованого користувача, який складає $\mathrm{PSNR}_{\text{авт}} \geq 20$ дБ. забезпечення необхідного рівня конфіденційності підтверджується оцінкою пікового відношення сигнал/шум при несанкціонованому доступі, який складає $\mathrm{PSNR}_{\text{нсд}} \leq 9$ дБ.

Висновки. Вперше запропоновано метод обробки відеозображення на етапі квантування, що дозволить при збереженні структурно – статистичної закономірності забезпечити необхідний рівень доступності, достовірності та конфіденційності при передачі відеоданих. Принцип обробки наближається до послідовної схеми, що незначною мірою збільшує час на обробку даних. Дана особливість не впливає на час доведення даних до користувача оскільки обробка відбувається після основних етапів компресії. Адже, основна кількість надмірностей усунуто на етапах колірного перетворення, дискретно-косинусного перетворення та за рахунок квантування.

Варто зазначити, що запропоновані підходи виконують поставлені завдання по рівню криптографічного захисту при заданому рівню достовірності. При цьому, метод використання шифрувальних таблиць має вищій рівень криптографічної стійкості ніж метод використання матриці-ключа. Це обумовлено більш складним математичним апаратом, що свою чергу призводить до збільшення часу на обробку даних. З метою виконання вимоги доступності даних запропоновано використовувати арифметичне кодування, що має вищу ефективність у порівнянні з методами кодових таблиць. При цьому, метод використання шифрувальних таблиць має більшу криптографічну стійкість, а метод використання матриці-ключа більшу швидкодію. При цьому, використання арифметичного кодування задовольнить потребу у доступності.

ЛІТЕРАТУРА

1. JPEGPrivacy &Security Abstract andExecutiveSummary [Electronicresource]. – 2015. – Accessmode: https://jpeg.org/items/20150910_privacy_ security_summary.html. – 7.06.2021.

2. Sharma, R. Data Security usingCompression andCryptography Techniques [Text] / R. Sharma, S. Bollavarapu // InternationalJournalofComputerApplications. – 2015. – Vol. 117, No. 14. – P. 15–18. DOI: 10.5120/20621-3342.

3. Announcing the ADVANCED ENCRYPTION STANDARD (AES) [Text]. – Federal Information Processing Standards Publication 197, 2001. – 51 p.

4. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. – Введ. 2015-07-01. – Київ : Мінекономрозвитку України, 2015. – 39 с.

5. DataEncryptionStandard (DES) [Text]. – FederalInformationProcessingStandardsPublication 46-3, 1999. – 26 p.

6. ДСТУ ГОСТ 28147:2009. Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89)[Текст]. – Введ. 2009-02-01. – Київ : Держспоживстандарт України, 2008. – 20 с.

7. Rivest, R. L. Amethodforobtainingdigitalsignatures and public-key cryptosystems [Text] / R. L. Rivest, A. Shamir, L. M. Adleman // CommunicationsoftheACM. – 1978. – Vol. 21, Iss. 2. – P. 120–126. DOI: 10.1145/359340.359342.

8. Naor, M. VisualCryptography [Text] / M. Naor, A. Shamir // ProceedingsoftheAdvances inCryptology – EUROCRYPT'94. Lecture Notes in Computer Science. – 1995. – Vol. 950. – P. 1–12. DOI: 10.1007/bfb0053419.

8. Chen, T.-H. Efficient multi-secret image sharing based on Boolean operation [Text] / T.-H. Chen, Ch.-S. Wu // Signal Processing. – 2011. – Vol. 91, Iss. 1. – P. 90–97. DOI: 10.1016/j.sigpro.2010.06.012.

9. Chen, Ch.-Ch. A secure Boolean-based multi-secret image sharing scheme [Text] / Ch.-Ch. Chen, W.-J. Wu // Journal of Systems and Software. – 2014. – Vol. 92. – P. 107–114. DOI: 10.1016/j.jss.2014.01.001.

10. Deshmukh, M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic [Text] / M. Deshmukh, N. Nain, M. Ahmed // IEEE 30 th International Conference on Advanced Information Networking and Applications (AINA). – 2016. – P. 690–697. DOI: 10.1109/aina.2016.56.

11. Yang, Ch.-N. Enhanced Boolean-based multi secret image sharing scheme [Text] / Ch.-N. Yang, Ch.-H. Chen, S.-R. Cai // Journal of Systems and Software. – 2016. – Vol. 116. – P. 22–34. DOI: 10.1016/j.jss.2015.01.031.

12. Farajallah, M. Chaos-based crypto and joint crypto-compression systems for images and videos [Electronic resource] / M. Farajallah. – 2015. – Access mode: https://hal.archives-ouvertes.fr/tel-01179610. – 7.06.2021.

13. Barannik, V. Binomial-PolyadicBinary Data Encodingby Quantity ofSeriesofOnes [Text] / V. Barannik, V. Barannik // 15thIEEEInternationalConferenceonModernProblemsofRadioEngineering, Telecommunications

andComputerScience (TCSET'2020). – 2020. -P. 775–780. DOI: 10.1109/TCSET49122.2020.235540.

14. Barannik, V. V. Structuralslottingwithuniformredistributionforenhancingtrustworthinessof informationstreams [Text] / V.V. Barannik, Yu.N. Ryabukha, S.A. Podlesnyi // Telecommunications andRadioEngineering. – 2017. -Vol. 76 No. 7. – P. 607-615. DOI: 10.1615/TelecomRadEng.v76.i7.40.

15. Yuan, L. SecureJPEGScramblingenablingPrivacy inPhotoSharing [Text] / L. Yuan, P. Korshunov, T. Ebrahimi, // 11thIEEEInternationalConference andWorkshopsonAutomaticFace andGestureRecognition (FG). – 2015. – P. 1–6. DOI: 10.1109/FG.2015.7285022.

16. Methodcodingefficiency segmentsfor informationtechnology processingvideo [Text] / V. Barannik, D. Tarasenko // 4thInternationalScientific-PracticalConferenceonProblemsofInfocommunications. Science andTechnology (PICS&T). – 2017. – P. 551-555. DOI: 10.1109/INFOCOMMST.2017.8246460.

к.т.н. Бовда Е.М. (ВІТІ)
д.т.н. Романюк В.А. (ВІТІ)
Бовда В.Е. (ВІТІ НЦЗІ)

СУЧАСНІ ПІДХОДИ В ПОБУДОВІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Існуючі інформаційно-телекомунікаційні мережі (ІТМ) в своєму складі мають велику кількість підсистем різного функціонального призначення та застосування. Такі системи потребують якісного управління.

Існуючі зараз технології управління інформаційно-телекомунікаційними мережами розраховані на статичні або квазістатичні умови їх функціонування та враховують особливості, що характерні для цивільних систем. Відмінностями між цивільними та військовими системами управління мережами полягають в наступному: різні цілі, етапи, функції, рівні управління, вимоги до оперативності управління, інтенсивність зовнішнього впливу дестабілізуючих факторів (вогневе враження, активні завади, радіоелектронна та інформаційна боротьба тощо), тобто, у військових системах зв'язок повинен бути за будь-яких умов. Підвищення ефективності використання ресурсів ІТМ, ефективне виконання завдань може бути досягнуто за рахунок розвитку і вдосконалення системи управління зв'язком ЗСУ, в першу чергу за рахунок її автоматизації.

В основу побудови системи управління ІТМ повинно максимально використати принципи застосування системного підходу. Тоді схема побудови ІТМ буде складатися з наступних етапів: визначення вихідних даних; визначення цілей функціонування ІТМ та СУ; визначення етапів та цілей управління мережами; визначення функцій та задач управління мережами; визначення моделей, алгоритмів управління та критеріїв оцінки ефективності СУ; визначення варіантів реалізації СУ та вибір раціонального (оптимального) варіанту СУ. В подальшому провести на основі критеріїв оцінки ефективності вибір оптимального варіанту побудови системи управління.

1. Вихідні дані та цілі функціонування.

Перспективна ІТМ складається з системи управління телекомунікаційними мережами (СУ ТКМ) та телекомунікаційних мереж (ТКМ) (рис. 1). На ці дві складові системи постійно впливають зовнішнє середовище та супротивник (*E*), що безпосередньо виявляється в вигляді бойового застосування військ, вогневого враження, радіоелектронної боротьби.

Телекомунікаційні мережі $s = 1 \dots S$ мають головну мету Z^S – передача інформації між органами військового управління з заданими параметрами. ТКМ складаються з наступних мереж: проводового зв'язку, радіозв'язку, радіорелейного зв'язку, тропосферного зв'язку, супутникового зв'язку, оптоелектронного зв'язку. Всі вони описуються наступними характеристиками, що в кінцевому випадку визначають вихідні дані мереж $\{X_{jS} = X_{1S}, X_{2S}, X_{3S}, X_{4S}, X_{5S}, X_{6S}, X_{7S}\}$:

параметри мережі: кількість вузлів, розміщення на місцевості, ступінь покриття території мережею, кількість базових станцій, час функціонування мереж, протоколи інформаційного обміну у відповідності з еталонною моделлю *OSI*, тощо $\{X_{1S}\}$; структура (топологія) мереж $\{X_{2S}\}$;

склад вузлів $\{X_{3S}\}$, каналів $\{X_{4S}\}$ (тип апаратури, обладнання; тип трафіку; рівень управління; кількість радіостанцій та їх типи, тощо);

навантаження (тип, максимальне значення) $\{X_{5S}\}$, тощо;

параметри вузлів $\{X_{6S}\}$, каналів $\{X_{7S}\}$ (пропускна спроможність; кількість абонентів, що обслуговуються; потужність передавачів; частотний діапазон; алгоритми управління, тощо).

Разом з тим, кожна з цих мереж має свою систему управління – проводовими засобами, радіозасобами, оптоелектроними засобами, повітряними засобами, радіорелейними, тропосферними, супутниковими засобами.

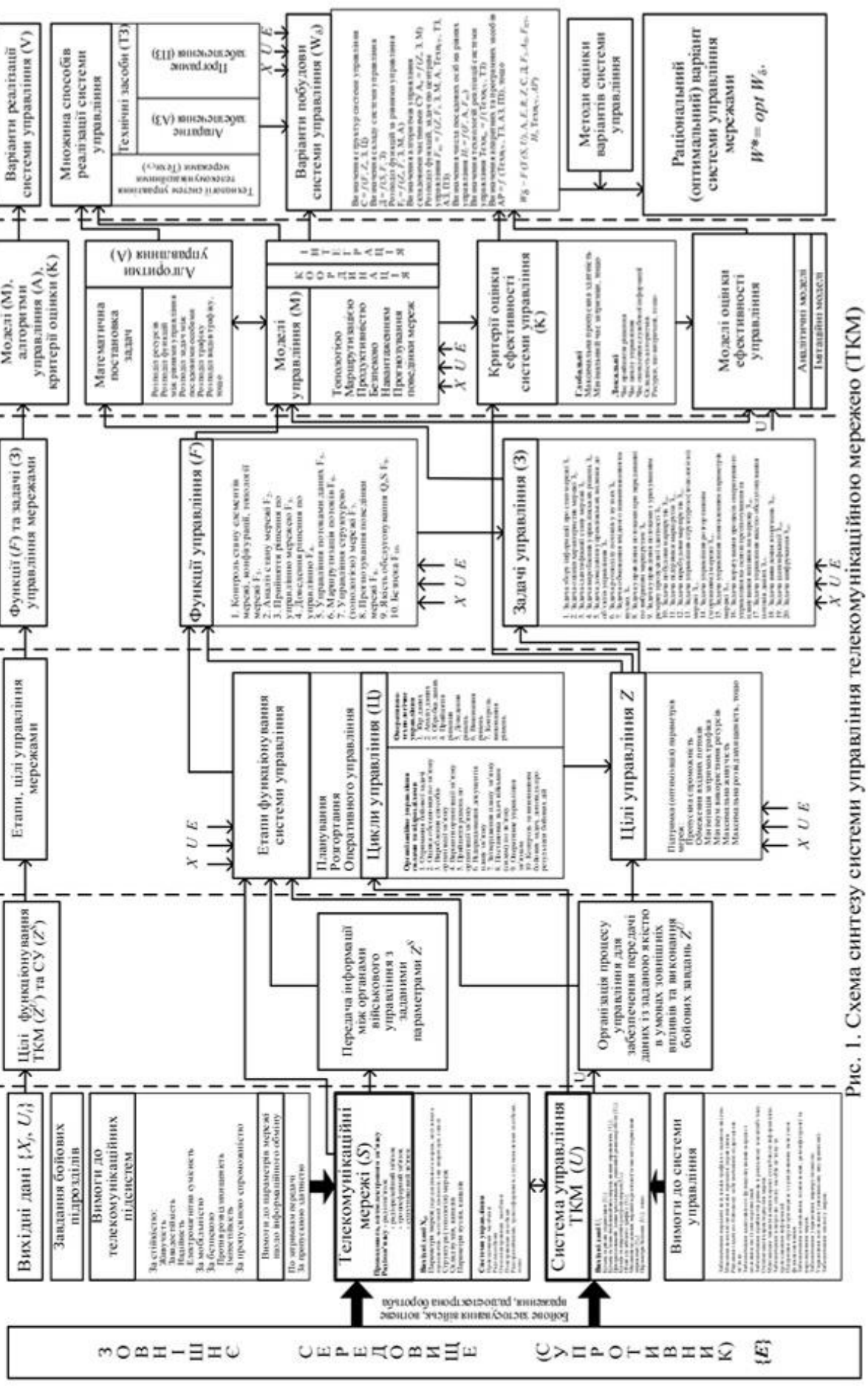


Рис. 1. Схема синтезу системи управління телекомунікаційною мережею (ТКМ)

Елементами та об'єктами управління ТКМ є: окремі мережі, зони, напрями, маршрути, вузли, канали, радіостанції, маршрутизатори, комутатори, шлюзи, телекомунікаційні платформи, сервера, АРМи посадових осіб, тощо.

До телекомунікаційних мереж пред'являються наступні вимоги [1]:

1. За стійкістю: живучість, завадостійкість, надійність, електромагнітна сумісність.
2. За мобільністю.
3. За безпекою: протирозвідзахищеність, імітостійкість.
4. За пропускною спроможністю.

В процесі експлуатації телекомунікаційних мереж до параметрів передачі даних (рекомендації міжнародного союзу електрозв'язку – сектор телекомунікацій *ITU-T*) пред'являють вимоги до [2]: затримок передачі інформації; швидкості передачі даних; імовірності помилок в пакетах; пропускної здатності мережі, тощо.

В основу синтезу СУ ТКМ покладено агрегативно-декомпозиційний підхід, що дозволяє представити майбутню систему у вигляді сукупності взаємопов'язаних елементів різного рівня деталізації [3]. Цей підхід включає послідовну декомпозицію цілей, функцій, задач, що виконуються системою та агрегування на відповідному рівні деталізації елементів для генерування варіантів побудови системи на рівні деталізації, що розглядається. В подальшому будемо використовувати цей підхід.

Система управління U телекомунікаційними мережами (ТКМ) має глобальну мету Z^U – забезпечення передачі даних із заданою якістю в умовах зовнішніх впливів та виконання бойових завдань.

До системи управління телекомунікаційною мережею пред'являються наступні вимоги [4, 5]:

1. Забезпечення передачі всіх видів трафіка з заданою якістю.
2. Максимальна автоматизація процесів управління.
3. Рішення задач по бойовому забезпеченню підрозділів зв'язку.
4. Забезпечення адаптивного функціонування мережі з можливістю її самоорганізації.
5. Забезпечення прийняття рішень в реальному масштабі часу.
6. Оптимізація характеристик мереж.
7. Мінімальне завантаження мережі службовою інформацією.
8. Забезпечення контролю стану засобів зв'язку та проходження інформації.
9. Підтримка структури (топології) мереж з урахуванням змін умов функціонування.
10. Забезпечення планування, поновлення, реконфігурації та нарощування мереж.
11. Забезпечення управління маршрутизацією.
12. Управління потоками (зовнішніми, внутрішніми).
13. Забезпечення кіберзахисту мереж, тощо.

Вихідними даними для системи управління телекомунікаційною мережею мають бути наступні дані $U = \{U_i\}, i = \overline{1,I}$:

1. Кількість рівнів управління $\{U_1\}$.
2. Кількість телекомунікаційних мереж, якими управляють $\{U_2\}$.
3. Централізований, децентралізований, змішаний режими роботи $\{U_3\}$.
4. Кількість апаратних та програмних ресурсів мереж $\{U_4\}$.
5. Обсяг службового трафіку $\{U_5\}$.
6. Множина можливих варіантів реалізації технології управління мережами $\{U_6\}$.
7. Параметри безпеки $\{U_7\}$, тощо.

2. Етапи, цілі управління мережами.

Етапами функціонування системи управління є планування,розгортання(організаційні способи реалізації) і оперативного управління (організаційно-технологічний спосіб).

Етап плануванняздійснюється центром управління мережі.Сутність плануванняполягає в організації діяльності органу управління, яка направлена на формування і прийняття рішення по організації мережі (способи побудови мережі),

своєчасну розробку документів і доведення їх до підлеглих (постановка задач перед силами зв’язку та розподіл сил та засобів [4, 5].

Система управління повинна реалізовувати наступні види управління зв'язком: ***організаційне, організаційно-технологічне і технологічне*** [4, 5].

1. На рівні ***організаційного управління*** повинні реалізовуватися цільові завдання функціонування системи зв'язку шляхом планування зв'язку, управління побудовою системи зв'язку і бойовим застосуванням з'єднань і частин зв'язку.

Завдання планування при управлінні мережами являють собою процес постановки цілей, які потребують досягнення і розробки програми їх досягнення, оформленої у вигляді сукупності документів по зв'язку, основним з яких є план зв'язку. Змістом процесу планування є розподіл ресурсів мереж і визначення порядку їх використання. Сутність і зміст планування зв'язку визначається її цільовим призначенням, характером функціонування та принципами застосування в той або іншої обстановки.

Завдання планування розбиваються на групи: для стаціонарного та мобільного компоненти, для радіозв'язку, для радіорелейного, для тропосферного та космічного зв'язку, для вузлів зв'язку та ліній прив'язки, для мереж доступу.

Завдання автоматизованого управління зв'язком на організаційному рівні повинні вирішуватися на основі застосування комплексів засобів автоматизації управління зв'язком, загального програмного забезпечення, спеціального програмного забезпечення організаційного управління та елементів інформаційного забезпечення – баз даних організаційного управління, реалізованих на основі сучасних засобів прикладної середовища систем підтримки прийняття рішень (СППР).

Для безпосереднього вирішення завдань організаційного управління зв'язком на організаційному рівні управління повинні виділятися наступні основні логічні підсистеми:

підсистема обліку даних обстановки по зв'язку;

підсистема моделювання функціонування мереж зв'язку;

підсистема планування зв'язку;

підсистема планування застосування елементів системи зв'язку (вузлів, центрів, ліній, мереж,

системи технічного забезпечення зв'язку і АСУ, резерву сил і засобів зв'язку та автоматизації);

підсистема оперативного управління зв'язком;

підсистема забезпечення оперативно-технічної служби на елементах системи зв'язку;

підсистема всебічного забезпечення функціонування системи зв'язку.

2. На рівні ***організаційно-технологічного управління*** повинні вирішуватися завдання по управлінню мережами і послугами зв'язку у взаємодії з підсистемами організаційного та технологічного управління.

Для вирішення завдань організаційно-технологічного управління зв'язком на відповідному рівні управління повинні виділятися наступні основні логічні підсистеми:

підсистема управління якістю надання видів і послуг зв'язку,

підсистема контролю стану і зміна структури мереж зв'язку.

Основу технічної реалізації даного рівня повинен становити комплекс засобів автоматизації оперативно-технічного управління мережами зв'язку, що включає:

автоматизовані робочі місця посадових осіб, об'єднані локальною обчислювальною мережею з серверами додатків, і бази даних;

програмне та інформаційне забезпечення, що забезпечує автоматизоване рішення задач оперативно-технічного управління.

3. На рівні ***технологічного управління*** повинні вирішуватися завдання контролю і зміни технічного стану засобів зв'язку (мережевих елементів) мереж зв'язку шляхом створення відповідної підсистеми.

Технологічне управління зв'язком здійснюється з використанням можливостей сучасних засобів зв'язку сприймати керуючі команди і сигнали з боку АСУЗ, змінювати під

їх впливом свої стани, а також видавати в АСУЗ інформацію про свій стан.

Для управління зв'язком і військами зв'язку в різних умовах обстановки може організовуватися шляхом створення окремих мереж управління (службового зв'язку) або шляхом використання канального ресурсу мереж зв'язку.

На мережу управління покладаються завдання по передачі командної інформації, передачі даних, передачі команд технологічного управління комплексами технічних засобів системи зв'язку військового призначення, управління рухомими одиницями тощо. Виконання даних завдань може забезпечуватися за рахунок створення відповідних підсистем мережі управління.

Крім цього в АСУЗ повинна створюватися підсистема безпеки функціонування, яка спрямована на забезпечення схоронності даних, що циркулюють в системі, розмежування доступу посадових осіб органів управління зв'язком до інформації, їх аутентифікацію і недопущення несанкціонованого втручання.

Етап розгортанняполягає в розгортанні мережі взаданому районі. При цьому задачі етапу розгортання (перепланування) мережі можуть виконуватися й на етапі оперативного управління при значних її змінах (ушкодженні, введенні нових угруповань військ й ін.). Контроль за етапом розгортання мережі здійснюється із центру управління мережею.

На етапі оперативного управлінняза прийнятими критеріями ефективності постійнооцінюється стан мереж, і приймаються міри (відповідно до плану та реальної обстановки) по втриманню показників ефективності функціонування в заданих межах або здійснюється їх системна (користувальницька) оптимізація.

Задачі оперативного управління (на відмінність задач планування) вирішуються змішаним способом (централізовано/децентралізовано) у режимі реального часу, а за змістом багаторазово їх повторюють. Цикл управління (Ц) мережі здійснюється органом управління (особою, що приймає рішення) та включає (див. рис. 1) [5, 6]:

– ***збір інформації про стан мережі*** (при цьому необхідно приймати рішення за об'ємом, типом, рівнями, функціями збору службової інформації);

– ***аналіз даної інформації та її обробка*** – визначаються: ступінь виконання мережею своїх функцій, необхідність управляючого впливу, цілі управління з подальшою деталізацією їх на підцілі;

– ***прийняття рішення*** (реконфігурація мережі, перерозподіл каналів транспортної мережі та мережі доступу, маршрутизація та обмеження потоків, оновлення елементів мережі тощо);

– ***доведення тавиконання рішення*** (видача та доведення управляючих команд, розсилання службової інформації, резервування ресурсу, налаштування обрання, встановлення потужності передавачів, спрямованість антен тощо);

– ***контроль виконання рішень*** у задані часові інтервали.

Цілями системи управління (Z^U) (рис. 1) можуть бути екстремум або підтримка (виступають як обмеження) заданих параметрів функціонування всієї мережі або її елементів (зона, напрямок, маршрут, вузол, канал), що можна представити в вигляді [4, 5]:

$$Z^U = f(C, P^e, P^{\text{зв}}, F, Y^{\text{СУ}}, O, R) \to opt$$
$$\text{при обмеженнях } R \le R_{\text{доп}} \text{ та } O \le O_{\text{доп}},\ \{T_{\text{ц}} \le T^{\text{доп}}\} \to min$$

де C – структура системи управління;

P^e – множина параметри елементів системи управління;

$P^{\text{зв}}$ – множина параметрів зв'язків між елементами системи управління;

F – сукупність функцій, що реалізуються системою управління ТКМ;

$Y^{\text{СУ}}$ – умови функціонування системи управління;

O – обмеження на значення характеристик властивостей системи управління, що створюється;

R – обмеження на ресурси, за допомогою яких буде синтезуватися система управління;

$T_{ц}$ – час циклу оперативного управління мережею;

$T^{доп}$ – час, що відведений на управління мережею або її етапи, який визначається директивними документами.

Разом з тим, у системі управління мережею існує ієрархія цілей Z^U. Загальна ціль поділяється на підцілі: планування та оперативного управління. Оперативне управління в свою чергу поділяється на управління якістю обслуговування, конфігурацією, несправностями, ресурсами тощо. В загальному випадку Z^U можна представити у вигляді списків підцілей, які пов'язані визначеними відношеннями [6, 7]:

$$Z^U = \left\{Z_0\Theta_{01}\{Z_{11}, Z_{12}, \dots, Z_{1n}\}\Theta_{12}\{Z_{21}, Z_{22}, \dots, Z_{2n}\} \dots \Theta_{ij}\{Z_{k1}, Z_{k2}, \dots, Z_{kn}\}\right\},$$

де Z^U – ієрархія цілей системи управління; Z_0– глобальна ціль;Z_{ij} – i-а підціль j-го рівня ієрархії цілей, $i = \overline{1,I}; j = \overline{1,J}$; Θ – множина відношень на підцілі ієрархії цілей.

3. Функції та задачі управління мережами.

Система управління ТКМ повинна забезпечити виконання основних функцій $F = \{F_\xi\}, \xi = \overline{1,\xi}$,як в циклі управління так окремі функції.

Цикл управління складається з функцій:

1. Контроль стану елементів мережі, конфігурації, топології мережі F_1.
2. Аналіз стану мережі F_2.
3. Прийняття рішення по управлінню мережею F_3.
4. Доведення рішення по управлінню F_4.

Окремі функції, що безпосередньо не входять до циклу управління.

5. Управління потоками даних F_5.
6. Маршрутизація потоків F_6.
7. Управління структурою (топологією) мережі F_7.
8. Прогнозування поведінки мережі F_8.
9. Якість обслуговування Q_oS F_9.
10. Безпека F_{10}, тощо.

На систему управління мережею покладаються наступні задачі $З = \{З_\eta\}, \eta = \overline{1,\eta}$:

1. Задача збору інформації про стан мережі $З_1$.
2. Задача оцінки характеристик мережі $З_2$.
3. Задача ідентифікації стану мережі $З_3$.
4. Задача вироблення управлінських рішень $З_4$.
5. Задача доведення управлінських впливів до об'єктів управління $З_5$.
6. Задача розподілу потоків у вузлах $З_6$.
7. Задача обмеження вхідного навантаження на вузлах $З_7$.
8. Задача управління потоками при передаванні по вибраним маршрутам $З_8$.
9. Задача управління потоками з урахуванням резерву пропускної здатності $З_9$.
10. Задача побудови маршрутів $З_{10}$.
11. Задача підтримки маршрутів $З_{11}$.
12. Задача перебудови маршрутів $З_{12}$.
13. Задача управління структурою (топологією) мережі $З_{13}$.
14. Задача управління розгортанням (згортанням) мережі $З_{14}$.
15. Задача управління поновленням параметрів мережі $З_{15}$.
16. Задача корегування процесів оперативного управління на основі прогнозування та планування впливів на мережу $З_{16}$.
17. Задача управління якістю обслуговування потоків даних $З_{17}$.
18. Задача виявлення вторгнень $З_{18}$.
19. Задача ідентифікації $З_{19}$.
20. Задача шифрування $З_{20}$, тощо.

Функції та задачі управління мережами визначають майбутню логіку роботи СУ ТКМ на всіх етапах функціонування (див. табл. 1). При виконанні кожної функції управління можливе вирішення однієї або кількох задач управління.

Таблиця 1

№ з/п	Функції управління	Задачі управління
1	Контроль стану елементів мережі, конфігурації, топології мережі F_1.	Задача збору інформації про стан мережі $З_1$ (для всіх функцій управління).
2	Аналіз стану мережі F_2.	Задача оцінки характеристик мережі $З_2$. Задача ідентифікації стану мережі $З_3$.
3	Прийняття рішення по управлінню мережею F_3.	Задача вироблення управлінських рішень $З_4$.
4	Доведення рішення по управлінню F_4.	Задача доведення управлінських впливів до об'єктів управління $З_5$.
5	Управління потоками даних F_5.	Задача розподілу потоків у вузлах $З_6$. Задача обмеження вхідного навантаження на вузлах $З_7$. Задача управління потоками при передаванні по вибраним маршрутам $З_8$. Задача управління потоками з урахуванням резерву пропускної здатності $З_9$.
6	Маршрутизація потоків F_6.	Задача побудови маршрутів $З_{10}$. Задача підтримки маршрутів $З_{11}$. Задача перебудови маршрутів $З_{12}$.
7	Управління структурою (топологією) мережі F_7.	Задача управління структурою (топологією) мережі $З_{13}$. Задача управління розгортанням (згортанням) мережі $З_{14}$. Задача управління поновленням параметрів мережі $З_{15}$.
8	Прогнозування поведінки мережі F_8.	Задача корегування процесів оперативного управління на основі прогнозування та планування впливів на мережу $З_{16}$.
9	Якість обслуговування Q_oS F_9.	Задача управління якістю обслуговування потоків даних $З_{17}$.
10	Безпека F_{10}.	Задача виявлення вторгнень $З_{18}$. Задача ідентифікації $З_{19}$. Задача шифрування $З_{20}$.

4. Моделі, алгоритми управління, критерії оцінки ефективності системи управління, моделі оцінки ефективності управління.

На основі визначених функцій $\{F\}$, задач управління $\{З\}$ здійснюється їх математична постановка та визначаються методи рішення. Для цього може використовуватися математичний апарат теорії множин, нечітких множин, графів, теорії ігор тощо. Далі синтезуються відповідні алгоритми управління $\{A\}$. В подальшому, на основі створених алгоритмів реалізуються моделі управління $\{M\}$ під можливі варіанти подій в мережі, здійснюється їх координація роботи та інтеграція в системне середовище.

Виконання цілей $\{Z\}$, функцій $\{F\}$, задач управління $\{З\}$, що були поставлені перед системою управління мережами, повинно гарантувати функціонування ТКМ в цілому, окремих мереж, напряму, каналу, вузла, маршруту, обладнання з необхідною ефективністю. Система управління мережами досить ефективна, якщо вона забезпечує заданий приріст

показника її ефективності. Наявність сукупності критеріїв ефективності обумовлює багатокритеріальність задач управління та значно ускладнює розробку формальних методів:

$$K = \{K_\upsilon\}, \upsilon = \overline{1, Y}.$$

Звичайним рішенням [6] є визначення головного критерій ефективності (виходячи з поточної ситуації в мережі), який підлягає оптимізації, а інші переводити в розряд обмежень. Наприклад, пропонується використати метод ієрархічного цільового динамічного оцінювання альтернатив [8, 9], а саме глобальні (максимальна пропускна здатність, мінімальний час затримки) та локальні (час циклу управління, об'єм службового трафіку) критерії.

Глобальні критерії(оцінюють якість прийнятих рішень системою управління)*:*

1. Максимум (завдане значення) пропускної здатності ρмережі, яка визначає сумарну пропускну здатність всіх напрямків передачі:

мережі $\rho_{\text{М}} = \sum_{i=1}^{I} \rho_{H_i}$.

2. Мінімальний час затримки пакетів (завдане значення) $t_{\text{з}}$:

$mint_{\text{з}}$ ($t_{\text{з}} \le t_{\text{з зад}}$).

Локальні критерії(оцінюють саму систему управління)*:*

1. Мінімальний час циклу управління:

$$T_{\text{ЦУ}} = t_{\text{зі}} + t_{\text{ан}} + t_{\text{пр}} + t_{\text{дов}}, T_{\text{ЦУ}} \le t_i^{\text{доп}} \to min,$$

де – $T_{\text{ЦУ}}$ – час циклу оперативного управління мережею – проміжок часу, протягом якого здійснюється послідовне рішення задач управління до повного її виконання в масштабі даної системи управління;

$t_{\text{зі}}$ – час на збір інформації про стан мережі;

$t_{\text{ан}}$ – час на оцінку характеристик мережі та ідентифікацію стану мережі;

$t_{\text{пр}}$ – час, який необхідний на вироблення управлінських рішень;

$t_{\text{дов}}$ – час доведення управлінських впливів до об'єктів управління;

$t_i^{\text{доп}}$ – час, що відведений на оперативне управління мережею, який визначається директивними документами.

2. Мінімальний об'єм службового трафіку$V_{\text{СТ}} \to min$– залежить від прийнятого в СУ мережею способу, об'єму, періоду розсилання службової інформації (маршрутні повідомлення, квитанції, hello-повідомлення, виміри трафіку), складності прийнятих алгоритмів управління, розмірністю мережі, тощо.

3. Фінансово-економічні: вартість розробки та експлуатації системи управління.

Для оцінки ефективності системи управління використовують два типи моделей – *аналітичні* й *імітаційні (статистичні)*.

За допомогою використання аналітичного або імітаційного моделювання проводиться оцінка ступеня виконання поставлених цілей управління кожного рівня управління та системи управління загалом з урахуванням цілей управління, показників якості функціонування ТКМ, виділеного ресурсу мережі, процесу функціонування ТКМ за відомими алгоритмами.

Множина функцій та задач управління разом з вихідними даними $\{X, U, E\}$ визначають функціональну модель управління. Авторами пропонується здійснювати цільову координацію функціональних моделей підсистем та інтеграцію рівнів еталонної моделі OSI.

5. Варіанти реалізації (W_{δ}).

На основі отриманих моделей (M), алгоритмів (A) управління формується множина способів реалізації системи управління, де враховуються технології СУ ТКМ, технічні засоби їх реалізації, апаратне та програмне забезпечення. З урахуванням способів реалізації системи управління, вихідних даних, критеріїв та моделей оцінки ефективності управління формується множина варіантів побудови системи управління (W_{δ}), яка включає наступні

складові: структура системи управління (С); склад системи управління (Д); розподіл функцій за рівнями управління (F_l); алгоритми управління підсистемами СУ (*АП*); розподіл функцій (задач) по центрам управління ($F_{ЦУ}$); число посадових осіб на рівнях управління (H_l); технології реалізації системи управління ($Техн_{СУ}$); апаратні та програмні засоби (*АР*), тощо:

$$W_\delta = F(Y\,(S,U),\ \Lambda, E,\ R,\ Z, С, Д,\ F_l,\ A_П,\ F_{ЦУ},\ H_l,\ Техн_{СУ},\ AP)$$

де W_δ– δ-й варіант побудови системи управління; Z – цілі управління; *R* – виділений ресурс; Λ – вхідні потоки даних; *E* – зовнішні впливи; *S* – телекомунікаційна мережа; *U* – управляючий вплив СУ на ТКМ; *Y* – реалізація вихідного процесу управління; С – структура системи управління; Д – склад системи управління; F_l – розподіл функцій за *l*-м рівнем управління; $A_П$ – алгоритми управління складовими частинами СУ; $F_{ЦУ}$ – розподіл функцій, задач по центрам управління; H_l – число посадових осіб на рівнях управління; $Техн_{СУ}$ – технології реалізації системи управління; *AP* – вибрані апаратні та програмні засоби; *l* – рівні управління СУ.

Структура системи управління повинна відповідати тим завданням, які ставляться перед системою управління по управлінню ТКМ. Система управління повинна являти собою ієрархічну організаційно-технологічну систему, що забезпечує змішане (централізоване/децентралізоване) управління телекомунікаційними підсистемами. Управління повинно здійснюватися в реальному масштабі часу.

Система управління повинна створюватися з орієнтацією на нові інформаційні технології, перспективу зрощування телекомунікаційних і комп'ютерних мереж, методи розподіленої обробки інформації, використання технологій *Internet, SDN, IP*, а також хмарні технології та інші технології віртуалізації.

В системі управління повинні передбачатися резервні експлуатаційно-технічні засоби для відновлення функціонування основних напрямків зв'язку, а також відновлення управління мережами у зонах відповідальності. Надійність і живучість системи управління повинні бути вище значень цих параметрів ТКМ. Для забезпечення надійності та живучості автоматизованої системи управління зв'язком ЗСУ основні інформаційні та обчислювальні ресурси повинні бути розміщені в географічно рознесених пунктах управління. В перспективі пропонується застосування технологій хмарних середовищ, що будуть реалізовані центрами обробки даних (ЦОД).

Для отримання оптимального варіанту системи управління мережами краще використовувати метод (векторної) послідовної оптимізації з використанням принципу максимізації суми зважених критеріїв з використанням методів експертних оцінок. Тоді раціональний (оптимальний) варіант системи управління мережами:

$$W^* = \mathrm{opt} W_\delta,\ \delta = \overline{1,\Omega}.$$

Таким чином, запропонована методологія синтезу сучасної автоматизованої системи управління телекомунікаційними системами військового призначення за п’ятьма етапами. Розглянуто цілі функціонування ТКМ та системи її управління, визначено вимоги до телекомунікаційних підсистем й системи управління та проведено їх детальний опис. Представлений процес функціонування системи управління за етапами та циклами управління. Описано основні функції та задачі управління, які потрібно вирішувати в циклі управління. Визначено перелік моделей й алгоритмів управління, множина функцій, задач управління, які формують функціональну модель управління.

Отримані результати складають основу методології синтезу систем управління інформаційно-телекомунікаційними мережами. Це дозволить у майбутньому побудувати ефективну систему управління системою зв’язку військового призначення для рішення різного роду завдань планування, розгортання та оперативного управління з використанням технологій інтелектуалізації.

ЛІТЕРАТУРА

1. ДСТУ 3265-1995 Зв'язок військовий. Терміни та визначення.

2. Битнер В. И. Нормирование качества телекоммуникационных услуг: Учебное пособие для вузов / В. И. Битнер, Г. Н. Попов. – М: Горячая линия-Телеком, 2009.

3. Цвиркун А. Д. Основы синтеза структуры сложных систем / А. Д. Цвиркун. – М: Наука, 1982. – 200 с.

4. Design of the Next Generation Military Network Management System Based on NETCONF [Електроннийресурс] / W.Zhu, N. Liu, W. Shan, G. Fu // Information Technology:New Generation. – 2008.

5. Бовда Е. М. Концептуальні основи синтезу автоматизованої системи управління зв’язком військового призначення / Е. М. Бовда, Ю. А. Плуговий, В. А. Романюк. // ВІТІ. – 2016. – №1. – С. 3–17.

6. Хиленко В.В.Методи підвищення показників якості системи управління телекомунікаційними мережами: Монографія / В.В. Хиленко,Л.Н. Беркман, Г.Ф. Колченко, О.Г. Варфоломеєва . – К.: Норіта-плюс, 2007.– 236 с.

7. Шибанов В.С. Средства автоматизации управления в системах святи / В.С. Шибанов.– М.: Радио и связь, 1990. – 232 с.

8. Боговик А. В. Эффективность систем военной связи и методы её оценки. / А. В. Боговик, В. В. Игнатов. – СПб: ВАС, 2006.

9. Романюк В.А. Цільові функції оперативного управління тактичними радіомережами /В.А. Романюк// Збірник наукових праць ВІТІ НТУУ "КПІ". – 2012. – № 1. – С. 109 – 117.

Гармаш Д. В. (ХНУ ім.Каразіна)
Малєєва Г. А. (ХНУ ім.Каразіна)

ЗДАТНІСТЬ АЛГОРИТМУ RAINBOW ПРОТИДІЯТИ РІЗНОМАНІТНІМ МЕТОДАМ КРИПТОАНАЛІЗУ

Багатовимірні квадратичні схеми є перспективним рішенням для потреби квантових систем, стійких до атак від квантового комп'ютера. Однак, оскільки цей клас відносно молодий і багато схем цього класу були порушені в минулому, існує дуже мало їх реалізацій, особливо на вбудованих мікроконтролерах. Щоб оцінити, чи можуть ці схеми колись замінити чинні стандарти, необхідно знати, наскільки ефективно їх можна впровадити на різних платформах. У процесі цієї роботи дано теоретичне введення до багатовимірних квадратичних схем. Потім впроваджуються схеми, які певний час витримували атаки: Unbalanced Oil and Vinegar (UOV), Rainbow та enTTS. Особлива увага приділяється виявленню усіх загальних моментів схеми Rainbow.

1. Загальні положення щодо схеми ЕП RAINBOW

Наразі криптосистеми, що засновані на квадратичних поліномах, пройшли за останні 10 років суттєвий розвиток та визнання. Теоретичною основою конструкцій Oil-Vinegar є доведена теорема, згідно з якою вирішення (визначення) набору багатоваріантних поліноміальних рівнянь над кінцевим полем є експоненційно складною проблемою, хоча це є у загальному випадку як необхідною, так і достатньою умовами [2].

Цей напрямок досліджень пов'язаний з появою конструкції Мацумото та Імаї, в тому числі з використанням рівняння лінеаризації [1]. Далі Патарін та його співробітники доклали великих зусиль для розробки безпечних багатоваріантних криптосистем. Один з конкретних напрямків, яким займались Патарін та його співробітники, пов'язаний з рівняннями лінеаризації Dragon, Oil and Vinegar, Unbalanced Oil-Vinegar [1]. Побудова механізму ЕП Rainbow на основі Oil and Vinegar, Unbalanced Oil-Vinegar грунтується на тому, що певні квадратичні рівняння можна легко розв'язати, якщо є можливість вгадувати декілька варіантів [1].

Нехай k буде кінцевим полем. Ключовою конструкцією є відображення (карта) F від k^{o+v} до k^{o}:

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = F(x_1,...,x_0,x_1^{'},...,x_v^{'}),...,F_0(x_1,...,x_0,x_1^{'},...,x_v^{'}) \quad (1)$$

і кожна F_l у формі

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = \sum a_{l,i,j}x_i x_j + \sum b_{l,i,j}x_i^{'}x_j^{'} + \sum c_{l,i}x_i + \sum d_{l,i}x_j^{'} + c_l, \quad (2)$$

де x_i, $i = 1,...,o$ це Oil значення та $x_j^{'}, j = 1,...,v$ значення Vinegar у кінцевому полі k.

Потрібно звернути увагу на схожість наведеної вище формули з рівняннями лінеаризації. Такий тип поліномів називається "поліномом Oil-Vinegar". Причина, по якій вона називається схема "Oil-Vinegar", пов'язана з тим, що в квадратичному вимірі змінні Oil та Vinegar не змішуються повністю. Це дозволяє легко знайти одне рішення для будь-якого рівняння виду

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = (y_1,...,y_o), \quad (3)$$

коли $(y_1,...,y_o)$ дано. Щоб знайти одне рішення, потрібно лише випадковим чином вибрати значення для Vinegar змінних та підключити їх до рівнянь вище, що дасть набір o лінійних рівнянь з o змінними. Це має, з імовірністю, близькою до 1, дати рішення. Якщо цього не сталося, можна спробувати ще раз, вибравши різні значення для Vinegar змінних, поки не вдасться знайти рішення [4].

Це сімейство криптосистем розроблено спеціально для схем підписів, де потрібно лише знайти одне рішення для даного набору рівнянь, а не унікальне рішення. Застосовуючи відображення (карту F), ми «приховуємо» її, складаючи її з лівої та правої сторін за двома

оборотними афінними лінійними відображеннями L_1 та L_2. Оскільки L_1 знаходиться на k^o, а L_2 на k^{o+v}, це генерує квадратичне відображення (карту)

$$F^{-} = L_1 \circ F \circ L_2 \tag{4}$$

від k^{o+v} до k^o.

Збалансована схема Oil-Vinegar характеризується тим, що $o = v$, але її удосконалили Кіпніс та Шамір, використовуючи матриці, що відносяться до білінійних форм, визначених квадратичними поліномами [3].

Для незбалансованої схеми Oil-Vinegar, $v > o$, показано, що конкретна атака має складність приблизно $q^{v-o-1}o^4$, коли $v \approx o$. Це означає, що якщо o не надто велике (менше ніж 100) і дане фіксоване поле розміром q, тоді $v - o$ має бути досить великим, але також не надто
великим, щоб забезпечити безпеку схеми.

Однак слід зауважити, що в цій схемі документ, що підписується, є вектором у k^o, а підпис – вектором у k^{o+v}. Це означає, що підпис має принаймні вдвічі більший розмір документа, і при великому $v + o$ система стає менш ефективною.

В рамках статті пропонується конструкція, яка використовує конструкцію Oil-Vinegar кілька разів, так що в підсумку підпис буде лише трохи довшим за документ. Отже, ця схема набагато ефективніша. Її називають схемою Rainbow.

2. Здатність супротиву атакам алгоритму Rainbow.

Представляється короткий криптоаналіз схеми підпису Rainbow, розглянувши його для наведеного вище прикладу. Є кілька способів атак, з якими будуть мати справу користувачі алгоритму. Для тих методів, де використовуються квадратні форми, слід пам'ятати, що теорія квадратних форм над скінченними полями відрізняється, коли характеристика дорівнює 2, у порівнянні з випадком, коли характеристика є непарною [6].

2.1. Метод зниження рангу

Метод зниження рангу використовується для розбиття схеми підпису бірaціональної перестановки Шаміра. Причина, по якій ця атака може спрацювати, полягає в тому, що простір, що охоплюється поліноміальними компонентами шифру схеми Шаміра, складається з прапора пробілів:

$$V1 \subset V2 \subset \cdots \subset Vt, \tag{5}$$

де V_t – простір, охоплений поліноміальними компонентами шифру, кожна V_i є власною підмножиною V_{t+1}, а ранг відповідної білінійної форми, що відповідає елементам у $V_{t+1} - V_i$, занадто більший, ніж у V_i, а різниця розмірів між V_i та V_{t+1} рівно 1. Завдяки цим властивостям, зокрема останньому, це дозволяє легко знайти цей прапор просторів, а саме всі V_i, спочатку знайшовши V_{n-1}, потім V_{n-2} і так далі шляхом зменшення рангу [8]. Але цей метод атаки вже не може працювати проти цієї схеми. Причиною цього є те, що, в нашому випадку, існує також такий прапор просторів, що кількість компонентів – це точно кількість рівнів,

розмірність кожного компонента прапора точно відповідає розміру V_{i+1}, $i = 1,...,u-1$, але різниця в розмірах останніх двох великих просторів – це точно $O_u - 1$, яка була обрана спеціально для досить великого числа 11, на відміну від випадку Шаміра, коли воно дорівнює 1.

Властивість, наведена вище, якраз і є причиною того, що атака більше не може працювати. Тут не можна використовувати метод зниження рангу через те, що $O_u - 1 = 11$ і більше
не 1. „Останній товстий рівень Oil" дозволяє схемі протистояти атаці зниження рангу [7].

2.2. Метод атаки на Oil-Vinegar схеми

Аналіз показав, що дія L_1 полягає у змішуванні всіх поліноміальних компонентів F. Отже, кожен компонент шифру *F* тепер належить до верхнього рівня поліномів Oil-Vinegar, а саме всі вони є елементами P_4. Це багаточлени Oil-Vinegar з 22 змінними Vinegar та 11 змінними Oil [1]. Для цього випадку можна застосувати метод для незбалансованої схеми підпису Oil-Vinegar, щоб спробувати атакувати систему, що дозволить відокремити змінні верхнього шару Oil-Vinegar. Для цього нам потрібно розділити верхній (або кінцевий) рівень з 11 змінних Oil та 22 змінних Vinegar. Відповідно до криптоаналізу складність атаки цього першого кроку становить $q^{22-11-1} \times 11^4 > 2^{90}$.

2.3. Метод Мінранка

Існує два абсолютно різних способи використання методу Мінранка. Перший – пошук полінома, асоційована матриця якого має найнижчий ранг серед усіх можливих варіантів. Цей набір поліномів із 6 змінними Vinegar та 6 Oil належить до першого рівня, тобто $P1$, і позначався $F^{\sim}_1$. Для цього спочатку ми прив'язуємо до кожного полінома білінійну форму, яка має матрицю розміром 33×33. Потім ми можемо використовувати лінійні комбінації матриць, пов'язаних із компонентами F, для виведення полінома, пов'язана з яким матриця має ранг 12 [3]. В цьому випадку, щоб атакувати систему, проблемою стає пошук матриці рангу 12 серед групи з 27 матриць розміром 33×33. З методу Мінранка ми знаємо, що складність пошуку такої матриці становить $q^{12} \times 27^3$, що набагато більше, ніж 2100.

Інша можливість – це пошук поліномів, що відповідають поліномам у другому останньому рівні, а саме той, який належить P_3 і походить від лінійних комбінацій $F^{\sim}_i, i < 4$. У цьому випадку метод Міранка однозначно не може бути використаний , оскільки вони взагалі мають ранг 22. Одним із шляхів, безсумнівно, є випадковий пошук. Оскільки розмірність P_3 дорівнює 16, це стає проблемою пошуку елемента в підпросторі розмірності 16 в загальному просторі розмірності 27. Отже, такий випадковий пошук потребує щонайменше q^{11} пошуків, щоб знайти його, але нам також потрібно визначити, чи дійсно рейтинг нижче 22 для кожного пошуку. У цьому випадку загальна складність повинна бути не менше $q^{11} \times (22 \times 33^2 / 3) > 2^{100}$. Ця ідея атаки насправді пов'язана з іншим методом атаки, і наведений вище аргумент пояснює, чому цей метод більше не може працювати [8].

З останніх результатів електронного друку в цьому напрямку, де вивчаються дуже загальна система, яка називається STS, ми знаємо, що їх метод може бути застосований і до нашого випадку. Відповідно до їх оцінки, безпека нашої системи становить принаймні $27 \times 33^3 \times (2^8)^{12} \times 5 > 2^{100}$.

2.4. Атака за допомогою структури багатошаровості.

Для випадку криптосистеми Мацумото – Імай Патарін зрозумів, що якщо шифр складається з декількох незалежних паралельних «гілок», можна виконати поділ змінних таким чином, що всі поліноми в шифрі виведені як лінійні комбінації поліномів над кожною групою змінних. Ця властивість насправді може бути використана для атаки на систему. На перший погляд, можна подумати, що рівні виглядають як різні «гілки». Тим не менше, слід усвідомити, що рівні жодним чином не є «незалежними», оскільки кожен з них будується на попередньому. Простіше кажучи, можна сказати, що всі рівні злипаються, і ми ніяк не можемо зробити будь-якого розділення змінних. Це зрозуміло, коли розглядаються поліноми останнього рівню P_4. Тому атака з використанням властивості паралельних незалежних гілок у тут не може працювати. Подібним чином можна стверджувати, що атака з використанням системних систем також не може працювати тут, оскільки немає гілок і все насправді «склеєно» [2].

2.5. Загальні методи

Іншими методами, які можуть бути використані для атаки на нашу схему підписів, є ті, які безпосередньо вирішують поліноміальні рівняння, наприклад метод XL та різні його узагальнення, або такі, що використовують основи Грубонера. Безумовно, дуже складно вирішити набір з 27 рівнянь із 33 змінними, оскільки для цього набору рівнянь існує надто багато рішень. Загалом, набагато краще розв'язувати рівняння лише з однією змінною. Через характер проєктування системи можна здогадатися про значення для будь-якого набору змінних $v_1 = 6$, і ми маємо ймовірність $1 / e < 1 / 2.71828 < 0.37$ отримати унікальне рішення.

Тепер задача стає проблемою вирішення набору з 27 квадратних рівнянь із 33 змінними. Ми повинні думати про це так, ніби це сукупність випадково вибраних квадратних рівнянь. Відповідно до того, що прийнято вважати, для вирішення цього набору рівнянь складність становить щонайменше $23 \times 27 > 281$.

З цього ми робимо висновок, що загальна складність атаки на наш приклад становить принаймні 280 [3].

2.6. Загальний аналіз безпеки

На основі цього можна побачити, що для атаки на систему можна підійти до неї або з верхнього рівня, або сформувати нижній рівень. Безпека нижнього рівня залежить від того, наскільки ефективно можна використовувати метод Minrank. Загалом складність атаки дорівнює $q^{(v2-1)} o^3{}_u - 1 if v_1 > o_1$, якщо $v_1 > o_1$, або $q^{2v1} o_u{}^3 - 1$, якщо $v_1 \le o_1$. З цього можна отримати, що не можна дозволити $v_2 = o_1 + v_1$ бути занадто малим. З останніх результатів електронного друку [WBP], безпека системи становить принаймні $(n - v_1) \times n^3 \times (q)^{o1+v1} \times u$, що, безсумнівно, вимагає, щоб $o_1 + v_1$ не був малим.

Що стосується випадку атаки зверху, метод атаки для незбалансованого методу Oil-Vinegar говорить, що $v_u - 1 - o_u - 1$ не може бути занадто малим. Також щоб уникнути випадкових атак пошуку $o_u - 1$ не повинно бути занадто малим [4].

3. Здатність алгоритму RAINBOW протидіяти атаці сторонніми каналами

Криптографічні системи повинні бути захищені від широкого кола атак, включаючи атаки сторонніми каналами. Атака сторонніми каналами належить до фізичної атаки, яка являє собою будь-яку атаку, засновану на інформації, отриманій в результаті фізичної реалізації криптографічних систем, а не на грубій силі чи теоретичних недоліках криптографічних алгоритмів. Основним принципом атаки бічного каналу є те, що інформація бічного каналу, така як споживання енергії, електромагнітні витоки, інформація про синхронізацію або навіть звук, може забезпечити додаткові джерела інформації про секрети в криптографічних системах, наприклад криптографічні ключі, часткова інформація про стан, повна або часткові звичайні тексти, які можна використовувати для розбиття криптографічних систем. Загальні класи атаки бічних каналів включають аналіз синхронізації, аналіз потужності, електромагнітний аналіз, аналіз несправностей, акустичний криптоаналіз, аналіз залишків даних та атаки аналізу молоткових рядів.

Атаки аналізу несправностей мають на меті маніпулювати екологічними умовами криптографічних систем, таких як напруга, годинник, температура, випромінювання, світло і вихровий струм, щоб генерувати несправності під час секретних обчислень, наприклад множення та інверсії в кінцевому полі, і спостерігати за пов'язаною поведінкою, яка може допомогти криптоаналітику зламати криптографічні системи. Атаки аналізу несправностей можна спроєктувати, просто підсвітивши транзистор лазерним променем, що змушує деякі біти приймати неправильні значення. Ідея використання несправності, індукованої під час секретного обчислення, для вгадування секретного ключа практично спостерігалася в реалізаціях RSA, що використовують китайську теорему про залишки.

Атака аналізу потужності може надати детальну інформацію, спостерігаючи за енергоспоживанням криптографічних систем, що приблизно поділяється на простий аналіз потужності (SPA) та аналіз диференціальної потужності (DPA). У сімействі атак аналізу потужності DPA представляє особливий інтерес і є статистичним тестом, який вивчає велику кількість сигналів енергоспоживання для отримання секретних ключів.

Можна виділити наступні атаки:

атака диференціального аналізу потужності на SFLASH;

атака на секретні ключі від модуля SHA-1 схем SFLASH.

атака стороннього каналу на enTTS, яка використовує диференціальний аналіз потужності та аналіз несправностей для атаки двох афінних перетворень та центральної трансформації карти. Цей метод показує, що можна отримати всі секретні ключі enTTS.

Оскільки конструкція Rainbow включає дві афінні перетворення та перетворення центральної карти, такі методи мають потенціал для отримання її секретних ключів. Таким чином, обговорюється захист від можливої атаки бічного каналу для Rainbow, а контрзаходи описані нижче:

Нехай це повідомлення і кожен елемент у полягає в $GF((2^4)^2)$;

Береться випадковий вектор $y'(y_0', y_1', ..., y_{25}')$, кожен елемент якого полягає в $GF((2^4)^2)$;

Обчислюється $y'' = y' + y$;

Обчислюється $\bar{y}' = Ay' + b$ та $\bar{y}'' = Ay''$, де A – матриця 26x26, b – вектор розміру 26;

Обчислюється $\bar{y} = \bar{y}' + \bar{y}''$, що еквівалентно $\bar{y} = Ay + b$;

Розраховано перше афінне перетворення; тоді ми беремо випадкові байти для Vinegar-змінних;

Двічі перевіряються випадкові байти для захисту від атак аналізу несправностей;

Обчислюються багатовимірні поліноміальні оцінки та розв'язування систем лінійних рівнянь до завершення перетворення центральної карти;

$\bar{x}(\bar{x}_0, \bar{x}_1, ..., \bar{x}_{42})$ – це результат трансформації центральної карти; після цього береться два випадкових вектори $\bar{x}'$ та $\bar{x}''$, де $\bar{x} = \bar{x}' + \bar{x}''$, та елементи полягають в $GF((2^4)^2)$;

Обчислюється $\bar{x}' = C\bar{x}'$ та $\bar{x}'' = C\bar{x}'' + d$, де C – матриця 43x43, b – вектор розміру 43;

Обчислюється $\bar{x} = \bar{x}' + \bar{x}''$, що еквівалентно $x = Cx + d$;

$x(x_0, x_1, ..., x_{42})$ це схема підпису Rainbow для $y(y_0, y_1, ..., y_{25})$.

Використовується аналіз несправностей для атаки випадкових байтів у центральних перетвореннях карти; таким чином ми двічі перевіряємо випадкові байти для захисту від атак аналізу несправностей. Також використовується аналіз диференціальної потужності для атаки модуля SHA-1; таким чином, ми беремо метод захисту афінних перетворень. Однак зазначений вище контрзахід є теоретичним; потрібна можливість впровадити та перевірити це на апаратному забезпеченні.

Висновки

1. Постквантова криптографія – частина криптографії, яка залишається актуальною і при появі квантових комп'ютерів і квантових атак. Так як за швидкістю обчислення традиційних криптографічних алгоритмів квантові комп'ютери значно перевершують класичні комп'ютерні архітектури, сучасні криптографічні системи стають потенційно вразливими до криптографічних атак. Більшість традиційних криптосистем спирається на проблеми факторизації цілих чисел або завдання дискретного логарифмування, які будуть легко розв’язані на досить великих квантових комп’ютерах, що використовують алгоритм Шора.

2. Багато криптографів ведуть розробку алгоритмів, незалежних від квантових обчислень, тобто стійких до квантовим атакам. Ці задачі розглянуті на другому етапі конкурсу NIST США.

3. Схема підпису Rainbow виглядає надійною проти великої кількості методів крипто-аналізу та проти атак сторонніми каналами.

4. У зв'язку з можливістю появи потужного квантового комп'ютера актуальними є завдання створення постквантових алгоритмів ЕП. В цьому напрямі уже розпочато дослідження, в певній мірі визначено математичні основи, на яких можуть бути побудовані пост-квантові алгоритми ЕП. Для цього можна застосувати схему Rainbow.

5. Реалізація квантово-захищених алгоритмів вимагає великих матеріально-технічних ресурсів. Вказане пов'язане з великими довжинами ключів та загальних параметрів. Сучасний рівень розвитку техніки дозволяє оптимістично ставитися до можливості ефективної реалізації квантово-захищених алгоритмів.

6. Мультиваріативні квадратичні перетворення можуть бути застосованими для розроблення постквантового стандарту ЕП. Вони вже були використані для побудови схем підпису, але всі спроби побудувати надійну схему поки не були успішними. Попередній аналіз показав, що мультиваріативні квадратичні перетворення можуть вирішити проблему захищеності від атак на основі квантових комп'ютерів, але для цього ще потрібно провести величезний обсяг досліджень та робіт, а також вкласти значні ресурси.

7. Попередній аналіз показує, що розміри загальних параметрів та ключів не викликають сумнівів відносно криптографічної стійкості стандарту, розробленого на основі мультиваріативного квадратичного перетворення. Але залишається проблема просторової складності, яка пов'язана зі значними довжинами загальних параметрів та відкритих ключів.

Список літератури

1. Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, DanielSmith-Tone. Report on Post – Quatum Cryptography. Nistir 8105 (draft).

2. Інтернет-ресурс. Режим доступу http://www.nkj.ru/archive/articles/5309/

3. Інтернет-ресурс. Режим доступу http HYPERLINK"http://www.win.tue.nl/diamant/symposium05/abstracts/wolf.pdf"pdf

4. Горбенко, Ю.І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем : монографія ; зааг. ред. І.Д. Горбенко. – Харків : Форт2015. – 959 с

5. Потій О.В, Горбенко Ю.І., Ганзя Р.С., Пономар В.І. // Матеріали V-ї міжнар. наук.-техн. конф. «Захист інформації і безпеки інформаційних систем». Львів, 2016, 02.0603.06. С. 52.

6. Reinier Broker. Constructing supersingular elliptic curves // J. Comb. Number Theory,(3): pp. 269–273, 2009.

7. McGrew D., Curcio M. Hash-Based Signatures draft-mcgrew-hash-sigs00[Електроннийресурс] / D. McGrew, M. Curcio – Режим доступу: https://tools.ietf.org/html/draftmcgrew-hash-sigs-00.

8. Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, DanielSmith-Tone. Report on Post – Quantum Cryptography. NISTIR 8105 (DRAFT).https://www.google.com.ua/search?

9. Bernstein D. J. Grover vs. McEliece // N. Sendrier, editor, Post-Quantum Cryptography,Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010.Proceedings, volume 6061 of Lecture Notes in Computer Science, pages 73–80. Springer, 2010.

д.т.н. Горбенко І.Д. (ХНУ ім. В.Н. Каразіна, АТ «ІІТ»),
д.т.н. Потій О.В. (ДССЗЗІ),
к.т.н. Єсіна М. В. (ХНУ ім. В.Н. Каразіна, АТ «ІІТ»),
к.т.н. Качко О.Г. (ХНУРЕ, АТ «ІІТ»),
к.т.н. Горбенко Ю.І. (АТ«ІІТ», ХНУ ім. В.Н. Каразіна,),
Кандій С.О. (ХНУ ім. В.Н. Каразіна, АТ «ІІТ»)

СТАН ТА ПРОБЛЕМА СТАНДАРТИЗАЦІЇ ТА ВПРОВАДЖЕННЯ ПОСТКВАНТОВИХ КРИПТОПЕРЕТВОРЕНЬ НА МІЖНАРОДНОМУ ТА НАЦІОНАЛЬНОМУ РІВНЯХ

Актуальність.Наразі, та в перспективі, для криптографічного захисту інформації будуть застосовуватись методи, механізми та алгоритми стандартизованих постквантових криптоперетворень. Вони є суттєвою складовою забезпечення кібербезпеки. Але є обґрунтовані підозри, що у постквантовий період існуючі стандарти асиметричних криптоперетворень електронного підпису (ЕП), асиметричного шифрування (АСШ) та протоколи інкапсуляції ключів (ПІК) будуть зламуватись та компрометуватись за допомогою квантових криптоаналітичних систем. Вирішення проблеми кібербезпеки та безпеки інформації в перехідний та постквантовий період здійснюється на основі розроблення, прийняття та застосування стандартизованих постквантових ЕП, АСШ та ПІК. Як на міжнародному, так і національному рівнях це досягається суттєвим обґрунтуванням та застосуванням нових математичних методів та механізмів криптоперетворень. Це дозволило розробити та приступити до впровадження в Україні національних постквантових стандартів, наприклад, в інфраструктуру відкритих ключів (ІВК). Але, як з'ясувалось, стандартизовані криптографічні перетворення необхідно впровадити більше, ніж в 10 млн. клієнтів та центри сертифікації ключів. Аналогічна проблема виникла і при впровадженні постквантової криптографії і в інші додатки.

Постановка задачі. Метою доповіді є аналіз стану стандартизації постквантової криптографії на міжнародному та національному рівнях, та проведення відповідних теоретичних та практичних досліджень і розробок, а також розгляд проблеми впровадження асиметричних та симетричних крипто перетворень, і існуючих інформаційних систем та технологій.

Основними напрямами розробок та досліджень АТ «ІІТ» в цьому напряму в Україні є:

- теоретичні дослідження та їх практичне застосування в криптології в частині обґрунтування вимог, визначення математичних основ та розроблення стандартів асиметричних і симетричних криптоперетворень для перехідного та постквантового періодів;
- проектування, створення, супроводження та модернізація PKI України для застосування на національному та міжнародному рівні;
- розробка програмного та програмно-апаратного забезпечення реалізації постквантових стандартів на практиці та практичне моделювання з його використанням.

Основні положення

1. Теоретичні дослідження та їх практичне застосування постквантової криптографії в Україні

1.1 Основні положення

Теоретичні дослідження АТ «ІІТ» в криптології направлені на оцінку, порівняльний аналіз та удосконалення існуючих та перспективних асиметричних криптоперетворень типу АСШ, ПІК, ЕП, а також симетричних криптоперетворень типу БСШ та ПСШ. Для оцінки та порівняльного аналізу вказаних асиметричних криптоперетворень застосовується комплексна методика, що включає методику оцінки та порівняння за безумовними, умовними, а також прагматичними критеріями.

Наразі розроблені, прийняті в якості національних та впроваджуються в Україні такі стандарти криптографічного захисту інформації (КЗІ):

- БСШ ДСТУ 7624:2014;
- функція гешування ДСТУ 7564:2014;
- ПСШ ДСТУ 8845:2019;
- АСШ КЕМ ДСТУ 8961:2019.

На етапі обговорення та прийняття в якості національних знаходяться проекти стандартів ЕП «Вершина 1» та «Вершина 2».

Особливістю цих стандартів є те, що в них забезпечується рівень безпеки включно до 512 біт від класичних атак та 256 біт від квантових, а також від атак на основі помилок та спеціальних атак.

Стандарт ДСТУ 8961:2019 розроблено на основі математики алгебраїчних решіток, а проекти стандартів «Вершина 1» та «Вершина 2» – на основі алгебраїчних решіток з відхиленням та алгебраїчних решіток з використанням спеціальних даних відповідно.

Особливістю реалізації вказаних криптоперетворень є оптимізація по швидкодії, що досягається оптимізацією на програмному рівні за рахунок застосування швидких перетворень при множенні поліномів.

У табл. 1 наведені результати аналізу кандидатів на постквантові міжнародні стандарти NIST США, що досліджуються на 3 етапі конкурсу).

Таблиця 1 – кандидати NIST США, 3 етап

Метод	Шифр/підпис	Сімейство	Стійкість
Classic McEliece	АСШ/ПІК	На основі коду	Декодув. кодів Гоппа
Crystals-Kyber	АСШ/ПІК	На основі решітки	Module-LWE
NTRU (svp)	АСШ/ПІК	На основі решітки	проблема svp
Saber	АСШ/ПІК	На основі решітки	Module-LWR
Crystals-Dilithium	Підпис	На основі решітки	Module-LWE і Module-SIS
Falcon	Підпис	На основі решітки	Кільце- SIS
Rainbow	Підпис	На основі багатоваріантності	Приховування Oil-та-Vinegar

Серед фіналістів 3 кандидати АСШ, ПІК, та ЕП, з них 5 кандидатів на алгебраїчних решітках, по одному – на основі застосування алгебраїчних решіток та багатовимірних перетворень. Їх оцінки та порівняння наводяться в доповіді.

В Україні в останні роки активно проводилися роботи щодо розробки національних криптографічних стандартів. Ця робота спиралася на великий досвід фахівців у гармонізації міжнародних криптографічних стандартів. За оцінками фахівців, вони можуть розглядадатися як квантово-захищені і можуть бути використані у постквантовий період.

Аналіз результатів дозволяє стверджувати, що Україна заздалегідь приступила до вирішення проблем квантових обчислень та готова до сучасних викликів, що обумовлені новими загрозами розвитку крипоаналітичних атак, в тому числі на основі квантових обчислень. У таблиці 2 наведені дані щодо квантово-захищених національних стандартів та проєктів стандартів України.

Таблиця 2 – Квантово-захищені національні стандарти (проєкти) стандартів України

ДСТУ 7624:2014 (Калина)	Розмір блоку і ключа (256–512біт, 10 режимів роботи)
ДСТУ 7564:2014 (Купина)	Довжиною геш від 8 до 512, крок 8 біт).
ДСТУ 8845-2019 (Струмок)	Ключ 256–512біт, IP швидкодія = $18 \cdot 10^9$ біт
ДСТУ 8961-2019 (Скеля)	Постквант. АСШ/ПІК, алгебр реш. $V=4 \cdot 10^6$
Проєкт ЕП ДСТУ («Вершина 1») – постквант.	Алгебраїчні решітки з відхиленнями. Стадія прийняття (Dilithium).
Проєкт ЕП ДСТУ («Вершина 2») – постквант.	Алгебраїчні решітки з відхиленнями. Стадія обговорення (Falcon).

Оцінки та порівняння національних стандартів наводяться в доповіді, а також частково наведені на рис. 1 та рис. 2.

1.2 Порівняльний аналіз національних та міжнародних проєктів стандартів

Результати порівняння перспективних механізмів ЕП, що засновані на перетвореннях на алгебраїчних решітках. В порівнянні приймали участь проекти стандартів «Вершина 1» та «Вершина 2», а також алгоритм Dilithium, який за попередніми дослідженнями мав кращі результати серед постквантових алгоритмів підпису, що засновані на перетвореннях на алгебраїчних решітках. Стійкість алгоритмів Вершини 128 біт відповідає 3-ому рівню стійкості NIST, 256 – 5-ому, тому пропорційно для виконання порівняння згідно шкали оцінок попарного порівняння параметрам 384 та 512 біт були надані відповідні рівні безпеки. На рис. 1 відображено гістограму загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів.

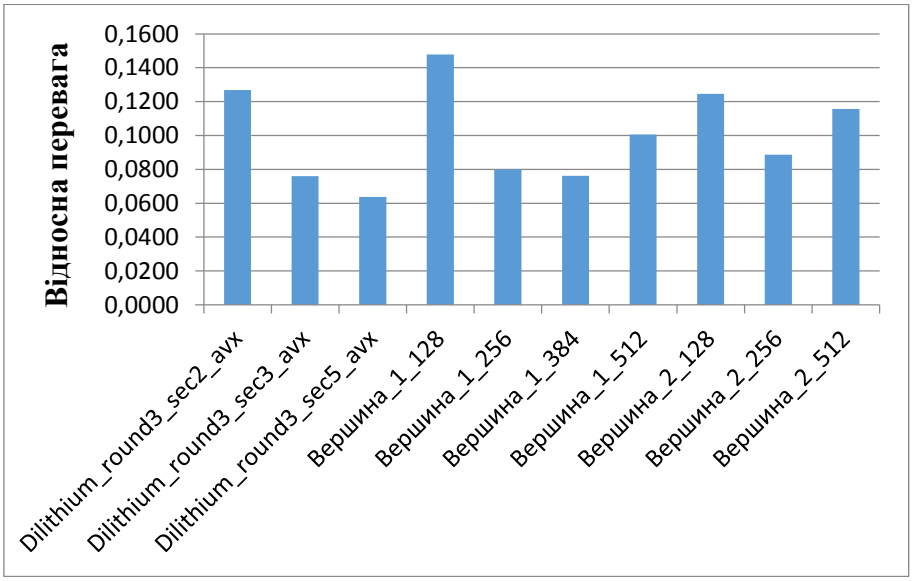


Рис. 1 Гістограма загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів

На рис. 2 відображено гістограму загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів характеристик.

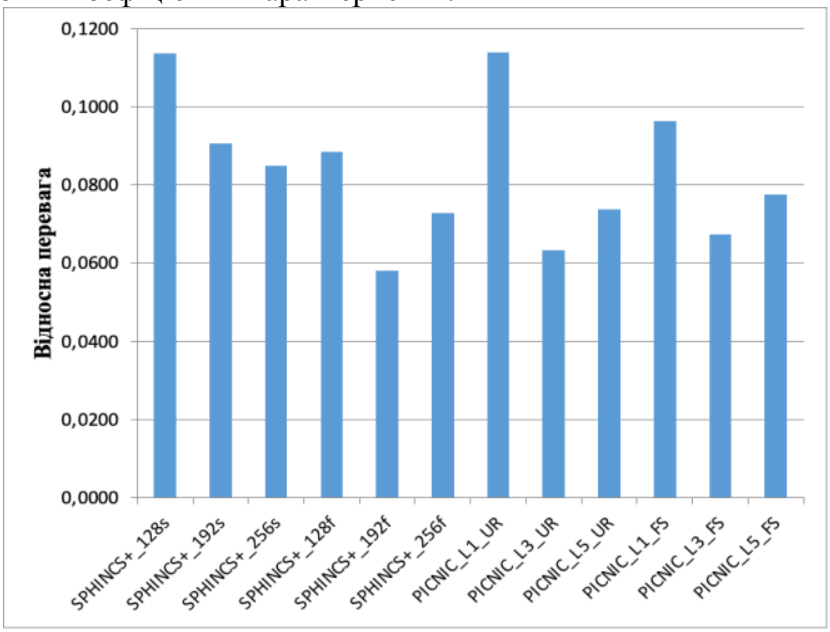


Рис.2 Гістограма загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів характеристик

Як видно з рис. 1 найбільшу перевагу має алгоритм «Вершина 1» з параметрами стійкості 128 біт, для більш стійких параметрів перевагу вже має алгоритм «Вершина 2».

Як видно з рис. 3 найбільшу перевагу має алгоритм «Вершина 1» з параметрами стійкості 128 біт, для більш стійких параметрів перевагу вже має алгоритм «Вершина 2».

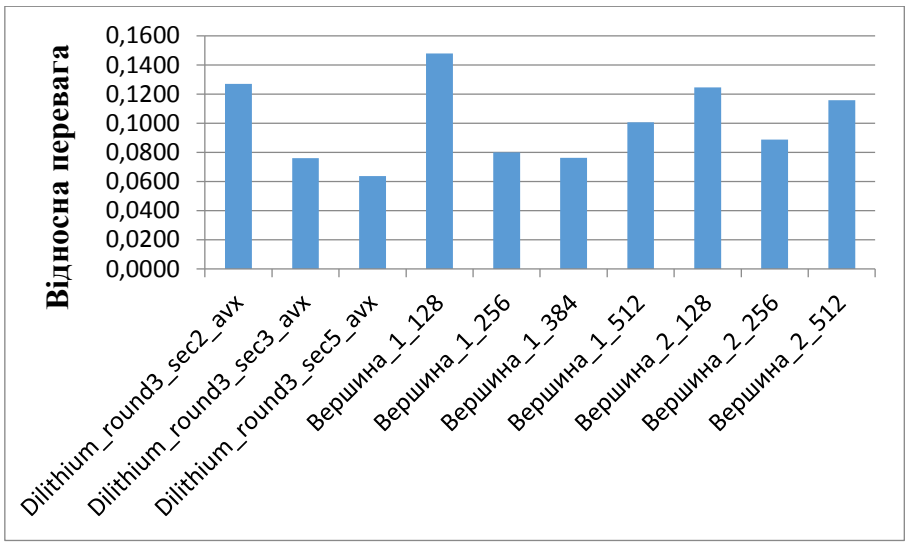


Рис. 3 Переваги алгоритмів ЕП

2. Проектування, створення, супроводження та модернізація PKI України для застосування на національному та міжнародному рівнях

Починаючи з початку 21-го століття в Україні були розроблені системи PKI для державного та комерційного застосування. На нинішній час це 21 кваліфікований надавач ЕДП, із яких 19 спроектовані, розроблені, впроваджені, супроводжуються в експлуатації та дороблюються АТ «ІІТ».

На національному рівні кваліфіковані надавачі ЕДП застосовують для криптографічного захисту інформації національні стандарти ДСТУ 4145:2002, ДСТУ ГОСТ 28147:2009, ДСТУ ISO/IEC 15946-3 тощо.

Особливістю надавачів кваліфікованих ЕДП, що розробляються АТ «ІІТ» є реалізація усіх криптоперетворень на апаратно-програмному рівні.

На національному рівні кваліфіковані надавачі ЕДП (рис. 4, 5) застосовують для криптографічного захисту інформації національні стандарти ДСТУ 4145:2002, ДСТУ ГОСТ 28147:2009, ДСТУ ISO/IEC 15946-3 тощо. На рис. 6 наведена Структурно-функціональна схема засобів (складових частин).

Особливістю надавачів кваліфікованих ЕДП, що розробляються АТ «ІІТ» є реалізація усіх криптоперетворень на апаратно-програмному рівні.

Рис. 4 Національна схема ЕЦП

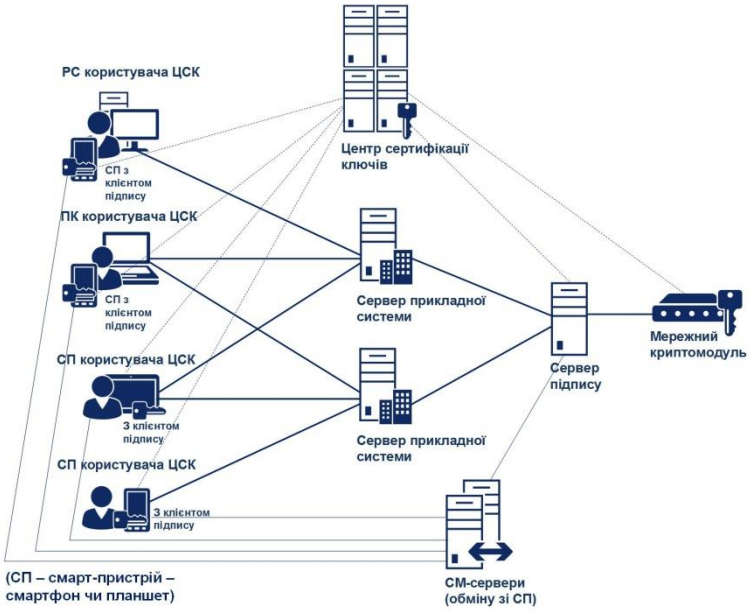


Рис. 5 Структурно-функціональна схема засобів (складових частин)

Таблиця 3 – Типи та характеристики мережних криптомодулів

Тип	Зовнішній вигляд та опис	Інтерфейси	Швидкодія формування підпису (ЕП)	Кількість наборів ключів
«Гряда-301» (мікро-пристрій) («ІІТ МКМ Гряда-201(МікП)»)	 Мініатюрна системна платформа, може встановлюватись в 19-ти дюймову стійку за допомогою полиці	USB (RNDIS), 2 x Ethernet 10/100	За ДСТУ 4145-2002, поле 257 – 8 мс, 125 формувань/с. За RSA, 2048 біт (SHA-256) – 132 мс, 8 формувань/с. За ECDSA, NIST P-256 (secp256r1), 256 біт – 10 мс, 100 формувань/с	384
«Гряда-301» (міні-пристрій) («ІІТ МКМ Гряда-301(МіП)»)	 Системна платформа висотою 2U, може встановлюватись в 19-ти дюймову стійку за допомогою полиці	2 x Ethernet 100/1000	За ДСТУ 4145-2002, поле 257 – 2,18 мс, 460 формувань/с. За RSA, 2048 біт (SHA-256) – 70 мс, 15 формувань/с. За ECDSA, NIST P-256 (secp256r1), 256 біт – 4,3 мс, 230 формувань/с	1 536
«Гряда-301» («ІІТ МКМ Гряда-301»)	 Системна платформа висотою 1U, призначена для встановлення в 19-ти дюймову стійку	2 x Ethernet 100/1000 Опціонально – 2 x Ethernet 100/1000BASE-SX (оптичні, LC)	За ДСТУ 4145-2002, поле 257 – 0,64 мс, 1560 формувань/с. За RSA, 2048 біт (SHA-256) – 18 мс, 55 формувань/с. За ECDSA, NIST P-256 (secp256r1), 256 біт – 1,3 мс, 770 формувань/с	12 288

«Гряда-401» (високопродуктивний пристрій) («ІІТ МКМ Гряда-301(ВП)»)	 Системна платформа висотою 1U, призначена для встановлення в 19-ти дюймову стійку	2 x Ethernet 100/1000 2 x SFP+ (1000/10000, оптичні SFP-модулі 1000BASE-SX, 10G-SR чи ін.)	За ДСТУ 4145-2002, поле 257 – 0,14 мс, 6 900 формувань/с. За RSA, 2048 біт (SHA-256) – 4,5 мс, 225 формувань/с. За ECDSA, NIST P-256 (secp256r1), 256 біт – 0,32 мс, 3 100 формувань/с	4 194 304

В таблиці 3 наведено типи та характеристики мережних криптомодулів.

В перспективі будуть застосовуватись високошвидкісні IP-шифратори на основі ДСТУ 8845:2019 (потокове шифрування зі швидкістю до 18 гБіт в секунду).

В таблиці 4 наведено типи та характеристики електронних ключів.

Також в надавачах застосовуються, розроблені та оптимізовані бібліотеки криптографічних перетворень на програмному рівні.

Таблиця 4 – Типи та характеристики електронних ключів

Тип	Зовнішній вигляд та опис	Інтерфейси	Швидкодія формування підпису (ЕП)
«Кристал-1» «ІІТ Е.ключ Кристал-1»	 Малогабаритний знімний USB-пристрій у металевому корпусі	USB-з’єднувач типу A-plug (вилка) Може мати програмний CCID-інтерфейс	За ДСТУ 4145-2002, поле 257 – 100 мс
«Алмаз-1К» «ІІТ Е.ключ Алмаз-1К»	 Малогабаритний знімний USB-пристрій у пластмасовому чи металевому корпусі	USB-з’єднувач типу A-plug (вилка) Має програмний CCID-інтерфейс	За ДСТУ 4145-2002, поле 257 – 300 мс
Bluetooth-адаптер «ІІТ Bluetooth-адаптер електронних ключів»	 Малогабаритний електронний пристрій, у пластмасовому корпусі, для електронного ключа «Алмаз-1К»	USB-з’єднувач типу A (розетка) Bluetooth 4.0 (та вище) BLE (бездротовий) USB-з’єднувач micro-USB (розетка)	
«Алмаз-1К» (Bluetooth-пристрій «ІІТ Е.ключ Алмаз-1К (Bluetooth-пристрій)»	 Малогабаритний електронний пристрій у вигляді пластикового брелоку	Bluetooth 4.0 (та вище) BLE (бездротовий)	За ДСТУ 4145-2002, поле 257 – 700 мс

Ряд розроблених кваліфікованих надавачів ЕДП розроблені на основі застосування міжнародних стандартів та використовуються для захисту інформації на міжнародному рівні

(центральний засвідчувальний орган, засвідчувальний центр Національного банку, кваліфіковані надавачі ЕДП: Національний банк, «Дія», Генеральний Штаб, «Вчасно»).

Наразі PKI України виготовляє та обслуговує на внутрішньому рівні безпечно більше 10 мільйонів сертифікатів відкритих ключів електронного підпису та шифрування.

Тому проблема впровадження постквантової криптографії є надзвичайно громіздкою та складною.

3. Розробка програмного та програмно-апаратного забезпечення в галузі кібербезпеки

АТ «ІІТ» має суттєвий досвід у розробці, верифікації, впровадженні, супроводженні та удосконаленні програмних та програмно-апаратних систем, комплексів та засобів КЗІ, що використовуються у державному управлінні, банківській та фінансовій сферах, а також у навчальному процесі.

Як правило початкові версії систем, комплексів та засобів КЗІ розробляються та випробовуються на програмному рівні з використанням систем програмування (C++, Java, Асемблер і т.д.). Також в АТ «ІІТ» розроблена спеціальна мова програмування елементів та систем кібербезпеки, що застосовується в банківській та ін. сферах.

На рис. 6 та 7 наведено функціональну схему комплексу та структурну схему комплексу технічних засобів ІВК України, а на рис. 6 структурну схему діючого комплексу технічних засобів.

Рисунок 6 – Функціональна схема комплексу

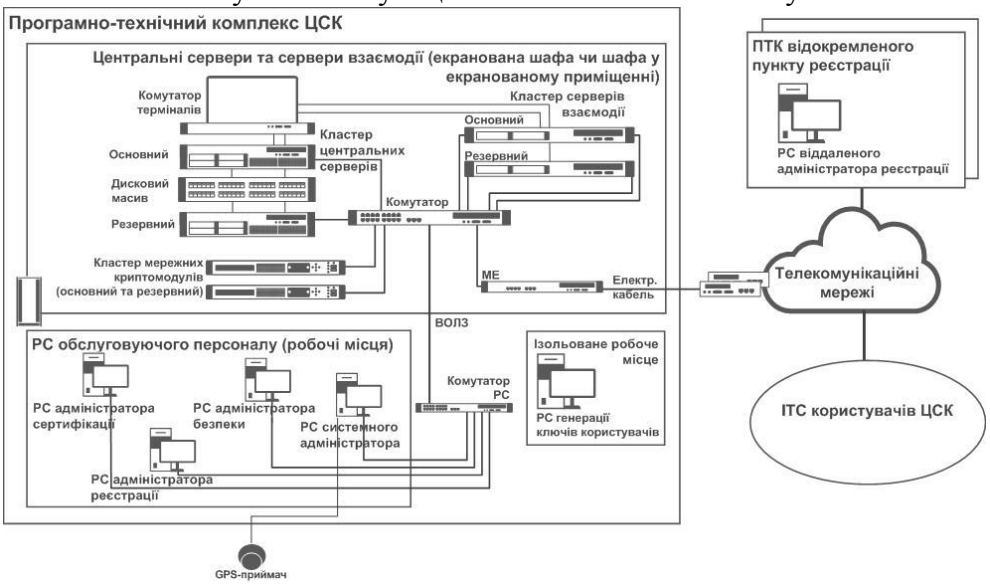


Рисунок 7 – Структурна схема комплексу технічних засобів

8 – Структурна схема комплексу технічних засобів АЦСК

Наведені на рис. 1-3 та таблицях 1, 2 дані дозволили оцінити складність вирішення проблеми впровадження постквантових стандартів, визначити концептуальні питання та формулювати основні положення відповідної концепції.

Висновок

1. Впровадження розроблених в Україні національних стандартів забезпечить безпеку інформації та кібербезпеку на основі надання електронних довірчих послуг в умовах застосування класичних, квантових спеціальних та атак на основі помилок.

2. Крім розробки постквантових стандартів в подальшому, необхідно розглянути фактичний перехід ІТ-систем на нові стандарти, найкраще за рахунок використання або забезпечення крипто-гнучкості чи застосування гібридного підходу.

Гулій В.С. (ВІТІ)

НАПРЯМКИ ВДОСКОНАЛЕННЯ СИСТЕМИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ЗАСОБІВ ЗВ`ЯЗКУ ТА АСУ ЗС УКРАЇНИ

У доповіді, на основі раніше проведеного аналізу системи технічного обслуговування засобів зв'язку і АСУ та у зв`язку з забезпеченням військ зв`язку ЗС України засобами звязку на новій елементній базі висвітлено питання видів та існуючих рівнів їх технічного обслуговування, які застосовуються фірмами виробниками, а також необхідність вдосконалення нині діючої системи технічного обслуговування та внесення змін до керівних документів з технічного забезпечення.

Постановка завдання. Для вирішення завдання щодо удосконалення існуючої системи технічного обслуговування (ТО), видів обслуговування, у зв'язку з прийняттям на постачання засобів зв'язку і АСУ розроблених на новій елементній базі, до сучасних вимог та внесення змін до керівних документів з технічного забезпечення військ зв'язку ЗС України, необхідно розглянути – які види, рівні технічного обслуговування, передбачаються, наприклад, фірмою розробником радіостанцій Harris, та які існуютьпідходи у збройних силах країн НАТО до технічного обслуговування.

Аналіз останніх досліджень і публікацій дозволяє зробити висновок, що моделям технічного обслуговування, видам технічного обслуговування, його організації, методам профілактичного обслуговування, визначенню показників якості технічного обслуговування на даний час приділено достатньо уваги, але питанням відповідності нині діючої в ЗС України системи технічного обслуговування техніки зв'язку і АСУ, обґрунтуванню шляхів та методів її удосконалення, тим більше, з урахуванням вимог положень концепції Державної цільової оборонної програми розвитку озброєння та військової техніки на період 2016 – 2020 років, Розпорядження Кабінету Міністрів України від 14 червня 2017 р. № 398 – Київ - Про схвалення Основних напрямів розвитку озброєння та військової техніки на довгостроковий період та з урахуванням нині діючих підходів в ЗС країн НАТО до технічного обслуговування, враховуючи, що на постачання військ зв'язку ЗС України надходить техніка зв'язку і АСУ на новій елементній базі - висвітлено недостатньо, а керівні документи з технічного забезпечення військ зв'язку та АСУ застарілі і потребують внесення змін, доповнень, а можливо, і переопрацювання їх в повному обсязі. Тому дослідження визначених завдань дозволить розглянути та прийняти до виконання нову систему технічного обслуговування техніки зв'язку і АСУ в ЗС України, а в майбутньому і використати ці дослідження при переопрацюванні керівних документів з технічного забезпечення в цілому.

Мета доповіді. Розкрити недоліки (невідповідності) існуючої системи технічного обслуговування техніки зв'язку та АСУ та обґрунтувати шляхи і методи її вдосконалення, в тому числі, з урахуванням підходів до технічного обслуговування та принципів і політики прийнятих в НАТО, а на прикладі виробництва радіостанцій фірмою HARRIS розкрити, які види та скільки рівнів технічного обслуговування пропонується нею мати.

Виклад основного матеріалу. Технічне обслуговування відноситься до заходів технічної експлуатації техніки зв'язку і автоматизації. Згідно ДСТУ технічне обслуговування – це комплекс операцій чи операція для підтримки справного стану чи працездатності об'єкта при використанні його за призначенням, під час простою, зберігання та транспортування. Головною метою обслуговування засобів зв'язку і АСУ в ході експлуатації є підтримання достатнього рівня їх безвідмовності за рахунок прогнозування і недопущення деякої частини потенційних відмов. Під стратегією ТО в військах зв'язку і АСУ необхідно розуміти – систему принципів організації і проведення обслуговування об'єктів, які бувають, як відомо, об'єкти що обслуговуються – це об'єкт, для якого проведення технічного обслуговування передбачено нормативно-технічною документацією та (чи) конструкторською (проектною) документацією (ДСТУ 2860-94) так і об'єкти, що не

обслуговуються – це об’єкт, для якого проведення технічного обслуговування не передбачено нормативно-технічною документацією та (чи) конструкторською проектною) документацією. Об’єкт може включати в себе технічні засоби, програмні засоби, технічний персонал або любе їх поєднання, а система технічного обслуговування і ремонту це не що інше як – сукупність взаємопов’язаних засобів, документації технічного обслуговування і ремонту та виконавців, необхідних для підтримки і відновлення якості виробів що входять до цієї системи.

У військах зв’язку на сьогодні встановлено шість видів обслуговування засобів зв’язку та АСУ поточного забезпечення: контрольний огляд (КО), щоденне технічне обслуговування (ЩТО); технічне обслуговування №1 (ТО-1); технічне обслуговування №2 (ТО-2); сезонне технічне обслуговування (СО); регламентоване технічне обслуговування (РТО).

Для засобів зв’язку і автоматизації, що знаходиться на тривалому зберіганні (ТЗ), системою передбачається три види технічного обслуговування:

технічне обслуговування №1, при зберіганні (ТО-Із);

технічне обслуговування №2 при зберіганні (ТО-2з);

регламентоване технічне обслуговування (РТОз).

Необхідно зазначити, що в ході експлуатації техніки зв’язку і АСУ встановлені та використовуються – періодичне (календарне, за напрацюванням або комбіноване) та неперіодичне обслуговування. Характеристика кожного із видів ТО приведені в ряді робіт. Причому, автори багатьох із цих робіт висловлюють думку, що перспективним видом ТО є обслуговування за технічним станом, але втілення в життя цього прогресивного виду ТО зразків засобів зв’язку і АСУ на новій елементній базі не дозволяє виконати через відсутність вбудованої автоматизованої системи контролю і прогнозування, яка б дозволяла документувати зміни основних параметрів апаратури за часом. Результати аналізу експлуатації техніки зв’язку і АСУ в ЗС України дозволяють зробити наступний висновок:

періодичність і обсяг ТО що визначені в інструкціях з обслуговування підприємствами виробниками тієї чи іншої техніки зв’язку та АСУ в багатьох випадках є необґрунтованими. Як правило, обсяг робіт є завищеним і не задовольняє вимогам їх мінімальній необхідності відносно підтримання технічного стану відповідного зразку на необхідному рівні в реальних умовах експлуатації;

з цієї ж причини для багатьох зразків техніки ці обсяги не можуть бути виконані в повній мірі особовим складом, що обслуговує техніку, в задані директивні терміни;

засоби вимірювання параметрів і характеристик апаратури, які згідно інструкції з технічного обслуговування рекомендуються, в ряді випадків відсутні, як на самих об’єктах так і в ремонтних підрозділах.

Таким чином, проведений аналіз доводить, що основними недоліками з організації технічного забезпечення засобів зв’язку та АСУ нині є:

велике число видів технічного обслуговування;

низька ефективність профілактичних робіт;

великий обсяг і вартість ТО;

неврахування структури об’єкту і, як наслідок, не оптимальність і неузгодженість режимів обслуговування, різних функціонально пов’язаних підсистем, що входять до одного зразку техніки зв’язку.

Не дивлячись на те, що на постачання військ зв’язку ЗС України поступає техніка на новій елементній базі, корінних змін в системі та організації технічного обслуговування не відбулося та вона і відстала від техніки, що поступила на постачання особливо за останні 3-4 роки. Крім того необхідно зазначити, що ускладнення апаратури зв’язку та АСУ, не підкріплене автоматизацією контролю її технічного стану, призводить до збільшення працевитрат на обслуговування. Не завжди корпорації, підприємства виробники, у яких закупається техніка зв’язку і АСУ, своєчасно передають технічну документацію щодо обслуговування та її ремонту до військ.

В цих умовах пропонується, передбачити наступні основні шляхи усунення вище зазначених недоліків з організації технічного обслуговуваннях:

перегляд як видів так періодичності технічного обслуговування;

вибір найбільш ефективних способів обслуговування;

введення прогнозованих режимів перевірки досягнення параметрами апаратури профілактичних допусків;

застосування конструкцій, що не потребують демонтажу, вибір оптимальної послідовності виконання операцій обслуговування;

перехід до перспективного виду технічного обслуговування техніки зв'язку і АСУ – обслуговуванню за технічним станом.

В умовах коли на постачання поступає новітня техніка, звичайно і система технічного обслуговування потребує змін та приведення її у відповідність до підходів з технічного обслуговування та принципів і політики прийнятих в у ЗС країн членів НАТО. Наприклад, в Інструкції по експлуатації радіостанції виробництва HARRIS, зазначається два види технічного їх обслуговування - профілактичне обслуговування, позапланове та три рівні обслуговування. Так, відповідно до інструкції з експлуатації сучасних тактичних короткохвильових радіостанцій, виробництва фірми HARRIS, профілактичне обслуговування – це система обслуговування, яке здійснюється по графіку. Під час профілактики обладнання перевіряється, щоб запобігти виходу з ладу і зменшити час простою. Профілактичне обслуговування полягає в утриманні обладнання в чистому та сухому стані, очищеному від пилу. Для очистки обладнання рекомендується використовувати чисту щітку, вологу губку і чисту тканину. Обладнання, яке використовується має оглядатися щоденно, зокрема:

- потрібно виконати вбудовані тести;

- перевірити надійність під'єднання батарейного відсіку і чистоту вентиляційного клапана;

- надійність під'єднання кабелів та роз'ємів до трансівера і антенної системи.

Якщо обладнання щодня не використовується, то його огляд та виконання відповідних
процедур має проводитися щотижня, а саме:

- огляд антени на наявність зламів і розтягнень (за потреби – відремонтувати чи замінити);

- огляд роз'ємів на предмет корозії чи пошкоджень;

- перевірка роз'ємів, які не використовуються, на наявність захисних ковпачків.

Профілактичне обслуговування крім щоденного, щотижневого обслуговування передбачає і щорічне обслуговування, під час якого проводиться перевірка в повному обсязі роботи радіостанції та заміна батареї HUB.

Позапланове технічне обслуговування проводиться, коли під час профілактичного обслуговування, чи під час роботи радіостанції, були виявлені ті чи інші несправності, або той чи інший дефект.

Крім того, компанією HARRIS, на відміну від системи технічного обслуговування що діє в ЗС України, передбачається – три рівні обслуговування:

перший – визначення рівня працездатності обладнання (виконується оператором без застосування додаткового обладнання);

другий – визначення працездатності обладнання радіостанції (виконується оператором
із застосуванням додаткового обладнання);

третій – визначення працездатності обладнання до модуля у пристрої (виконується сертифікованим персоналом із застосуванням, яким повинен бути обладнаний спеціалізований автомобіль).Таким чином, порівнюючи, діючу в ЗС України, систему технічного обслуговування та види технічного обслуговування засобів зв'язку і АСУ, з тими видами які застосовуються в ЗС країн членів НАТО та в зв'язку з отриманням на постачання

у війська зв'язку новітньої техніки, обслуговування якої, згідно з інструкції з експлуатації (наведена вище для сучасних тактичних короткохвильових радіостанцій, виробництва фірми HARRIS) значно відрізняється від обслуговування аналогової техніки зв'язку і є підтвердженням необхідності вдосконалення діючої системи технічного обслуговування у ЗС України. Напрями удосконалення пропонується мати наступні: визначити головну ціль обслуговування в процесі експлуатації засобів зв'язку і АСУ на новій елементній базі, які надходять на постачання; визначити сукупність взаємопов'язаних засобів, виконавців і документації з обслуговування, призначеної для підтримання справного і працездатного стану; оптимізувати періодичність і види технічного обслуговування засобів зв'язку та характеристики кожного із них.

Під час розгляду можливої (перспективної) системи технічного обслуговування необхідно виходити із завдань вимог до цієї системи, таких як:

експертне (директивне) завдання вимог, що базується тільки на загальній інженерній інтуїції та практичному досвіді;

завдання вимоги з прототипу, яке основується на аналізі наявної статистичної інформації з надійності новітньої техніки зв'язку та АСУ близькою за призначенням, структурою і елементній базі;

завдання оптимального рівня надійності, яке виникає тільки в тому випадку коли вихідний ефект від функціонування системи вимірюється в тих же одиницях, що і затрати на її створення.

В цьому випадку необхідно мати на увазі, що завдання вище зазначених вимог щодо перспективної системи технічного обслуговування зводиться до максимізації цільової функції наступного вигляду:

$$F_k(R) = E_k(R) - C_k(R),$$

де R – показник надійності системи, який залежить від к- го варіанту структури системи S_k і від надійності елементів і- го Ri, тобто R= R (S_k, Ri, k= 1, 2...m, i = 1,2... n), де в свою чергу, m – кількість розглянутих варіантів структури, а n – кількість різних комплектуючих елементів, що підлягають обслуговуванню, $E_k(R)$ - вихідний ефект від функціонування k–го варіанту нової системи технічного обслуговування в вартісних показниках при рівні надійності - R; $C_k(R)$ – затрати на забезпечення рівня надійності, рівного – R, для k–го варіанту системи.

Розрахунки, щодо показників надійності для декількох варіантів системи технічного обслуговування засобів зв'язку і АСУ, дозволять визначити найкращий варіант системи, який дозволить мати найменші затрати на забезпечення рівня надійності.

Отже, результати аналізу експлуатації техніки зв'язку і АСУ в ЗС України, а на їх основні недоліки з організації технічного обслуговування, а також підходи до технічного обслуговування та принципів і політики прийнятих в НАТО з цього питання, та наведеного прикладу з застосування видів та рівнів технічного обслуговування вказаних в інструкції з експлуатації радіостанції тактичного рівня виробництва HARRIS, а також іншої новітньої техніки зв'язку, що поступає на постачання до військ зв'язку ЗС України, дозволяють зробити висновок щодо необхідності вдосконалення нині діючої системи технічного обслуговування та приведення її, як у відповідність до вимог діючої системи в ЗС країн членів НАТО так і до застосування тих видів технічного обслуговування, які б забезпечували під час обслуговування найкращий показник надійності нової, чи вдосконаленої системи з обслуговування.

Перспективи подальших досліджень. В подальших дослідженнях доцільно розглянути періодичність та характеристику кожного із видів технічного обслуговування засобів зв'язку і АСУ розроблених на новій елементній базі та прийнятих (які плануються бути прийнятими) на постачання у ЗС України.

Дерев’янко Я. А. (ХНУ ім. В.Н.Каразіна, АТ «ІІТ»)
д.т.н. Горбенко І. Д. (ХНУ ім. В.Н.Каразіна, АТ «ІІТ»)
д.т.н. Кузнецов О.О. (ХНУ ім. В.Н.Каразіна, АТ «ІІТ»)

МЕТОД РОЮ ЧАСТОК ДЛЯ ГЕНЕРАЦІЇ НЕЛІНІЙНИХ ПІДСТАНОВОК

Актуальність. Ефективність симетричних криптоалгоритмів визначається багатьма факторами [1-3]: базовою структурою перетворення, схемою ключового розкладу, показниками стійкості криптопримітивів тощо.

Генерація нелінійних підстановок (S-boxes) є важливим завданням проектування сучасних симетричних криптоалгоритмів. Одним із ключових примітивних блоків симетричної криптографії є нелінійні підстановки (S-box, таблиці заміни) [4-6]. Нелінійність, збалансованість, дельта-рівномірність, кореляційна та алгебраїчна імунність та інші показники характеризують стійкість S-box до лінійного, диференціального, алгебраїчного та інших методів криптоаналізу. Отже, завдання генерації підстановок з необхідними властивостями є важливим та актуальним науковим завданням [7-9].

Постановка задачі. В цій роботі ми розглядаємо модифікацію методу Particle Swarm Optimization (PSO) для задачі генерації високо-нелінійних підстановок, який було запропоновано в роботі [10]. Ми реалізовуємо цей обчислювальний алгоритм і показуємо, що показники нелінійності згенерованих підстановок є незадовільними (див. наш коментар [11]). Зокрема, ми стверджуємо, що запропонований в [10] варіант PSO не здатен генерувати підстановки навіть з показником нелінійності понад 98. Наші експерименти це наочно демонструють. Також ми наводимо можливі модифікації алгоритму обчислювального пошуку, які здатні суттєво покращити ефективність PSO для генерації підстановок. Зокрема, ми показуємо, що запропонована нами покращена реалізація дозволяє впевнено генерувати S-блоки із нелінійністю 104, дельта-рівномірністю 8, лінійною збитковістю 0 та алгебраїчним імунітетом 3.

Основні положення. PSO оптимізує функцію, підтримуючи популяцію можливих розв'язків, названих частками, і переміщаючи ці частки в просторі розв'язків згідно із встановленими правилами [12]. Переміщення підпорядковуються принципу найкращого знайденого в цьому просторі положення, що постійно змінюється при знаходженні частками вигідніших положень. На положення кожної частинки у рої впливає як найбільш оптимістична позиція під час її руху (індивідуальний досвід, що називається особистим кращим чи *pBest* частинки), так і положення найбільш оптимальної частинки в її сусідстві (близький досвід, що називається найкращим серед усіх або *gBest*).

В роботі [10] було запропоновано модифікацію PSO для генерації нелінійних підстановок. Цей алгоритм складається із наступних кроків:

1. Ініціалізація популяції.

Популяція із N S-box генерується випадковим методом. Одним із елементів початкової популяції є S-box шифру AES. Це ключовий елемент авторської модифікації PSO, який, за задумом, повинен був значно покращити ефективність генерації підстановок.

2. Обчислення нелінійності.

Для кожної частки обчислюється нелінійність. Згідно з нелінійністю сортується популяція часток (за спаданням нелінійності).

3. Ініціалізація векторів розташування часток PSO.

Ініціалізація кожного вектору розташування відбувається з використанням відповідного S-Box в популяції. Вектор швидкості оновлюється за формулою (1), а вектор розташування оновлюється за формулою (2):

$$v_{id}^{k+1} = v_{id}^{k} + c_1 r_1 (pBest_{id}^{k} - x_{id}^{k}) + c_2 r_2 (gBest_{id}^{k} - x_{id}^{k}) \quad (1)$$

$$x_{id}^{k+1} = x_{id}^{k} + v_{id}^{k+1} \quad (2)$$

де:

v_{id}^k та x_{id}^k це швидкість та позиція частки «i» на її «k» кроці відповідно та d-розмірне значення її позиції;

$pBest_{id}^k$ представляє собою d-розмірне значення кожного «i» елемента у його найбільш оптимістичній позиції;

$gBest_{id}^k$ – d-розмірне значення найбільш оптимістичної позиції для всього «рою»;

параметри c_1, c_2, r_1, r_2 генеруються випадковим чином у межах $[0,1]$.

Вектор найбільш оптимістичних позицій під час виконання ітерації ($pBest$) оновлюється для кожної згенерованої популяції, якщо значення нелінійності нових блоків є кращими за попередні. Найбільш оптимальною з усіх є частинка з найбільшою нелінійністю у популяції;

4. Ініціалізація параметрів PSO. Параметри PSO, такі як c_1, c_2, r_1 та r_2 обираються випадковим чином. Протягом оптимізаційної фази роботи алгоритму ці параметри випадково змінюються на кожній ітерації. Коефіцієнт інерційності (інерційна вага) задається за формулою [10]:

$$w_{curIter} = w_1 + (curIter - 1)\left(\frac{w_2 - w_1}{maxIter}\right) \quad (3)$$

де w_1 та w_2 є початковим та кінцевим значенням коефіцієнту відповідно.

5. Покращення та регулювання.

Вектори швидкості та розташування оновлюються згідно з (1) та (2) відповідно. Процес покращення генерує певні значення, які повторюються або ж від'ємні значення.

6. Фінальний крок ітерації

Далі для всіх нових згенерованих блоків також обчислюється значення нелінійності, всі S-box, включаючи ті, що вже знаходилися в популяції, знову сортуються за спаданням нелінійності. В популяції залишаються N кращих за нелінійністю S-box, всі інші блоки відкидаються. Вектори $pBest$ та $gBest$ оновлюються.

В цій роботі ми пропонуємо нову реалізацію PSO. Модифікований нами метод PSO майже повністю повторює алгоритм з роботи [10]. Головна різниця полягає в першій ітерації циклу при формуванні першого блоку в новій популяції, а також при заповненні векторів найбільш оптимальних вузлів. Додатково ми оцінюємо інші показники ефективності S-box (алгебраїчну імунність, дельта-рівномірність та лінійну надмірність).

Сутність модифікованого алгоритму наведено нижче:

1. Ініціалізація популяції

Як і в алгоритмі з [10], кожен блок 8×8 приймається за частку. Популяція S-box генерується випадковим методом, таким чином, щоб S-box залишалися бієктивними. Генерація повторюється доти, доки популяція розміру N не буде заповнено.

2. Обчислення нелінійності

Далі для кожного блоку обчислюється нелінійність. Згідно з цією нелінійністю сортується сама популяція блоків (за спаданням нелінійності).

3. Ініціалізація вектору PSO

Вектор швидкості заповнюється нулями і оновлюється на кожній вдалій ітерації. Ініціалізація кожного вектору розташування відбувається з використанням відповідного S-Box в популяції. Вектор швидкості оновлюється за формулою (1), а вектор розташування оновлюється за формулою (2). Відмінністю в нашому алгоритмі є те, що при формуванні нової популяції перший блок нової популяції формується за рахунок взаємодії першого блоку з початкової популяції з самим собою. А далі, якщо після застосування такого способу нелінійність є більшою ніж 98, блок додатково перемішується випадковим чином, щоб покращити інші параметри, такі як лінійна збитковість, дельта рівномірність та алгебраїчний імунітет. Це робиться для того, щоб досягти певного компромісу, щоб не виникало ситуацій коли один параметр є дуже хорошим, а інші поганими. Завдяки такому методу вдається досягти того, щоб всі параметри були достатніми та задовольняли більшості умов. Вектор

найбільш оптимістичних позицій під час виконання ітерації (*pBest*) оновлюється для кожної згенерованої популяції, якщо значення нелінійності нових блоків є кращими за попередні. Найбільш оптимальною з усіх є частинка в нашому методі, що також оновлюється на кожному кроці і прирівнюється до найкращого блоку у векторі найбільш оптимістичних позицій *pBest* .

4. Ініціалізація параметрів PSO

Параметри PSO, такі як c_1, c_2, r_1 та r_2 обираються випадковим чином. Протягом оптимізаційної фази роботи алгоритму ці параметри випадково змінюються на кожній ітерації. Коефіцієнт інерційності також задається за формулою (3).

5. Покращення та регулювання

Для збереження бієктивності S-box в нашій реалізації застосовується наступний алгоритм: після формування блоку кожен його елемент перевіряється на співпадіння з іншим елементом в цьому блоці. Якщо при перевірці певного елементу такий елемент вже є в даному блоці, тоді змінна contains стає одиницею, і значення оновлюється шляхом додавання до нього випадкового значення, та взяття його за модулем 256. Так відбувається доти, доки в S-box залишаться тільки унікальні значення від 0 до 255.

6. Фінальний крок ітерації

Далі для всіх нових згенерованих блоків також обчислюється значення нелінійності, всі S-box, включаючи ті, що вже знаходилися в популяції, знову сортуються за спаданням нелінійності. В популяції залишаються *N* кращих за нелінійністю S-box, всі інші блоки відкидаються. Вектори *pBest* та *gBest* оновлюються.

Для проведення експериментальних досліджень розглянутий алгоритм [10] було програмно реалізовано та протестовано його ефективність. Під час тестування було обрано наступні критерії:

- нелінійність = 104,
- алгебраїчний імунітет = 3,
- лінійна збитковість = 0.

Результати тестових запусків оригінального алгоритму на Персональному комп’ютері з ОС Windows та процесором на 32 ядра наведено у таблиці 1.

Таблиця 1 – Результати тестування алгоритму з роботи [10]

N (число блоків в популяції)	MaxIter (задана кількість ітерацій)	Кількість ітерацій на знаходження необхідного блоку	Час роботи
5	10	Не знайдено	77,26 с
5	50	Не знайдено	424,55 с
5	100	Не знайдено	857,82 с
5	150	Не знайдено	1313,70 с
5	200	Не знайдено	1809,64 с
10	10	Не знайдено	167,16 с
10	50	Не знайдено	928,32 с
10	100	Не знайдено	1855,84 с
10	150	Не знайдено	2773,92 с
10	200	Не знайдено	3665,48 с
20	10	Не знайдено	354,22 с
20	50	Не знайдено	1877,70 с

20	100	Не знайдено	3743,54 с
20	150	Не знайдено	5712,89 с
20	200	Не знайдено	7543,10 с
40	10	Не знайдено	748,98 с
40	50	Не знайдено	3798,19 с
40	100	Не знайдено	7741,10 с
40	150	Не знайдено	11434,93 с
40	200	Не знайдено	14933,59 с

Як можна спостерігати за результатами проведених тестових запусків, оригінальний метод не здатен знаходити блоки з заданими параметрами. Оригінальний алгоритм не може перевершити результат по нелінійності більше ніж 98, хоча автори статті вказували у результатах, що їх метод здатен генерувати блоки з нелінійністю 110 та більше.

Приклад знайденого за допомогою оригінального алгоритму блоку надано в таблиці 2.

Таблиця 2 – Приклад згенерованого алгоритмом з роботи [10] S-box

S-Box	Параметри
(133, 242, 9, 87, 55, 238, 98, 146, 89, 213, 187, 37, 173, 74, 245, 57, 234, 111, 18, 81, 27, 65, 228, 109, 83, 48, 159, 54, 239, 106, 80, 119, 46, 17, 95, 84, 141, 148, 251, 219, 165, 191, 237, 232, 199, 77, 247, 102, 130, 139, 73, 43, 140, 209, 201, 241, 86, 222, 31, 160, 104, 240, 7, 23, 250, 113, 227, 171, 243, 178, 78, 97, 202, 14, 16, 217, 67, 20, 121, 91, 132, 196, 177, 82, 192, 125, 13, 190, 183, 220, 34, 58, 105, 249, 255, 100, 62, 229, 8, 163, 61, 99, 181, 128, 94, 216, 137, 96, 206, 38, 155, 207, 28, 29, 144, 169, 203, 45, 195, 51, 1, 120, 0, 53, 47, 134, 224, 246, 19, 69, 186, 162, 253, 90, 15, 248, 72, 88, 233, 221, 60, 32, 115, 179, 50, 158, 21, 161, 210, 176, 40, 147, 101, 25, 59, 184, 212, 4, 26, 116, 254, 152, 197, 103, 168, 127, 164, 6, 198, 225, 154, 145, 85, 252, 3, 236, 10, 193, 226, 79, 66, 194, 149, 156, 205, 215, 218, 123, 64, 93, 151, 170, 182, 129, 200, 118, 24, 172, 33, 108, 126, 110, 189, 136, 44, 12, 208, 92, 124, 112, 22, 180, 153, 36, 39, 42, 56, 75, 117, 175, 35, 68, 138, 70, 204, 71, 188, 41, 157, 49, 76, 2, 214, 230, 63, 235, 223, 135, 211, 5, 185, 122, 114, 11, 244, 150, 131, 30, 52, 166, 174, 142, 143, 167, 231, 107)	Нелінійність = 98 Алгебр. імунітет = 3 Лінійна збитковість = 0

В роботі ми запропонували нову реалізацію PSO. Відмінністю в нашому алгоритмі є те, що при формуванні нової популяції перший блок нової популяції формується за рахунок взаємодії першого блоку з початкової популяції з самим собою. Тобто головна різниця полягає в першій ітерації циклу при формуванні першого блоку в новій популяції, а також при заповненні векторів найбільш оптимальних вузлів. Результати тестових запусків оригінального алгоритму на Персональному комп’ютері з ОС Windows та процесором на 32 ядра наведено у таблиці 3.

Таблиця 3 – Результати тестування модифікованого алгоритму

N (число блоків в популяції)	MaxIter (задана кількість ітерацій)	Кількість ітерацій на знаходження необхідного блоку	Час роботи
5	10	Не знайдено	77,67 с
5	50	7	48,54 с
5	100	Не знайдено	785,60 с

5	150	Не знайдено	1209,89 с
5	200	Не знайдено	1615,53 с
10	10	Не знайдено	165,72 с
10	50	Не знайдено	868,91 с
10	100	73	1192,63 с
10	150	Не знайдено	2515,39 с
10	200	195	3237,48 с
20	10	Не знайдено	354,79 с
20	50	Не знайдено	1742,73 с
20	100	Не знайдено	3437,68 с
20	150	Не знайдено	5130,86 с
20	200	Не знайдено	6792,29 с
40	10	Не знайдено	750,21 с
40	50	Не знайдено	3545,66 с
40	100	Не знайдено	6870,33 с
40	150	Не знайдено	10212,32 с
40	200	11	699,60 с

Як видно із результатів тестування, запропонована нами нова модифікація PSO дозволяє за порівняно короткий час формувати S-блоки з нелінійністю 104, дельта-рівномірністю 8, лінійною збитковістю 0 та алгебраїчним імунітетом 3. Як приклад наведемо один із таких S-box (таблиця 4).

Таблиця 4 – Приклад згенерованого модифікованим алгоритмом S-box

S-Box	Параметри
(99, 124, 119, 123, 242, 107, 111, 197, 48, 1, 103, 43, 254, 215, 171, 118, 202, 130, 201, 125, 250, 89, 71, 240, 173, 212, 162, 175, 156, 164, 114, 192, 183, 253, 147, 38, 54, 63, 41, 58, 52, 165, 229, 241, 113, 216, 49, 21, 4, 199, 35, 195, 24, 150, 5, 154, 7, 18, 128, 226, 235, 39, 178, 117, 9, 131, 44, 26, 27, 110, 90, 160, 82, 59, 214, 179, 106, 227, 47, 132, 83, 209, 0, 237, 32, 252, 177, 91, 146, 203, 190, 57, 74, 76, 88, 207, 208, 239, 170, 251, 67, 77, 51, 133, 69, 249, 2, 127, 80, 60, 159, 168, 81, 163, 64, 143, 93, 157, 56, 245, 188, 182, 218, 33, 16, 255, 243, 210, 205, 12, 19, 236, 95, 151, 68, 23, 196, 167, 126, 61, 100, 78, 25, 115, 96, 129, 79, 220, 34, 42, 144, 136, 70, 238, 184, 20, 222, 94, 11, 219, 224, 50, 174, 10, 73, 6, 36, 92, 194, 211, 172, 98, 145, 149, 158, 121, 231, 200, 55, 109, 141, 213, 148, 169, 108, 86, 244, 234, 101, 122, 198, 8, 186, 120, 37, 46, 28, 166, 180, 155, 232, 221, 116, 31, 75, 189, 139, 138, 112, 62, 181, 102, 72, 3, 246, 14, 97, 53, 87, 185, 134, 40, 29, 204, 225, 248, 161, 17, 105, 217, 142, 137, 104, 30, 135, 233, 206, 85, 191, 223, 230, 152, 13, 84, 176, 153, 140, 187, 65, 66, 247, 193, 45, 22, 228, 15)	Нелінійність = 104 Алгебр. імунітет = 3 Лінійна збитковість = 0

Таким чином, формований блок підстановок задовольняє всім необхідним критеріям, тобто має необхідний рівень показників: нелінійність, алгебраїчний імунітет та лінійна

збитковість.

Висновок. В результаті проведених досліджень нами було розглянуто метод оптимізації рою часток та досліджено його практичне застосування до генерації нелінійних підстановок. Зокрема, ми розглянули запропонований в роботі [10] алгоритм та показали на його недосконаліть. Наприклад, в наших чисельних експериментах при застосуванні цього алгоритму не вдалося сформувати жодного s-блоку із нелінійністю вище за 98. В даній роботі ми запропонували покращену версію алгоритму, яку було експериментально досліджено за однакових умов. За результатами досліджень встановлено, що метод PSO дозволяє формувати S-блоки з нелінійністю 104, дельта-рівномірністю 8, лінійною збитковістю 0 та алгебраїчним імунітетом 3.

Перспективним напрямком досліджень є подальша оптимізація PSO, дослідження його ефективності та порівняння із іншими методами евристичного пошуку.

ЛІТЕРАТУРА

1. B. Schneier, Applied cryptography: protocols, algorithms, and source code in C, New York: Wiley, 1996. http://archive.org/details/appliedcryptogra00schn_328 (accessed July 25, 2020).
2. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2018. https://doi.org/10.1201/9780429466335.
3. S. Rubinstein-Salzedo, Cryptography, Springer International Publishing, Cham, 2018. https://doi.org/10.1007/978-3-319-94818-8.
4. K. Nyberg, Perfect nonlinear S-boxes, in: D.W. Davies (Ed.), Advances in Cryptology — EUROCRYPT ’91, Springer, Berlin, Heidelberg, 1991: pp. 378–386. https://doi.org/10.1007/3-540-46416-6_32.
5. W. Millan, How to improve the nonlinearity of bijective S-boxes, in: C. Boyd, E. Dawson (Eds.), Information Security and Privacy, Springer, Berlin, Heidelberg, 1998: pp. 181–192. https://doi.org/10.1007/BFb0053732.
6. J. Álvarez-Cubero, Vector Boolean Functions: applications in symmetric cryptography, 2015. https://doi.org/10.13140/RG.2.2.12540.23685.
7. D. Souravlias, K.E. Parsopoulos, G.C. Meletiou, Designing bijective S-boxes using Algorithm Portfolios with limited time budgets, Applied Soft Computing. 59 (2017) 475–486. https://doi.org/10.1016/j.asoc.2017.05.052.
8. J. McLaughlin, Applications of search techniques to cryptanalysis and the construction of cipher components, phd, University of York, 2012. http://etheses.whiterose.ac.uk/3674/ (accessed August 16, 2020).
9. C. Carlet, Vectorial Boolean functions for cryptography, Boolean Models and Methods in Mathematics, Computer Science, and Engineering. (2006).
10. M. Ahmad, I.A. Khaja, A. Baz, H. Alhakami, W. Alhakami, Particle Swarm Optimization Based Highly Nonlinear Substitution-Boxes Generation for Security Applications, IEEE Access. 8 (2020) 116132–116147. https://doi.org/10.1109/ACCESS.2020.3004449.
11. A. Kuznetsov, K. Kuznetsova, Comment on “Particle Swarm Optimization Based Highly Nonlinear Substitution-Boxes Generation for Security Applications,” in: 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, September 22-25. http://www.idaacs.net (accessed October 15, 2021).
12. J. Kennedy, R. Eberhart, Particle swarm optimization, in: Proceedings of ICNN’95 - International Conference on Neural Networks, 1995: pp. 1942–1948 vol.4. https://doi.org/10.1109/ICNN.1995.488968.

д.т.н. Жук О.В. (ВІТІ ім. Героїв Крут)

МЕТОДОЛОГІЯУПРАВЛІННЯ НЕОДНОРІДНИМИ БЕЗПРОВІДНИМИ СЕНСОРНИМИ МЕРЕЖАМИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Актуальність.Відповідно до стратегічного оборонного бюлетня України завданням 1.4.3 є ,,Створення автоматизованих систем C^4ISR на оперативному і тактичному рівнях для видів (родів) Збройних Сил України та інших складових сил оборони на основі стандартів, доктрин і рекомендацій НАТО". Очікуваним результатом є: ,,впровадження системи C4ISR на оперативному та тактичному рівнях до командира відділення (та їм рівних) у складі таких базових можливостей: захищений цифровий голосовий зв'язок, обмін текстовими повідомленнями, обмін графічними документами, геопросторова інформація, взаємна ідентифікація, інтеграція сенсорів (датчиків), інтеграція БпЛА, сумісність з стандартними угодами НАТО (STANAG)"

У відповідності до завдань стратегічного оборонного бюлетня України на даний час ідуть інтенсивні розробки безпроводових сенсорних мереж військового призначення, що забезпечуватимуть прийом і передачу розвідувальної інформації про супротивника та видачу її органам управління військами та зброєю адже досягнення інформаційної переваги саме в тактичній ланці управління військами представляється як об'єктивна необхідність успішного ходу бою (операції).

Основні положення. Безпровідні сенсорні мережі (*WirelessSensorNetwork)* – розподілені мережі, що складаються з маленьких вузлів (сенсорів), з інтегрованими функціями моніторингу навколишнього середовища, обробки і передачі даних [1]. Основними елементами сенсорних вузлів є: датчики для контролю зовнішнього середовища, блок мікрокомп'ютера, батареї, прийомопередавач (додатково система позиціонування, наприклад, система GPS).

Загальна ідея функціонування БСМ полягає у використанні великої кількості неоднорідних безпроводових сенсорів, які можуть бути розташовані на значних географічних територіях для моніторингу за цілями або різнорідних параметрів навколишнього середовища (в деяких випадках побудови радіонапрямку (ів) при знищенні основної опорної мережі зв'язку). Отримана безпроводовим сенсорним вузлом інформація передається на спеціальні шлюзи безпосередньо, або шляхом ретрансляції через проміжні сенсорні вузли. У випадку, якщо площі території для моніторингу дуже великі, у якості шлюзів можуть використовуватися сенсорні вузли на базі безпілотних літальних апаратів (БЛА) чи аероплатформ (АП).

Загальна класифікація безпроводових сенсорних мереж приведена на рис. 1.

Рис. 1 Класифікація безпроводових сенсорних мереж

Стаціонарні, рухомі та гібридні сенсорні мережі. Можливо використовувати стаціонарні сенсорні вузли для моніторингу та рухомі сенсори (роботи) для збору інформації серед сенсорних вузлів (гібридна мережа) або навпаки. Мобільні сенсорні мережі відносяться до класу мобільних радіомережі (МР) або MANET (*mobilead-hocnetworks*), а стаціонарні до класу чарункових безпровідних мереж (*WirelessMeshNetwork*).

Децентралізовані, ієрархічні і гібридні сенсорні мережі. Ієрархічна організація мережі припускає розбиття мережі на зони (кластери) з виділенням в кожній зоні головних і простих сенсорів-вузлів, а також сенсорів-шлюзів (для зв'язку між зонами). Вона є комбінацією централізованого (у зонах) і децентралізованого (між головними вузлами) способів управління.

Наземні, підземні, морські, повітряні. В даний час сенсорні мережі ефективно використовуються для проведення військових операцій. Деякі з них проходили „бойові" випробування в Афганістані та Іраку, де збройні сили США розмістили декілька тисяч сенсорів з метою відстежування пересувань бойової техніки. При проведенні антитерористичної операції застосування сенсорних вузлів на блокпостах, лінії розмежування сторін, сірих зонах для проведення розвідки, тимчасове створення радіо напрямів зв'язку передачі інформації бойового управління, тимчасової організації зв'язку (ретрансляції).

Тактична медицина. Медичні сенсорні мережі можуть бути інтегровані з 3G мультимедійними мережами, для забезпечення повсюдної роботи польової медичної служби. Військовослужбовці матимуть медичні сенсори контролюючі певні параметри такі як (температура тіла, кров'яний тиск, пульс, дихальна активність), що дозволить ефективно знаходити та евакуювати поранених з поля бою.

Акустичні, хімічні, сейсмічні тощо. Залежно від середовища моніторингу в сенсорах використовують датчики, які реєструють певні параметри (наприклад, рівень радіації).

Існуючи технології управління безпроводовими сенсорними мережами розраховані на статичні або квазістатичні умови їх функціонування та не враховують особливостей сенсорних мереж військового призначення.

Як зазначається в [1], основними відмінностями між цивільними та військовими системами управління сенсорними мережами є: різні цілі, етапи, функції, рівні управління та вимоги до оперативного управління.

Так відповідно до концепції [2], за етапами задачі діляться на задачі планування розгортання і оперативного управління (рис. 2).

Рис. 2 Етапи функціонування БСМ

Предметом розгляду даної доповіді є задачі, які вирішуються в процесі оперативного управління (рис. 3).

На етапі оперативного управління за прийнятими критеріями ефективності постійно оцінюється стан сенсорної мережі, і приймаються заходи (відповідно до плану та реальної обстановки) з підтримання її показників ефективності функціонування в заданих межах або здійснюється їх оптимізація. Задачі оперативного управління (на відміну від задач планування) вирішуються змішаним способом (централізовано/децентралізовано) у режимі реального часу, а за змістом багаторазово повторюються.

Оперативне управління сенсорною мережею представляється як управління моніторингом та телекомунікаційною складовою зі зворотнім зв'язком $U^*(t) = \{ U_{мон} / U_{тел} \}$.

*Управління моніторингом*включає наступні етапи $U_{\text{мон}}(t) = \left\{U^{\text{розм}}, U^{\text{пок}}, U^{\text{спост}}\right\}$:

– $U^{\text{розм}}$ – *управління розміщенням* (збір інформації про об'єкти спостереження, визначення методів розміщення вузлів, вибір типу сенсорних вузлів (з врахуванням параметрів та середовища моніторингу), типу організації сенсорної мережі, тощо);

– $U^{\text{пок}}$ – *управління покриттям* (визначення типу покриття (покриття цілі (точки), покриття площі (зони, сектора), бар'єрне покриття), вибір моделі покриття в залежності від ступеня та коефіцієнта покриття);

– $U^{\text{спост}}$ – *управління спостереженням* (розрахунок сесій спостереження сенсорів та мережевої зв'язності).

Управління телекомунікаційною складовою включає наступні етапи $U_{\text{тел}}(t) = \left\{U^{\text{зб}}, U^{\text{ан}}, U^{\text{вц}}, U^{\text{рр}}\right\}$:

– $U^{\text{зб}}$ – збір інформації про стан мережі (рішення про об'єм, частоту, глибину способу збору інформації необхідно приймати на наступних етапах);

– $U^{\text{ан}}$ – аналіз даної інформації: ідентифікація ситуації в мережі (зоні і самому вузлі), перевірка виконання мережею своїх функцій та визначення необхідності управляючого впливу;

– $U^{\text{вц}}$ – виявлення цілі управління з подальшою деталізацією їх на підцілі і виробка рішення (вибір протоколу доступу, вибір метода спостереження та передачі, способу розсилки службової інформації і т.п.);

– $U^{\text{рр}}$ – реалізація рішення (встановлення потужності передачі, способу моніторингу, резервування ресурсу, розсилка службових повідомлень).

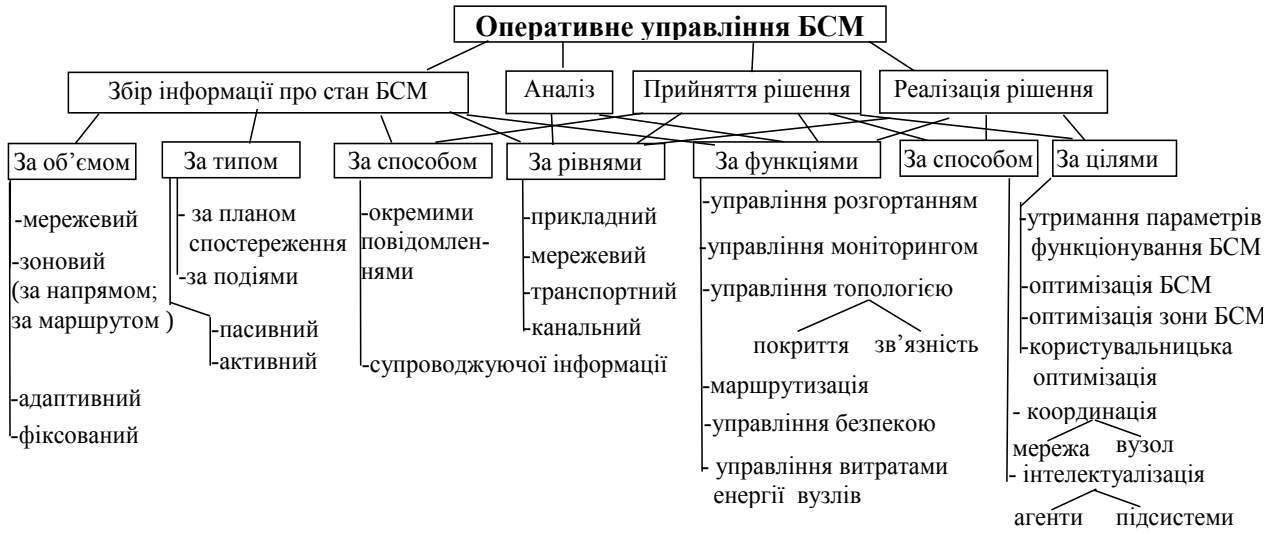


Рис. 3 Класифікація задач оперативного управління БСМ

Кількість і конкретні задачі оперативного управління визначаються характеристиками і умовами функціонування мережі, а також прийнятими технологічними рішеннями на етапі її проектування.

Принцип адаптивного управління. Внаслідок значної початкової невизначеності БСМ (обумовлена інерційністю контролю стану мережі та її ідентифікації), а також невизначеністю стану зовнішнього середовища оперативне управління повинне бути адаптивним.

Принцип функціональності управління. Об'єднання функцій системи управління у відносно незалежні групи дозволяє здійснити декомпозицію управління мережею на підсистеми (що значно спрощує задачу розробки математичного забезпечення управління):

– збір службової інформації про стан мережі для кожної з підсистем;

– прийняття рішень (управління покриттям, управління топологією мережі, управління побудовою та підтримкою маршрутів, управління витратами енергоресурсу вузлів, управління моніторингом, управління радіоресурсом, управління навантаженням, управління безпекою тощо);

– реалізації рішень для всіх підсистем.

Принцип ієрархічності управління. Функціональну структуру системи управління можна представити ієрархічною структурою з вертикальними зв'язками, які визначають підпорядкованість задач, що виконуються: на нижньому рівні вирішуються задачі управління сенсорним вузлом мережі; на верхньому – задачі управління всією БСМ.

Принцип координації та взаємодії. Внаслідок децентралізованого управління вирішення задач управління припускає взаємодію між вузлами за цілями, функціями управління, розподілом ресурсів тощо.

Принцип оптимальності управління. Якість управління визначається двома властивостями: обґрунтованість та своєчасністю управляючих впливів. Оптимальне управління являє собою компроміс між оперативністю та обґрунтованістю управляючих впливів, що є однією із найбільш складних задач, які належить розв'язати при побудові системи управління БСМ.

Принцип автоматизації та інтелектуалізації процесів управління. Його реалізація призвана мінімізувати участь людини в процесі управління тактичними мережами.

За способом реалізації частина задач оперативного управління вирішується ізольовано (окремим вузлом, наприклад, сенсором-шлюзом), а більша частина – кооперовано, сукупністю вузлів (наприклад, маршрутизація інформаційних повідомлень та ін.).

За охопленням задачі управління діляться на управління функціонуванням всієї сенсорної мережі (її зони) або процесом передачі інформації за напрямом між виділеними сенсорними вузлами.

За видом постановки та математичному апарату задачі діляться на задачі розміщення, розподілу ресурсів, розкладу роботи, маршрутні задачі та ін.

За функціями задачі управління БСМ діляться на 2 основні групи.

1. Задачі, які притаманні сенсорним мережам:

– задачі покриття території певного типу (площа, бартер, ціль) та способу покриття (*к*-покриття, α-покриття);

– задачі моніторингу;

– задачі енергозбереження при реалізації всіх функцій управління;

– задачі переміщення мобільних сенсорів на місця спостереження тощо.

2. Задачі, які характерні для будь-якої телекомунікаційної мережі, але мають свою специфіку через обмеженість ресурсів та децентралізацію управління:

– задача управління (побудови та підтримки) топологією мережі, яка повинна забезпечити зв'язність вузлів з врахуванням наявного покриття, якості потенційних маршрутів передачі при ресурсних обмеженнях;

– задача побудови та підтримки маршрутів передачі різних типів трафіка в умовах частої зміни топології та різних цільових функцій управління БСМ при ресурсних обмеженнях.

За способом реалізації частина задач оперативного управління вирішується ізольовано (окремим вузлом, наприклад, сенсором-шлюзом), а більшачастина – кооперовано, сукупністю вузлів (наприклад, маршрутизація інформаційних повідомлень й ін.).

За охопленням задачі управління діляться на управління функціонуванням всієї сенсорної мережі, її покриттям, напрямом, маршрутом передачі інформації за напрямом між сенсорними вузлами, вузлом, каналом.

За видом постановки та математичному апарату задачі діляться на задачі розміщення, розподілу ресурсів, складання розкладу, маршрутні задачі та ін.

Конкретна реалізація системи управління БСМ повинна враховувати її призначення та особливості архітектури (розмірність, мобільність, продуктивність, тип покриття, особливості об'єктів моніторингу й ін.) та умов функціонування. В той же час існують вагомі труднощі створення БСМ, які полягають у необхідності вирішення значної кількості наукових задач пов'язаних з управлінням мережею (управління покриттям, управління топологією, управління маршрутизацією, управління витратами енергії тощо) при обмеженнях на використання ресурсів вузлів (за ємністю пам'яті, продуктивністю процесора, енергоємністю батареї).

Основним завданням БСМ є покриття, моніторинг (виявлення і ідентифікація) об'єктів спостереження та передача інформації моніторингу користувачам через шлюзи.

Ефективність та тривалість функціонування БСМ залежить від взаємодії методів управління моніторингом з методами управління телекомунікаційною складовою. В зв'язку з цім виникає задача координації та інтеграції підсистеми моніторингу БСМ (розгортання, покриття, ідентифікація об'єктів, якість моніторингу) з підсистемою управління телекомунікаційною складовою (управління топологією, управління маршрутами, управління радіоресурсом, управління якістю обслуговування при передачі).

Об'єднання функцій системи управління у відносно незалежні групи дозволяє здійснити декомпозицію управління мережею на підсистеми: збору та зберігання службової інформації про стан мережі; аналізу та прийняття рішень (управління моніторингом та телекомунікаційною складовою), управління витратами енергоресурсу вузлів, інтеграції і координації; реалізації рішень.

З урахуванням наведених вище підходів щодо забезпечення функціонування БСМ військового призначення, а також класифікації задач оперативного управління БСМ пропонується принципово новий підхід побудови системи управління мереж даного класу, яка здійснює реалізацію принципу адаптації до умов функціонування, забезпечує задану якість обслуговування по послідовності реалізації функцій управління: покриття, моніторингу та передачі даних з врахуванням ресурсних обмежень.

Основні труднощі реалізації даного підходу це визначення цільових функцій і параметрів координації між підсистемами телекомунікаційної складової (за функціями і рівнями моделі OSI) і підсистемою моніторингу та визначення методів прийняття рішення, які дозволять отримати мережеву (зонову) оптимізацію.

Функціональна модель системи оперативного управління, яка реалізується кожним вузлом наведена на рисунку 4.

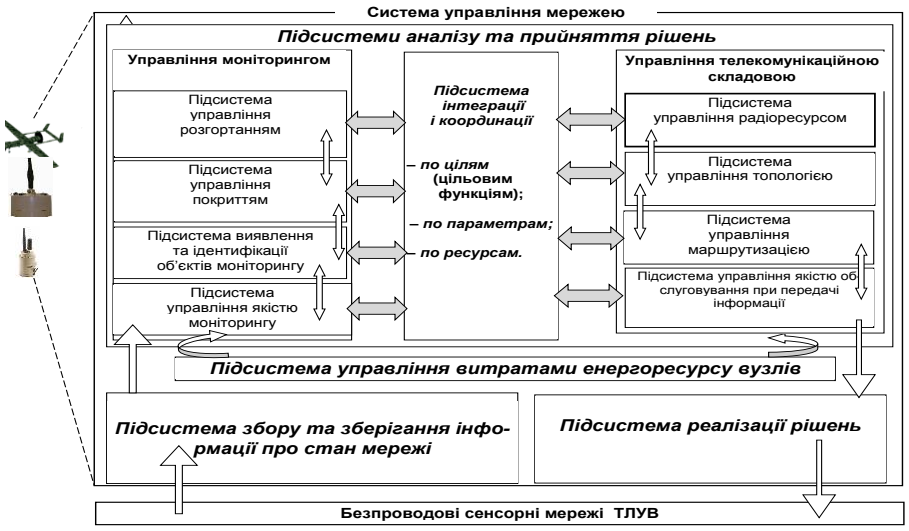


Рис. 4 Функціональна модель системи оперативного управління мережею (вузлом)

Загальна ідея – на першому етапі будується покриття території певного типу (площа, бартер, ціль) та способу покриття (*к*-покриття, α-покриття) (рис. 5).

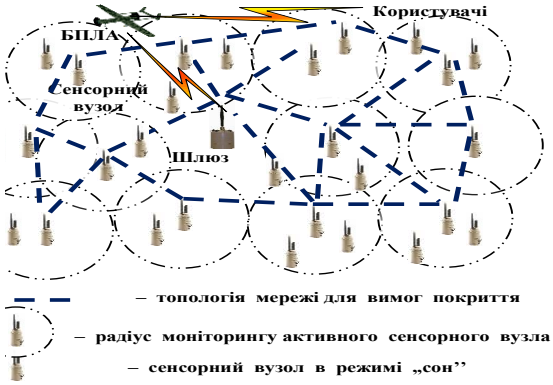


Рис. 5 Топологія мережі з врахуванням вимог покриття

На другому етапі здійснюється побудова топології та маршрутів передачі, яка реалізує скоординовану цільову функцію управління (рис. 6).

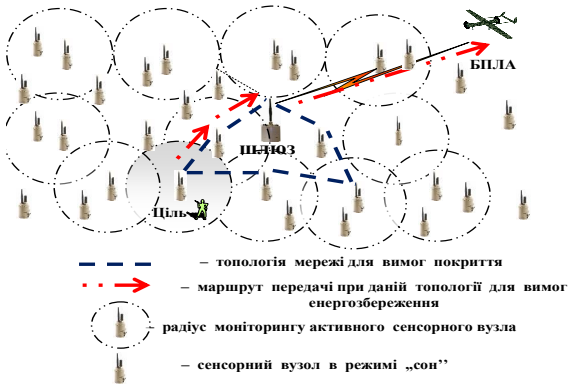


Рис. 6 Топологія мережі з врахуванням вимог покриття та маршрутів передачі інформації

В умовах змішаного управління (частка функцій виконується центром управління (шлюзом) БСМ, а друга децентралізовано – вузлами) можна визначити дві взаємозалежні групи цілей:

мережеві (зонові) – оптимізація мережевих або зонових показників ефективності центром управління БСМ;

користувальницькі – досягнення заданої якості моніторингу і передачі отриманої інформації та функціонування елементів мережі за напрямком передачі при децентралізованому управлінні.

До мережевих (зонових) цілей управління можна віднести оптимум наступних параметрів $C_i = \{ C_1, C_2, ..., C_n \}$: C_1 – час планування, розгортання, відновлення мережі, її зони; C_2 – якість покриття площі (зони, сектору) сенсорною мережею; C_3 – якість моніторингу; C_4 – якість передачі даних від вузла до шлюзу; C_5 – зв'язність мережі, її зони; C_6 – тривалість функціонування мережі, її зони; C_7 – продуктивність всієї БСМ, зони БСМ; C_8 – обсяг службового трафіку.

В умовах гібридного управління та наявності протиріч між оптимальною інформованістю керуючого об'єкта і своєчасністю керуючих впливів (цілей, зон спостереження) неможливо досягти глобальної оптимізації. Тому необхідно здійснювати локальну оптимізацію в рамках окремого вузла (зони моніторингу, радіоканалу, маршруту тощо). У зв'язку з цим основна мета управління декомпозується на наступні складові:

покриття, моніторинг, побудова топології для забезпечення визначеного типу покриття, маршрутизація та передача інформації між парою відправник – шлюз із заданою якістю при прагненні мінімізувати витрати мережевих (зонових) ресурсів на її здійснення або досягнення сприятливих умов для виконання цілей управління інших елементів мережі.

Отже, як видно з вищезазначеного, ефективність функціонування БСМ залежить як від рішень які приймаються окремими вузловими СУ, так і від узгодженості цих рішень між собою За таких умов створення СУ БСМ потребує обґрунтування множини задач, які повинні вирішуватись кожною функціональною підсистемою вузлової СУ (рис. 4), обґрунтування цілей функціонування вузлових СУ та вибір методів (методик та моделей) їх досягнення з урахуванням обмежень Ω на вузлові та мережеві ресурси.

Проведений аналіз особливостей сенсорних мереж, особливостей побудови системи управління, вимог до перспективних сенсорних мереж та системи управління ними показує, що на сьогодні існує протиріччя між можливостями існуючих методів та методик управління ресурсами сенсорних мереж та вимогами до перспективних БСМ і процесу управління ними (рис. 7).

Зокрема, існуючі методи та методики не забезпечують здатність БСМ до самоорганізації та адаптацію вузлів до різних умов функціонування, мають централізований характер, не пристосовані для прийняття рішень в реальному часі, не враховують особливостей покриття військових об’єктів та поля бою, використовують обмежену кількість параметрів для оцінки процесу функціонування БСМ (мобільних вузлів), мають значну розрахункову складність.

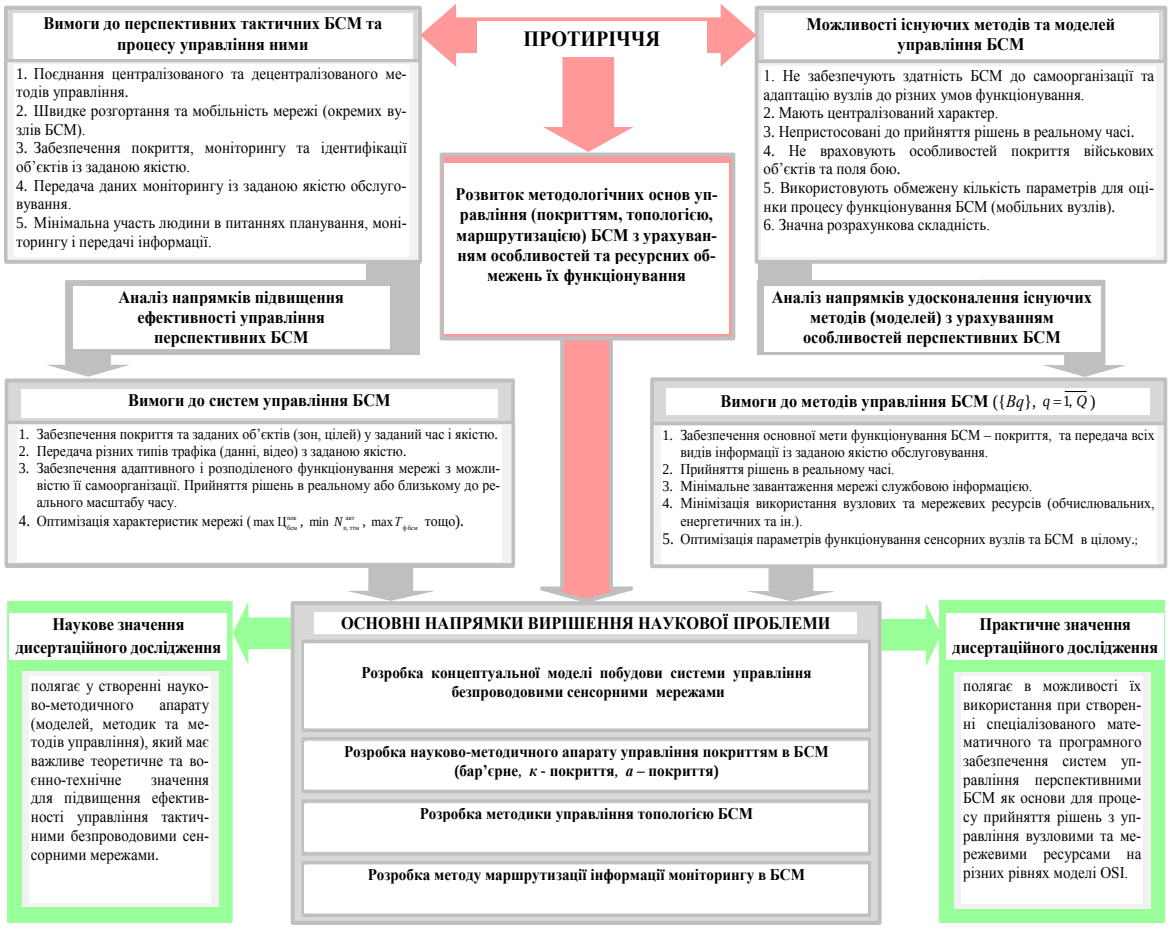


Рис. 7 Загальна схема вирішення проблеми управління БСМ

Існуючи спроби створення СУ тактичними сенсорними мережами носять фрагментарний характер, задачі розробки методів управління ресурсами БСМ вирішуються відокремлено для кожної підсистеми вузлової СУ та на різних рівнях еталонної моделі OSI, а відсутність понятійного апарату управління – тільки ускладнює цей процес.

Тому актуальною є проблема спрямована на усунення зазначеного вище протиріччя шляхом розробки нових методів (методик, моделей) управління ресурсами вузлів безпроводових сенсорних мереж з урахуванням особливостей та ресурсних обмежень функціонування мереж даного класу.

Для їх розробки пропонується схема системного аналізу і синтезу (рис. 8), яка передбачає поділ загального процесу синтезу на послідовність етапів. Як видно з рисунку, через високу взаємозалежність між етапами, неповноту вихідних даних та необхідність корегування отриманих результатів завдання синтезу методів управління вирішується ітераційно.

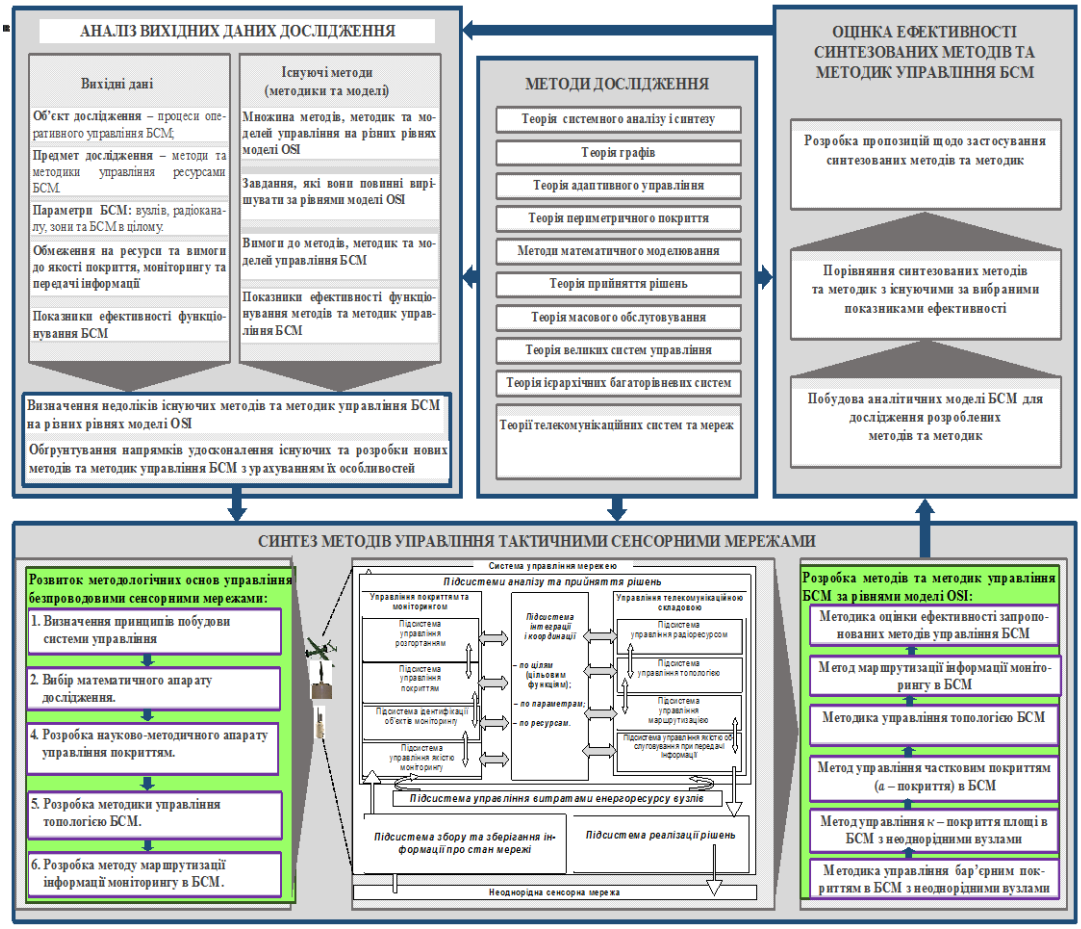


Рис. 8 Схема системного аналізу та синтезу методів управління БСМ

ВИСНОВОК. Запропоновано методологію управління неоднорідними безпровідними сенсорними мережами військового призначення. Проведено класифікацію сенсорних мереж, визначено цілі управління неоднорідними безпроводовими сенсорними мережами, запропоновано нові підходи щодо функціонування даних мереж. Розроблена схема системного аналізу і синтезу, яка визначає напрями розробки нових методів (методик, моделей) управління ресурсами вузлів безпроводових сенсорних мереж з урахуванням особливостей та ресурсних обмежень функціонування.

ЛІТЕРАТУРА:

1. Жук О.В., Романюк В.А., Бовда Е.М. Управління перспективними неоднорідними безпровідними сенсорними мережами тактичної ланки управління військами: проблема і шляхи рішення. *Збірник наукових праць "Труди університету"*. №1 (140). 2017. С. 171–180.

2. Жук О.В. Концепція побудови системи управління безпроводових сенсорних мереж військового призначення. Збірник наукових праць "Труди університету". *Збірник наукових праць "Труди університету"*. 2011. №7 (106). С. 156–166.

Кузавков В.В. (ВІТІ)

ОЦІНКА МОЖЛИВОСТІ ЗМІНИ КОНСТРУКТИВУ ВСТАНОВЛЕННЯ АНТЕНИ СУПУТНИКОВОГО ЗВ'ЯЗКУ

В доповіді розглянуто спосіб підвищення ефективності застосування офсетної антени супутникового зв'язку шляхом зміни конструктиву її встановлення та кріплення. Передумовою для впровадження такого підходу є можливість застосування для прийому (передачі) сигналів зі супутника "нижньою" частиною дзеркала прямофокусної антенної системи - "нижньої" вирізки - офсета.

Вступ.

Аналіз дій в умовах АТО (ООС) показав що, надійний зв'язок залишається одним із головних факторів, умовою забезпечення ефективності управління військами, та лише сучасні засоби зв'язку дозволяють керувати військами на якісно новому рівні [1].

На сьогодні, в бойових частинах і підрозділах зони АТО, обмін інформацією здійснюється за допомогою сучасних, захищених цифрових засобів. ЗС України майже на 100% відійшли від аналогових засобів зв'язку. Кардинально змінилися і погляди на організацію зв'язку з використанням нових технічних засобів. Аналіз підвищення рівня боєготовності ЗС України в період з 2014 по 2017 року свідчить про те що, то процес удосконалення та модернізації військової техніки, зокрема і засобів зв'язку, не повинен припинятися [2]. Зважаючи на те, що Підрозділи ЗС України в зоні АТО перебувають в обороні, найбільшого застосування набули: дротовий та супутниковий види зв'язку.

Постановка завдання.

Виходячи з викладеного, одним з основних завдань підрозділів зв'язку ЗСУє необхідність використовувати такі зразки техніки, які адаптовані для роботи саму у польових умовах, а основну увагу звернути на спрощення процесу їх налаштування та підвищення скритності використання. Напрямком удосконалення та модернізації військової техніки є підвищення ефективності функціонування системи зв'язку (системи управління військами).

Супутниковий зв'язок має широкий спектр можливостей, на нього покладається рішення багатьох завдань і тому проблема розвитку та модернізації (вдосконалення) систем супутникового зв'язку (антенних систем супутникового звязку) є актуальною [3].

Аналіз останніх досліджень та публікацій.

Аналіз джерел [1; 3; 5-7] виявив, що широке застосування системи супутникового зв'язку обумовлене її надійністю, простотою використання, можливістю функціонувати в будь який місцевості. Але, під час застосування подібної системи в зоні бойових дій були виявлені певні незручності використання цивільних технологій (верхньої вирізки параболоїду обертання) у військовій сфері. Матеріал наведений нижче присвячений обґрунтуванню можливості зміни конструкції встановлення (кріплення) антени супутникового зв'язку. Мова ідеться не про виготовлення нової антени. Зміна конструкції кріплення вже існуючого зразку розкриває нові можливості при використанні системи супутникового зв'язку в ЗСУ.

Виклад основного матеріалу.

Найбільш розповсюдженим варіантом антенних систем супутникового зв'язку є дзеркальні параболічні антени. Характерною рисою таких антен є значні геометричні розміри. Площа антени S_a (дзеркала, відбивача) - найважливіший параметр, оскільки саме від неї залежать енергетичні характеристики (параметри) всього тракту передачі інформації [4, 5]. Коефіцієнт підсилення передавальної (приймальної) антени $G_{П}$ ($G_{ПР}$) показує забезпечення нею виграш (по потужності сигналу) в порівнянні з ненаправленою антеною :

$$G_{\max} = \frac{4\pi S_a}{\lambda^2}$$

де G_{max} - максимальне значення коефіцієнту підсилення; S_a - ефективна площа антени; λ - довжина хвилі [6].

Дзеркальні параболічні антени бувають не лише прямофокусні (PrimeFocus). На практиці широко використовуються офсетні (Offset) антени.

Дзеркало прямофокусної антени – параболоїдобертання, її геометрична вісь співпадає з електричною віссю. На цій вісі розміщується конвертор (фрагмент приймально-передавального тракту). В свою чергу, офсетна антена представляє собою вирізку з параболоїда, яка утворюється в наслідок перетину параболоїду та циліндра, вісі яких паралельні. Таким чином, дзеркало офсетної антени може мати форму еліпсу, а напрямок електричної вісі буде на 20^0-30^0 вище (нижче) за геометричну вісь (рис. 1).

Обидва типи антен мають свої переваги та недоліки.

У офсетних антен більш ефективно використовується площа дзеркала. Офсетна антена має таку ж ефективну площу, як прямофокусна антена з діаметром рівному розміру офсета по меншій вісі.

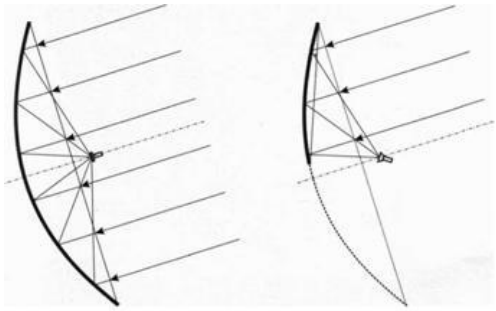


Рис. 1. Геометрія прямофокусної та офсетної антени

Крім того, у прямофокусної антени дзеркало частково затуляється конвертором та елементами кріплення (для антен малого діаметру до 1,5 м, конвертер та елементи кріплення можуть затуляти більше 10% площі). Тому, антени малих розмірів (що характерно для військ та умов ведення бойових дій) роблять офсетними, а антени великих розмірів – прямофокусними.

Різними є і способи встановлення цих антен. Прямофокусна антена завжди піднята на деякий кут, тому представляє собою «чашу» (рис. 2), в якій можуть накопичуватися осади (вода, сніг).

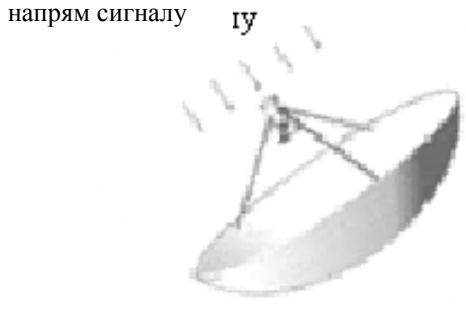


Рис. 2. Прямофокусна антена

Офсетні антени встановлюються майже вертикально (рис. 3). Це позбавляє їх зазначеного недоліку, але така конструкція має підвищене вітрове навантаження. Це навантаження е додатковим зовнішнім впливом для системи керування антеною.

напрям сигналу

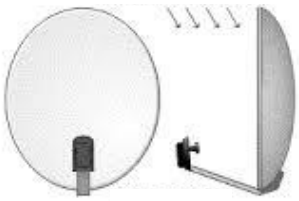


Рис. 3. Офсетна антена

Можна зробити висновок, що офсетні антени за своїми властивостями є більш придатними для застосування у військовій сфері (незначні габарити, маса, а отже – можливість швидкого розгортання та згортання, мобільність під час транспортування). Розмір антени в умовах бойових дій є основною демаскуючою ознакою та стійкою розвідувальною ознакою приймально - передавального центру (командного пункту; пункту управління).

На сьогодні, підрозділами зв'язку ЗСУ для організації супутникового зв'язку використовуються офсетні антени діаметром 0,75 м. Послуги, щодо забезпечення супутниковим зв'язком покладаються на реселера компанії з Італії «Скайлоджик» - «Дата Груп», яка є найбільшим в Україні VSAT-оператором [7].

Варіанти встановлення офсетної антени (в населеному пункті) наведено на рис. 4.

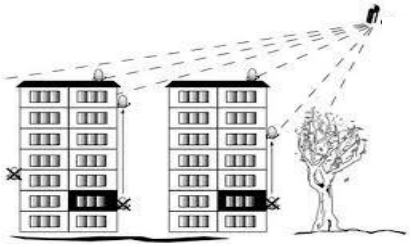


Рис. 4. Варіанти встановлення офсетних антен

При застосуванні системи супутникового зв'язку в таких умовах слід враховувати:
необхідність присутності прямої видимості штучного супутника Землі;
встановлення антен на більшій висоті може викликати ослаблення сигналу в кабелі зниження (від антени до приймача або модему);
час необхідний для монтажу;
можливість впливу грозових розрядів;
вплив вітрового навантаження.

До переваг слід виділити відносну надійність кріплення до елементів споруди, порівняно з варіантом встановлення на відкритій місцевості.

Зважаючи на те, що антена знаходиться на відкритий місцевості (в зоні прямої видимості штучного супутника Землі), такий варіант встановлення робить антену схильною до аеродинамічних впливів (стохастичних характеристик напору вітрового потоку, який може бути спричинений і вибуховою хвилею).

Прийнятий варіант встановлення офсетної антени в укриті (в 2015 та 2017 роках широко застосовувався в зоні АТО) не в повній мірі, а лише частково вирішує питання забезпечення розвідзахищеності (рис. 5) та зменшення аеродинамічного впливу. Крім того обладнання укриття потребує певного часу та людських ресурсів.

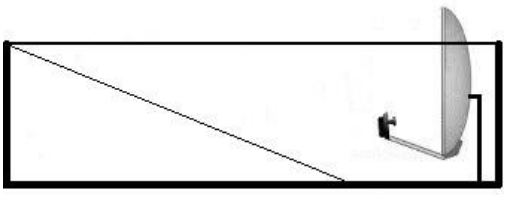


Рис. 5. Варіант встановлення офсетної антени в укритті

Головними недоліками які впливають на бойове застосування супутникових антен є:

демаскуючі ознаки;
жорсткі вимоги до місця (місцевості) розгортання антени;
обмеження в довжині кабелю, який з'єднує антену з модемом;
вплив вітрового навантаження (вибухових хвиль);
складності забезпечення електромагнітної сумісності радіозасобів які розміщені в обмеженому просторі (на одній транспортній базі);
екрануючи властивості АС супутникового зв'язку, які спотворюють діаграму направленості напівхвильових вібраторів (антен інших радіозасобів, що розміщено поруч).

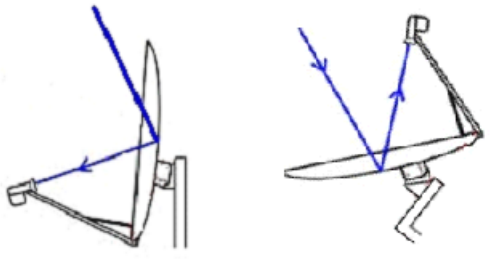


Рис. 6. Варіанти встановлення офсетної антени

З метою підвищення ефективності застосування офсетних антен супутникового зв'язку запропоновано змінити підхід при встановленні та кріпленні офсетної антени. Сутність змін відображує рис. 6. В наслідок зміни конструктиву напрям електричної вісі залишається незмінним, а геометрична вісь нахиляється та наближується до горизонтального положення.

Висновки.

Під час проведення натурних випробувань з метою оцінки характеристик офсетної АС супутникового зв'язку до (вертикальне положення) і після зміни (горизонтальне положення) АС з'ясовано:
зменшується вітрове навантаження на конструкцію АС та вузли автоматичної (автоматизованої) системі стеження (наведення);
енергетичні характеристики антени не змінилися під час зміни її геометричної вісі;
альтернативний варіант встановлення АС створює умови для забезпечення електромагнітної сумісності радіоелектронних засобів у ближній зоні;
з'являється можливість збільшити розвідзахищеність АС (приймально – передавального центру) завдяки зменшенню видимої площі АС.

ЛІТЕРАТУРА

1. Сучасні засоби зв'язку — складова ефективної системи управління військами //Народна Армія 29.12.2015 - с. 3–5.
2. http://milnavigator.com.ua/як змінилися війська зв'язку з початку/ 07.08.2017.
3. Розпорядження Кабінету Міністрів України №600-р від 30 серпня 2017 р./ Деякі питання розвитку критичних технологій у сфері виробництва озброєння та військової техніки.
4. Спутниковая связь и вещание/ Под ред. Л.Я. Кантора // Справочник. - 2 изд., передраб. и доп.– М.Радио и связь - 1988.
5. Бородич С.В. ЭМС наземных и космических радиослужб // М: Радио и связь, - 1990.Одесса: УГАС, 1996. – с. 30–63.
6. Паламарчук С.В., Коротченко Л.А., Кузавков В.В., Зарубенко А.О. Методика проведення енергетичного розрахунку в трактах системи супутникового зв'язку. Збірник наукових праць випуск №3, Київ: ВІТІ, 2017. с. 42-47.
7.Ка-революция в спутниковом ШПД //Журнал "Технологии и средства связи" №2, 2011, с.64-70.

Панченко І.В. ORCID 0000-0001-5690-3813 (ВІТІ)

КОНЦЕПТУАЛЬНИЙ ПІДХІД ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ ДЛЯ ЗАХИСТУ МЕРЕЖІ FANET ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

З розвитком штучного інтелекту та інших технологій, таких як розподілене машинне навчання та ройовий інтелект, група безпілотних літальних апаратів (БпЛА) може спільно вирішувати складніші завдання, такі як розвідка, спостереження пошук цілі, її супроводження та знищення. Зазвичай група БПЛА працює цілеспрямовано. Це означає, що кілька БпЛА будуть залучені для створення групи та спільного виконання отриманого завдання.

Під час побудови групи та виконання завдань БпЛА багато взаємодіють один з одним. Коли вони працюють у ненадійному чи ворожому середовищі, питання забезпечення аутентифікації між БпЛА є особливо важливим.

Також група БпЛА може взаємодіяти з різними мережевими середовищами, у тому числі зі складною багаторівневою архітектурою, показаною на рисунку 1. За рівнями мережі поділяються: для висотних БпЛА (HAU) – понад 20 км, середньовисотних БпЛА (MAU) – до 11 км та маловисотних БпЛА (LAU) – до кількох кілометрів.

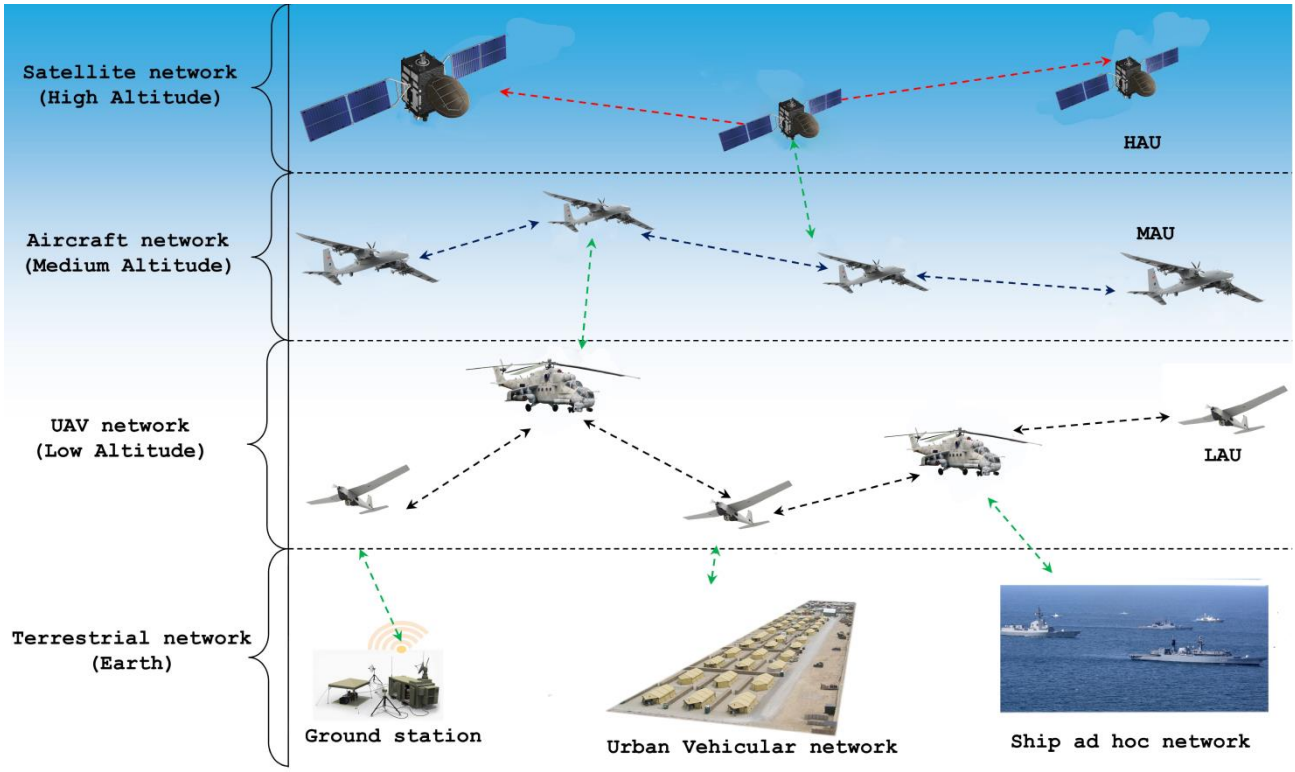


Рис.1. Багаторівнева мережева архітектура FANET

У процесі створення групи, БпЛА можуть ефективно обмінюватися даними один з одним та з наземною станцією, якщо вони функціонують в одній групі, а також можуть використовувати зовнішнє мережеве середовище. Саме при підключенні до зовнішньої мережі, з’єднання стає ненадійним, що називається слабким зв'язком. Ці зміни стану мережевого підключення вносять великі технічні проблеми при розробці моделей аутентифікації для БпЛА.

Для забезпечення конфіденційності, достовірності та безпеки передачі даних існують відповідні протоколи маршрутизації, які подано в таблиці 1. Ця категорія захищених протоколів маршрутизації розроблена відповідно до особливостей FANET (рис.2.).

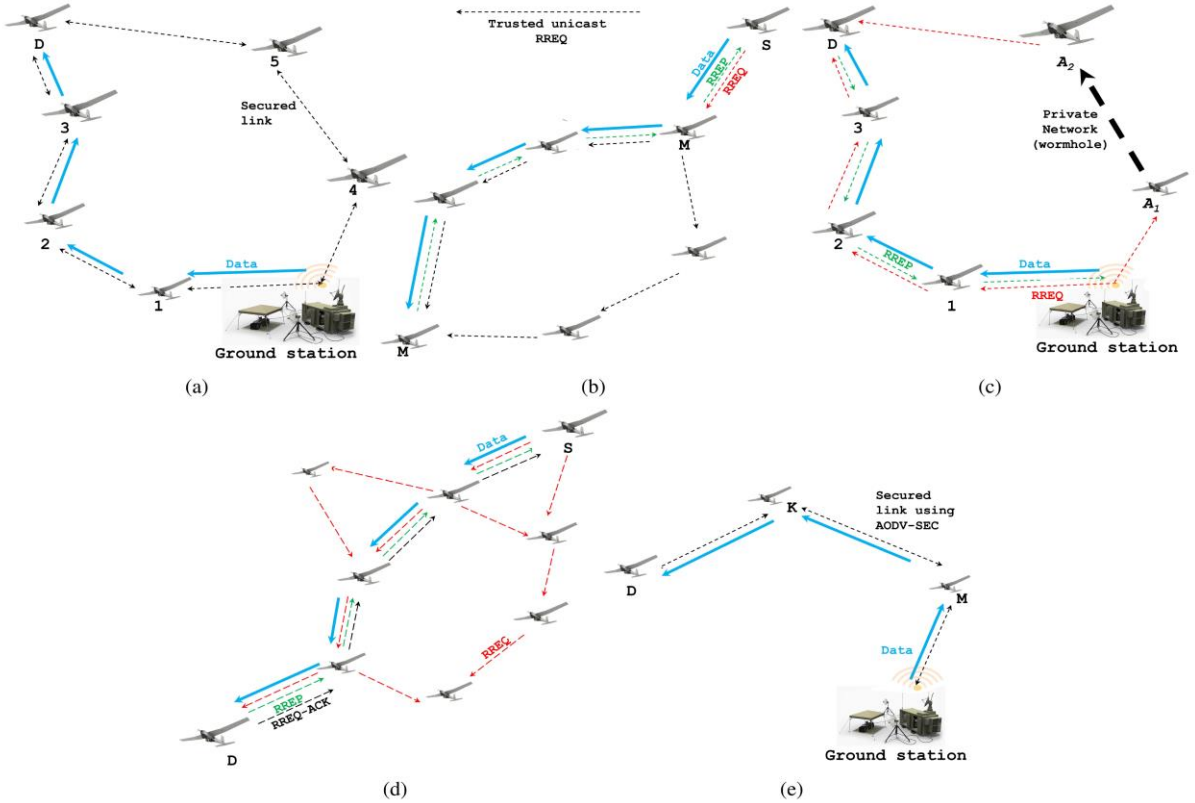


Рис.2. Захищені протоколи маршрутизації. (a) Протокол SUANET. (b) Протокол PASER. (c) Протокол SUAP. (d) Протокол AODV-SEC. (e) Протокол SRPU.

Таблиця 1

		Маршрути-зація	Щільність	Складність	Переваги	Недоліки
1	SUANET (Secure UAV Ad-hoc NETwork)	Динамічна	Середня	Висока	Підвищення безпеки та якості з'єднання	Недостатня стабільність з'єднання
2	PASER (Position-Aware, Secure, and Efficient mesh Routing)	По запиту	Висока	Середня	Забезпечення масштабування та безпеки	Висока ресурсоємкість і ступінь затримки з'єднання
3	SUAP (Secure UAV Ad hoc routing Protocol)	По запиту	Висока	Середня	Несприйнятли-вість масовій кількості атак	Низька мобільність мережі
4	AODV-SEC (Ad hoc On-Demand Distance VectorSecure)	По запиту	Висока	Середня	Безпечний процес виявлення	Використовує складну обробку
5	SRPU (Secure Routing Protocol for UAVs)	По запиту	Висока	Середня	Підвищує механізми безпеки	Висока ресурсоємкість

На превеликий жаль, розглянуті вище захищені протоколи маршрутизації для БпЛА в основному зосереджені на тому, як покращити безпеку та знизити обчислювальні витрати.

Щоб вирішити питання з обмеженістю обчислювальних ресурсів БпЛА, доцільно розглянути технологію блокчейн через її децентралізацію та розподіл інформації.

Це дозволяє отримати виграш через більш надійну та легку аутентифікацію, та зберігати ідентифікаційну інформацію пристроїв, яка надійно зберігається в блоці, щоб полегшити запит під час аутентифікації та вирішити проблему при відмові з'єднання з централізованим сервером.

Щоб адаптуватися до динамічного мережевого середовища та низької якості з'єднання, з якими може стикається БпЛА, необхідно поділити аутентифікацію БпЛА на аутентифікацію при побудові групи в зовнішній мережі та внутрішньогрупову аутентифікацію з двоетапною структурою аутентифікації.

Аутентифікація на основі блокчейну для створення групи.

При надходженні завдання, система визначає найбільш надійний БпЛА, що функціонуватиме в якості вузла mUAV. Потім mUAV, який отримує завдання від наземної станції керування, почне створювати групу, орієнтовану на завдання. При цьому mUAV повинен забезпечити безпеку приєднання до інших БпЛА за допомогою протоколів автентифікації на основі блокчейн.

Процес використання технології блокчейну для захисту мережі FANET від несанкціонованого доступу показано на рис.3.

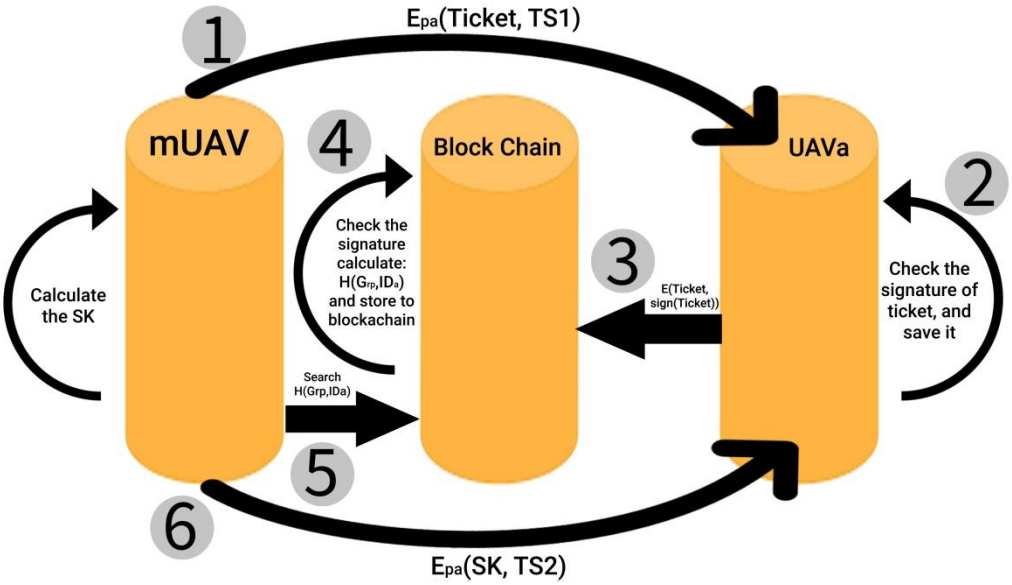


Рис.3. Процес аутентифікації та ініціалізації БпЛА
при створені групи на основі блокчейну

Кроки процесу такі:

0 крок. Коли mUAV отримує завдання, він генерує попередній загальний ключ SK для цієї групи та завдання на кожен БПЛА вибираються таким чином:

$$\text{Ticket\_to\_A} = (\text{GrpID}|\text{IDa}|\text{sign}(\text{GrpID}, \text{IDa})),$$

де, GrpID є унікальним ідентифікатором групи БпЛА, створеної mUAV, який є загальнодоступним;

IDa – це приватна ідентифікація, що генерується mUAV для UAVa;

sign(GrpID, IDA) – підпис із закритим ключем mUAV.

1 крок. Після знаходження відкритого ключа UAVa через блокчейн mUAV використовує цей відкритий ключ, шифрує та відправляє (Ticket, TS1) на UAVa.

2 крок. Після того, як UAVa розшифровує повідомлення своїм закритим ключем, він оцінює час та підпис TS1, потім отримує відкритий ключ mUAV через блокчейн, перевіряє підпис у завданні, і після підтвердження справжності завдання зберігає GrpID та IDA.

3-4 кроки. БпЛА викликає смарт-контракт, завантажує (ticket, sign (ticket)), а потім смарт-контракт використовує відкритий ключ БпЛА для перевірки підпису, а потім використовує відкритий ключ mUAV для перевірки підпису в квитку. Після підтвердження їх правильності смарт-контракт записує H(GrpID, IDa) блокчейн.

5 крок. mUAV викликає смарт-контракт пошуку існування H(GrpID, IDa).

6 крок. Якщо результат пошуку на кроці 5 існує, mUAV надсилатиме зашифровані повідомлення, включаючи попередній загальний ключ SK та тимчасову мітку TS2, використовуючи загальнодоступні ключі UAVa.

Внутрішньогрупова аутентифікація

Спрощена процедура аутентифікації та ініціалізації БпЛА при створені групи на основі блокчейну (рис.4). Передбачається робота тільки з мережею групи.

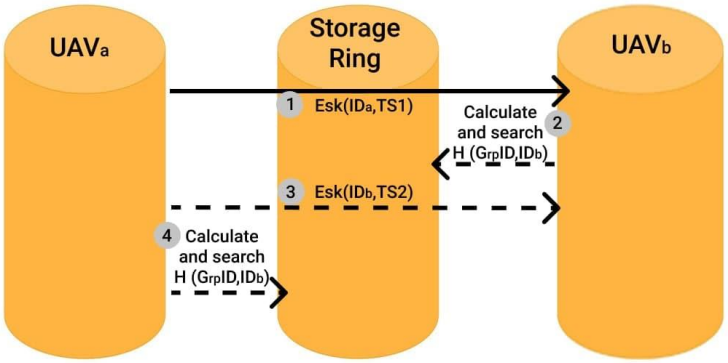


Рис.4. Процес внутрішньогруповоїаутентифікації та ініціалізації БпЛА на основі блокчейну

Кроки процесу наступні:

1 крок. UAVa шифрує свій IDa та тимчасову мітку TS1 за допомогою попереднього загального ключа SK та відправляє на UAVb.

2 крок. UAVb розшифровує повідомлення та перевіряє мітку часу TS1, обчислює хеш (GrpID, IDa), а потім робить порівняння та підтвердження існування UAVa.

3 крок. Після того, як UAVb успішно підтвердив існування UAVa, він шифрує (IDb, TS2) та відправляє його на UAVa.

4 крок. Після того, як UAVa розшифровує повідомлення, він перевіряє мітку часу TS2 та обчислює хеш (GrpID, IDb), потім виконує пошук у списку та перевіряє результати.

Якщо результат перевірки є вірним, відбувається процес переходу до етапу комунікації. UAVa та UAVb зберігають ідентифікатори один одного в локальному кеші, що зручно для швидкої перевірки наступного разу.Цей протокол аутентифікації відрізняється високою надійністю. Також можна зберігати інформацію про БпЛА групи розподіленим чином, уникаючи проблеми відмови з'єднання.Коли завдання ініціюється, створюється група довірених БпЛА, орієнтована yf завдання. Аутентифікація між БпЛА та mUAV виконується шляхом виклику смарт-контракту блокчейну. Смарт-контракт автоматично підтверджує справжність БпЛА та записує результат підтвердження до блоку. Усі мережні вузли можуть підтвердити, що аутентифікація ідентичності успішна, запитуючи блокчейн. З одного боку, блокчейн відіграє роль центру сертифікації, виконуючи безпечну автентифікацію БпЛА децентралізованим способом. З іншого боку, всі ідентифікатори БпЛА зберігаються у вигляді хеш-значень у блокчейні, і усі БпЛА також використовують ідентифікатор.

Якщо ж зловмисник зчитує аутентифікаційну інформацію при спробі підключення до групи БпЛА, він може отримати тільки ідентифікатор групи і хеш-значення БпЛА. Зрештою, кожна група виконує завдання лише один раз. Після завершення завдання група автоматично розпускається і всі дані про аутентифіковані пристрої, квитки, токени та інші сертифікати аутентифікації всіх БпЛА групи знищуються. Це забезпечує безпечну маршрутизацію при створенні групи БпЛА та виконанні поставлених групі завдань.

Таким чином, запропонований концептуальний підхід для захисту мережі FANET від несанкціонованого доступу полягає у використанні процедури аутентифікації БпЛА при створенні групи на основі блокчейна, який поділяє аутентифікацію БПЛА на групову аутентифікацію та внутрішньогрупову аутентифікацію з двоетапною аутентифікаційною структурою є актуальним і потребує поглибленого дослідження.

Чміль В.В. (ПрАТ «НВП «Сатурн»)
к.т.н. Ожінський В.В. (ЦКДЗ НЦУВКЗ)
к.т.н. Поіхало А.В. (НЦУВКЗ)
к.т.н. Сундучков І.К. (ПрАТ «НВП «Сатурн)

МЕТОДИ, СТРУКТУРА ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ УПРАВЛІННЯ КАНАЛАМИ ПРИЙМАННЯ ТЕЛЕМЕТРИЧНОЇ ІНФОРМАЦІЇ ВІД КОСМІЧНИХ АПАРАТІВ З ДОСЛІДЖЕННЯ СОНЯЧНОЇ СИСТЕМИ

На прикладі пункту приймання телеметричної інформації (РТ-32) в Центрі космічних досліджень та зв`язку Національного центру управління та випробувань космічних засобів, м. Золочів Львівської області, описано принципи побудови системи управління каналами приймання інформації. Наведено приклад практичної реалізації такого пристрою.

ВСТУП

Система управління пристроєм приймання телеметричної інформації з космічних апаратів повинна вирішувати такі завдання: управління антенним комплексом для наведення та програмне супроводження космічного об`єкта; управління процесом виходу на режим радіоастрономічного приймального комплексу; управління процесами частотно-часової синхронізації та прив`язки до світової шкали часу; управління процесом обробки одержаної інформації та процесом передачі інформації зацікавленим сторонам; управління процесами прийняття рішень у випадках відхилення від норми в роботі окремих систем чи підсистем за результатами контролю технічного стану; дистанційне управління роботою, включаючи формування планів-завдань.

Управління технічним станом РТ-32 та його роботою - це складний процес, що вимагає наявності достовірної інформації про поточний стан складових частин (систем та підсистем) радіотелескопа, ефективних механізмів її обробки для забезпечення їх чіткої взаємодії. У зв`язку з цим, також важливим є: контроль технічного стану систем та підсистем пункту приймання інформації (радіоастрономічної приймальної системи, частотно-часового забезпечення, систем зв`язку, накопичення та передавання даних, системи управління антенним комплексом, системи енергозабезпечення, підсистем кріогенного охолодження, забезпечення вакуумної складової).

Принципи побудови.

Головним завданням в ході приймання телеметричної інформації з космічних апаратів є забезпечення надійності роботи систем, в тому числі системи управління, забезпечення приймання інформації, навіть за виникнення часткових відмов окремих складових систем. На якість приймання інформації також впливають зовнішні умови (погодні, аварії енергозабезпечення, виникнення зовнішніх електромагнітних завад та інше).

Все це потребує під час процесів управління функціонувати в просторі високого ступеня невизначеності. В таких умовах для прийняття рішень доцільно використовувати методи статистичного аналізу, теорію нечітких множин, ймовірнісні способи визначення стану нечітких параметрів.

Теорія нечітких множин та заснована на ній логіка дозволяють описувати неточні категорії, уявлення і знання, оперувати ними і робити відповідні висновки.

Наявність можливостей теорії нечітких множин описувати неточні категорії дає метод для формування моделей різноманітних об’єктів, процесів та явищ на якісному рівні, визначає інтерес до організації інтелектуального направлення.

Нечіткі системи керування використовують наявну базу знань і елементи штучного інтелекту та можуть бути реалізовані за логічними формулами, що використовують логічні операції « І », « АБО », «ЯКЩО» і т. ін.

Процес управління можливо описати як лінгвістичні змінні, згрупувавши їх за напрямками та характерним рисам.

Модель управління технічним станом РТ-32 може бути представлено виразом

$Y = fx(x_1 x_{2.} \dots x_n)$, де х – чинники, які впливають на роботу системи
серед $(x_1 x_{2 \dots} x_n)$ є чинники, які мають постійний та більше сталий характер, а є чинники, які залежать, у свою чергу, від чинників наступного рангу.

$$x_n = f(c_1 c_2 \dots c_m)$$

Модель управління буде представляти собою матрицю управлінських рішень.

$$Y_1 = fx(x_{11} + x_{12} \dots + x_{1n})$$
$$Y_2 = fx(x_{21} + x_{22} \dots + x_{2n})$$

$Y_m = fx(x_{m1} + x_{m2} \dots + x_{mn})$,
де x_{mn} – чинники, які впливають на роботу системи,
а Y_m – управлінські рішення за результатами логічної обробки даних контролю технічного стану x_{mn}., або вхідних даних для проведення сеансу спостережень (зв'язку).
Чинники впливу на технічний стан радіотелескопа можливо поділити на декілька груп: дефекти, що виникають під час проектування та виготовлення; дефекти, пов`язані зовнішніми факторами та ті, що виникають в процесі експлуатації.
Щоб перейти від отриманих нечітких множин до кількісної оцінки необхідно виконати процедуру дефазифікації, тобто перетворення нечіткої інформації в чітку форму.
Серед різних методів дефазифікації найбільш поширеними є знаходження середньостатистичного рівня, розрахунку ймовірності події і т.д. Необхідно звернути увагу на окремі задачі управління, не пов`язані з процесом контролю технічного стану складових частин радіотелескопа. Мати можливість: дистанційного (мережею Internet) введення план-завдань на проведення сеансів спостережень; дистанційного (мережею Internet) контролю ходу проведення сеансів; дистанційного (мережею Internet) управління первинним оброблянням отриманих даних.

Також важливе місце в роботі РТ-32 займає процес передавання отриманої інформації для подальшої обробки в кореляційні центри (центри обробки) індивідуальних замовників.

Сукупність цих додаткових потреб та необхідність в прийнятті рішень різнорідного характеру, як можливість продовження сеансу зв`язку під час приймання телеметричної інформації незважаючи на виникнення нестандартної ситуації, можливість проведення сеансу спостережень в заданий час, за відхилень у стандартному робочому режимі окремих систем та підсистем, збільшує ступінь невизначеності в прийнятті управлінських рішень.
В цілому, в силу високої ступені невизначеності, зміни великої кількості чинників впливу, високий рівень впливу зміни параметрів зовнішнього середовища, в процесі управління сеансами приймання телеметричної інформації, неможливо виключити людський фактор (оператора), який включається в процес прийняття рішення, хоча більшість рішень під час аварійних ситуацій приймається автоматично системою управління радіотелескопом.

Структурна схема управління показана на рис.1

Як видно з рис.1 схема прийняття рішень має три рівні:
- Оператор (людський фактор) – І рівень
- Штучний інтелект - ІІ рівень
- Індивідуальні рішення та жорсткі схеми управління складових частин РТ-32 - ІІІ рівень

Пріоритет прийняття рішень з І до ІІІ рівнів. Вищий рівень може відмінити рішення нижчого рівня.

І-ий (вищий рівень) управління застосовується в процесі за умов окремих операцій під час нештатних (аварійних) ситуацій.

Тактичні рішення (наприклад, перехід на резервний вхід системи енергозабезпечення або інформування оператора про відхилення від стану «норма») приймаються ІІІ-м (нижчим) рівнем управління.

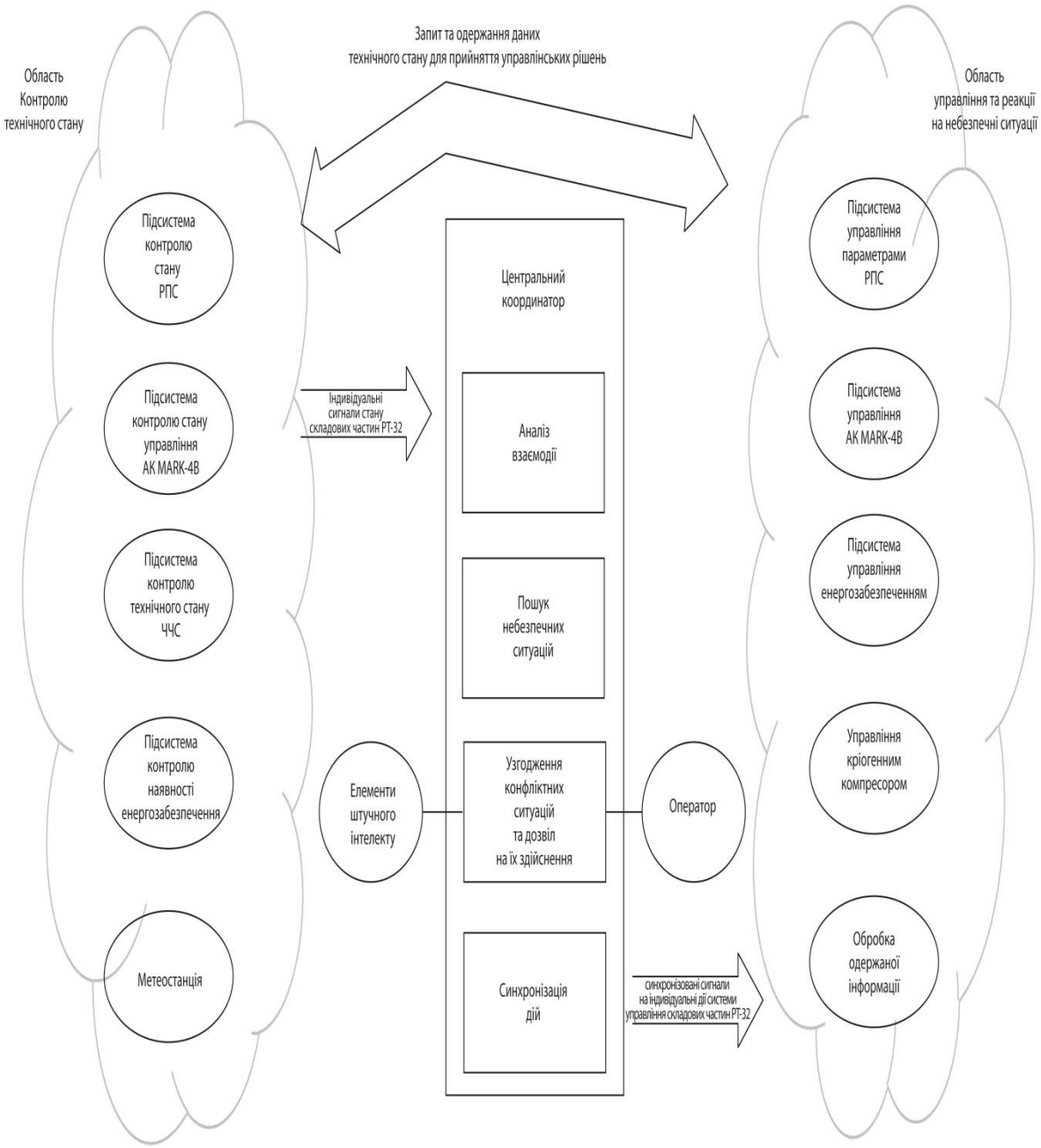


Рис.1

Структура систем контролю технічного стану та керування РТ-32

Для підвищеної стійкості процесу управління ряд функцій управління дублюються (повторюються) як на II-му так і на III-му рівнях управління.

Практичним результатом даного принципу побудови є алгоритм управління РТ-32 з більш ніж 95-ма логічними операціями (Рис. 2) та таблиця 1 з 2 із 227 ймовірних, в тому числі нештатних ситуацій на базі яких розроблена матриця управлінських рішень (1).

В цілому алгоритм роботи комплексу та реакція системи управління на нестандартні ситуації потребували розробки 32 програм та підпрограм. В таблицях 1, 2 показані приклади нестандартних ситуацій та програм.

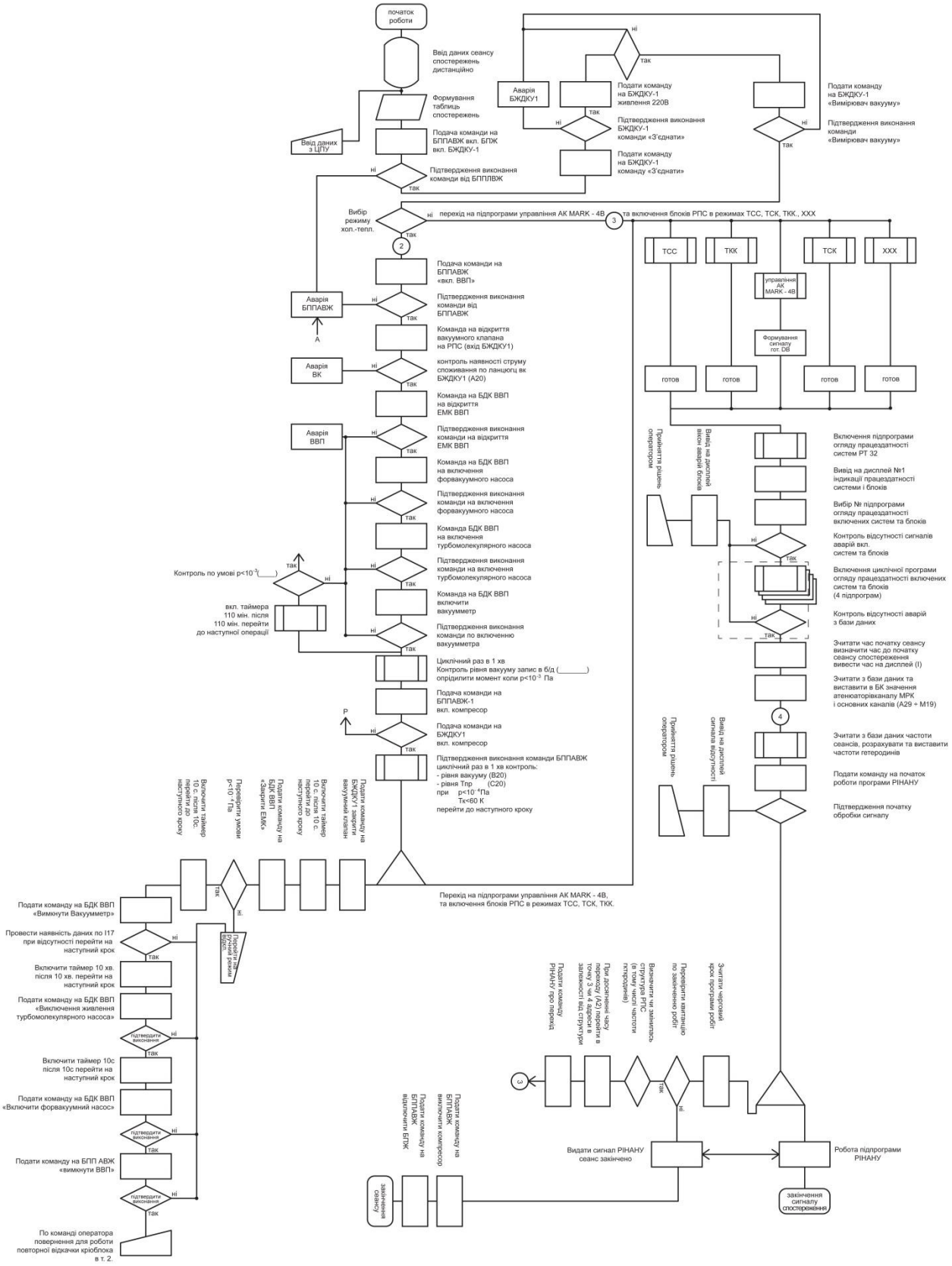


Рис.2

Алгоритм роботи РТ-32

В таблиці 1 описано 2 з 227 різних нестандартних ситуацій:

Таблиця 1

Ймовірні події та управлінські рішення про дії в нештатних (аварійних) ситуаціях

Код аварійної ситуації	Нештатна ситуація (опис)	Управлінські рішення Y_m		
		Дії індивіду-альних складових частин РТ-32	Дії штучного інтелекту	Дії оператора
011А	Через дві години після включення МКС температура в кріоблоці >70К	-	Якщо «Так» то видати сигнал аварії якщо «Ні» то продовжу-вати сеанс зв'язку	Прийняти одне з рішень: - усунути несправність в процесі підготовки до сеансу спостережень в умовах експлуатації за допомогою ЗМП; - закінчити сеанс спостережень з наступним виявленням причин несправності та усуненням їх в умовах експлуатації або на підприємстві-виробнику.
011В	Немає позитивної динаміки зміни температури	-	Якщо «Так» то видати сигнал аварії якщо «Ні» то продовжу-вати сеанс зв'язку	Прийняти одне з рішень: - усунути несправність в процесі підготовки до сеансу спостережень в умовах експлуатації за допомогою ЗМП; - продовжити сеанс спостережень, очікуючи доки аварія не зникне (температура в кріоблоці стане < 60К), або програма не видасть код аварії.

Таблиця 2

Приклад переліку програм (підпрограм) СПЗ СКіУ РТ-32

№ п/п	Назва програми (підпрограми)	Розташу-вання	Функція	Статус в ієрархічній структурі
1	Програма контролю та управління технічним станом системи контролю і управління РТ-32 (ПКУ ТС СКіУ РТ-32)	ЦПУ	Приймати завдання на проведення сеансу спостережень через локальну мережу, або мережу Internet, керувати сеансом спостереження згідно з прийнятими завданнями, проводити диспетчеризацію процесів управління та контролю, ведення та зберігання протоколів стану контрольованих систем та даних МРК	І рівень запускається оператором у відповідності з описом програмного забезпечення
1.1	Програма процесу сеансу спостережень (ППСС)	ЦПУ	Координує процес обрання структури РПС С-, К-, задіяної в сеансі спостережень, процес послідовності включення вузлів та блоків РПС С-,К-, процес обміну даними з програмою СК АС MARK-4B	ІІ рівень запускається автоматично програмою ПКУ ТС СКіУ РТ-32

ВИСНОВКИ

Дослідна експлуатація РТ-32 показала дієвість побудови системи управління.

Відкритість системи, можливість введення додаткових систем контролю технічного стану, можливість введення додаткових функцій управління дають необмежені можливості подальшої модернізації та поліпшення параметрів інструмента.

Багатоцільове призначення РТ-32 в значній мірі забезпечується гнучкою системою управління.

Можливість приймання план-завдань від віддаленого абонента та в автоматичному режимі проведення сеансу зв'язку розширює ареал спеціалістів, що можуть використовувати можливості РТ-32 в своїх дослідженнях.

Система управління дає можливість виконання поставлених задач за часткового відхилення параметрів систем від номіналу (збої в системах охолодження, відхилень первинного та вторинного енергозабезпечення та інші). Передбачена робота комплексу протягом не менше 20 хвилин при повній відсутності первинного енергозабезпечення.

З метою економії ресурсу блоків, систем та підсистем передбачено можливість задіяння в сеансах зв`язку (спостережень) тільки необхідних для даного сеансу складових частин.

Такі заходи дають можливість підняти вірогідність одержання достовірної інформації, особливо під час приймання телеметричної інформації від космічних об'єктів штучного походження, ресурс яких в деяких випадках не дозволяє повторне проведення таких сеансів.

СПИСОК ЛИТЕРАТУРИ

1. *Е.М. Глушеченко, О.М.Пилипенко, І.К.Сундучков, В.В.Чміль, П.О.Яцик* Створення сучасної наземної радіоастрономічної інфраструктури на базі антенних комплексів в м. Золочів.

Збірник наукових праць конференції «Радіолокація. Супутникова навігація. Радіомоніторинг 24-26 жовтня 2017 р., Україна, м. Харків с. 145-147.

2. *С.Б.Данилевич, С.С.Колєсніков, Ю.А.Пальчук* Застосування імітаційного моделювання при атестації методик контролю і випробувань.

Вимірювальна техніка 2011 №7 с 70-73.

3. *Г.С.Ратушняк, О.І.Ободянська* Моделювання надійності систем газопостачання на основі лінгвістичної інформації

Сучасні технології, матеріали і конструкції в будівництві. 2009, №1, с.97-103.

4. *Ю.І.Матюшкін, Б.І.Мокін, А.П.Ротштейн,* SoftComputing: ідентифікація закономірностей нечіткими базами знань.

Вінниця: УНІВЕРСУМ-Вінниця, 2002, с.145

5. *А.П.Ротштейн* Інтелектуальні технології ідентифікації. Нечіткі множини, генетичні алгоритми, нейронні мережі.

Вінниця: УНІВЕРСУМ-Вінниця, 1999, с.320

6. *К.С.Сундучков, А.Л.Голік, С.Є.Волков, О.С.Ящук, І.К.Сундучков.* Метод розрахунку параметрів радіоканалу безпровідного доступу до мобільних терміналів в міліметровому діапазоні.

ISS. Вісті вузлів. Радіоелектроніка 2014, №8 с.1-8

7. *О.М.Пилипенко, І.К.Сундучков, В.В.Чміль, В.М.Чміль, П.О.Яцик*

Радіометричний приймальний комплекс і шляхи зниження погрішності, що вноситься ним, в радіометричні виміри.

Технологія і конструювання в електронній апаратурі, Одеса №5-6, 2015 р. с.14-21.

д.т.н. Андрощук О. С.(НАДПСУ)
к.техн. н. Кльоц Ю. П.(ХНУ)
к.техн. н. Тітова В. Ю. (ХНУ)

ЗАСТОСУВАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗЛОЧИНІВ

Характерною особливістю теперішнього часу є прискорений темп розвитку нових інформаційно-телекомунікаційних технологій та їх широке проникнення практично у всі сфери людської діяльності. Це активно використовується різного роду зловмисниками, несанкціонований вплив яких на інформаційний ресурс автоматизованих інформаційних систем (далі – АІС) призводить до порушення цілісності, конфіденційності або доступності інформації, що зберігається, обробляється і передається, і в результаті – до порушення надійності функціонування АІС в цілому по її прямому призначенню. Виявлення кібератак та наслідків їх здійснення покладається на адміністраторів захисту інформації та на підрозділи кіберзахисту (кіберполіції) тощо. У цьому напряму усе більшого значення набуває кримінальний аналіз.

У процесі кримінального аналізу забезпечується цілеспрямований пошук, виявлення, фіксація, отримання, систематизація, аналіз та оцінка кримінальної інформації, її представлення (візуалізація), передача та реалізація.Найбільш поширеним аналітичним інструментом, що використовується у повсякденній роботі органів Національної поліції, Служби безпеки та Державної прикордонної служби України, є Microsoft Office (Excel), хоча в деяких департаментах застосовується аналітичне програмне забезпечення (зокрема, i2 Analyst’s Notebook, E-Gismaps, ArcGIS тощо).

Кримінальний аналіз кіберзлочинів в органах правоохоронної діяльності є складним, недостатньо розробленим напрямом в теоретичному плані. Дослідження проблеми, а також узагальнення передового досвіду в даній сфері, наприклад, у масштабі Державної прикордонної служби України ведуться не в достатній мірі, як наслідок, до цього часу не існує адекватних розроблених та апробованих методів кримінальногоаналізу – у результаті відсутнє адекватне програмне забезпечення.

Наукова робота присвячена вирішенню науково-теоретичного завдання – розробці математичних методів кримінального аналізу кіберзлочинів.Значна частина наукових досліджень, що стосується кримінального аналізу використовує ймовірнісно-статистичні методи. Це пов’язано з тим, що сучасні аналітики у більшості випадків навчились аналізувати статистичні дані. При застосуванні цієї групи методів, для досягнення точних результатів, висуваються сурові вимоги до вихідних даних. Це стосується таких показників вихідних даних як: обсяг (кількість), достовірність, однорідність тощо.Досвід дослідження застосування цих методів для кримінального аналізу у правоохоронній діяльності свідчить, що вони не є у більшості випадків адекватними тому, що, як раз більшість вихідних даних не відповідає заявленим вимогам. Зазвичай, даних тут недостатньо та більшість з них носить нечіткій та неоднорідний характер тощо.Визначення ступенязлочину проводиться з використанням, як правило якісних методів.

Авторами запропоновано для здійснення кримінального аналізу застосовувати методи штучного інтелекту. Гіпотеза дослідження – методи нечіткого логічного виводу є адекватними та достатньо ефективними для кримінального аналізу кіберзлочинів. Поряд з дослідженням та можливим удосконаленням методу нечіткого логічного виводу будуть досліджуватись методи експертного оцінювання, з точку зору уточнення результатів кримінального аналізу. У цьому плані будуть розглянуті підходи щодо підбору експертів, підвищення їх фаху та залучення до кримінального аналізу (експертизи).

Розробка зазначених методів дозволить розробите відповідне програмне забезпечення, що, у свою чергу, повинне підвищити якість кримінального аналізу кіберзлочинів правоохоронними органами.

Андрушко М.В., Аркушенко П.Л.
к.т.н. ДНДІ ВС ОВТ
Андрушко А.М. (ЧНТУ “Чернігівська політехніка”0

АНАЛІЗ ЗАВДАНЬ РАДІОТЕЛЕМЕТРИЧНИХ СИСТЕМ ПРИ ПРОВЕДЕННІ ВИПРОБУВАНЬ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

Міністерство оборони України щороку планує та реалізує заходи щодо переоснащення Збройних Сил України сучасними та модернізованими зразками ракетно-артилерійського озброєння. Кожен з нових зразків ракетно-артилерійського озброєння під час випробувань потребує виважених та науково-обґрунтованих технічних рішень з вибору вимірюваних параметрів, встановлення вимог до точності вимірювань, обрання методів і засобів вимірювань. Для якісного проведення випробувань існує необхідність застосовувати інформаційно-вимірювальні системи, які дозволяли б розширювати функціональні можливості випробувального обладнання шляхом додавання, зміни набору вимірюваних параметрів та характеризувалися нескладністю конструктивної реалізації, прийнятною вартістю, габаритами і вагою, незначною трудомісткістю.

Питання необхідності створення універсальної інформаційно-вимірювальної радіотелеметричної системи для забезпечення проведення випробувань озброєння та військової техніки (ОВТ) відповідно до сьогоденних запитів викликано стрімким розвитком технічних засобів вимірювання та обміну даними всередині системи та між іншими елементами для якісної оцінки характеристик та параметрів роботи систем об’єкту випробувань.

Метою статті є аналіз завдань існуючих та перспективних інформаційно-вимірювальних радіотелеметричних систем для удосконалення процесу організації проведення випробувань дослідних зразків ОВТ, в тому числі ракетно-артилерійського озброєння.

Однією з важливих задач обробки телеметричної інформації випробувальних об’єктів є оперативна оцінка його стану при їх випробуваннях на заводах-виробниках та полігонах. Від ефективності та безпомилковості оперативної оцінки стану об’єкту досліджень залежить якісне виконання завдань випробувального процесу.

Складність оцінки полягає в тому, що:

телеметрична інформація є різнорідною за фізичною природою і динамічними характеристиками;

в процесі вимірювання можуть виникнути зовнішні фактори, які впливають на точність та достовірність вимірювальних величин;

існують жорсткі часові обмеження на отримання результатів аналізу;

існує безліч ситуацій, в яких комбінація відхилень контрольованих параметрів від штатних значень дає певну “нечіткість” в прийняті рішення про оцінку виниклої ситуації.

Тому, для якісної та ефективної оцінки процесу випробувань дослідних зразків є необхідна потреба застосування інформаційно-вимірювальних систем (ІВС) заснованих на сучасних методах ідентифікації стану багато параметричної системи і підтримки прийняття управлінських рішень.

Радіотелеметрична система в своєму складі має:

бортові (системи збору, комутації, реєстрації і передачі інформації) та наземні засоби (вимірювальні пункти, мобільні програмно-апаратні комплекси обробки і аналізу інформації).

Різноманітні форми функціонування і взаємодії систем об’єкту випробувань, великі потоки різної вимірювальної інформації, необхідність застосування досить складного математичного апарата для її обробки й аналізу – усе це приводить до того, що проведення випробувань сучасних зразків ОВТ в необхідний термін без широкого застосування засобів

реєстрації і обробки на базі сучасних носіїв інформації та ПЕОМ практично не представляється можливим. В результаті обробки телеметричних повідомлень формується оцінка телеметричного параметра, що зображає значення параметра або функціональну залежність його від часу чи іншого чинника. Оцінка відрізняється від істинного значення наявністю внесених похибок. В доповіді проаналізовані можливості радіотелеметричних систем та засобів траєкторних вимірювань, визначені їх основні переваги і особливості експлуатації. Важливою перевагою радіотелеметричних систем є можливість по радіоканалу зв'язку отримувати інформацію не тільки про параметри руху дослідного зразка ОВТ, але й про стан систем та агрегатів об'єкта досліджень, а також про роботу різної апаратури та інформацію про параметри навколишнього середовища.

На основі отриманих оцінок телеметричних параметрів здійснюється аналіз результатів вимірів, визначається стан систем випробувального об'єкту та приведення результатів обробки до виду, зручного та подальшого використання для прийняття рішення по управлінню процесом випробування.

Інформаційно-вимірювальні радіотелеметричні системи вирішують наступні завдання:

збір, перетворення і передача вимірювальної аналогової та цифрової інформації про просторове положення, температурні та вібраційні режими, положення органів керування, тощо з дослідних зразків ОВТ до наземних автоматизованих комплексів обробки;

передача скороченого об'єму вимірювальної інформації з наземних автоматизованих комплексів обробки на командні пункти з метою забезпечення безперервного контролю технічного стану систем та агрегатів дослідних зразків ОВТ та своєчасного виявлення збоїв та відмов для прийняття дієвих заходів з безпеки (у тому числі застосування та введення в дію системи автоматичного припинення польоту для ракетного озброєння);

додаткова реєстрація вимірювальної інформації безпосередньо на об'єкті випробувань із збереженням її на бортовому накопичувачі;

обробка та аналіз вимірювальної інформації.

Висновок. В контексті наведеного є подальша необхідність та доцільність в розробці та впроваджені інформаційно-вимірювальної радіотелеметричної системи на комплексах ОВТ Збройних Сил України з точки зору виконуємих завдань сучасної автоматизованої інформаційної системи збору, логічної обробки і аналізу, виробки управлінських рішень та збереження інформації. Розгляд можливостей бортової складової інформаційно-вимірювальної радіотелеметричної системита відповідних наземних автоматизованих комплексів обробки телеметричної інформації показує, що вони в сучасних умовах дають дієвий імпульс в широкому використанні її для визначення технічного стану дослідного зразка ОВТ та підвищення безпеки процесу випробувань.

Список використаних джерел

1. В.В.Балабін, І.В.Замарусов, С.В.Ленков, Л.О.Рось. Інформаційні системи нового покоління, як чинник забезпечення національних інтересів. – Наука і оборона, – 2007. – с.40–45.

2. Фролов В.С. Структурно-логична схема Єдиної автоматизованої системи управління Збройних Сил України. – Наука і оборона, – 2012, № 1.

3. Основы военно-технических исследований. Теория и приложения. Система полигонных испытаний вооружения и военной техники: методологические основы. /Монография, под ред. И.Б. Чепкова. – К.: ЦНИИ ВВТ ВС Украины, 2016.

4. Сковорода-Лузин В.И. Телеметрия. Глаза и уши Главного конструктора. //М: ООО "Овердлей", 2009. – 320 с.

5. Назаров А.В. Современная телеметрия в теории и на практике. Учебный курс//СПб: Наука и Техника, 2007. – 672 с.

Андрющенко О.А. (в/ч А2533)
к.т.н. Штаненко С.С. (ВІТІ ім. Героїв Крут)

ПІДХІД ДО ПРОЕКТУВАННЯ ВІДМОВОСТІЙКИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ В БАЗИСІ ПЛІС

На сьогоднішній день розвиток засобів обчислювальної техніки диктується необхідністю вирішення складних завдань науки, техніки, економіки, оборони країни, тощо, а також створенням технологічних систем різного призначення. Очевидно, що вимоги (підвищення продуктивності, надійності та достовірності), які на даний час пред'являються до обчислювальних (мікропроцесорних) систем, які є основою побудови технологічних систем, повною мірою не можуть бути задоволені, якщо використовувати класичні принципи побудови електронно-обчислювальних машин (ЕОМ), використовуючи «жорстку» фон-неймановську або гарвардську внутрішню архітектуру [1].

Під технологічною системою будемо розуміти автоматизовану або автоматичну систему, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних [2].

Слід зазначити, що важливість завдань які вирішуються сучасними технологічними системами, з одного боку, і складність таких систем, з іншого боку, вимагають від таких систем високої не тільки продуктивності, надійності і достовірності, а й відмовостійкості (живучості), а також правильного функціонування в умовах «несприятливого впливу», а також кібератак.

Останнім часом для підвищення відмовостійкості (живучості) і, як наслідок, надійності технологічних систем, широко використовується підхід, заснований на застосуванні в якості сучасної елементної бази не універсальних процесорів з «жорсткою» архітектурою, мікроконтролерів і замовних великих інтегральних схем, а програмованих логічних інтегральних схем (ПЛІС). ПЛІС відносяться до класу спеціалізованих інтегральних схем з програмованою структурою, представляють собою реконфігуровані пристрої, здатні змінювати свою внутрішню логічну структуру при виникненні відмов, збоїв апаратного і програмного забезпечення безпосередньо в процесі функціонування, а також кібератак.

На сьогоднішній день ПЛІС представляють собою матрицю програмованих логічних елементів з *SPLD* (*Simple Programmable Logic Devices*), *CPLD* (*Complex Programmable Logic Device*), *FPGA* (*Field-Programmable Gate Array*), *FLEX* (*Flexible Logic Element Matrix*) структурами. За допомогою даних структур, застосовуючи на нижньому рівні (рівень регістрових передач) мови опису апаратури *AHDL, VHDL, Verilog*, на блочному (середньому) – технологію *System-on-Chip, SoC* (система на кристалі) і на верхньому – високорівневі мови програмування *C/C++, SystemC, Python, Java, MATLAB,* ми отримуємо можливість, використовуючи програматор і інтегроване середовище розробки (*IDE – Integrated Development Environment*), проектувати не тільки комбінаційні та послідовні цифрові пристрої, цифрові автомати Мілі та Мура, а й обчислювальні (мікропроцесорні) системи.

Однією з основних особливостей ПЛІС є можливість використання принципу паралельної обробки даних (розпаралелювання обчислень) при вирішенні широкого кола завдань, а також проектування багатопроцесорних ЕОМ, що містять велику кількість універсальних процесорів, кожний з яких може автономно виконувати програму і які під управлінням операційної системи можуть об'єднуватися для спільного вирішення однієї задачі [3].

Так, прообразом організації паралельних обчислень в багатомодульних системах, в яких модулі представляли собою елементарні машини, що володіють можливостями зберігання, переробки і транспортування даних з'явилися багатомодульні

мультитрансп'ютерні обчислювальні системи, які в подальшому сприяли появі нового напряму *System-on-Chip, SoC* реалізованого на ПЛІС [1].

Дані системи володіють внутрішньокристальною пам'яттю і вбудованими ефективними засобами сполучення, при цьому основна ідея, яка була в них закладена це мати властивість ре конфігурування, як на рівні зв'язків між модулями, так і на рівні функцій окремого модуля. Ця ідея дозволила в рамках однієї моделі (одного кристала) об'єднати різні архітектури, відповідні підмножини допустимих конфігурацій.

Крім цього, запропоновані методи і засоби організації паралельної обробки даних зв'язуються з поданням паралельних алгоритмів у вигляді, що відображають в першу чергу «внутрішній» паралелізм задач, а не структури системи, на якій відповідні програми будуть виконуватися.

Високий ступінь внутрішнього паралелізму задач дозволяє при управлінні паралельними обчисленнями підбирати не тільки структуру технічної системи до системи паралельного алгоритму, а й, навпаки, структуру алгоритму до структури системи. Зазначені властивості, з одного боку, дають реальну можливість побудови реконфігурованих обчислювальних систем і паралельних алгоритмів, а з іншого – забезпечити методологічну основу для досить універсального підходу при створенні спеціалізованих форм організації обробки даних, що базуються на часткових конфігураціях систем і алгоритмів.

Іншою важливою особливістю ПЛІС є адаптація (реконфігурація) до процесу, який виконується, тобто можливість зміни алгоритму роботи в залежності від умов, які змінюються або вимог. При цьому мається на увазі, що модифікований алгоритм (або ряд алгоритмів) у вигляді файла, який завантажується в кристал, повинен бути виготовлений заздалегідь. Завантажувальний файл є результатом процесу проектування та верифікації пристрою, апаратно реалізує заданий алгоритм.Так, на базі багатопроцесорної технології і реконфігурованих програмованих інтегральних схем, якими є ПЛІС, побудовані динамічно реконфігуровані системи (ДРС – *Dynamically Reconfigurable Systems*) – клас обчислювальних систем, здатних змінювати свою внутрішню логічну структуру безпосередньо в процесі функціонування за час, який значно менше часу виконання задач, що обчислюються, між якими відбувалася зміна структури [4].Подальший розвиток технології ДРС, на основі ПЛІС, дозволив перейти до проектування адаптивних обчислювальних пристроїв, здатних змінювати свою внутрішню структуру в залежності від функцій, що реалізуються і поставлених завдань [4].Таким чином, технологія ПЛІС на сьогоднішній день відкриває нові можливості реалізації на спеціалізованих інтегральних схемах з програмованою структурою паралельної обробки даних (розпаралелювання обчислень) з багатопроцесорною організацією обчислювальних структур, а також дистанційне перепрограмування мікросхеми. Крім цього дає можливість створювати динамічно реконфігуровані системи, що в сукупності дозволяє проектувати відмовостійкі (живучі) обчислювальні (мікропроцесорні) систем, які є основою побудови технологічних систем з можливістю адаптації як до внутрішніх, так і зовнішніх несприятливих впливів, в тому числі, а також до кібератак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Хорошевский В.Г. Архитектура вычислительных систем.: Учеб. пособие. 2-е изд., перераб. и доп. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. 520 с.

2. Закон України № 2163 VIII от 05.10.2017 Про основні засади забезпечення кібербезпеки України.

3. Vaibbhav Taraate. PLD Based Designwith VHDL RTL Design, Synthesisand Implementation, Springer Nature Singapore Pte Ltd, p. 423, 2017.

4. Филиппов А.К. Теоретические основы проектирования динамически реконфигурируемых систем обработки информации: учеб. пособие / А. К. Филиппов; Владим. гос. университет. – Владимир: Изд-во Владим. гос. университета, 2009. − 119 с.

д.ф. Бабарика А.О. (НАДПСУ)
д.т.н. Катеринчук І.С. (НАДПСУ)
д.т.н. Рачок Р.В. (НАДПСУ)

АНАЛІЗ ОСНОВНИХ ПЕРЕВАГ ВИКОРИСТАННЯ „ХМАРНИХ ТЕХНОЛОГІЙ” ПРИ ПОБУДОВІ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Актуальність. Системи відеоспостереження є одним із основних компонентів комплексних систем безпеки об’єктів. Основною функцією систем відеоспостереження є ведення спостереження за визначеними об’єктами.

Постановка задачі. Такі явища як загроза тероризму, транскордонна злочинність, активізація розвідувальної діяльності ряду держав тощо, призвели до підвищення попиту на технології суспільної безпеки. Це, у свою чергу, спонукало комерційні компанії та уряди країн до розгортання великих систем відеоспостереження. Для прикладу, метро в м. Лондон та аеропорт Хітроу мають понад 5000 камер кожна. Для обробки цього великого обсягу інформації такі питання, як масштабованість та зручність використання (як потрібно надавати інформацію потрібним людям у потрібний час) стають дуже важливими.

Основні положення. Розвиток „хмарних технологій”обумовив появу нової парадигми, яка окреслює „четверте покоління” систем відеоспостереження, та характеризується появою такого поняття як „Відеоспостереження як послуга” (VSaaS). До переваг „хмарного підходу” при побудові систем відеоспостереження можна віднести:

1. Простота розгортання системи. При розгортанні „хмарних ” систем, необхідно лише встановити камери відеоспостереження та організувати доступ до мереже передачі даних.
2. Технічна підтримка розгорнутої системи. Традиційні системи вимагають значних затрат людської праці з боку кваліфікованих спеціалістів, через необхідність постійного моніторингу стану розгорнутої системи, оновлення програмного забезпечення тощо. При використанні „хмарних систем”, технічну підтримку забезпечує постачальник послуги VSaaS.
3. Фінансові затрати. Традиційні системи потребують значних фінансових затрат на закупку обладнання та на утримання фахівців служби технічної підтримки. Модель VSaaS передбачає затрати на закупку камер відеоспостереження та поточні витрати на оренду телекомунікаційних каналів і послуги постачальника VSaaS.
4. Гнучкість системи. Збереження даних в традиційних системах, зазвичай, організовано з використанням сховищ, які знаходяться безпосередньо на об'єкті відеоспостереження. Хмарні системи дозволяють зберігати інформацію як на локальних носіях так і в „хмарному” сховищі.
5. Можливість розширення системи. Традиційні системи відеоспостереження можуть працювати як з аналоговими так і з IP камерами відеоспостереження. Хмарні системи, зазвичай, працюють з IP камерами відеоспостереження.
6. Безпека. Для забезпечення віддаленого доступу до відеоінформації традиційних системах відеоспостереження необхідна організація ряду заходів з метою недопущення витоку корпоративної інформації чи виникнення передумов до втручання зловмисників у роботу інформаційної системи. Безпека у хмарних системах відеоспостереження організовується централізовано з використанням технологій віртуалізації як каналів передачі інформації так і програмного забезпечення.

Висновок. Відеоспостереження як послуга (VSaaS) було одним із перших напрямків застосування хмарних технологій, оскільки має переваги у вартості, простоті впровадження, обслуговування, використання, масштабування та високому рівні безпеки. Тому, актуальним завданням є дослідження ефективності використання вказаних підходів у побудові відомчих систем відеоспостереження.

Баканов В.С. (ВІТІ)
к.т.н. Хусаінов П.В. (ВІТІ)

НАВЧАННЯ КЛАСИФІКАТОРА СИСТЕМИ ОБРОБЛЕННЯ ПОДІЙ ДЛЯ ОПЕРАТИВНОГО РЕАГУВАННЯ НА КІБЕРАТАКИ (КІБЕРІНЦИДЕНТИ)

Організаційно-технічна модель кібербезпеки, яка введена Законом України "Про основні засади забезпечення кібербезпеки України", визначає, зокрема, необхідність забезпечення комплексу заходів, сил і засобів для оперативного (кризового) реагування на кібератаки (кіберінциденти) у межах компетенції того чи іншого органу кіберзахисту. Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Сукупність узгоджено функціонуючих засобів технічного, програмного та математичного забезпечення організаційних процесів оперативного (кризового) реагування на кібератаки (кіберінциденти) розглядається у контексті системи класу *SecurityInformationandEventManagement* (далі – *SIEM*-система) або система оброблення подій. Розглядаючи цілі кібератаки як змістовне іменування класів кібератак, а кіберінцидент як множину ознак можливої (потенційної) кібератаки функціонування *SIEM*-системи можна представити у формі агрегатного елементу типу "класифікатор".

Класифікатор *SIEM*-системи визначає приналежність сукупності ознак тому чи іншому образу класу кібератаки (кіберінциденту) за принципами розпізнавальної системи. Сукупність ознак називається сигналом. Він формується на підставі відомостей про події функціонування об'єкту кіберзахисту. Образ – підмножина об'єктів, які мають загальні суттєвими властивостями. Об'єкти, які відповідають одному образу можуть відрізнятися другорядними несуттєвими властивостями. Образ є абстрактним поняттям, яке відповідає деякій підмножині об'єктів. При розпізнанні образів прагнуть до того, щоб рішення для всіх об'єктів одного образа були однаковими. Початкові дані розпізнавання образів можуть бути представлені у формі результату спостереження, безпосереднього вимірювання чи бути їх функціями. Вміст сигналу є підставою для прийняття рішення про приналежність об'єкта до одного з заданих класів шляхом встановлення відповідності тобто доведення їх ідентичності, аналогічності, подібності, збігання і т. ін.

Викладення гіпотез про те, як сукупність ознак об'єкта залежить від тих суттєвих характеристик об'єкта відносно яких необхідно прийняти рішення називається моделлю розпізнавання. Такі залежності не є функціональними, тому певній характеристиці об'єкта розпізнавання може відповідати множина можливих значень сигналів, які спостерігалися у минулому з вказівкою приналежності кожного з них певному класу (навчальна вибірка). Навчання класифікатора полягає у формуванні його моделі розпізнавання на основі навчальної вибірки. При цьому потужність вищезгаданої множини сигналів залежить від ступеня невизначеності, у широкому сенсі, складної технічної системи обраної в якості об'єкта управління.

Висновки. Комунікаційній або технологічній системі об'єкта кіберзахисту, яка контролюється засобами *SIEM*-системипритаманна висока ступінь складності та, очевидно, невизначеності. Це обумовлює необхідність навчання класифікатора на етапі підготовки до експлуатації*SIEM*-системи на основі якомога повної множини сигналів ознак кібератак (кіберінцидентів). В якості методичного базису моделювання навчальної вибірки кібератак (кіберінцидентів) на об'єкт кіберзахисту пропонується використовувати MITREATT&CK.

Безносенко С.Ю. (ВІТІ)
Коротченко Л.А. (ВІТІ)
Атаманенко М.В. (ВІТІ)
Гуржій І.А.(ВІТІ)

ПЕРСПЕКТИВИ РОЗВИТКУ МЕТРОЛОГІЧНОГО ОБСЛУГОВУВАННЯ У ВІЙСЬКАХ ЗВЯЗКУ

Головною метою розвитку системи зв'язку Збройних сил України є створення єдиного інформаційно-телекомунікаційного середовища на основі впровадження сучасних інформаційних систем та автоматизованих систем управління, протоколів обміну інформацією, комплексів, систем та засобів зв'язку спеціального призначення, що дасть можливість забезпечити обмін усіма видами інформації між органами й пунктами управління (всіх ланок) з відповідною пропускною спроможністю, достовірністю та надійністю.

Вивчення досвіду армій провідних країн світу при формуванніта розвитку засобівзв'язку показав, що сучасні системи зв'язку відрізняються високою ефективністю та якістю за рахунок використання новітніх досягнень інформаційних технологій, штучного інтелектута робототехніки, що дозволяє зробити висновки, що застосування штучного інтелекту та штучних нейронних мереж є однією з найбільш перспективних та популярних сьогодні у всіх сферах, і збройні сили не є виключенням.

Впровадження стандартів та процедур НАТО в процеси організації та забезпечення зв'язку, захисту інформації та кібербезпеки в інформаційно-телекомунікаційних системах за останні роки зазнали певного розвитку, заміна застарілих зразків техніки зв'язку (ТЗ) новими, перспективними зразками, а саме новітніми засобами радіозв'язку, радіорелейного, тропосферного і супутникового зв'язку, засобами волоконно-оптичного зв'язку, цифрового телекомунікаційного обладнання, сучасними засобами та технологіями передачі інформації, даних дало можливість успішного виконання ними завдань за призначенням.

Для управління експлуатацією ТЗ необхідна інформація про технічний стан їх підсистем і елементів, а також про фактори зовнішнього середовища, які впливають на експлуатаційні процеси. Вимоги до обсягу, достовірності і оперативності подання цієї інформації постійно зростають, що пов'язано з істотним підвищенням складності ТЗ і глибини процесів, які в них відбуваються, необхідністю підтримання високого рівня її бойової готовності протягом тривалого терміну експлуатації та досягнення найвищої ефективності, все більш широким використанням систем вимірювання та контролю і збереженням безпосередньої участі людини у вирішенні завдань експлуатації [1]. Основним джерелом інформації про стан підсистем і елементів ТЗ служить вимірювальний контроль параметрів і характеристик [2], що проводиться під час їх метрологічного обслуговування (МОб).

Враховуючи викладене можна стверджувати, що ТЗ ЗС України як об'єкт МОб має ряд особливостей, найважливішими з яких є:

– складність та ієрархічність структури, наявність великої кількості підсистем і елементів;

– різноманітність і складність виконуваних функцій підсистем і елементів;

– високий ступінь надійності агрегатів і підсистем, стійкість до зовнішніх впливів;

– наявність електронних, електричних та механічних елементів у складі ТЗ;

– різноманітність і складність протікаючих фізичних, енергетичних та інформаційних процесів;

– великий обсяг інформації, необхідної для управління ТЗ з метою досягнення її високої ефективності і бойової готовності.

Отже, відповідальні завдання, що вирішуються ТЗ ЗС України, вимагають високого ступеня достовірності та оперативності контролю ТС їх підсистем, точності вимірювання значень параметрів при жорстких обмеженнях за часом проведення вимірювань. Ці завдання

вирішуються системою МОб (СМОб) ТЗ ЗС України, технічною основою цієї системи є засобів вимірювальної техніки (ЗВТ).

Під системою будемо розуміти сукупність деяких об'єктів довільної природи, зазначених властивостей об'єктів і відносин між ними [3]:

$$F = [\lambda, \sum(\lambda), \tau(\lambda)],$$

де λ – множина деяких об'єктів; $\sum(\lambda)$ – множина зазначених властивостей об'єктів λ;$\tau(\lambda)$ – множина відносин між об'єктами множини λ.

Виходячи з цього, визначити СМОб ТЗ ЗС України – означає задати множини об'єктів, що входять до неї, виділити коло властивостей цих об'єктів і встановити характер відносин між ними. СМОбТЗ ЗС України як основний компонент повинна містити: об'єкт МОб, активні засоби МОб та органи управління МОб. Стосовно ТЗ, об'єктом МОб є контрольована частина її підсистем і елементів. В якості активних засобів МОб використовуються ЗВТ, засоби їх МОб та ресурси, що виділяються на МОб ТЗ. Управління МОб ТЗ здійснюється відповідними органами на підставі організаційних вказівок вищих ланок управління за допомогою технічних засобів.

Для вдосконалення СМОб ТЗ ЗС України необхідно виявити основні протиріччя, характерні при синтезі цієї системи, та шляхи їх усунення. Протиріччя, що мають місце при синтезі будь-якої системи і, зокрема, для СМОб ВТЗ ЗС України – це протиріччя між необхідністю ефективної та економічної реалізації заданої сукупності функцій і складністю відповідної структури, призначеної для їх реалізації. Вони зумовлюють взаємозалежність і суперечливий характер показників якості систем. Конкретні технологічні можливості, обмеження на енергетичні, матеріальні і трудові ресурси загострюють зазначені протиріччя.

Основними протиріччями при створенні СМОб ТЗ ЗС України є:

1. Протиріччя між функціональною повнотою і вимогами мінімізації структури системи, яке проявляється у формі протиріччя між кількістю типів модулів, необхідних для реалізації заданих функцій, і їх загальною кількістю.

2. Протиріччя між якістю використовуваних ЗВТ при МОб ТЗ та їх вартістю.

3. Протиріччя між вимогою мінімального часу зниження бойової готовності ТЗ при проведенні МОб ТЗ і обсягом та достовірністю інформації про стан ТЗ, необхідної для ефективного управління МОб.

4. Протиріччя між постійним зростанням складності МОб ТЗ і кваліфікацією обслуговуючого персоналу. Ці протиріччя вирішуються автоматизацією операцій МОб та впровадженням оптимальних алгоритмів управління МОб ТЗ.

Проведений аналіз існуючої ТЗ ЗС України та динаміки її розвитку, а також основних протиріч, що мають місце при синтезі СМОб ТЗ ЗС України, дозволяє окреслити основні напрями її удосконалення, а саме:

підвищення точності вимірювальних операцій при МОб ТЗ, яке може бути досягнуто впровадженням як високоточних ЗВТ;

підвищення достовірності одержуваної в процесі МОб ТЗ вимірювальної інформації;

підвищення оперативності проведення основних заходів МОб ТЗ, отримання інформації та доведення керуючих впливів. Оперативність проведення МОб ТЗ визначається його тривалістю та періодичністю, при цьому зменшення тривалості і збільшення періодичності МОб не повинно призводити до погіршення його якості;

забезпечення необхідної повноти МОб ТЗ, що дозволяє підтримувати необхідний рівень якості МОб, точного дотримання вимог нормативних документів, організації контролю за проведенням МОб ТЗ;

зменшення енергетичних, часових і матеріальних витрат на операції МОб ТЗ і на організацію управління МОб ТЗ.

Таким чином, напрями удосконалення СМОб ТЗ ЗС України дійсно мають чимало протиріч, які можуть бути в значній мірі усунуті на основі оптимізації за обраним критерієм з урахуванням всіх обмежень, що виникають в процесі функціонування цієї системи.

к.пед.н. Бірюков П.В.(ВІТІ ім. Героїв Крут)
Селюк В.М. (ВІТІ ім. Героїв Крут)

ТАКТИКА ЗАСТОСУВАННЯ УДАРНИХ БЕЗПІЛОТНИКІВ ПІД ЧАС ЗБРОЙНИХ КОНФЛІКТІВ

Актуальність. За останні 20 років XXI сторіччя безпілотники стали невід'ємною частиною війни. Уявлення про те, як виглядає бойовий безпілотник і як він повинен застосовуватись, також змінилося, оскільки безпілотникі і боєприпаси до них стали різноманітнішими. Ударні безпілотні літальні апарати (далі – БпЛА) до останніх років використовувалися (перш за все США) для нанесення точкових ударів по військовим об'єктам в Іраку, Афганістані та Сирії, ліквідації ватажків терористичних організацій "Аль-Каїди" та "Ісламської держави". Крім того, далекобійні ударні БпЛА США підтримували війська в Афганістані, де було важко забезпечити базування великої кількості "традиційних" літаків. Більшість функцій на полі бою, як і раніше, виконувала пілотована авіація: винищувачі, бомбардувальники, штурмовики та вертольоти. Для України, яка вже сім років потерпає від російської агресії, з військової точки зору особливий інтерес становить досвід застосування безпілотників у збройному конфлікті, особливо класу ударно-розвідувальних та ударних дронів, адже такі повітряні операції складають елементи дистанційних війн майбутнього.

Постановка задачі. Вивчення досвіду запровадження розгляд та аналіз застосування безпілотників у збройних конфліктах сьогодення, визначення їх ролі у бойових умовах.

Основні положення. Аналіз останніх війн та збройних конфліктів XXI століття (Сирія, Ірак, Нагорний Карабах, Схід України) свідчить про зростаючу роль розвідувально-ударних та ударних БпЛА. Під час російської операції в Сирії станом на весну 2016 року було розгорнуте угруповання з 70 російських БпЛА (переважно безпілотні авіаційні комплекси "Орлан 10" і "Форпост"), що становило близько 30 комплексів. Найбільш масовими завданнями для російських безпілотних авіаційних комплексів (далі – БпАК) в Сирії була розвідка цілей для ударів авіації, оцінка шкоди, коригування артилерійського вогню сирійської артилерії. Виконувалися ними й інші завдання, від аерофотозйомки і 3D картографування місцевості до супроводу гуманітарних конвоїв та пошуково-рятувальних операцій. Більш важкі комплекси "Форпост", оснащені потужною оптикою, в переважній більшості випадків використовувалися для спостереження і контролю ударів по найбільш пріоритетних цілях. Під час військових дій на території сирійської провінції Ідліб у лютому - березні 2020 року турецька армія застосувала нову концепцію повітряно-наземного бою, за якою наступ військ забезпечувався масованою атакою БпЛА типу "Bayraktar TB2" і "AnkaS", що несли високоточні боєприпаси. Застосування БпЛА відбувалося за підтримки систем радіоелектронної боротьби (далі -РЕБ) та сучасних засобів ураження (ствольної та реактивної артилерії). Нова концепція повітряно-наземного бою передбачала використання БпЛА замість класичної авіації й вертольотів.Тактика застосування дронів проти американських Збройних Сил може бути стратегією іранського Корпусу стражей ісламської революції, що спеціалізується на нетрадиційних способах ведення війни, координуючи свої дії з іракськими збройними угрупуваннями. Проте, вище військове керівництво США знищило іранського генерала Касема Сулеймані 3 січня 2020 року також за допомогою безпілотника за його зв'язок з терористами, що здійснили напад на американські авіабази в Іраку. Війна між Азербайджаном та Вірменією стала першою, в якій основні завдання, що вирішувалися звичайною авіацією: розвідка, цілевказування, нанесення ударів по техніці, позиціях і резервам – виконали БпЛА. В основному це стало можливим завдяки використанню розвідувально-ударних БпЛА виробництва Туреччини ("Bayraktar TB2") та малих одноразових ударних БпЛА виробництва Ізраїлю ("Harop", "SkyStriker", "Orbiter 1K").

Військовий конфлікт в Нагорному Карабасі показав, що крім класичних БпЛА, все частіше стали застосовуватись так звані баражуючі безпілотні боєприпаси. По суті це

альтернатива розвідувально-ударним БпЛА, але більш простий і дешевий засіб боротьби, що поєднує функції розвідки, спостереження та ураження. З їх допомогою максимально скорочується цикл "виявлення-ураження" і ефективно вирішуються завдання, що вимагають оперативних дій в мінливій бойовій обстановці, яка властива гібридним війнам і локальним збройним конфліктам. Баражуючі безпілотні боєприпаси є більш високоточною і вибірковою зброєю, ніж, наприклад, артилерійські системи. Їх використання дозволяє знизити супутні втрати, в тому числі серед цивільного населення та здійснити вибіркове вогневе ураження тільки певних елементів об'єктів противника та зберегти недоторканість важливих об'єктів інфраструктури. Активні бойові дії на сході України, зумовлені російською агресією, продемонстрували потребу не лише у застосуванні на полі бою БпЛА для корегування артилерії та збору розвідувальних даних, а й ударних, здатних вражати броньовані та важкодоступні цілі противника. Якщо до 2018 року основу безпілотної авіації Збройних Сил України складали розвідувальні БпЛА як вітчизняного, так і іноземного виробництва, то починаючи з 2018 року ситуація почала поступово змінюватися. Українська армія отримала перші ударні безпілотні авіаційні комплекси турецького виробництва, а вітчизняні виробники почали пропонувати власні рішення щодо виробництва ударних БпЛА. Тому, є необхідність визначити чинники, які впливають на використання ударних БпЛА у збройних конфліктах.Бойові дії в останніх локальних війнах і збройних конфліктах, що можна віднести і до зони проведення операції Об'єднаних Сил (далі – ООС), характеризувалися відсутністю чітко позначеної лінії бойового зіткнення сторін, високим рівнем мобільності та диверсійно-терористичним характером дій противника з порушенням норм міжнародного гуманітарного права та певними обмеженнями щодо застосування авіації, артилерійських систем та реактивних систем залпового вогню у місцях з великою скупченістю цивільного населення та знаходження небезпечних об'єктів. Це вимагає покращення ситуаційної обізнаності командувачів усіх рівнів та їх штабів під час планування й ведення операцій (бойових дій). БпЛА дедалі активніше використовуються для розвідки противника, наведення й координації вогню артилерії, здійснення автономних високоточних атак. Для цього необхідно мати відповідний комплект БпЛА різних класів в залежності від виду операції (бойових дій) та конкретних умов обстановки.Серед перспективних українських розробок, які проходять випробування і незабаром мають поступити на озброєння армії, ударний безпілотний комплекс ST35 "Тихий грім" НВП "Атлон Авіа" та "PD2" ударна версія відомого розвідника "People Drone PD1", який розробила компанія ТОВ "Укрспецсистемс". Апарат спочатку створювали для ведення розвідки, проте у 2018 році йому додали нових опцій, що робить його ударним. Результатом співпраці з турецькою компанією BaykarDefence має стати ударний БПлА Akincі з українськими двигунами AI – 450 потужністю 900 – 950 к.с. (розробник – ДП «Івченко-Прогрес», Запоріжжя). БпАК Raybird-3/ACS-3 української авіаційної виробничої компанії «Скаетон» здатний виконувати задачі розвідки цілодобово в будь-яку пору року за умов застосування РЕБ противника. Слід відзначити, що значна частина вітчизняних ударних БпЛА на теперішній час перебуває на стадії розробки та заводських випробувань.

Висновок. У ході проведення ООС в умовах заборони застосування авіації використання ударних БпЛА є доцільним та критично необхідним. При цьому, слід звернути увагу на такий клас ударних БпЛА, як баражуючий боєприпас, який є альтернативою розвідувально-ударним БпЛА, але більш простий і дешевий засіб боротьби, що поєднує функції розвідки, спостереження та ураження. З метою повної реалізації спроможностей пілотованої (розвідувальної, бомбардувальної, штурмової, винищувальної) та безпілотної авіації, організації ефективної взаємодії між силами та засобами протиповітряної оборони Сухопутних військ, ракетними військами та артилерією, військовими частинами (підрозділами) радіоелектронної боротьби, ВМС, Десантно-штурмових військ, Сил спеціальних операцій, іншими складовими сил оборони доцільно планувати повітряну операцію як складову ООС.

к.т.н. Бовда Е.М. (ВІТІ)
Білявський Г.О. (ВІТІ)

ПІДСИСТЕМА ПРОПУСКУ НА ОБ'ЄКТИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Актуальність теми. В Збройних Силах України активно використовуються різні системи контролю управлінням доступом на військові об'єкти. Враховуючи те, що таких об'єктів багатота кожен з них має свою специфіку, а сил та засобів для їх охорони та контролю постійно не вистачає, то потрібно для їх охорони створювати все нові та нові системи контролю та управлінням доступом. В самих військових частинах зберігається багато службової інформації та зброї. Тому проникнення в військову частину або на об'єкт може призвести до викрадення інформації та матеріальних засобів, що може спричинити значну шкоду Збройним Силам України. Для вирішення даної задачі можливе використання новітніх засобів та технологій для покращення системи контролю та управління доступом на військові об'єкти. Це призведе до підвищення рівня її безпеки та збереження інформації та матеріальних засобів в цілісному вигляді, а також підвищить швидкодію роботи системи.

В подібних системах (підсистемах) використання нейронних мереж, як альтернативного інструментарію пропуску на об'єкти військового призначення, значно підвищить ефективність та надійність. Технології створення та використання нейронних мереж постійно розвиваються і вони показують все більшу ефективність в вирішенні подібних задач.

Метою дослідження є забезпечення високого рівня безпеки та ефективності підсистеми пропуску на об'єкти військового призначення на основі використання елементів штучного інтелекту.

Для досягнення мети дослідження у роботі сформульовано наступні завдання:

- обґрунтувати необхідність автоматизації систем контролю та управління доступом.
- проаналізувати принципи забезпечення безпеки.
- розробити програмний модуль автентифікації та авторизації користувача.

Виклад основного матеріалу.Головним завданням даної підсистеми є забезпечення високого рівня безпеки та ефективності роботи, також можливість планувати заздалегідь відвідування різних військових частин, без довгого очікування на контрольно пропускному пункті частини, яку потрібно відвідати. Це буде забезпечено за допомогою використання багато етапної ідентифікації користувача. Першим етапом буде ідентифікація за допомогою унікальної для кожного користувача карти ключа. Другим етапом буде ідентифікація за допомогою нейронної мережі, яка створена за допомогою бібліотеки Dlib, та має точність у розпізнаванні обличчя 98%, що задовольняє вимогам захисту. Для зручності використання було створено web додаток, в якому є можливість авторизуватись та відправити запит для відвідування військової частити з можливістю визначити дату та час відвідування. Бази даних реалізовані за допомогою MySQL – це зручні та надійні бази даних, в яких є все необхідне функції для реалізації даної підсистеми. Внутрішня мережа будується за допомогою технології Entranet, що забезпечить високий рівень захисту та швидкості обробки даних в мережі.

Висновки. В роботі розроблено підсистему контролю та управління доступом на військові об'єкти, в якій реалізовано основні аспекти: високий рівень захисту, зручності та швидкості обробки даних.

Для зручності використання створено web додаток для автоматизації відвідання військових частин. Також є можливості контрою переміщення особового складу по частині за допомогою відміток в базах даних. Дана підсистема реалізує унікальний підхід забезпечення принципів безпеки системи контролю та управління доступом, з урахуванням сучасних інформаційних систем.

к.т.н. Бовда Е.М. (ВІТІ)
Космінський Я. В.(ВІТІ)

ІНФОРМАЦІЙНА СИСТЕМА ОБЛІКУ ЗАХВОРЮВАНЬ ВІЙСЬКОВОСЛУЖБОВЦІВ У ВІЙСЬКОВІЙ ЧАСТИНІ

Актуальність. Враховуючи активний перехід ЗСУ на стандарти NATO, їх використання у процесі організації обліку особового складу, речового майна, озброєння та організації логістики, на сьогоднішній день актуальним є питання автоматизації рутинної роботи із великою кількістю паперової документації.Однією з головних задач для військових командирів є збереження життя та здоров'я військовослужбовців, тому з розробкою даної системи обліку захворювань військовослужбовців вся інформація про військовослужбовців буде зберігатися в електронному вигляді. Лікар зможе швидко в пошуку знайти певного військовослужбовця, який звертається до нього та вести статистику, з якими найчастішими хворобами приходять військовослужбовці і в який приблизний проміжок часу їх турбує дана хвороба. Завдяки цьому лікар може наперед знати, що краще порадити військовослужбовцям для профілактики щоб минути певну хворобу.

Мета. Автоматизація обліку захворювань військовослужбовців військової частини з генерацією звітів та будь-якої інформації щодо захворювань військовослужбовців.

Виклад основного матеріалу. Так як дана медична інформаційна система створена для ведення обліку захворювання військовослужбовців з метою надання рекомендацій в процесі лікування хворого, то система повинна мати наступні складові:

1. Персональний кабінет військовослужбовця, де в кожного з них буде медична книжка в електронному вигляді. Доступ до неї матимуть лікарі і сам військовослужбовець.
2. Результати аналізів.
3. Рецепти ліків.
4. Дистанційні консультації.

Для виконання поставленого завдання передбачається вирішення серії завдань:

- проаналізувати існуючі підходи по формалізації предметної області дослідження. Визначення обмежень, ускладнень та проблем, що не дозволяють досягнути максимальної ефективності процесу обліку захворювань військовослужбовців;
- визначення технологічних підходів в автоматизації процесу обліку захворювань військовослужбовців. Обґрунтування архітектури, структури алгоритмів роботи, веб орієнтованого застосування спрямованого на автоматизацію процесу дослідження;
- з'ясувати вибір оптимальної архітектури для інтерактивних систем;
- реалізація вибраного рішення.

Огляд сучасних рішень в реалізації інтерактивності інструментів всієї Web–системи розглянуто в рішеннях таких провідних вчених. В роботі вчених відзначається, що безумовними перевагами інтерактивної системи є:

- одностороння прив'язка даних, що дозволяє з першого погляду визначати причини змін/помилок, що істотно прискорює налагодження;
- ніякої обов'язкової прив'язки до класів, що полегшує код;
- компоненти інтерфейсу можна виразити у вигляді наборів чистих функцій.

Для реалізації поставленої практично задачі перевага віддана технологічним інтерактивним підходам.

Висновок. ЗС України потребують використання нових технологій, для того щоб покращити не лише умови праці, але й функціонування медичних пунктів військових частин.Сучасні технології дозволяють забезпечити більш високий рівень безпеки, автоматизацію робочих процесів та поліпшити ведення обліку та складання звітів стосовно захворюваності військовослужбовців. Очікується, що запропонований програмний модуль дозволить підвищити ефективність процесу обліку захворюваності у військових частинах.

к.т.н. Бовда Е.М. (ВІТІ)
Бовда В.Е. (ВІТІ)
Кузьменко Д.В. (ВІТІ)

МОДУЛЬ З ОЦІНЮВАННЯ СЛУЖБОВОЇ ДІЯЛЬНОСТІ ВІЙСЬКОВОСЛУЖБОВЦІВ

Актуальність теми: Існуючі напрями розвитку Збройних Сил України, в сучасних умовах зумовлюють необхідність реалізації заходів комплексного вирішення завдань їх кадрового забезпечення, комплектування професійно підготовленими військовослужбовцями з необхідним потенціалом та перспективами подальшого службового зростання.

Атестування військовослужбовців проводиться для забезпечення підготовки військових кадрів шляхом об'єктивного оцінювання професійного рівня, ділових та моральних якостей військовослужбовців, їхвідповідності займаним посадам, визначення перспектив службового використання, створення резерву кандидатів для просування по службі. Результати атестування є основою для прийняття кадрових рішень.

Метою дослідження є підвищення ефективності роботи начальників (командирів) по організації і проведення атестування військовослужбовців Збройних Сил України з розробкою інформаційної системи.

Для досягнення мети дослідження у роботі необхідно вирішити наступні завдання:

– обґрунтування необхідності автоматизації системи оцінювання військовослужбовців;

– аналіз критеріїв оцінювання службової діяльності військовослужбовців.

Виклад основного матеріалу:

Результативність діяльності військовослужбовців підлягає щорічній оцінці для виявлення якості виконання завдань, а також для прийняття рішень щодо преміювання, планування кар’єри. Така оцінка базується на показниках ефективності, на результатах та якості, визначених з урахуванням посадових обов’язків службовців, а також їх відповідності етичним вимогам поведінки та вимогам законодавства, спеціальної програми навчання та визначених показників у контракті про проходження військової служби.

Даний модуль призначено для поліпшення оцінювання та складання характеристики військовослужбовців з метою прийняття рішення щодо планування їх кар’єри.

До критеріїв оцінювання відносяться: рівень теоретичних знань, рівень практичних умінь та навичок, рівень готовності до виконання (забезпечення) бойових завдань, результативність виконання посадових обов’язків, якість виконання завдань за призначенням, рівень сформованості ідейних та моральних якостей, рівень особистої військової дисципліни (стан військової дисципліни у підпорядкованому підрозділі), рівень вогневої підготовки, рівень фізичної підготовки, стан здоров’я.

Реалізація модулю з оцінювання службової діяльності військовослужбовців:

Дія 1.Введення початкових даних (звання, ПІБ, займана посада, особистий номер).

Дія 2.Заповнювання таблиці з оцінками.

Дія 3.Ознайомлення зі складеною характеристикою, заповнення висновку та рекомендацій безпосереднього начальника.

Дія 4. Заповнення висновку та рекомендації прямого начальника.

Дія 5.Заповнення результату періодичного оцінювання.

Дія 6.Заповнення висновку атестаційної комісії.

Дія 7.Написання рішення особи, яка затверджує скорочену оцінну картку.

Висновок:Таким чином, в роботі розроблено web додаток для автоматизації оцінювання військовослужбовців та складання на них характеристики. Запропонована реалізація модулю з оцінювання службової діяльності військовослужбовців дозволяє проводити більш точне щорічне оцінювання військовослужбовців, а також швидко та зручно здійснювати заповнювання характеристики виходячи з отриманих оцінок.

к.т.н. Бовда Е.М. (ВІТІ)
Бовда В.Е. (ВІТІ)
Полосін. А. В.(ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ АВТОМАТИЗОВАНОГО ОБЛІКУ ОСОБОВОГО СКЛАДУ НА ОСНОВІ ЧАТ-БОТУ

Актуальність теми. Повсякденна діяльність військовослужбовців є дуже насиченою в часі, тому потребує вирішення деяких питань шляхом її автоматизації. Наприклад, покращення процесу навчання та служби в цілому, постановка завдань, облік військовослужбовців, облік майна, створення, підписання рапортів та наказів, тощо. Вирішення цих завдань можливо завдяки створенню чат-боту, який зможе об'єднати все разом, що дасть можливість в сучасному світі оперативно приймати рішення та віддавати накази. Це дасть можливість військовослужбовцям вчасно виконувати їх згідно до посадових обов'язків, а також відслідкувати їх виконання на різних етапах.

Актуальність питання полягає в автоматизації діючих методів роботи командирів та начальників у вирішенні завдань повсякденної діяльності: облік особового складу, подачі та підписанні рапортів та наказів, постановки завдань як одноосібно так і на курс чи факультет. Загалом, всієї інформації, яка зберігається в паперовому вигляді: це стосується видачі майна, проведення анкетувань, покращення умов проживання шляхом застосування сучасних інформаційних технологій. Розробка чат-боту з відповідними функціональними можливостями, який буде відповідати висунутим вимогам (зручність в керуванні та орієнтуванні, зрозумілість, тощо), дозволить застосувати його у курсантських підрозділах у ВВНЗ.

Метою дослідження є автоматизація обліку роботи з особовим складом військовослужбовців військової частини.

Виклад основного матеріалу. Дана інформаційна система створена для ведення обліку роботи з військовослужбовцями, що покращить умови їх служби. Система повинна мати наступні складові:

1. Спосіб аунтентифікації посадової особи.
2. Можливість створювати різного роду документацію.
3. Редагування та перегляд документів.
4. Дистанційний підпис.

Для виконання поставленого завдання передбачається вирішення серії завдань:

- проаналізувати існуючі підходи по формалізації предметної області дослідження. Визначення обмежень, ускладнень та проблем, що не дозволяють досягнути максимальної ефективності процесу обліку особового складу військовослужбовців;

- визначення технологічних підходів в автоматизації процесу обліку особового складу військовослужбовців. Обґрунтування архітектури, структури алгоритмів роботи, веб орієнтованого застосування спрямованого на автоматизацію процесу дослідження;

- з'ясувати вибір оптимальної архітектури для інтерактивних систем;

- реалізація вибраного рішення.

Висновки. ЗС України потребують використання нових технологій, для того щоб покращити не лише умови служби, але й функціонування військових частин.Сучасні технології дозволяють забезпечити більш високий рівень безпеки, автоматизацію робочих процесів та поліпшити ведення обліку та складання звітів стосовно усіх аспектів служби військовослужбовців.

Очікується, що запропонований програмний модуль дозволить підвищити ефективність процесу обліку особового складу у військових частинах.

к.т.н. Бовда Е.М. (ВІТІ)
Бовда В.Е. (ВІТІ)
Решетніков М.О. (ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ АВТОМАТИЗОВАНОГО ОБЛІКУ НАУКОВИХ ДОСЯГНЕНЬ КУРСАНТІВ

Актуальність теми: Під час проходження навчання курсантів у вищих військових навчальних закладах постає питання аналізу не тільки їх здобутків в навчанні, але й їх наукових досягнень. Кожен курсант приймає участь в роботі наукових гуртків, де проходить його становлення як майбутнього професіонала, інженера, науковця. Він вивчає наукові підходи до досліджень, пише тези, наукові статті та приймає участь в дослідженнях на різні наукові тематики.

Навчання у вищих військових навчальних закладах передбачає набуття курсантами компетенцій, вмінь, знань та навичок, які йому знадобляться під час проходження служби офіцером на відповідних посадах. Це дасть змогу в перспективі стати професіоналом у своїй спеціальності та на основі цього постійно вдосконалювати отримані знання. Але лише постійний пошук до нових знань дозволить йому мати сталий розвиток. І це можливо лише через критичне мислення, пошук нових рішень, технологій, підходів у вирішенні постійно виникаючих питань.

Створення будь-якого рейтингу покращує особистісні властивості та індивідуальні якості кожного курсанта. Він стимулює курсантів на постійне покращення своїх здобутків. Актуальність питання полягає в автоматизації діючих методів обліку курсантських досягнень в науковій діяльності шляхом застосування сучасних інформаційних технологій з розробкою програмного рішення з відповідними функціональними можливостями, яке буде відповідати висунутим вимогам (зручність в керуванні та орієнтуванні, зрозумілість, тощо) та дозволить реалізувати його реальні перспективи застосування у ВВНЗ.

Мета роботи: автоматизація обліку наукових досягнень курсантів для активізації їх пізнавальної діяльності під час проходження служби у ВВНЗ та використання отриманих результатів при створенні підсумкового рейтингу курсантів на випускному курсі.

Виклад основного матеріалу: Створення будь-якого рейтингу сприяє виявленню найбільш підготовлених курсантів в любій області знань, надає стимул для навчання та розвитку у інших.Програмний комплекс побудований за принципами трьохярусної архітектури побудови, яка складається з таких компонентів: клієнт, сервер і база даних. На основі проведеного аналізу та поставлених завдань обрано набір інструментів для практичної реалізації розроблюваного веб-ресурсу, а саме: стек MERN, що включає в себе СКБД MongoDB, базову платформу Express.js, бібліотеку React та програмну платформу Node.js.

Використовуючи документо-орієнтовану базу даних MongoDB для зберігання даних в JSON форматі пришвидшується маніпулювання даними в CRUD операціях порівнянні з іншими БД. Використовуються стандартні вхідні дані про курсанта, його діяльність в наукових гуртках. Розроблена система рейтингів з ваговими коефіцієнтами, які будуть враховуватись при обрахуванні вихідних даних кожного курсанта з наукової діяльності. Завдяки тому, що використовується React для побудови web-application на виході буде швидкий, компонетний додаток з простим і розумним інтерфейсом.

Висновки: Розроблений веб-додаток для обліку діяльності курсантів в наукових гуртках дозволить командирам та начальникам відслідковувати їх здобутки в наукових гуртках. Таким чином, створення рейтингу за науковими досягненнями буде сприяти підвищенню загального рейтингу курсанта на випускному курсі та буде впливати на розподіл після навчання у вищих військових навчальних закладах.

к.т.н. Бовда Е.М. (ВІТІ)
Луцюк М.В.(ВІТІ)

ТЕЛЕГРАММ БОТ ДЛЯ ОТРИМАННЯ ПЕРСОНАЛЬНИХ НОВИН НА ВІЙСЬКОВУ ТЕМАТИКУ

Актуальність: В Збройних Силах України в визначені дні робочого тижня проводиться інформування, під час, якого до них доводять новини, які відбулись в певному проміжку часу про стан справ на сьогоднішній день, просування розвитку держави. З використанням телеграм-бота буде спрощене проведення інформування тим, що буде затрачено менше часу на пошук конкретної новини чи інформації. З телеграм-ботом може бути збережена знайдена інформація для надання військовослужбовцям питання на запам'ятовування піднесеної інформації.

Мета дослідження полягає у підвищенні ефективності процесів надання персоналізованих новин військовослужбовцям. Для вирішення поставленого завдання необхідно виконати **наступні часткові завдання дослідження**:

– аналіз сучасного підходу у висвітленні новин у Збройних Силах України, спираючись на вимоги керівних документів з морально-психологічного забезпечення;

– вдосконалення самого алгоритму планування висвітлення новин та процесів, що пов'язані з цією задачею, з урахуванням недоліків та обмежень сучасної моделі;

– автоматизація процесів надання персоналізованих новин за рахунок розробки програмного модулю для отримання персональних новин на військову тематику.

Мета роботи: автоматизація збору новин на військову тематику для військовослужбовців ЗСУ з розробкоютелеграм-бота. Користувач вводить потрібне йому слово чи дату, визначає певний проміжок часу, а створений додаток – виводить всі новини на військову тематику, які починаються на зазначене слово чи на вказану дату.

Виклад основного матеріалу. Проведено аналіз предметної області. Розглянуто вимоги, яким повинен задовольняти телеграм-бот. Визначено основні властивості додатку, який розробляється. Побудовано алгоритм роботи телеграм-боту, який показує взаємодію основних складових додатку. Проведено аналіз існуючих додатків та підходів для їх реалізації. Запропоновано використати агрегативно-декомпозиційний підхід.

Реалізація даного підходу вимагає розробки спеціальної людино-машинної процедури пошуку раціональної структури системи, яка складається з трьох взаємопов'язаних завдань:

– визначення ресурсів для отримання новин, які задовольняють умовам.

– вибірка новин індивідуально для кожного користувача;

вибір технічних засобів для виконання завдання. Програмний комплекс побудований за принципами трьохланкової архітектури побудови програм, яка складається з таких компонентів: клієнт, сервер і база даних. Для створення програмного продукту будуть використані такі інструменти, а саме: стек MERN, що включає в себе СКБД MongoDB, базову платформу Express.js, Python, , бібліотеку React та програмну платформу Node.js.

Був створений телеграм-бот для спрощення збору новин на тематику, яка найбільш інтересна користувачу. В ході виконання завдання був створений зручний інтерфейс, який має зручну навігаційну панель та інтуїтивно зрозумілу логічну структуру.

Базуючись на етапі проектування структури системи, використовуючи класичний підхід проектування було розроблено узагальнену архітектуру і алгоритми роботи програмного модулю отримання персональних новин на військову тематику.

Висновки. Отже, в роботі запропоновано використання агрегативно-декомпозиційного підходу, на його основі реалізовано програмний модуль отримання персональних новин на військову тематику.

к.т.н. Бовда Е.М. (ВІТІ)
Ревуцький В.А. (ВІТІ)

ПІДСИСТЕМА ОПОВІЩЕННЯ ОСОБОВОГО СКЛАДУ ПІДРОЗДІЛУ «SONAR»

Актуальність дослідження обумовлена необхідністю впровадження системи оповіщень підрозділів військових частин в Збройних Силах України і, як слідство, у підвищенні ефективності задачі оповіщення та доведення відповідної інформації. Адже порівневе узгодження рішення задач оповіщень є надзвичайно важливим питанням, що визначає ефективність функціонування системи оповіщень підрозділів та доведення інформації в цілому.

Мета дослідження полягає у підвищення ефективності процесів оповіщень підрозділів, підрозділів зв'язку за рахунок виконання **наступних часткових завдань дослідження:**

– аналіз сучасного підходу в доведення наказів, оповіщень, сигналів у Збройних Силах України, спираючись на вимоги керівних документів з оповіщення особового складу підрозділів;

– вдосконалення самого алгоритму оповіщень, доведення наказів та процесів, що пов'язані з цією задачею, з урахуванням недоліків та обмежень сучасної моделі;

– автоматизація процесів оповіщення підрозділів за рахунок розробки підсистеми оповіщення особового складу підрозділу «SONAR». Апробація моделей.

Виклад основного матеріалу. Автоматизація оповіщення особового складу може підвищити бойової можливості військ (сил) до 40% і одночасно в сотні разів скоротити час, які витрачають органи управління на розрахунки і доведення завдань та часу виконання до підлеглих, тобто час, який витрачається на цикл управління та доведення інформації. Також, збільшити конфіденційність повідомлень, правильність донесення до відповідних осіб, збільшення часу на перехоплення та розшифрування повідомлень, тим самим роблячи інформацію, яка передається не актуальною. Збільшити ефективність оповіщення можливо за допомогою автоматизації процесів оповіщення особового складу – створення автоматизованої системи оповіщення (АСО). Реалізація даного підходу вимагає розробки спеціальної людино-машинної процедури пошуку раціональної структури системи, яка складається з чотирьох взаємопов'язаних завдань:

– визначення числа рівнів і вузлів системи (характеристики, що враховуються: цілі і стратегії функціонування системи управління; організаційно-штатна структура);

– розподілення завдань по рівням і вузлам системи (характеристики, що враховуються: ефективність рішення завдань; витрати на їх взаємозв'язок і розробку);

– вибір технічних засобів для вузлів системи (характеристики, що враховуються: системні вимоги до технічних засобів);

– імітаційне моделювання роботи системи (уточнення вимог до характеристик якості).

Базуючись на етапи проектування структури системи, використовуючи класичний підхід проектування було розроблено узагальнену архітектуру і алгоритми роботи підсистеми оповіщення особового складу підрозділу «SONAR». Під час оцінки ефективності отримано приблизний результат затрат часу на прийняття управлінських рішень. Коефіцієнт відносної економії часу у випадку частоти рішення задач 10 разів за добу дорівнює приблизно 43%.

Висновки. Отже, в роботі запропоновано використання агрегативно-декомпозиційного підходу для проектування структури АСО та на його основі реалізовано підсистему оповіщення особового складу підрозділу «SONAR».

к.т.н. Бовда Е.М. (ВІТІ)
Савенок О.О. (ВІТІ)
Лазута Р.Г. (ВІТІ)

ІНФОРМАЦІЙНИЙ ВЕБ-ПОРТАЛ ВВНЗ ТА ВІЙСЬКОВИХ НАВЧАЛЬНИХ ПІДРОЗДІЛІВ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Актуальність теми. На сьогоднішній час в Україні працюють достатня кількість військових інститутів та коледжів, які здійснюють підготовку висококваліфікованих спеціалістів та фахівців своєї справи. Багато розумних випускників шкіл не беруть до уваги військові заклади. Для вирішення даної проблеми почалася активна автоматизація процесу агітації ВВНЗ за допомогою програмно-апаратних засобів. Тому, постає питання про створення web-ресурсу, який допоможе коротко ознайомитись з навчальними закладами, прочитати коротку інформацію безпосередньо про сам заклад та бали, які потрібні для вступу на вибрану спеціальність. Дізнатись про розташування ВВНЗ, а також наприкінці сторінки буде вказане посилання безпосередньо на сам військовий навчальний заклад, де можливо більш детально ознайомитись з інформацією про навчальний заклад. А для самих навчальних закладів буде інформації про учнів, точніше з яких областей найбільша зацікавленість тим чи іншим навчальним закладом, який в подальшому допоможе спрогнозувати потік абітурієнтів, а саме майбутніх курсантів в ті чи інші військові навчальні заклади.

Метоюдослідження є автоматизація пошуку інформації про військові навчальні заклади зі подальшим створенням інформаційного порталу ВВНЗ, що несе інформування майбутнім абітурієнтам та їх батькам, полегшує пошук необхідної інформації, що здійснюється за допомогою узагальненої web-сторінки, в якій зібрана база даних безпосередньо навчальних закладів.

Для досягнення поставленої мети було вирішено наступні часткові **завдання:**

1. проведено аналіз предметної області, обґрунтування потреби в розробці програмного продукту;
2. аналіз архітектурної будови та розробки алгоритмів роботи програмного модуля веб-порталу;
3. розроблено інтерфейс користувача;
4. проведено оцінка ефективності програмного модуля.

Виклад основного матеріалу.Для досягнення своїх цілей по залученню абітурієнтів вищий навчальний заклад повинен враховувати при розробці свого веб-сайту таки вимоги, як зручність та зрозумілість, зацікавити своїм дизайном та інформативністю та зосередити основну увагу на користувачеві.

Виходячи з цього, даний інформаційний портал був розроблений легким у використані, інтерактивним та простим для будь-якого покоління користувачів, яке буде користуватись даною інформацією з сторінки. За результатами проведеного тестування виявлено, що інформаційний портал є доцільним, інформативним та загалом зручним.

При розробці веб-сайта були проаналізовано сучасні веб-технології, що дозволяють створювати інтерактивні веб-сторінки. Розроблений сайт задовольняє всім вимогам, поставленим на етапі постановки завдання.

Як подальше вдосконалення веб-сайта представляється можливим розробка модулів доступу, можливе доопрацювання інтерфейсу сайту з метою подальшого підвищення його інформативності, привабливості і зручності у пошуку та використанні інформації.

Висновок: Таким чином, в роботі розроблений додаток для автоматизації процесу інформування населення про військові навчальні заклади різних рівнів акредитації, їх місце знаходження та іншої інформації. Запропонована реалізація модулю дозволяє більш точно спрогнозувати кількість абітурієнтів, які будуть вступати до військових закладів освіти.

к.т.н. Бовда Е.М. (ВІТІ)
Шкорупський В.М. (ВІТІ)
Орда М.В. (ЦВСД)

ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ МОДУЛЬ АВТОМАТИЗОВАНОГО РОЗРАХУНКУ ТОЧОК РОЗМІЩЕННЯ РАДІО-РЕЛЕЙНИХ ЗАСОБІВ ДЛЯ ПОБУДОВИ РАДІО-РЕЛЕЙНИХ ЛІНІЙ

Актуальність теми. В даній роботі проведено аналіз існуючих підходів щодо впровадження сучасних технологій автоматизації розрахунку точок розміщення радіо-релейних засобів для побудови радіо-релейних ліній. Проведено дослідження шляхів автоматизації роботи тактичної ланки управління. Обґрунтовано розробку програмного модулю підтримки прийняття рішень при плануванні та організації зв'язку з відображенням розрахунку точок розміщення радіо-релейних засобів для побудови радіо-релейних ліній.

Програмна реалізація модулю дозволяє підвищити ефективність процесів планування зв'язку, за рахунок автоматизації: відображення точок розміщення радіо-релейних засобів для побудови радіо-релейних ліній.

Метою дослідження єпідвищення ефективності процесів планування бойового застосування частин, підрозділів зв'язку за рахунок розробки програмного модулю автоматизації розрахунку точок розміщення радіо-релейних засобів для побудови радіо-релейних ліній.Виходячи з мети роботи, виникають наступні **завдання**:

- обґрунтувати необхідність автоматизації завдань з планування організації зв'язку в інформаційно-аналітичній підсистемі підтримки прийняття рішень органів управління зв'язком;
- проаналізувати архітектурну будову та розробити алгоритм роботи модуля, що проектується;
- розробити програмну реалізацію модуля автоматизації розрахунку точок розміщення радіо-релейних засобів для побудови радіо-релейних ліній;

провести оцінку ефективності запропонованих рішень.

Виклад основного матеріалу. На сьогоднішній день управління системою зв'язку і автоматизації ЗСУ здійснюється у неавтоматизованому режимі. Використання службовими особами персональних електронних обчислювальних машин та інформаційних систем автоматизує лише незначний обсяг функціональних обов'язків, примушуючи службових осіб органів та пунктів управління використовувати технології минулого сторіччя, внаслідок чого на прийняття рішення витрачається неприпустимо велика кількість часу. Проаналізувавши діючі нормативні документи, що регламентують життєвий цикл програмного забезпечення, використовуючи класичний підхід проектування було розроблено узагальнену архітектуру і алгоритми роботи інформаційно-аналітичного модулю автоматизації розрахунку точок розміщення радіо-релейних засобів для побудови радіо-релейних ліній. Дана архітектура та алгоритми дозволять розробити програмну реалізацію, що дозволить автоматизувати розрахунок точок розміщення радіо-релейних засобів для побудови радіо-релейних ліній.

Ґрунтуючись на задану архітектуру та використовуючи обрані інструментальні засоби реалізації програмної логіки було створено інформаційно-аналітичного модулю розрахунку точок розміщення радіо-релейних засобів для побудови радіо-релейних ліній, який відповідає вимогам оперативної постановки.

Розроблений модуль був представлений та апробований в ході роздільного штабного тренування, що відбувалось в Головному управлінні зв'язку та інформаційних систем ГШ ЗСУ. За результатами даних тренувань програмний продукт показав високий рівень ефективності.

Висновки. Завдяки розробленому інформаційно-аналітичному модулю розрахунку точок розміщення радіо-релейних засобів для побудови радіо-релейних ліній було підвищено ефективність процесів нанесення даних на карту командирами частин, підрозділів зв'язку.

к.т.н. Бовда Е.М. (ВІТІ)
Яремич О.Д. (ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ ПРОГРАМНОГО КОДУ МОВИ ПРОГРАМУВАННЯ JAVA.

Актуальність. Навчання у вищих військових навчальних закладах передбачає набуття курсантами вмінь та навичок для того щоб стати професіоналом у своїй спеціальності.

Для покращення особистісних властивостей та індивідуальних якостей вимагається організація проведення якісного навчального процесу, максимальна відданість від викладачів та сучасна матеріально-технічна база, яка в свою чергу потребує автоматизації в деяких аспектах навчання.

Актуальність питання полягає в автоматизації діючих методів проведення практичних занять з курсу Кросплатформне програмування шляхом застосування сучасних інформаційних технологій та розробки програмного рішення з відповідними функціональними можливостями, яке буде відповідати сучасним вимогам (зручність в керуванні та орієнтуванні, зрозумілість, тощо), які дозволять реалізувати його реальні перспективи застосування у ВВНЗ у навчальному процесі на кафедрі комп'ютерних інформаційних технологій.

Мета роботи є підвищення якості процесу перевірки практичних знань та завдань з програмування мовою Java курсантів ВВНЗ з розробкою вебдодатку.

До **часткових завданьдослідження** роботи відноситься:

аналіз існуючого підходу до автоматизації проведення практичних занять з курсу Кросплатформне програмування;

дослідження вже існуючого програмного забезпечення для оптимізації та підвищення якості перевірки практичних знань курсантів ВВНЗ;

вдосконалення алгоритму проведення практичних занять та процесів, що пов'язані з цією задачею з урахуванням недоліків та обмежень існуючих моделей;

автоматизація процесу проведення практичних занять та перевірки практичних знань курсантів ВВНЗ з курсу Кросплатформне програмування, за рахунок розробки програмного модулю автоматизованого тестування програмного коду мови програмування Java.

Виклад основного матеріалу. Програмний комплекс побудований за принципами триланкової архітектури побудови програм, яка складається з таких компонентів: клієнт, сервер і база даних. На основі проведеного аналізу та поставлених завдань обрано набір інструментів для практичної реалізації розроблюваного вебресурсу, а саме: стек MERN, що включає в себе СКБД MongoDB, базову платформу Express.js, бібліотеку React та програмну платформу Node.js.

Було створено вебдодаток для спрощення проведення практичних занять з програмування шляхом автоматизації перевірки виконаного завдання. В процесі розробки було побудовано зручний та інтуїтивний інтерфейс, який має зручну навігаційну панель та інтуїтивно зрозумілу логічну структуру. Після проведених тестувань вебдодаток працює коректно та відповідає поставленим вимогам.

Висновок: розробка вебдодатку для спрощення процесу проведення практичних занять з програмування, перевірка знань курсантів є вкрай важливою для покращення навчального процесу. Використання такого способу тестування курсантів значно пришвидшує процес проведення занять, а також спрощує роботу викладача в перевірці виконаних курсантами практичних завдань.

к.т.н. Борисов О.В. (ВІТІ ім.Героїв Крут)
к.т.н. Борисов І.В. (в/ч А1906)

ВДОСКОНАЛЕНИЙ МЕТОД ДЕМОДУЛЯЦІЇ СИГНАЛУ В СИСТЕМАХ З ПРОСТОРОВО-ЧАСОВОЮ ОБРОБКОЮСИГНАЛУ

В даний час неухильно зростає попит на широкосмугові послуги, користувачі яких потребують здійснення доступу з будь-якого місця,в будь-який час і з високою якістю. Таким умовам задовольняють системи зв'язку третього й наступних поколінь, наприклад, універсальна система рухомого зв'язку (UMTS), система бездротового доступу міського масштабу (WiMax) [1]. Одна з технологій, що використовується даними системами і дозволяє значно збільшити пропускну здатність бездротових каналів зв'язку – MIMO (Multiple-input-multiple-output) – система з декількома передавальними й приймальними антенами й використанням просторово-часового кодування.

Системи MIMO пропонують одночасну передачу й приймання декількох потоків даних в одній смузі частот. Частковим випадком є система просторово-часової архітектури BLAST – (Bell Laboratories Layered Space-Time).

Процес демодуляції в системі BLAST зводиться до розв’язання системи рівнянь. Але оскільки в ній є присутнім випадковий компонент у вигляді гаусівського шуму, традиційні методи вирішення систем лінійних рівнянь у цьому випадку можуть призвести до значних енергетичних втрат [1], для зменшення яких можуть використовуватися різні методи демодуляції для обчислення оцінок переданих символів [2]:

метод мінімуму середньоквадратичної помилки;

алгоритм V-BLAST (Vertical Bell Laboratories Layered Space Time Architecture);

метод максимальної правдоподібності.

Найкращими характеристиками серед них володіє метод максимальної правдоподібності [1]. Запропонований метод використовує подібний принцип, тобто прийнятий потік сигналів розбивається на дві підгрупи, які потім демодулюються з використанням методу максимальної правдоподібності. Відмінність полягає в тому, що на кожній ітерації враховується не тільки оцінка, отримана на попередньому кроці, але й ступінь точності оцінювання символів. У системі WiMax з 4 передавальними й 4 приймальними антенами для демодуляції одного інформаційного символу (з періодичністю проходження 100 мкс) з модуляцією 16-QAMцей метод дозволяє зменшити необхідну кількість операцій, виконуваних у реальному часі, з 10^7 у випадку оптимального демодулятора до $4x10^5$. Таким чином, обчислювальні затрати для реалізації запропонованого алгоритму в 25 разів менше в порівнянні з алгоритмом максимальної правдоподібності.

Таким чином, запропонований вдосконалений метод демодуляції передбачає, що оцінки символів обчислюються з використанням методу максимальної правдоподібності, але при значно меншій кількості можливих комбінацій вектора інформаційних символів, а також з урахуванням неточності оцінювання символів на кожній ітерації, що дозволить досягти високої ефективності демодуляції при відносно малих обчислювальних затратах. Метод забезпечує характеристики, близькі до оптимальних за критерієм максимальної правдоподібності (програш менше 1 дБ), при значно меншій обчислювальній складності. Він може використовуватися для демодуляції також в системах і з більшою кількістю антен та з вищою кратністю модуляції.

ЛІТЕРАТУРА.

1.Report ITU-R M.2074. Radio aspects for the terrestrial component of ITM-2000 and systems beyond ITM-2000.2006.

2.*Hamid Jafarkhani.* Space-Time Coding: theory and practice //Cambridge University Press 2005.

Василець А.А. (ВІТІ ім.Героїв Крут)
Пилипенко М.Г. (ВІТІ ім.Героїв Крут)

ВАРІАНТ ПРОЕКТУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ВІДОМЧОГО ПРИЗНАЧАННЯ З УРАХУВАННЯМ ДОСВІДУ АТО/ООС

Актуальність теми. Практичне застосування інформаційних систем і технологій в державному управлінні зачіпають питання якості управління, в першу чергу вчасного отримання і доведення рішення, мають вплив складові національної безпеки.З'являється необхідність не відставати від прогресу в сфері інформаційних технологій. Важливо знати і вміти застосовувати нові послуги, рішення та наукові досягнення.

Їх оптимальне використання дозволяє по новому підійти до вирішення старих завдань, а також сформувати оригінальне рішення для задач, раніше нерозв'язних. Повсюдне впровадження і використання інформаційно-комунікаційних технологій в сучасному житті піднялось на значний рівень можливості комунікативної і виконавської діяльності, а так само призвело до корінної перебудови різних сторін діяльності.Сьогодення вимагає від системи зв’язку безперебійного обміну інформацією, своєчасної передачі наказів, донесень, чим вона забезпечить якісне і безперебійне управління військами, особливо у зоні проведення операції об’єднаних сил .

Постановка задачі. Проаналізувати переваги та недоліки технології SDH при використанні в мережах військового зв'язку.

Аналіз основних можливостей телекомунікаційної мережі відомчого призначання; порівняння основних методів проектування телекомунікаційної мережі відомчого призначання;оцінка варіанту проектування телекомунікаційної мережі відомчого призначання з урахуванням досвіду АТО/ООС.

Для розв’язування задач оптимального проектування мережі зв’язку обов’язковим є побудова її аналітичної моделі. Модель мережі на основі теорії масового обслуговування дала можливість вирішити ряд задач топологічного проектування, зокрема, це задача вибору пропускних продуктивність каналу та задача розподілу потоків. Однак одержані оптимальні вирішення вказаних задач можуть бути використані лише для сформульованих в цих задачах вихідних даних. В ряді випадків вихідні дані для побудови моделі мережі відрізняються, тому для вирішення задач проектування мереж зв’язку запропоновано багато інших методів синтезу та аналізу.

Аналіз задач показує складність їх строго формального розв'язання аналітичними методами через велику кількість змінних, що характеризують структуру та параметри системи. З огляду на викладене при дослідженні таких систем доцільно застосовувати традиційні для теорії складних систем методи поетапної оптимізації, субоптимізації підсистем, поєднання аналітичних та імітаційних методів моделювання, доповнюючих один одного і забезпечуючих можливість дослідження структур системи при вихідних даних, що відповідають різному ступеню адекватності моделі та об'єкту дослідження. Вимоги до зв’язку і автоматизація управління військами Зв’язок є основним засобом управління військами, бойовими засобами та зброєю. Командири та начальники штабів зобов’язані постійно, за будь-яких обставин, мати зв’язок з вищестоящими та підлеглими командирами та штабами, а також із своїм штабом. Зв’язок виконує завдання по обміну інформацією в системах управління військами.

Для виконання цих завдань зв’язок і АУВ повинні задовольняти вимоги щодо своєчасності, достовірності, скритності. Своєчасність – здатність військового зв’язку забезпечувати обмін інформацією, її обробку та рішення інформаційних і розрахункових задач в задані (нормативні) строки. У сучасному бою (операції) пред’являються високі вимоги у відношенні своєчасності зв’язку. Це обумовлюється швидкоплинністю і високими

темпами розвитку бойових дій військ, а також частими і різкими змінами обстановки, внаслідок застосування ракетно-ядерної зброї.

При різких змінах обставин потрібні негайне реагування з боку командира, особливо у відповідальні моменти бою. Різко підвищилося значення своєчасності зв'язку при одержанні повідомлень від усіх видів розвідки, при передачі сигналів про повітряного противника, радіоактивного, хімічного і бактеріологічного зараження. Особливого значення своєчасність зв'язку здобуває в ракетних військах і військах протиповітряної оборони.

Висновки.

Проблема задоволення постійно зростаючих вимог до швидкості і достовірності передачі інформації стає особливо актуальною у сучасному суспільстві. При цьому передача інформації здійснюється в умовах обмежених частотних і енергетичних ресурсів каналів зв'язку, а отже, досягати необхідної швидкості передачі даних та якості зв'язку необхідно шляхом розумного використання відведеного ресурсу.

Для оцінки ефективності використання ресурсу каналу зв'язку використовується поняття інформаційної ефективності як відношення продуктивності джерела повідомлень, яка характеризує швидкість передачі інформації, яку отримує кінцевий користувач до пропускної здатності каналу зв'язку, яка використовується як для передачі інформації користувача, так і для передачі технічної інформації.

Загальним підсумком даної роботи є варіант проектування телекомунікаційної мережі відомчого призначання з урахуванням досвіду АТО/ООС

ЛІТЕРАТУРА

1. Жураковський Ю.П., Полторак В.П. Теорія інформації та кодування. – К.: Вища шк., 2001. – (255с.)

2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. –М.: Мир, 1986. – (576с).

3. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. – М.: Мир, 1978. – (576с).

4. Габидулин Э.М., Афанасьев В.Б. Кодирование в радиоэлектронике. – М.: Радио и связь, 1986. – (176с.)

Власенко О.В. (ВІТІ)
Палиця В.О. (ВІТІ)

АВТОМАТИЗАЦІЯ ОЦІНЮВАННЯ ВИПИСНИКА ВВНЗ ЗА «ПРИНЦИПОМ 360»

Актуальність у сучасних умовах реформування військової освіти особливої актуальності набувають проблеми виокремлення закономірностей – детермінант та визначення загальних принципів формування змісту військової освіти, на яких повинні базуватися процеси навчання і діагностування рівня підготовки військових фахівців.

Щорічне оцінювання має важливе значення в забезпеченні успішної адаптації молодих офіцерів. Цей процес постійного спостереження, вивчення і оцінювання службової діяльності за визначеними критеріями результатів його діяльності являє собою дієвий інструмент виважених кадрових рішень в процесі якісного управління кар'єрою офіцера.

Мета дослідження визначення якості підготовки військових фахівців у ВВНЗ, здатності ефективно виконувати службові обов'язки за посадою.

Досягнення мети передбачає вирішення наступних завдань:

–Проаналізувати оцінювання результатів навчання випускників ВВНЗ за принципом 360.

–Проаналізувати бібліотеки та існуючі технологій для розробки програмного модулю.

–Розробка програмного модулю.

Виклад основного матеріалу. Оцінка випускника ВВНЗ за принципом 360 дозволяє порівняти оцінки, які військовослужбовець вказав під час самооцінки, з результатами зафіксованими його командиром, підлеглими та командирами сусідніх підрозділів, внаслідок чого зробити необхідні висновки щодо своїх сильних сторін, зон розвитку, а також отримати різнобічні думки про свою роботу. Даний метод незалежних експертних оцінок надає підґрунтя для ретельного самоаналізу випускником своєї службової діяльності та застосування триманих знань у практиці. Отриманні результати важливо враховувати в організації освітнього процесу у Вищих військових навчальних закладах. Також важливою є оцінка професійно важливих компетентностей та виведення узагальнених результатів по кожному значенню. Збір, аналіз та узагальнення результатів професійної діяльності випускників у військах, розробка рекомендації щодо удосконалення навчальних планів, програм і методик з підготовки курсантів та слухачів є важливою складовою в організації підготовки військових кадрів у ВВНЗ. У військових вишах впроваджена система роботи з відгуками на випускників, щодо проходження ними служби у військах. Існуюча система дозволяє визначити рівень підготовки офіцерів, готовність їх до самостійного виконання обов'язків за призначенням у військах, а також виявити слабкі місця у їх підготовці. Електронна версія відгука на випускника за принципом 360 повинна бути більш інформативною, доступною та зручною у впровадженні. Порівняльний аналіз усіх професійних складових у підготовці молодого офіцера як фахівця, а також як особистості носить конструктивний характер у динаміці соціально-психологічного супроводу. На сьогоднішній день є актуальною розробка комп'ютеризованої системи роботи з відгуками на випускників. Наявна система є застарілою та незручною у використанні. Доцільно створити єдину базу даних для усіх ВВНЗ з метою висвітлення об'єктивної та доступної картини стосовно підготовки офіцерів-випускників. Позитивний та негативний досвід у підготовці молодих офіцерів керівництву ВВНЗ слід враховувати при організації освітнього процесу, морально-психологічного забезпечення, а також при вихованні курсантського складу шляхом методу активного впливу на особистість з метою прищеплення випускникам якостей притаманних висококваліфікованим офіцерам.

ВисновокВиходячи з мети роботи було проаналізовано підхід оцінювання результатів навчання випускників ВВНЗ за принципом 360, та основні переваги над іншими підходами та системами. На основі цього було прийнято рішення щодо створення програмного модулю, який автоматизує та прискорить процес оцінювання офіцерів, як фахівців.

Власюк Т.С. (ВІТІ ім.Героїв Крут)
Пилипенко М.Г. (ВІТІ ім.Героїв Крут)

АНАЛІЗ МЕТОДІВ ЗАВАДОСТІЙКОГО КОДУВАННЯ У ПРОВОДОВИХ МЕРЕЖАХ ЗВ'ЯЗКУ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Актуальність теми. Ефективність функціонування Збройних Сил України залежить від організованого і безперервного управління військами, яке дозволяє в будь-яких, навіть найскладніших умовах обстановки, добиватися успішного виконання поставлених задач у встановлені терміни. Основним показником системі зв'язку є імовірність помилки, яка характеризує достовірність передачі, а також надійна завадозахищенність даних.

Якщо узяти достатньо довге речення та спотворити його шляхом заміни або вилучання чи додавання букв у деяких місцях, то при використанні знань щодо структури окремих слів та речення у цілому, попереднього та наступного тексту, знання предмету, про який їде мова, можна майже у повному обсязі відтворити початкове речення або безпомилково визначити його зміст. Це доводить, що природна мова має велику надмірність.

У техніці також дуже часто використовують однакові дублюючі пристрої на випадок виходу з ладу одного з них. У деяких випадках за допомогою того ж самого пристрою виконуються двічі ті ж самі розрахунки, і якщо результати співпадають, то приймається рішення про безпомилкове виконання розрахунків або працездатність пристроїв, що контролюються. При різниці у розрахунках вони повторюються ще раз, і знайдена помилка усувається або приймається рішення про непрацездатність відповідних пристроїв. Розглянуті випадки є прикладом того, що надмірність може допомогти з'ясувати наявність помилок і підвищити надійність системи.

Постановка задачі. Проаналізувати методи завадостійкого кодування; класифікація і основні характеристики завадостійких кодів; підвищення рівня завадозахищенності в проводових мережах зв'язку.

Основні положення.При передачі інформації по каналах зв'язку виникають помилки унаслідок завад і спотворень сигналів. Для їх виявлення і виправлення використовуються завадостійкі (коректуючі) коди.

Завадостійкими називають коди, що дозволяють виявляти і (або) виправляти помилки в прийнятому повідомленні. Здібність коду до виявлення і виправлення помилок заснована на введенні надмірності в кодоване повідомлення. Надмірні символи формуються за певними правилами і називаються перевірочними або контрольними. Збільшення числа таких символів в кодовій комбінації підвищує виявляючу і виправляючу здібності коду, але призводить до зниження швидкості передачі інформації.

Спрощена схема системи передачі інформації при завадостійкому кодуванні приведена на рис.1.1.

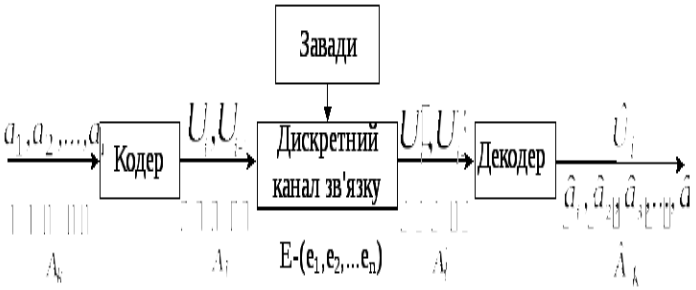


Рис. 1.1. – Спрощена схема системи передачі інформації

На сьогодні відома значна кількість коректувальних кодів, які використовуються в системах цифрового зв'язку. Двійкові коректувальні коди можна поділити на два великих класи: блокові та згорткові. До блокових відносяться такі коди, в яких кодування та декодування здійснюються в межах блока, що складається з визначеного числа кодових символів. До згорткових кодів, відносяться такі коди, в яких процес кодування має безперервний характер без виділення меж при формуванні послідовності кодових символів. Важливою відмінністю згорткового кодування є те, що кодові символи на виході кодера залежать не тільки від інформаційних символів, що надійшли на даний момент часу, але й від попередніх символів на його вході. У найпростішому ланцюговому коді кожен перевірочний елемент формується шляхом додавання по модулю 2 сусідніх або віддалених один від одного на визначене число позицій інформаційних елементів. До каналу зв'язку передається послідовність імпульсів, у якій за кожним інформаційним надходить перевірочний. Подібну послідовність розрядів, що чергується, має, наприклад, кореляційний манчестерський код. Блокові коди, в свою чергу, розподіляються на лінійні та нелінійні. До лінійних відносяться такі коди, в яких формування блоків, тобто кодування здійснюється з використанням лінійних операцій (підсумовування та множення над інформаційними символами з урахуванням арифметики за модулем 2). В іншому випадку, коректувальні коди відносяться до нелінійних, тому що сума двох кодових комбінацій (КК) з заданими властивостями не утворює комбінацію, що належить до даного коду.

В свою чергу, лінійні коди розподіляються на систематичні та несистематичні. В систематичних кодах інформаційні символи на виході кодера формуються в кінці кодового слова. Належність до систематичних або несистематичних кодів визначається вибором коду та алгоритму кодування. Значну частину лінійних кодів займають циклічні коди (ЦК), які знаходять застосування у цифрових системах передачі (ЦСП) різного роду повідомлень. До них відноситься досить велике число коректувальних кодів, серед яких найбільш відомими є:

-коди Хемінга, що виправляють однократні та виявляють 2-кратні помилки;

-коди БЧХ, що володіють високою коректувальною здатністю, які запропоновані Боузом, Чоудхурі та Хоквінгемом;

-коди Ріда-Соломона, що являють собою важливий підклас кодів БЧХ з коефіцієнтами кінцевих полів Галуа, які знайшли застосування у системах космічного зв'язку;

-мажоритарно-декодовані коди (МДК), що виправляють багаторазові помилки, яким властиві прості алгоритми декодування.Згорткові коди (ЗК), вперше запропоновані Елайесом, як і блокові, також розподіляються на систематичні та несистематичні. Перші, до яких відносяться самоортогональні згорткові коди (ССК), декодуються надто простим пороговим методом, а інші – з використанням алгоритму послідовного декодування (СК АПос. Д). Проблема завадостійкого кодування являє собою велику область теоретичних і прикладних досліджень. Основними задачами при цьому є наступні: пошук кодів, що ефективно виправляють помилки необхідного виду; методів кодування та декодування і прості способи їхньої реалізації. Найбільш розроблені ці задачі стосовно до систематичних кодів. Такі коди успішно застосовуються в обчислювальній техніці, різних автоматизованих цифрових пристроях і цифрових системах передачі інформації.

Висновки.Проблема задоволення постійно зростаючих вимог до швидкості і достовірності передачі інформації стає особливо актуальною у сучасному суспільстві. При цьому передача інформації здійснюється в умовах обмежених частотних і енергетичних ресурсів каналів зв'язку, а отже, досягати необхідної швидкості передачі даних та якості зв'язку необхідно шляхом розумного використання відведеного ресурсу. Для оцінки ефективності використання ресурсу каналу зв'язку використовується поняття інформаційної ефективності як відношення продуктивності джерела повідомлень, яка характеризує швидкість передачі інформації, яку отримує кінцевий користувач до пропускної здатності каналу зв'язку, яка використовується як для передачі інформації користувача, так і для передачі технічної інформації.

Гавриленко О.А(ВІТІ ім.Героїв Крут)
Османов Р.Н.(ВІТІ ім.Героїв Крут)

ОЦІНКА ЯКОСТІ СИСТЕМ МОНІТОРИНГУ ВОЛОКОННО-ОПТИЧНИХ ЛІНІЙ ЗВ'ЯЗКУ, ЯКІ ВИКОРИСТОВУЮТЬСЯ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Актуальність. Кожна технологія, в тому числі й волоконно-оптична, повинна мати систему моніторингу, яка зможе дати оптимальну оцінку якості та справності як всієї мережі так і окремих елементів. Контроль параметрів оптичного волокна необхідний для полегшенняпроцесуексплуатаціїоптичних ліній та забезпечення високої якості передачі сигн алів.

Система моніторингу оптичних середовищ оптимізує навантаження на технічний та обслуговуючий склад, що робить управління ВОЛЗ більш простою та зручною. Системи діагностують та локалізують проблеми мережі, повністювиключаютьпоявуаварії через старіння та деградацію кабеля, надаючи операторам зв'язку точну інформацію по пошкодженнях.

Постановка задачі. Провести аналіз систем та засобівмоніторингу волоконно-оптичнихлінійзв'язку, яківикористовуються у Збройних Силах України.

Основні положення. Запровадження волоконно-оптичних ліній зв'язку набуло дуже великих масштабів, використання волоконно-оптичних ліній зв'язку може надати майже необмежені можливості для швидкісної передачі інформації.Моніторинг та тестування ВОЛЗ, де вони розгорнуті, проводиться такими приладами як: рефлектометр для оптичних кабельних ліній, вимірювачі оптичної потужності, оптичний тестер, джерело лазерного випромінювання та інші.

Для контролю якості волоконно-оптичних ліній зв'язку шляхом вимірювання в них втрат необхідно і достатньо застосування двох типів вимірювальної апаратури. Це оптичні тестери (OLTS - OpticalLossTestSet), що дозволяють вимірювати повні втрати в лінії і оптичні рефлектометри (OTDR - OpticalTimeDomainReflectometer), за допомогою яких можна виміряти розподіл втрат уздовж лінії.

Властивості систем моніторингу ВОЛЗ:

– майже моментальне виявлення місця аварії чи пошкодження;

– проективне обслуговування;

– всеосяжна мережева документація;

– повний аналіз функціонування коректності роботи через Інтернет

– реєстр управління і сигналізації;

– ведуться журнали чергувань, також зберігається контактна інформація кожного інженера і у випадку аварії;

– моніторинг темних і робочих волокон;

– моніторинг темних волокон також простий і ефективний - система виявляє більше 80% пошкоджених кабелів.);

– безпека системи;

– можливість відновлення системи з резервного сервера і / або постійний сервер, який знаходиться в режимі готовності негайно замінити основний сервера в разі збою.

Що в себе включають профілактичні роботи ВОЛЗ:

вимірювання параметрів передачі незадіяних ОВ на ВОЛЗ (доцільно проводити в автоматичному режимі при оснащенні системою автоматичного моніторингу ОК);

вимірювання в ручному режимі характеристик активних ОВ на ВОЛЗ при наявності WDM мультиплексорів і фільтрів;

вимір опору ізоляції пластмасової оболонки ОК, що містить металеві конструктивні елементи (виконується по ділянках лінії, між оптичними муфтами);

контроль глибини залягання ОК і уточнення картограм проходження траси ВОЛЗ. Періодичність контролю глибини залягання ОК і вибір перевіряємих ділянок траси;

Основні відмінності різних моделей OTDR.

Відмінності ці можна описати наступними характеристиками: динамічний діапазон вимірювань OTDR, одно- або багатомодульна конструкція OTDR, функціонал оптичного модуля, розміри пристрою, ергономічність, операційна система, інтерфейс і інше.

Методи вимірювання параметрів ВОЛЗ в ручному режимі:

Таким чином ми можемо виміряти: оптичну довжину траси, кілометричне загасання ОВ, втрати на неоднорідностях.

Висновок: Волоконна оптика одна з провідних технологій нашого часу. Вона все більше набирає популярності через свої очевидні переваги. Експлуатація таких технологій вимагає постійного моніторингу для забезпечення безперебійної роботи. Може проводитись як оптичними рефлектометрами в ручному режимі так і автоматичному, без втручання особового складу. Автоматичний моніторинг може робити запис показників на сервер чи на визначене програмою місце накопичування задля аналізу волоконно-оптичних втрат, проблемних зон та аварій, які виникли в результаті експлуатації лінії передачі.

Провівши аналіз існуючих систем моніторингу та комплексів тестування волоконно-оптичних ліній зв'язку, було вирішено, що автоматизовані системи моніторингу більш практичні для використання у великих волоконно-оптичних мережах на дальніх відстанях, в свою чергу невеликі мережі можна тестувати без допомоги системи моніторингу, а лише окремими оптичними рефлектометрами, оптичними вимірювачами потужності та іншими засобами.

ЛІТЕРАТУРА

1. Кузнєцов О.Д.: Преминение оптоволокна.2000 – 105с.
2. СлєповМ.М.:Современные технологи цифровых оптоволоконных сетей связи, 2000-1510с.
3. Бутусов М.М. Волоконно – оптические системы передачи / Бутусов М.М., Верник С.М., Балкін С.Л. – М.: Радио и связь, 1992. – 416 с.
4. Гауэр Дж. Оптические системы связи / Гауэр Дж. – М.: Радио и связь, 1989. − 504с.
5. Голь В.Д./Дружченко С.С. К: Моніторинг і діагностика систем передачіSDH, 2002 - 96с.

Гаврилюк О. Г.
Ткач В. О.
Паламарчук С.А.

ОБҐРУНТУВАННЯ ОСНОВНИХ НАПРЯМІВ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Вступ

Досвід ведення операцій (бойових дій) останніх років свідчить про зростаючу роль інформаційних систем (ІС) спеціального призначення у досягненні мети операції (бойових дій). Специфічність ІС спеціального призначення полягає в тому, що, з однієї сторони, вони вирішують завдання передачі та обробки інформації, а, з іншої, повинні відповідати вимогам з живучості при впливі засобів противника.

З метою здійснення дезорганізації управління та досягнення інформаційної переваги противником широко застосовуються засоби радіоелектронного та кібернетичного впливу на ІС спеціального призначення. З огляду на це, кібератаки на ІС стали реальною загрозою і є однією з пріоритетних проблем національної безпеки та управління ризиками.

Визнання кіберпростору як сфери ведення бойових дій (операцій) вимагає зосередити увагу на захисті інформації та недопущенні втручання в процеси планування, управління, координації, контролю управління військами (силами), зброєю (озброєнням).

Для виконання спільних функцій у рамках підтримки операцій (об'єднаної операції) в кіберпросторі здійснюються заходи кіберрозвідки. Протидія реальним загрозам та мінімізація потенційних загроз потребує низки кроків держави в ключових сферах життєдіяльності, що мають особливе значення для забезпечення кібернетичної безпеки.

Метою доповіді є визначення основних напрямів забезпечення кібернетичної безпеки мереж спеціального призначення.

Виклад основного матеріалу дослідження

Проведемо обґрунтування основних напрямів забезпечення кібернетичної безпеки мереж спеціального призначення за групами декомпозиції:

1. У зовнішньополітичній сфері:

підвищувати роль України як активного учасника формування стандартів світової політики по відношенню до кіберпростору;

підтримувати міжнародні ініціативи у сфері кібербезпеки з урахуванням національних інтересів України; сприяти недопущенню мілітаризації кіберпростору;

неухильно дотримуватись взятих на себе міжнародних зобов'язань у сфері кібернетичної безпеки та боротьби з кібернетичною злочинністю;

підвищувати рівень міжнародного співробітництва у сфері забезпечення кібернетичної безпеки на загальнодержавному та відомчому рівнях;

сприяти створенню міжнародних правил поведінки держав у кіберпросторі та удосконаленню міжнародної нормативно-правової бази у відповідності до кібербезпекових викликів національній та міжнародній безпеці;

підтримувати як існуючі багатосторонні навчання із протидії кібернападам на державну та приватну інформаційну інфраструктуру, так і ініціювати нові види таких навчань.

2. У сфері державної та внутрішньополітичної безпеки:

створити Національну систему кібернетичної безпеки України;

встановити обов'язкові вимоги щодо кіберзахисту критичних об'єктів національної інформаційної інфраструктури в незалежності від форми власності, порядок захисту та контролю за його дотриманням;

здійснювати заходи реформування системи захисту інформації з обмеженим доступом з урахуванням реалій сьогодення задля уникнення витоків такої інформації;

посилювати технічні та технологічні можливості, науковий та людський потенціал Служби безпеки України, розвідувальних органів та Державної служби спеціального зв'язку і захисту інформації у кіберпросторі;

посилювати боротьбу з кібертероризмом та кібершпигунством, захист від їх проявів критичних об'єктів національної інформаційної інфраструктури;

забезпечити імплементацію положень Конвенції Ради Європи про кіберзлочинність у національне законодавство, зокрема, щодо:

– надання повноважень органам дізнання та слідства щодо видачі обов'язкових до виконання провайдерами приписів про термінове фіксування та подальше зберігання комп'ютерних даних, які потрібні для розкриття злочину;

– обов'язковості збереження провайдерами даних про трафік на строк до 90 днів із можливістю дальшого продовження терміну до 3 років;

– зобов'язання суб'єкта, який зберігає комп'ютерні данні, не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом визначеного законодавством періоду;

– надання провайдером органу дізнання або слідства інформації для ідентифікації постачальників послуг і маршруту, яким було передано інформацію;

– удосконалювати кримінальне законодавство, виділити окремі склади злочинів де об'єктом протиправних посягань є елементи національної критичної інформаційної інфраструктури;

– сприяти розвитку мережі команд реагування на комп'ютерні надзвичайні події (*CERT*);

3. У Збройних Силах України:

здійснювати підготовку до застосування Збройних Сил України в умовах "кібервійни";

створювати можливості для відбиття військової агресії в кіберпросторі з урахуванням нових викликів та загроз;

захищати військову інформаційну інфраструктуру від реальних та потенційних кіберзагроз;

створити систему підготовки кадрів у сфері кібербезпеки для потреб Збройних Сил України та інших органів сектору безпеки і оборони України;

створювати сприятливі умови для молодих фахівців в ІТ-сфері, що має сприяти їх працевлаштуванню в Україні;

підтримувати зусилля громадянського суспільства та бізнесу щодо підвищення обізнаності населення з актуальних кіберзагроз;

забезпечити безперервне підвищення кваліфікації державних службовців та працівників, що задіяні на ключових об'єктах критичної інфраструктури;

сприяти розробці вітчизняної інноваційної продукції, що може бути використана з метою посилення кібернетичної безпеки держави.

Висновки

За результатами проведеного дослідження встановлено, що забезпечення кібернетичної безпеки мереж спеціального призначення є комплексною проблемою, що вимагає комплексного підходу до її вирішення.

Проведено декомпозицію напрямків забезпечення кібернетичної безпеки мереж спеціального призначення. Відповідно до наведених напрямів необхідно сформулювати комплексну концепцію організації кібернетичної безпеки в інформаційних системах спеціального призначення, з прийняттям державних (управлінських) рішень для вироблення єдиних підходів забезпечення кібернетичної безпеки.

Гаман О.В.
Зінченко К.А.
д.т.н., с.н.с. Сова О.Я.

АНАЛІЗ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ІНТЕРНЕТУ БОЙОВИХ РЕЧЕЙ

Стрімке поширення Інтернету речей (Internet of Things, IoT) це наслідок розвитку машинного інтелекту та мережевих комунікацій, причому коли "речі" активно обмінюються інформацією, це приносить ще більше користі. Це стосується й інтелектуальної техніки на полях бою - Інтернету бойових речей (Internet of Battle Things, IoBT): такі «речі», обмінюючись даними, можуть бути корисними як солдатам у бою, так і командуванню при плануванні та проведенні бойових операцій. На сьогоднішній день IoBT вже реальність, але мине ще не один рік поки ця технологія охопить все поле бою.

Для втілення IoBT в життя потрібно вирішити цілу низку завдань:

- управління великою кількістю динамічних активів (кінцеві пристрої, мережеве обладнання, обчислюючі потужності і т.ін.);
- адаптація мережі, управління нею, а також її реорганізація за необхідності має здійснюватися в автономному режимі, без залучення персоналу;
- оперативне виділення корисної інформації з величезного потоку різнотипних даних, що генеруються елементами IoBT;
- захист мережевої та серверної інфраструктури від кібератак, а також можливих варіантів впливу на систему в цілому.

Інфраструктуру побудови IoBT умовно можна поділити на 3 компоненти.

Перша компонента являє собою кінцеві пристрої. Топологія їх підключення зазвичай виконана по схемі "зірка", і статистично більшу частину робочого часу пристрої знаходяться в режимі сну (щоб зекономити електроенергію, для збільшення часу автономної роботи). Такі пристрої зазвичай збирають інформацію, і за її наявності передають до центрів обробки даних, або приймають, як виконавчі пристрої. Фізично вони малогабаритні, так як мають невеликі акумуляторні батареї.

Друга компонента представлена у вигляді хабів-ретрансляторів, які можуть взаємодіяти між собою за схемою "mesh", частково можуть виконувати роль датчиків чи виконавчих пристроїв, але головною їх задачею є доставка повідомлень від (до) кінцевих пристроїв до (від) головних контролерів IoBT.

Вимоги до мережі на даному етапі: висока відмовостійкість (надійність), тривалий термін служби кінцевих пристроїв від одного заряду елементів живлення, підтримка великої кількості одночасних підключень, забезпечення достатнього рівня захисту інформації, яка передається.

Третя компонента забезпечує зв'язок IoBT з системами хмарного обчислення.

Особливості функціонування кожної із наведених компонент призводять до генерування трафіка різної природи, що, з одного боку, забезпечує повну ситуаційну обізнаність, а з іншого боку - ускладнює процеси керування мережевою інфраструктурою. У зв'язку з цим, виникає потреба розробки нових та вдосконалення існуючих механізмів обробки даних в системах управління мережевою інфраструктурою IoBT.

Метою подальшого дослідження є розробка методики, що дозволяє обробляти різнотипні дані в інтелектуальних системах управління мережевою інфраструктурою IoBT.

D. Harmash (ХНУ ім.Каразіна)
A. Maleeva (ХНУ ім.Каразіна)

ABILITY OF RAINBOW ALGORITHM TO COUNTER VARIOUS METHODS OF CRYPTOANALYSIS

Multidimensional quadratic schemes are a promising solution for the needs of quantum systems that are resistant to attacks from a quantum computer. However, because this class is relatively young and many circuits of this class have been violated in the past, there are very few implementations, especially on embedded microcontrollers. To assess whether these schemes can ever replace existing standards, it is necessary to know how effectively they can be implemented on different platforms. In the course of this work the theoretical introduction to multidimensional quadratic schemes is given.

1. Ability to resist attacks Rainbow algorithm.

A brief cryptanalysis of the Rainbow signature scheme is presented, considering it for the above example. There are several attack methods that users of the algorithm will deal with. For those methods where square shapes are used, keep in mind that the theory of square shapes over finite fields differs when the characteristic is 2, compared to the case when the characteristic is odd.

1.1. Rank reduction method

The method of decreasing rank is used to break the scheme of signing the birational permutation of Shamir. The reason this attack can work is that the space covered by the polynomial components of the Shamir scheme cipher consists of a space flag: $V1 \subset V2 \subset \cdots \subset Vt$,

where V_t – the space covered by the polynomial components of the cipher, each V_i is its own subset V_{t+1}, and the rank of the corresponding bilinear form, which corresponds to the elements in $V_{t+1} - V_i$,

much more, then in V_i, and the size difference between V_i and V_{t+1} equals 1. Due to these properties, in particular the latter, it makes it easy to find this flag of space, namely all V_i, first found V_{n-1}, then V_{n-2} and so on by decreasing rank [8]. But this method of attack can no longer work against this scheme. The reason for this is that, in our case, there is also such a flag of spaces that the number of components is exactly the number of levels, the dimension of each component of the flag exactly corresponds to the size V_{i+1}, $i = 1,...,u-1$, but the difference in the size of the last two large spaces is for sure $O_u - 1$, which was chosen specifically for a fairly large number 11, in contrast to the case of Shamir, when it is equal to 1. The property listed above is the reason that the attack can no longer work. Impossible to use the downgrade method here because $O_u - 1 = 11$ The "last thick Oil level" allows the scheme to resist the onslaught of demotion.

1.2Attack method of Oil-Vinegar schemes

The analysis showed that the action L_1 is to mix all polynomial components F. Therefore, each component of the cipher F now belongs to the upper level of the Oil-Vinegar polynomials, and they are all elements P_4. These are Oil-Vinegar polynomials with 22 Vinegar variables and 11 Oil variables. In this case, you can use the method for an unbalanced Oil-Vinegar signature scheme to try to attack the system, which will separate the variables of the top layer of Oil-Vinegar. To do this, we need to divide the upper (or final) level from 11 variables Oil and 22 variables Vinegar. According to cryptanalysis, the complexity of the attack of this first step is $q^{22-11-1} \times 11^4 > 2^{90}$.

2.3. Minrank method

There are two completely different ways to use the Minrank method. The first is the search for a polynomial whose associated matrix has the lowest rank among all possible variants. This set of polynomials with 6 variables Vinegar and 6 Oil belongs to the first level, ie $P1$, and specified as $F\tilde{}_1$. To do this, we first bind to each polynomial a bilinear form that has a matrix of size 33×33. We can then use linear combinations of matrices associated with the components F, to derive a polynomial associated with a matrix of rank 12. In this case, to attack the system, the problem is to find a matrix of rank 12 among a group of 27 matrices of size 33×33. From the method of the Ministry of Finance, we know that the difficulty of finding such a matrix is $q^{12} \times 27^3$, which is much more than 2100. Another possibility is to find polynomials that correspond to polynomials in the second last level, namely the one that belongs to P_3 and comes from linear combinations $F\tilde{}_i, i < 4$.

In this case, Miranka's method can definitely not be used, because they generally have a rank of 22. One way, of course, is a random search. Since the dimension P3 is 16, it becomes a problem to find the element in the dimension subspace, in the total dimension space 27. Therefore, such a random search requires at least q^{11} searches to find it, but we also need to determine if it really ranks below 22 for each search. In this case, the overall complexity should be at least $q^{11} \times (22 \times 33^2 / 3) > 2^{100}$. This idea of attack is actually related to another method of attack, and the above argument explains why this method can no longer work.

Conclusions

Rainbow's signature scheme looks robust against a large number of cryptocurrency methods and attacks through third-party channels. Implementation of quantum-protected algorithms requires large material and technical resources. This is due to the large key lengths and general parameters. The current level of technology allows you to be optimistic about the possibility of effective implementation of quantum-protected algorithms.

к.т.н. Голобородько М.Ю. (ЦВСД НУОУ імені Івана Черняховського)
к.т.н. Гречанінов В.Ф. (ІПММС НАНУ)

СУЧАСНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ РОБОТИ ПРАЦІВНИКІВ НАУКОВО-ДОСЛІДНИХ УСТАНОВ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ У ВІДДАЛЕНОМУ РЕЖИМІ

Провідні країни світу вже давно використовують альтернативні способи організації праці. Їх досвід демонструє певні переваги дистанційної роботи працівників. Компанії мають від цього певні фінансові вигоди, оскільки економлять на витратах на оренду приміщень, електроенергію, техніку, витратні матеріали тощо.

Пандемія гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2, дала суттєвий поштовх для переосмислення стандартної організації роботи у наукових установах Міністерства оборони України відповідно до затвердженого розпорядку дня за визначеним робочим місцем. Але досі залишаються невирішеними безліч юридичних, технологічних та технічних питань стосовно переведення наукових працівників на віддалений режим роботи, зокрема це питання щодо опрацювання, погодження та, саме головне, визнання на відомчому рівні певного порядку (алгоритму), в основі якого буде письмовий договір між науковим працівником та керівником установи, за умовами якого науковий працівник зобов'язується виконувати передбачену його функціональними обов'язками (посадовою інструкцією) роботу поза межами установи відповідно до затвердженого плану наукової та науково-технічної діяльності, а керівник установи зобов'язується виплачувати науковому працівникові грошове забезпечення (заробітну плату) й забезпечувати умови його роботи (інформаційно-комунікаційне забезпечення), необхідні для виконання завдань за призначенням.

Виходячи із зазначеного обов'язковою вимогою щодо забезпечення віддаленого режиму роботи є наявність відповідних технічних можливостей як з боку наукової установи, так і з боку наукового працівника.

Згідно з дослідженням компанії "Cisco", до пандемії тільки у 19% компаній більше половини працівників працювали у віддаленому форматі, наразі – 62%, а коли людство нарешті впорається з вірусом, очікується, що віддалена робота залишиться основною у 37% компаній у всьому світі. За результатами проведеного компанією "IT-Інтегратор" аналізу слідує, що тенденція переходу на віддалений режим роботи призвела до значного росту в Україні кількості та якості кібератак, спрямованих на прогалини в забезпеченні безпеки інформаційних ресурсів. На їх переконання є два ключових правила, про які потрібно пам'ятати керівництву установи для успішного переведення працівників на дистанційну роботу: по-перше, потрібно забезпечити безпечне робоче середовище на стороні користувача; по-друге, необхідно забезпечити цілодобовий доступ до корпоративних ресурсів і даних установи, надійно захистивши їх від кібератак.

Дуже часто з міркувань економії використовують одне або рідше кілька типових технічних рішень і підходів для забезпечення безпеки, таких як міжмережевий екран та антивірус. Але довід компанії "IT-Інтегратор" стосовно створення сучасних інформаційних систем, свідчить, що цього не достатньо щоб уникнути атак і витоків даних. Тому щоб захищати свою IT-інфраструктуру доцільно використовувати комплекс рішень, зокрема:

1. Захист на стороні користувача, що передбачає:

безпечне підключення до мережі;

перевірку безпеки пристрою, який підключається;

верифікацію того, хто намагається підключитися до корпоративної мережі.

Зазвичай наукові працівники підключаються з особистого пристрою (персональний комп'ютер, планшет, смартфон тощо), а це пов'язано з підвищеними ризиками. Наприклад, користувач може підключатися до корпоративної мережі установи за допомогою імовірно ураженого шкідливим програмним забезпеченням пристрою. Згодом зазначене шкідливе

програмне забезпечення може вразити всі пристрої, що підключені до корпоративної мережі, зокрема сервера центру оброблення даних, та завдати непоправної шкоди установі через виток або втрату даних. Для захисту від таких ризиків недостатньо мати лише класичний антивірус, тому що він не може забезпечити комплексний захист корпоративної мережі установи. Фахівці компанії "IT-Інтегратор", для забезпечення безпечного віддаленого доступу працівників до корпоративних ресурсів пропонують використовувати сучасні рішення щодо захисту від шкідливого коду в комплексі з багатофакторною аутентифікацією, і автоматизованою перевіркою безпеки пристрою, що підключається. Також, на їх думку, дуже важливо забезпечити можливість автоматизації налаштування всіх цих компонентів на віддаленому робочому місці.У якості комплексного варіанту для захисту від кіберзагроз доцільно застосовувати рішення компанії "Cisco", зокрема Cisco AMP, CiscoAnyConnect у комплекті з функціоналом VPN (Virtual Private Network), CiscoDuo тощо. Станом на цей час зазначені рішення найкращим чином зарекомендували себе у всьому світі.

Слід зауважити про найбільш спірний та досі нормативно неврегульований аспект віддаленої роботи це контроль продуктивності працівників з боку керівництва установи. У цьому питанні можуть допомогти рішення класу UAM (User Activity Monitoring). Саме рішення класу UAM надає роботодавцю ефективний інструмент ведення докладної статистики продуктивності працівників та попередження витоку службової інформації.

Для наукових працівників, що працюватимуть у віддаленому режимі, UAM є дієвим інструментом кількісного виміру і демонстрації керівництву установи власної ефективності. Також слід зазначити, що конфіденційність працівника завжди залишається під його особистим контролем: для запуску агентської частини UAM потрібно ввести облікові дані, тільки після цього активуються функції моніторингу продуктивності.

Розгортати UAM в умовах суворого карантину найкраще з хмари, отримавши його як сервіс. В цьому випадку програмне забезпечення достатньо завантажити з хмарної консолі управління і встановити на персональний комп'ютер. Головна перевага такого формату, це безперервність сервісу незалежно від того, з якої мережі і з якого пристрою (власного або корпоративного) підключається працівник.

Водночас за умови віддаленої роботи важливо зберегти звичне зручне середовище, мати можливість проводити наради і контролювати обмін робочими матеріалами та потрібною інформацією. Для цього рекомендується використовувати сервіси організації спільної роботи, наприклад Cisco Webex Meetings. Цей сервіс надає спільний віртуальний простір для роботи, обміну повідомленнями, перегляду робочих файлів, організації відеозустрічей та багато іншого.

Оскільки віддалені робочі місця працівників фактично стають частиною корпоративного середовища, вони так само, як і корпоративні, потребують централізованого управління, діагностики та моніторингу. У цьому може допомогти система класу MDM (Mobile Device Management). Наприклад, Cisco Meraki.

Поєднання перерахованих рішень дозволить забезпечити базовий рівень безпеки віддаленого формату роботи для науково-дослідних установ Міністерства оборони України.

2. Захист на стороні установи-роботодавця

Корпоративні ресурси установи традиційно набагато краще захищені, оскільки у них є можливість краще контролювати політики інформаційної безпеки і, що дуже важливо, реалізувати централізоване резервне копіювання критичних даних. Щоб забезпечити цілодобовий доступ до корпоративних систем установи і зберегти їх в безпеці, рекомендується використовувати рішення класу VDI (Virtual Desktop Infrastructure). Рішення VDI допомагає істотно підвищити захищеність від кібератак, а також дає можливість оперативно відновити працездатність віддалених робочих місць. Наразі компанією "IT-Інтегратор" в інтересах Міністерства оборони України створюється відповідна Інформаційна інфраструктура, яка вже у найближчий час буде здатна за необхідності забезпечувати користувачів Міністерства оборони України зазначеними сервісами, зокрема забезпечувати віддалений режим роботи наукових працівників науково-дослідних установ.

к.т.н. Голобородько М.Ю. (ЦВСД НУОУ імені Івана Черняховського)
к.т.н. Гречанінов В.Ф. (ІПММС НАНУ)

МЕРЕЖА СИТУАЦІЙНИХ ЦЕНТРІВ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ ЯК ІНСТРУМЕНТАРІЙ ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Державне управління національною безпекою – це специфічний вид управління, який охоплює усі сфери життя та пов'язаний з безпекою суспільства, захистом національних цінностей та інтересів. Спеціалісти, робота яких пов'язана з експертно-аналітичною, консультативно-дорадчою та організаційно-розпорядчою діяльністю у сфері національної безпеки, зіштовхуються зі складними й неструктурованими управлінськими завданнями та повинні оперативно обґрунтовувати рішення в умовах невизначеності та нестачі часу, зважати на значну кількість чинників, іноді досить суперечливих. Це обумовлює необхідність належного інформаційно-аналітичного забезпечення зазначених процесів.

Ключовим елементом інструментарію стратегічного управління у сфері національної безпеки повинна стати єдина мережа ситуаційних центрів органів державної влади сектору безпеки і оборони та забезпечення інформаційної сумісності їх функціонування шляхом створення єдиного інформаційного середовища. До основних аспектів ефективності мережі ситуаційних центрів належить поглиблена аналітична обробка інформації, моделювання можливого розвитку ситуацій, візуалізація результатів моделювання, використання формалізованих і неформалізованих знань, методів мозкового штурму, залучення резервів образного асоціативного мислення. На даний час у Сполучених Штатах Америки та країнах Європейського союзу у сфері безпеки і оборони вже створені та працюють мережі ситуаційних центрів, які обробляють інформацію політичного, економічного, розвідувального та військового характеру. В Україні кожен орган державної влади, в тому числі і сектора безпеки і оборони, має відповідних спеціалістів (експертів, аналітиків), які, створюють і розвивають бази знань щодо можливих кризових ситуацій та сценаріїв їх нейтралізації з оцінкою можливих наслідків для держави; свій науково-методичний та технологічний апарат створення та наповнення відповідних баз даних; свої системи автоматизованої підтримки процесу прийняття рішень з питань, які підпадають під його компетенцію, але, з ряду причин, діють достатньо автономно, не враховуючи позицію та можливості інших державних органів. Це найчастіше призводить до певних непорозумінь, протиріч, звинувачень один одного, суттєвого збільшення часу та матеріальних ресурсів, необхідних для виходу з певної кризової ситуації. Існуючий стан справ не є задовільним для будь-якої країни, а для України, в умовах гібридної агресії та анексії частини її території, є особливо неприпустимим. Виходячи з цього, вкрай необхідно створити умови для оперативної взаємодії всіх органів державної влади сектора безпеки й оборони, зокрема:

запровадити єдину автоматизовану систему підтримки прийняття як колективних, так і індивідуальних державних рішень, у вигляді мережі ситуаційних центрів органів державної влади сектора безпеки і оборони України;

забезпечити інформаційну сумісність діяльності органів державної влади сектора безпеки і оборони створивши єдине інформаційне середовище шляхом об'єднання програмно-апаратних засобів ситуаційних центрів, баз даних та знань, науково-методичного апарату, досвіду та спроможностей відповідних фахівців (експертів, аналітиків);

вирішити питання створення сукупності захищених інформаційних мереж, як технічної основи для забезпечення швидкодіючих горизонтальних і вертикальних каналів обміну інформацією між органами державної влади сектора безпеки й оборони. Зазначене дозволить поєднати можливості керівників вищих щаблів органів державної влади сектору безпеки і оборони, сучасних досягнень техніки та інформаційних технологій чим забезпечить автоматизацію процесів підтримки прийняття управлінських рішень у сфері національної безпеки та підвищення ефективності зазначеного роду діяльності в умовах невизначеності та нестачі часу.

Гопанчук Ю.О. (ВІТІ)
к.т.н. Гурський Т.Г. (ВІТІ)
Цімура Ю.В. (ВІТІ)

УДОСКОНАЛЕННЯ СИСТЕМ РАДІОЗВ'ЯЗКУ З ППРЧ ЗА РАХУНОК АДАПТИВНОЇ ЗМІНИ ЇХ ПАРАМЕТРІВ

Актуальним завданням в умовах постійного вдосконалення можливостей систем радіоелетронного подавлення (РЕП) є підвищення завадозахищеності систем військового радіозв'язку (СВРЗ). Найбільш поширеним способом вирішення цього завдання є застосування методу псевдовипадкового переналаштування робочої частоти (ППРЧ).

Аналіз технічних характеристик та можливостей сучасних СВРЗ з ППРЧ дозволив виявити їх основний недолік – відсутність автоматичної адаптації до завадової обстановки в каналі зв'язку.

Тому актуальним завданням є визначення напрямків удосконалення СВРЗ з ППРЧ та способів його реалізації.

Підвищення завадозахищеності при забезпеченні заданих швидкостей передачі та дальності зв'язку при впливі навмисних завад, в залежності від їх типу та характеристик, можна досягнути наступними заходами:

зміна ширини смуги ППРЧ (хопсета), її центральної частоти;

збільшення потужності передавача;

відключення частот (припинення передачі корисної інформації), перекритих завадами;

зміна швидкості переналаштування частоти;

раціональне планування сукупності радіомереж для роботи у спільному частотному діапазоні.

У сучасних ЗРЗ з ППРЧ зміну ширини хопсета можливо реалізувати двома шляхами:

перший дозволяє змінювати відповідні налаштування на радіостанції;

другий полягає у створенні запасних каналів з хопсетами в інших ділянках робочого діапазону частот, та/або з хопсетами з більшою (меншою) шириною.

В обох випадках успішність функціонування радіомережі визначатиметься організаційними заходами, які визначать порядок входження в зв'язок у випадку впливу засобів РЕП, та досвідом операторів (користувачів). Слід зауважити, що зі збільшенням ширини хопсета погіршується якість зв'язку, а отже – зменшується дальність зв'язку. Якщо дальність необхідно зберегти на тому ж рівні – слід зменшувати швидкість передачі інформації.

Подібні міркування справедливі і для зміни швидкості стрибків частоти (її можна змінити вручну, або заздалегідь підготувати відповідні запасні канали, а із зростанням швидкості стрибків знижується якість радіоканалу).

Тому напрямком удосконалення радіозасобів при впливі навмисних завад є розробка методик вибору параметрів радіостанцій, які дозволять без участі оператора забезпечувати автоматичний вибір необхідної середньої частоти та ширини хопсета, швидкості стрибків частоти, потужності передавача, кількості активних (невідключених) частот у хопсеті для забезпечення заданої швидкості, якості та дальності зв'язку.

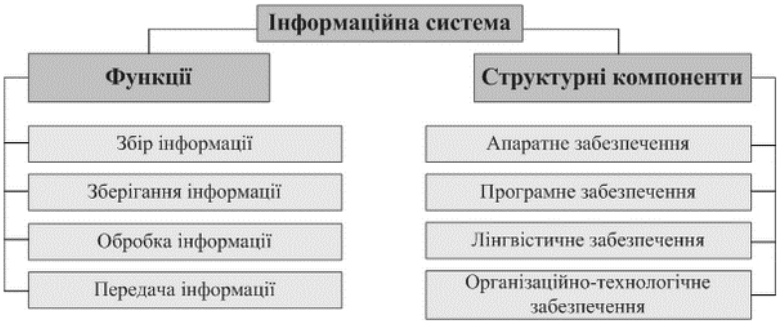
Для практичної реалізації таких методик доцільно обмежити крок дискретності при зміні допустимих значень параметрів радіозасобів, а також використати математичний апарат теорії ігор та нечіткої логіки для прогнозування стратегії системи РЕП. Першочерговим завданням для практичного впровадження таких методик є реалізація процедур оцінки стану каналу, ідентифікації типу завад, поточних значень їх параметрів та стратегії постановника завад в цілому.

к.т.н. Горбенко В.І. (ВІТІ ім. Героїв Крут)
Голота Р.С. (ВІТІ ім. Героїв Крут)

МОДУЛЬ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ «АРХІТЕКТУРА ОБЧИСЛЮВАЛЬНИХ СИСТЕМ» ВИЩОГО ВІЙСЬКОВОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Створення та функціонування інформаційного забезпечення в процесах управління підрозділами (частинами) Збройних Сил України тісно пов'язане з розвитком інформаційних технологій. Сучасна інформаційна технологія орієнтована на застосування найширшого спектру технічних засобів електронно-обчислювальних машин і засобів комунікацій. Створюючи модуль інформаційного забезпечення дисципліни «Архітектура обчислювальних систем» вищого військового навчального закладу (ВВНЗ) необхідно врахувати розробку зручного інтерфейсу для користуванням модулем, застосувати компоненти які реалізують технологію клієнт-сервер, а також реалізувати можливості пошуку інформації у базі даних (БД). Модуль містить вікно входу, яке ідентифікує та авторизує користувача за двома параметрами: курсант чи викладач. Основна частина модуля – головне вікно програми, на якому знаходиться головне меню програми та основні елементи, які дозволять викладачузручно проводити заняття. За допомогою цієї частини викладач керує основними таблицями БД та веде облік поточних балів по кожному курсанту. Завдяки модулю, викладач також має змогу автоматично згенерувати журнал по поточним оцінкам в групах, редагувати та створювати презентації в *PowerPoint*, зберігати та розробляти навчально методичні матеріали для усіх видів занять. Модуль буде комунікувати з *Telegram* для створення робочих груп по дисципліні. Курсант може бачити поточний рейтинг своєї групи, свій власний рейтинг в групі та кількість балів. Модуль також надає можливість користуватися різною документацією та електронними посібниками. У модулі знаходяться всі потрібні інструменти та методичні посібники для програмування мовою *Assembler*.

Інформаційне забезпечення дисципліни Архітектура обчислювальних систем є складовою інформаційної системи, яка реалізує функції збирання, зберігання, розповсюдження і



обробки інформації. На рисунку наведені функції інформаційної системи через її структурні компоненти. Отже, в доповіді проаналізовано основні можливості та компоненти модуля інформаційного забезпечення дисципліни «Архітектура обчислювальних систем» ВВНЗ, який дозволить викладачу проводити заняття в умовах Covid-19, представлено структуру та алгоритм його роботи.

ЛІТЕРАТУРА

1. ДСТУ 2392-94 Інформація та документація. Базові поняття.

2. Горбенко В.І., Сілко О.В. Програмування мовою асемблера Intel-сумісних мікропроцесорів. Навч. посібник. – К: ВІТІ НТУУ КПІ, 2009. – 180 с.

3. Горбенко В.І., Сілко О.В, Нестеренко М.М. Системне програмування та архітектура комп'ютерів. Навч. посібник. К: ВІТІ, 2018. 176 с.

к.т.н. Горбенко В.І. (ВІТІ ім. Героїв Крут)
Коник О.Я. (ВІТІ ім. Героїв Крут)

МОДУЛЬ ОБЛІКУ ТА РУХУ ЗАСОБІВ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ НАВЧАЛЬНО-ЛАБОРАТОРНОГО КОМПЛЕКСУ КАФЕДРИ ВВНЗ

Автоматизація повсякденної діяльності ЗСУ, зокрема обліку та руху засобів обчислювальної техніки (ОТ) підрозділів залишається актуальним завданням. У доповіді пропонується вирішення цього завдання шляхом розробки відповідного модуля для навчально-лабораторного комплексу (НЛК) кафедри ВВНЗ. При створенні та розробцімодулю необхідно врахувати реалізацію візуально приємного та зручного інтерфейсу користувача, використати компоненти які реалізують технологію клієнт-сервер з метою пошуку потрібної інформації в базі даних (БД).Базою модуля є головне вікно, де знаходяться основні функції та головне меню, які дозволяють організувати та спростити роботу працівника НЛК. Завдяки цьому працівник НЛК має змогу вводити параметри запитів до БД, що забезпечує фільтрування та пошук потрібної інформації, керувати основними таблицями БД та вести облік майна. Головне меню виступає “основою” для взаємодії з іншими віконними формами програми, а також забезпечує візуалізацію та редагування інформації, що міститься у БД. За своєю структурою модуль складається з чотирьох блоків. Кожен із блоків має своє чітко визначене призначення, яке полягає в реалізації певної функції модуля.

Перелік блоків:

1. Блок взаємодії з користувачем – відповідає за діалог користувача з модулем;
2. Блок управління забезпечує роботу з БД та управлінням даними, що в ній знаходяться;
3. Блок доступу до БД дозволяє доступатися до даних використовуючи *ORM*технологію, яка реалізована в бібліотеці *FluentNhibernate*;
4. Блок обміну даними відповідає за дії, що надає модуль для роботи з БД, а саме: додавання, редагування та видалення даних.

Функціональні залежності між блоками представлені на узагальненій структурній схемі модуля і забезпечують доступ до БД, взаємодію з користувачем, обмін даними та управління.

Отже, в доповіді аналіз бліку та руху майна у ЗСУ, надається структура модуля та обгрунтовується вибір засобів його реалізації.

ЛІТЕРАТУРА

1. Облік військового майна у Збройних Силах України: [посіб. для фахівців бюдж. військ, частин, установ та орг. Збройних Сил України] / [О.І. Ворона, Р.Т. Джога, В.В. Ткаченко, Г.О. Іва- нов, В.Л. Рихтюк]. – К.: Знання України, 2017. – 512 с.

Ph.D Viktor Grechaninov, IMMSP NASU
Ph.D Mihajlo Androsenko, IMMSP NASU
Anatoliy Lopushanskyi, IMMSP NASU

APPLICATION OF A STATIC DICTIONARY FOR INFORMATION EXCHANGE BETWEEN COMPONENTS OF INFORMATION SYSTEMS IN A SPECIAL PERIOD

Relevance. In modern information systems (IS) there is a need to transfer large amounts of information between its components through telecommunication systems and networks. Most information systems are based on the use of relational databases (DB). It is recommended to exchange information between such ISs using the XML format, which is textual and has a known information redundancy due to the use of a significant number of tags and the representation of the numerical values of the fields of the database tables in text form in HEX encoding, which gives double redundancy even without taking into account special text characters. The JSON format is less redundant and it is often used when creating online services. However, JSON is also textual and has a slight redundancy advantage over XML.

In the presence of modern high-speed telecommunication systems and networks, the issue of redundancy is not relevant. Preference is given to text formats that are more visual and easier to use when creating (programming) information exchange between components of IS and between different types of IS.

However, under the conditions of a special period, there is a possibility of the state of functioning of telecommunication systems and networks in the presence of passive and active interference with the communication radio signal and the absence of wire lines. In such conditions, when using anti-jamming technologies, the capabilities of communication facilities in terms of the digital data transmission rate are sharply reduced, and, if it is necessary to transfer significant volumes, these capabilities can go beyond the acceptable efficiency.

Problem Statement. There is an urgent task to develop new approaches to the organization of information exchange between a IS components of the critical infrastructure.

Main provisions. One of the options for solving this problem is to eliminate the statistical redundancy of the XML format by developing special methods for its processing, as it was developed by the author for the Microsoft Office 2007-2013 - docx format. However, if the developer has the structure of a relational IS database, it is proposed to use a static dictionary compression method, in contrast to the dynamic one available with well-known archivers. As a static dictionary, it is proposed to use the names of tables and their fields, which are intended for information exchange and, accordingly, are present in XML format. This approach allows each table and its fields to be identified by their numbers, respectively, in the database and in the table (one or two bytes). In this case, the field numbers of the tables will match, which has a positive effect on the compression ratio when using statistical encoding or one of the available archivers.

When encoding the numerical values of tables fields, redundancy reduction is possible if, in the development of the IS, we use exactly those types of numeric fields that are sufficient for the practical use of the IS.

Thus, when using a static dictionary and binary encoding, it is possible to significantly reduce the amount of data to be transferred. With binary encoding, there is no need to use special characters to denote tags and field values, as is done in XML and JSON formats. The compression capabilities of archivers in the binary version of the input information will be used to compress mainly the information itself, rather than a significant number of special characters in XML and JSON text formats.

Conclusion. This approach to information encoding will allow for information exchange between the components of the IS in difficult conditions of a special period with a significant improvement in efficiency indicators.

Гримуд А.Г. (ВІТІ)

АНАЛІЗАЛГОРИТМІВ ПОШУКУНАЙКОРОТШОГО МАРШРУТУ ОБЛЬОТУ ТЕЛЕКОМУНІКАЦІЙНОЮ АЕРОПЛАТФОРМОЮКЛАСТЕРИЗОВАНИХВУЗЛІВ НАЗЕМНОЇ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Одним з завдань збору даних моніторингу телекомунікаційною аероплатформою (ТА) з вузлів наземної безпроводової сенсорної мережі (БСМ) військового призначення є прокладання маршруту (траєкторії) їх обльоту.

Для скорочення часу збору даних моніторингу з вузлів БСМ, розміщених на місцевості, пропонується:

провести віртуальну кластеризацію мережі (наприклад, за алгоритмами кластерного аналізу FOREL або *k*-середніх);

визначити точки збору даних ТА з вузлів в кожному кластері (положення ТА у просторі) в залежності від цільової функції управління БСМ;

побудувати найкоротший маршрут обльоту ТА точок збору даних.

Останнє завдання розглядається як рішення задачі комівояжера. Для її рішення запропонована значна кількість алгоритмів (методів): повного перебору, найближчого сусіда, за спіраллю, FPPWR (FastPathPlanningwithRules), ConvexHullInsertionHeuristic(CHIS) та інші. Рішення задачі комівояжера відноситься до класу NP-складних. Отримання точного рішення для мережі значної складності проблематично. Тому на практиці застосовують алгоритми (методи) отримання приблизного рішення.

Алгоритм найближчого сусіда визначає наступну точку збору даних, яка ближче знаходиться до точки поточного положення ТА. В алгоритмі FPPWR мережа поділяється на квадрати, наступна точка обльоту визначається в найближчому квадраті по горизонталі. Алгоритм за спіраллю визначає маршрут обльоту за зовнішню областю розміщення вузлів в вигляді спіралі. Алгоритм CHIS складається з початкової обгортки всієї множини точок по зовнішньому радіусу, після чого вибирається початкова точка та напрямок руху до подальшої точки за певними критеріями.

Здійснена програмна реалізація (в середовищі C#) основних алгоритмів рішення задачі комівояжера для мережі розмірності 100, 200, 500 вузлів. За допомогою алгоритму FORELздійснена кластеризація мережі на 7 – 17 кластерів (зміна зони покриття ТА), побудовані маршрути обльоту згідно визначених алгоритмів пошуку найкоротшого шляху. Результати моделювання – залежності довжини маршруту від кількості кластерів наведені на рис. 1.

Метод повного перебору є актуальним для мереж, які мають до 10 кластерів. Кращі показники (коротші маршрути обльоту) для кластеризованої мережі продемонстрував алгоритм Convex Hull Insertion Heuristic (до 15 % коротші маршрути в порівнянні з іншими).

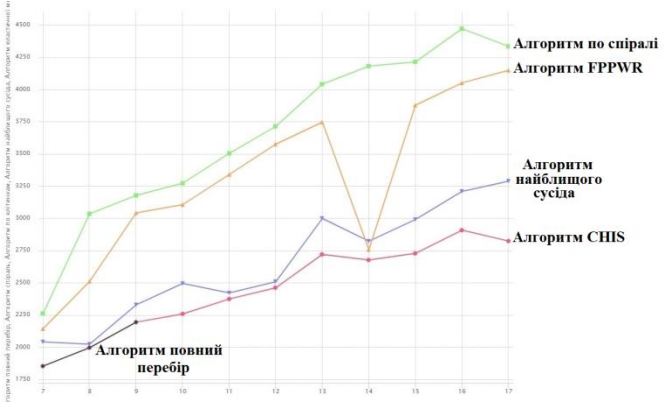


Рис. 1. Результати моделювання

Таким чином, метод CHIS (Convex Hull Insertion Heuristic) забезпечує кращу оптимізацію маршруту руху ТА з метою мінімізації часу доставки інформації моніторингу користувачеві і подальшому буде запропонована його модифікація.

A. Hrymud (MITI)
d.t.s. V. Romaniuk (MITI)
PhD Ye. Stepanenko (A0106)

MODEL FOR TEMPORAL CLUSTERING OF A WIRELESS SENSOR NETWORK BY A TELECOMMUNICATION AERIAL PLATFORM FOR MONITORING DATA COLLECTION

The method of direct data collection from military wireless sensor network (WSN) nodes of use by telecommunication aerial platform (TA), which in the basic version needs telecommunication aerial platform flying around each sensor node or flying around the whole territory of nodes placement on the battlefield, etc., is considered [1]. The main advantage of the direct data collection method is the absence of additional algorithms to control the process of data transmission in sensor nodes with the telecommunications aerial platform, which leads to a significant simplification of node control system and cheaper equipment of nodes in general; the main drawbacks - very long time of data collection and increasing the requirements for flight time TA.

To eliminate these disadvantages, it is proposed to combine nodes into temporary clusters with the help of TA, that is, it is proposed to put a role of the main node of the cluster on TA [2]. Ground control center (CC) of the network (or itself TA in conditions of autonomous flight), which has information about the coordinates of nodes position, calculates data collection points (determines the position of TA in space), for example, as the center of mass of the virtual cluster. In contrast to existing centroid clustering algorithms, it is proposed to use two clustering algorithms, k-means and FOREL (FORmal ELement), which are characterized by lower computational complexity.

After determining the data collection points, the control center (or TA) calculates the so-called basic trajectory of the TA flight (route and altitude) between them. A modified ConvexHullInsertionHeuristicmethod is proposed to solve the traveling salesman problem. Then TA flies along the route to the defined collection points and collects monitoring data from the nodes of each cluster.

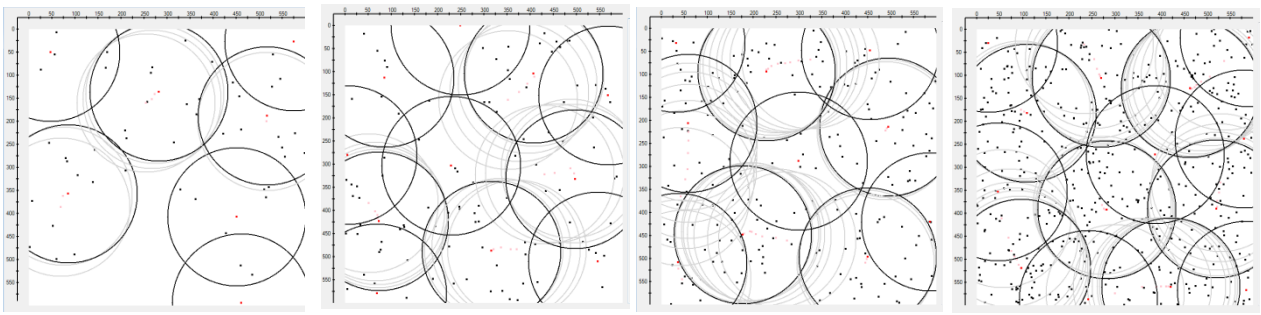
It is proposed to modify the FOREL and k-means algorithms taking into account the target control functions of the WSN during monitoring data collection.

It is proposed to modify the FOREL and k-means algorithms, considering the target control functions of the WSN during monitoring data collection.

The FOREL algorithm (FORmal ELement) is an algorithm for cluster analysis, which solves the clustering problem by minimizing the total quadratic deviation of cluster elements (network nodes) from the centers of mass of these clusters.

The cluster size is specified in the FOREL algorithm (in our case the size of TA coverage area). In two-dimensional geometric plane problem, R is the maximum distance from a cluster element to its center of mass (radius). Each element is also considered as a point on the plot and characterized by its coordinates (x_j, y_j).

Fig. 1 shows the results of the clustering of WSNs size n = 50, 100, 200 and 500 nodes using FOREL algorithm in C# environment. As a result of clustering, the WSN was divided into 7 clusters in a network of 50 nodes, 12 clusters in a network of 100 nodes, 10 clusters in a network of 200 nodes, 14 clusters in a network of 500 nodes.



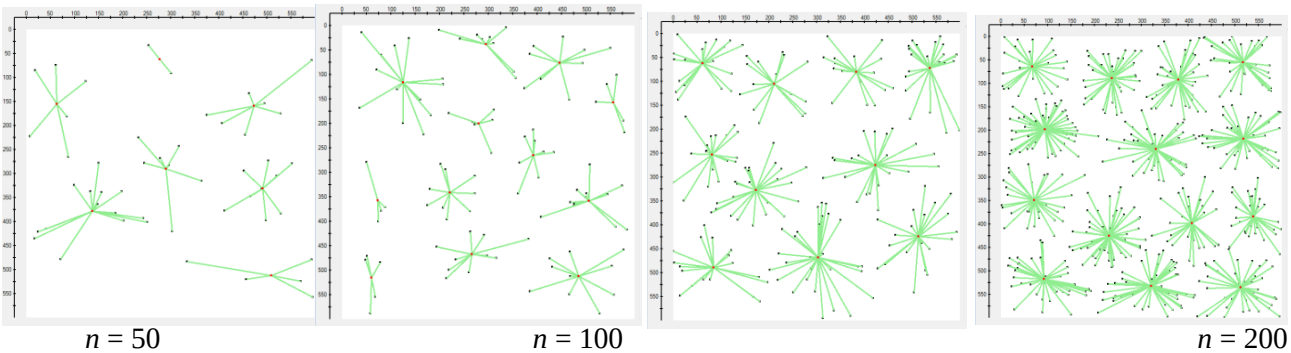
n = 50 n = 100 n = 200 n = 500

Fig. 1. Results of network clustering (FOREL method)

From the classical approaches to the implementation of FOREL when solving the data collection problem, we propose its modification (adaptation of the coverage area and taking into account the number of nodes in the cluster; the initial cluster is created in the place of the largest concentration of nodes) in order to

implement the target control functions (minimum collection time or maximum WSN functioning time) and consider resource restrictions.

The k-means algorithm is a classical variant of the algorithm which solves the cluster analysis problem by minimizing the total quadratic deviation of cluster elements from the centers of these clusters. The function of the minimization can be written as: як: $M = \sum_{i=1}^{k} \sum_{x_j \in S_i} (x_j - \mu_i)^2$, where k – number of clusters, S_i– multiplicity of the elements for i-th cluster; μ_i- coordinates to the mass center for i-th cluster; x_j– coordinates to the mass center for j-th element of the cluster. The value $(x_j - \mu_i)$ represent the euclidean distance between the cluster element and the center of the cluster mass. Fig. 2. shows the results of the clustering of the WSN size $n = 50$, 100, 200 and 500 nodes using the k-means method in the C# environment. As a result of clustering, the WSN was divided into 7 clusters in the network of 50 nodes, 12 clusters in the network of 100 nodes, 10 clusters in the network of 200 nodes, and 14 clusters in the network of 500 nodes.



$n = 50$ $n = 100$ $n = 200$

$n = 500$

Fig. 2. Results of network clustering (k-means method)

The considered methods obtain close to optimal solutions, so in practical applications it is useful to use both methods and choose the most acceptable result. Thus, unlike using the FOREL algorithm, using the k-means algorithm requires multiple solutions of the clustering problem. However, it allows to obtain a more uniform distribution of collection points over service areas.

The heuristic rules for adjusting (adding) exchange points and the basic route of TA flight in clusters to achieve certain target network management functions are proposed.

Conclusions.

1. The main stages of synthesizing the method of direct data collection from WSN nodes with their TA clustering are proposed: methods of network clustering and data collection points construction are defined.

2. For temporal clustering of the network as the main cluster node it is proposed to use TA, which implements (in contrast to existing centroid algorithms) modified iterative algorithms of cluster analysis FOREL (k-means) and finds the minimum (given) number of data collection points.

3. It is proposed a generalized data collection algorithm that builds a finite minimum (given) number of clusters based on the known TA coverage radius and sensor node position coordinates.

4. To check in practice the results of the algorithm functioning, the software implementation in the C# environment was performed. The model allows to reduce the length of the route around nodes on the telecommunication aerial platform by 10-15% in comparison with the centroid algorithms.

References

1. Romaniuk V., Lysenko O., Romaniuk A., Zhuk O. Increasing the efficiency of data gathering in clustered wireless sensor networks using UAV // Information and Telecommunication Sciences 11 (1), 102-107.

2. Romaniuk A., Romaniuk V., Sparavalo M., Lysenko O., Zhuk O. Synthesis of data collection methods by telecommunication aerial platforms in wireless sensors networks // Information and telecommunication sciences 12 (2), 63-73.

к.т.н. Гріньков В.О. (ВІТІ ім. Героїв Крут)
Грінькова Г.В. (в/ч А1906)

АНАЛІЗ СИСТЕМИ ПОКАЗНИКІВ ОЦІНКИ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність. Якість та ефективність функціонування інформаційної системи визначається рівнем її захищеності від зовнішнього та внутрішнього впливів. Дані світової і вітчизняної статистики свідчать про тенденцію зростання масштабу комп'ютерних зловживань, що призводять до значних втрат суб'єктів різного рівня. Усунення та запобігання інформаційним загрозам різного характеру передбачає побудову чіткої системи діагностики, яка повинна базуватися на оцінці інформаційних ризиків та оцінці зміни економічних, соціальних, техніко-технологічних та інших показників, спричинених зміною стану інформаційної системи. Таким чином аналіз показників, які впливають на рівень інформаційної безпеки є важливим і актуальним завданням.

Постановка задачі. Провести аналіз показників, які впливають на рівень безпеки інформаційних систем (ІС) з метою кількісної оцінки рівня інформаційної безпеки ІС.

Основні положення. Важливість цього напрямку дослідження полягає, перш за все, в обґрунтуванні необхідності формування комплексної системи діагностики рівня інформаційної безпеки та кількісної і якісної оцінки стану рівня інформаційної захищеності інформаційних систем ЗСУ.Проведений аналіз дозволив визначити два основних підходи до оцінки інформаційної безпеки інформаційних систем: заснований на характеристиці захисних для об'єкта оцінки механізмів і достатності системи захисту; другий підхід заснований на тісному зв'язку системи показників кількісних оцінок інформаційної безпеки з ефективністю функціонування інформаційної системи в умовах впливу всіх видів загроз інформаційної безпеки.В результаті проведеного аналізу можна виділити наступну систему показників оцінки рівня інформаційної безпеки, яка базується на основних напрямах захисту інформації та враховують: оцінці організаційного забезпечення захисту інформації, оцінці програмно-технічної захищеності інформації, оцінці інформаційної надійності персоналу, оцінку захищеності інформації, що обробляється, зберігається, та передається для прийняття рішення, або аналізу, оцінці підрозділів або осіб, які вирішують проблеми у випадку загрози ІС, та забезпечують контроль за дотриманням правил і нормативів щодо захисту інформації.

Під організаційним забезпеченням захисту інформації маються на увазі адміністративні заходи захисту інформації спрямовані на видання наказів, розпоряджень, інструкцій, спрямованих на забезпечення виконання всіма військовослужбовцями заходів та вимог із захисту інформації. Критерієм оцінки організаційного забезпечення захисту інформації може бути наявність на кожному робочому місті таких наказів, розпоряджень та інструкцій а також знання цих інструкцій, наказів та розпоряджень військовослужбовцями, діяльність яких пов'язана з інформаційними системами.

Програмно-технічна захищеність інформації це наявність антивірусного програмного забезпечення (ПЗ), своєчасне актуальне оновлення з безпеки на операційну систему та встановлене програмне забезпечення (згідно з паспортом на ПЗ).

Інформаційна надійність персоналу це неухильне виконання наказів, розпоряджень і інструкцій по захисту інформації. До захищеності інформації відносяться правила обов'язкового резервного копіювання, правила криптографічного захисту інформації, правила електронного цифрового підпису.

До показників компетентності підрозділів або спеціалістів з кібербезпеки відносяться вміння та навики протидіяти погрозам з ззовні та подолання наслідків інцидентів кібербезпеки.

Висновок. Проведено аналіз показників, які впливають на рівень інформаційної безпеки ІС ЗСУ. В подальшому напрямок роботи може бути використаний для визначення кількісної оцінці рівня інформаційної безпеки інформаційних систем ЗСУ.

Гриньков В.О. (ВІТІ ім.Героїв Крут)
Янковий Д.П. (ВІТІ ім.Героїв Крут)

РОЗРОБКА ПРОГРАМНОГО МОДУЛЯ КОМПЛЕКСНОЇ ОЦІНКИ РІВНЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ЗСУ

Актуальність. За останні час інформаційні технології значно поширились в застосуванні в рядах Зборених Силах України (ЗСУ) методи пошуку, обробки, зберігання, збору, представлення, розповсюдження інформації, є найважливішою складовою роботи працівника ЗСУ в інформаційні сфери.

Здійснення електронного обмін даними і документами між працівниками роблять виконання поставлених завдань простішим однак збільшується і ризики, пов'язані з існуванням загроз безпеки документам і даних . Захист інформаційних ресурсів від викрадення , видалення, зміни достовірності документів і даних та некерованого доступу до них, є одним з важливих та актуальним завданням з забезпечення безпеки інформаційних і телекомунікаційних систем.

Постановка завдання. Провести класифікацію та аналіз основних методів оцінки рівня безпеки інформаційної системи, провести аналіз можливих загроз для інформації що циркулює на об’єкті інформаційної діяльності .

Основні положення. Інформаційна безпека – це стан захищеності інформаційної системи в якій здійснюється обробка і зберігання даних, при якій забезпечено конфіденційність, доступу і цілісності інформації та обробки її, використання й розвиток в інтересах громадян або комплекс заходив, спрямованих на забезпечення захищеності.

Зазначимо, що загально прийнятої оцінки рівня безпеки інформаційних систем не існує, але можна відділити основні загрози безпеки інформаційної системи до них відносяться

-несанкціоноване використання інформаційної системи;

-витік інформації;

-незаконне використання привілеїв;

-несанкціонованій обмін інформацією між користувачами;

-використання технічних розвідок;

-використання недоліків операційних систем та мов програмування;

-незаконне підключення до інформаційної системи та ліній передач спеціально розроблених апаратних засобів що забезпечують не керований доступ до інформації;

Отже після оцінки ймовірних загроз ми зможемо знайти комплексну оцінку захищеності інформаційної системи за допомогою якої можливо буде створити програмний додаток який буде шукати ймовірні вразливості інформаційної системи і надаватиме комплексну оцінку захищеності системи та нейтралізація вразливостей в інформаційній та телекомунікаційних системах .

Висновок. Основною метою створення системи оцінки безпеки інформаційної систем є попередження та нейтралізація загроз які можуть виникнути при використані користувачем інформаційної системи..

д.т.н. Денисов Ю. О. (ДНДІВСОВТ)
Кохан В.В. (ДНДІВСОВТ)

ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ СИСТЕМ ЕНЕРГОЖИВЛЕННЯ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ ЗА ДОПОМОГОЮ ЦИФРОВИХ ТА АДАПТИВНИХ РЕГУЛЯТОРІВ

Актуальність. Актуальність дослідження пов‘язана з постійно зростаючими вимогами до підвищення енергоефективності систем енергоживлення роботизованих комплексів та безпілотних літальних апаратів (БПЛА) спеціального та цивільного призначення.

Постановка задачі. Системи енергоживлення безпілотних літальних апаратів – це системи енергетичної електроніки, які включають у своїй структурі напівпровідникові перетворювачі, що перетворюють параметри і якість електроенергії (інвертування, перетворення частоти) і, одночасно, виконують функції стабілізації і регулювання вихідного параметру (струм, напруга, температура, швидкість і т.п.). У таких системах необхідно забезпечити високу якість процесів керування.

Метою доповіді. Розглянути використати нових законів керування бортовими напівпровідниковими перетворювачами електроенергії за допомогою цифрових та адаптивних регуляторів.

Основні положення. Експлуатація безпілотних літальних апаратів підтверджує вплив великої кількості факторів на показники енергоефективності систем енергоживлення. Одним з таких факторів є оптимізація процесів керування процесами перетворення електроенергії на борту БПЛА. Існує проблема врахування впливу таких показників як динамічні характеристики: швидкодію, перерегулювання, стійкість, з подальшою їх оптимізацією.Одним з напрямків досліджень полягає в синтезі цифрового регулятора головного контуру керування енергоживленням який забезпечує перехідні процеси з урахуванням впливу пульсацій перетворювача та забезпечує більш м’який темп споживання струму від бортового акумулятора БПЛА [1-2]. За попередніми розрахунками використання нових законів керування процесами перетворення електроенергії дає можливість підвищити показники енергоефективності систем енергоживлення БПЛА на 10-15 відсотків.

Підвищення точності стабілізації напруги, покращення динаміки системи керування енергоживленням, відбувається також за рахунок розробки нових структур перетворювачів та використання адаптивних алгоритмів керування ними [3]. Нові структури систем енергоживлення включають в себе високочастотні перетворювачі електроенергії з адаптивним керуванням процесами комутації. Використання вищевказаних перетворювачів дає можливість зменшити масогабаритні показники систем енергоживлення на 30-40 відсотків.

Висновок. Використання нових технічних рішень що до керуванням процесів енергоперетворення на борту БПЛА дозволить підвищити надійністькерування та час польоту літального апарату. В свою чергу це покращить тактико-технічні характеристикибезпілотних літальних апаратів вітчизняного виробництва.

ЛІТЕРАТУРА

1.Денисов Ю. О.Войтенко В.П., Городній О.М., Димерець А.В. Оптимізація енергодинамічних процесів в системах електроприводу квадрокоптера.Праці ІЕД НАН України 2020. – Вип. 56. – С. 47 – 52.

2. Denisov Y.O Denisov O.I., Bursala O.O.Synthesis of the digital regulator of the main contour of the three-circuit system of the linear electric drive of the working body of the mechanism of onboard aviation equipment.Electrical Engineering & Electromechanics, 2021, no. 4, pp. 39-45

3.Єршов Р., Войтенко В. Частотно-імпульсний модулятор з адаптивною корекцією тривалості імпульсу // Технічні науки та технології : науковий журнал / Черніг. нац. технол. ун-т. – Чернігів : Черніг. нац. технол. ун-т, 2020. – № 1 (19). – С. 177 – 190.

Дєдов М.А. (військова частина А1906)
Жуков Є.В. **(**військова частина А1906**)**
Вакуленко В.Р. **(**військова частина А1906**)**

ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ПРОГНОЗУВАННЯ

Актуальність. Питання прогнозування подій завжди були і залишаються актуальними як у повсякденному житті, так і для прийняття управлінських рішень із залученням інформаційних систем. Інформаційна система є сукупністю програмних і апаратних засобів для збору, зберігання, пошуку і оброблення великого обсягу даних. Великий обсяг зібраної інформації є фактологічною основою для отримання людиною нових знань, необхідних при прогнозуванні певної ситуації або поведінки спостереженого об'єкта.

На сьогодні під час прогнозування за допомогою простих методів аналізу неможливо точно визначити наявність і характер зв'язків між певними ознаками. Але це не означає, що зв'язку не існує, а він може мати складний характер. Тому слід знайти метод, що дасть змогу найточніше визначити наявність / відсутність будь-якого зв'язку. Штучні нейронні мережі здатні розпізнавати об'єкти та виявляти складні зв'язки, які людина не має змоги виявити своєчасно.

Одним з інструментів, які імітують роботу головного мозку людини, є штучні нейронні мережі, що дають змогу скоротити час та підвищити якість у виробленні інформаційного рішення. Прогнозування складається з інформаційних рішень, а правильне інформаційне рішення є основою для прийняття своєчасного і якісного управлінського рішення (передбачення).

Отже, актуальним завданням ефективного управління є підвищення якості інформаційних рішень за допомогою штучних нейронних мереж в інформаційних системах для вирішення завдань прогнозування.

Постановка задачі. Проаналізувати основні типи штучних нейронних мереж для застосування в інформаційних системах.

Основні положення. Штучні нейронні мережі є розділом штучного інтелекту, в якому для оброблення інформації застосовуються явища, аналогічні нейронам головного мозку людини (природного інтелекту).

Особливості штучних нейронних мереж:

паралельне оброблення інформації всіма ланками, що дає змогу прискорити час на її оброблення;

здатність до навчання й узагальнення накопичених знань із масиву апріорної інформації (даних);

здатність до прогнозування часових рядів із множини статистичних звітів (вибірок): навчальних, тестувальних і контрольних. Часовий ряд – це зібраний у різні моменти статистичний матеріал про будь-які значення параметрів досліджуваних процесів.

Доцільно розглянути основні типиштучних нейронних мереж залежно від покладених на них завдань:

багатошаровий персептрон;

радіально-базисний;

узагальнено-регресійний;

мережа Вольтера;

мережа Ельмана.

Багатошаровий персептрон є штучною нейронною мережею прямого поширення, яка складається з трьох шарів: вхідний, скритий та вихідний. Цей тип мереж використовує алгоритм зворотного поширення помилки. До переваг мереж багатошарового персептрону належить простота реалізації алгоритму і стійкість до аномалій та викидів даних за рахунок усереднення помилки, а до недоліків – тривалий процес навчання та вразливість алгоритму

до потрапляння в локальний мінімум функції помилки. Цей тип мереж підходить для розпізнавання звуку та візуальних об’єктів.

Радіально-базисний тип є мережею, яка може містити радіальні та базисні функції, а також функції активації. Основу мереж цього типу становлять функції розподілу Гауса та алгоритм Баєса, побудований за принципом максимуму апостеріорної імовірності. Штучні нейронні мережі радіально-базисного типу зазвичай застосовуються для автоматизації завдань класифікації об’єктів.

Штучні нейронні мережі узагальнено-регресійного типу є сукупністю (симбіозом) мереж багатошарового персептрону та радіально-базисного типу. Перевагами мереж цього типу є візуалізація об’єктів-аналогів у статистичній вибірці, а недоліком – надчутливість до вибору метрики вихідних даних. Цей тип мереж ідеально підходить для прогнозування статистичних показників і виявлення залежностей між окремими ознаками (характеристиками).

Мережі Вольтера дають змогу будувати моделі для ідентифікації нелінійних об’єктів, усуваючи інтерференцію шумів, а також прогнозувати зміни в часі нестаціонарних сигналів. Ці мережі можуть застосовуватися в прогнозуванні транспортних потоків і пошуку оптимальних шляхів (маршрутів) за різними показниками якості. Тобто мережі цього типу дають змогу автоматизувати розв’язання задач упорядкування з дисципліни “Дослідження операцій”.

Штучні нейронні мережі Ельмана побудовані на основі алгоритмів рекурентного типу. За допомогою таких алгоритмів формується апріорна база послідовності дій об’єкта спостереження. Ці мережі можуть застосовуватися для автоматичного управління безпілотними та роботизованими рухомими об’єктами (транспортними засобами), оскільки їх особливістю є запам’ятовування певної послідовності дій.

Висновок. Аналіз зазначених типів штучних нейронних показав їх ефективність з вирішення окремих завдань розпізнавання, класифікації, упорядкування та запам’ятовування певної послідовності дій.

Прогнозування передбачає комплексне застосування різних типів штучних нейронних мереж в інформаційних системах, оскільки комплексному вирішенню можуть підлягати зазначені завдання в тісному взаємозв’язку.

При цьому слід зазначити, що ефективно вирішити завдання прогнозування можна, якщо штучна нейронна мережа навчається на великому обсязі даних. У разі малорозмірної або неякісної вибірки навіть найбільш якісний алгоритм не сприятиме позитивному результату, оскільки без відповідного набору даних штучна нейронна мережа не здатна навчатися.

Дудка А.С. (ВІТІ ім.Героїв Крут)
Османов Р.Н. (ВІТІ ім.Героїв Крут)

АНАЛІЗ ВИБОРУ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Актуальність теми. На сьогоднішній день існує велика кількість телекомунікаційних мереж, для надійної роботи яких використовуються різноманітні протоколи маршрутизації, кожен з яких має свої особливості.Розглядаючи сучасні методи багатошляхової маршрутизації, можна зробити висновок, що графокомбінаторний підхід залишався домінуючим в ході протокольних рішень завдань маршрутизації – протокол маршрутної інформації RIP (RoutingInformationProtocol), протокол внутрішнього шлюзу IGRP (InteriorGatewayRoutingProtocol), удосконалений протокол внутрішнього шлюзу EIGRP (ExtendedIGRP), протокол маршрутизації проміжних систем IS-IS (IntermediateSystem - to - IntermediateSystem), протокол з відстежуванням стану каналів зв'язку «найкоротший відкритий шлях першим» OSPF (OpenShortestPathFirst) та ін.

Перераховані протоколи, в основу яких покладені графові моделі і методи пошуку найкоротшого шляху за допомогою алгоритмів Дейкстри, Беллмана-Форда або Флойда-Уоршела реалізують переважно одношляхову стратегію маршрутизації. Основною перевагою комбінаторних алгоритмів є розв'язання задачі пошуку найкоротшого шляху, але це заздалегідь відома обчислювальна складність їх реалізації. Недоліки подібних моделей і алгоритмів пов'язані з обмеженими можливостями забезпечення збалансованого завантаження мережі і QoS одночасно за кількома показниками. Відповідно до вимог часу з метою забезпечення збалансованого завантаження ТКМ в ряді протоколів маршрутизації передбачене балансування навантаження, що припускає багатошляхову маршрутизацію.

Постановка задачі. Проаналізувати протоколи маршрутизації (за використовуємими типами алгоритмів); визначити переваги та недоліки існуючих протоколів маршрутизації; запропонувати подальший напрямок розвитку.

Основні положення.Протокол маршрутизації –це мережевий протокол, який використовується маршрутизаторами для визначення можливих маршрутів прямування даних в комп'ютерній мережі. Застосування протоколу маршрутизації дозволяє уникнути ручного введення всіх допустимих маршрутів, що, у свою чергу, знижує кількість помилок, забезпечує узгодженість дій усіх маршрутизаторів в мережі і полегшує працю адміністраторів.

Протоколи маршрутизації призначені для автоматичної побудови таблиць маршрутизації (ТМ), на основі яких виконується переміщення пакетів. Такі таблиці містять дані яких достатньо для прийняття рішення та пересилання будь–якого пакета, що надійшов до маршрутизатора. Вміст ТМ залежить від технології складеної мережі. Як правило обирається "найкоротший" маршрут.

Маршрутизація (англ. Routing) –процес визначення маршруту прямування інформації між мережами. Маршрутизатор або роутер приймає рішення, що базується на IP–адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують IP–адресу отримувача.

Маршрутизація на основі таблиць в свою чергу поділяється на статичну і динамічну (адаптивну). При статичній маршрутизації маршрути задаються вручну адміністратором. Така маршрутизація при зміні структури мережі потребує ручного змінення маршрутів.

У випадку динамічної маршрутизації маршрути обчислюються автоматично за допомогою протоколів.

Якщо порівняти статичну та динамічну маршрутизацію, можна дійти висновку, що динамічна маршрутизація має більше переваг так як потребує меншого втручання адміністратора, конфігурація менш схильна до помилок, протокол автоматично реагує на зміну топології мереж, в той час як статична маршрутизація хоча й легша за своїм

використанням, але потребує більше часу для обслуговування та виправлення помилок, а також для підтримки змінної маршрутної інформації потрібне втручання адміністратора.

Так як динамічна маршрутизаціє є найбільш ефективною у використанні, вона залишається і найскладнішим способом маршрутизації.

Залежно від обраної стратегії коригування маршрутів розрізняють централізовану, розподілену, локальну і гібридну маршрутизації.

Ефективнішим методом маршрутизації можна вважати гібридну маршрутизацію, яка поєднує позитивні властивості локальної і централізованої маршрутизацій. Прикладом є «дельта-маршрутизація», за якої менеджер з деяким запізненням стежить за глобальною ситуацією у мережі, тоді як вузлам надана певна свобода дій з тим, щоб вони могли швидко реагувати на локальні коливання навантаження мережі та зміни стану її окремих компонентів.

Вибір конкретного протоколу динамічної маршрутізації залежить від розмірів і вимог, які висуваються конкретною корпоративной мережею. На сьогоднішній день найбільш досконалими внутрішніми протоколами динамічної маршрутизації є OSPF і EIGRP. Їх перспективність підтверджує і впровадження підтримки перспективного протоколу IPv6. І, якщо OSPF вже став фактично стандартним внутрішнім протоколом Internet, то з ростом ринку обладнання фірми Cisco Systems позиції EIGRP в однорідних корпоративних мережах будуть зміцнюватися. Протокол IGRP, мабуть, також поступиться йому своїм місцем. Проте, переваги простоти протоколу RIP для невеликих мереж продовжують залишатися затребуваними, про що, наприклад, свідчить поява нової версії протоколу Riping, в якій також передбачена підтримка протоколу IPv6.

Дистанційно–векторні протоколи більш схильні до створення петель маршрутизації, ніж протоли стану зв’язку, проте останні відмічаються швидшою сходимістю. З іншого боку, протоколи стану зв’язків характеризуються більш складними розрахунками відстаней у порівнянні з дистанційно–векторними протоколами, що потребують більшої процесорної потужності та пам’яті. В наслідок чого, собівартість реалізації протоколів стану зв’язків стає більш коштовною. Не дивлячись на їх розбіжності, обидва типи протоколів добре себе зарекомендували у різноманітних ситуаціях та постійно вдосконалюються.

Висновки. Отже, перспективним є подальший розвиток гібридних протоколів маршрутизації, які б під час вибору маршруту передачі даних мали змогу одночасно аналізувати:

– надійність каналів зв’язку на основі статистичних даних за певний період;

– важливість інформації, що передається (автоматично дублював передачу пакетів, використовуючи альтернативний маршрут);

–пропускну здатність каналу зв’язку;

– кількість переходів. Враховуючи все це –є необхідність у розробці новітнього протоколу маршрутизації, в логіку роботи якого буде закладено набагато складніший алгоритм вибору маршруту. Незважаючи на складність реалізації та значну собівартість майбутній ефект має бути вражаючим.

Дячина В.П.(ВІТІ ім. Героїв Крут)
к.т.н. Ільїнов М.Д.(ВІТІ ім. Героїв Крут)

МЕТОДИКА РОЗРАХУНКУ ФАЗООБЕРТАЮЧОГО ПРИЛАДУ КОЛІНЕАРНОЇ АНТЕНИ ПОСЛІДОВНОГО ТИПУ

Найважливішим елементом системи мобільного радіозв'язку являється її антено фідерний пристрій, який дозволяє не тільки забезпечити енергетичний потенціал радіолінії але й побудувати систему в цілому. В даний час найбільш перспективним напрямком розвитку таких антен являється антени з ненаправленим випромінюванням в азимутальній площині, які носять назву колінеарні антени.

Колінеарна антена послідовного типу представляє собою лінійну, синфазну антенну решітку, виконану із симетричних вібраторів різної довжини та конструкції. Основним елементом даних антен являється фазообертаючий прилад (ФП), який розташовується між випромінюючими елементами колінеарної антени і призначений для синфазного їх живлення. ФП визначає як зовнішні так і внутрішні характеристики антени в цілому.

У самому простому вигляді ФП виконується у вигляді короткозамкненого чвертьхвильового відрізка двохпроводової лінії, як показано на рис.1.1 б

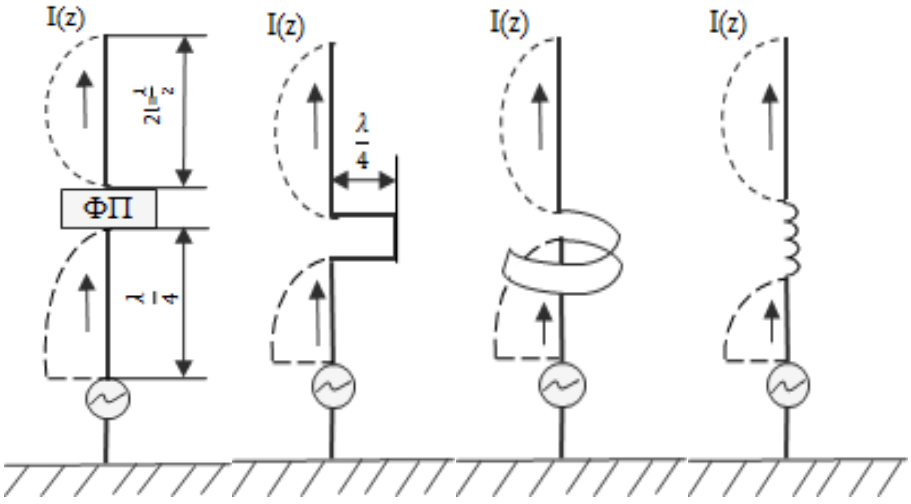


Рис. 1.1. Колінеарна антена послідовного типу

Найбільше практичне застосування отримали ФП у вигляді індуктивного дроселя. Для визначення принципу роботи такого ФП, його можливо представити у вигляді спірального хвилеводу радіусом a з кроком спіралі S і кутом намотки Ψ , як показано на рис.1.2.

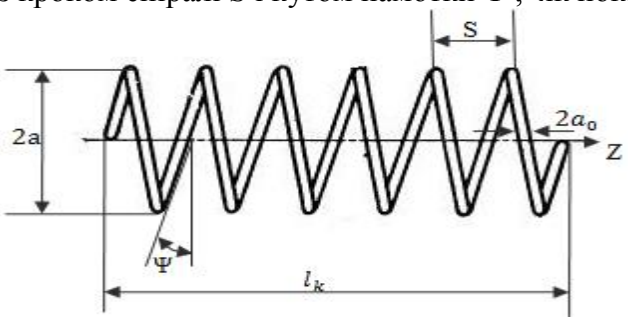


Рис. 1.2. Індуктивний дросель

Якщо припустити, що електромагнітна хвиля поширюється вздовж гвинтової лінії з фазовою швидкістю

$$V_{\text{ф}} = C,$$

де: $C = 3 \cdot 10^8$ м/сек – швидкість світла, а $V_ф$ – фазова швидкість, то коефіцієнт сповільнення ($К_{зо}$) буде визначатися наступним виразом

$$К_{зо} = \frac{C}{V_ф} = \frac{\sqrt{(2\pi a)^2 + S^2}}{S} \approx \frac{2\pi a}{S} \approx \frac{1}{sin\Psi}$$

Тоді для забезпечення зсуву хвилі в 180˚ довжина котушки (l_k) вибирається з умови

$$l_k = \frac{\lambda}{2} = \frac{\lambda_0}{2\pi\alpha} \cdot S$$

Спосіб розрахунку параметрів ФП у вигляді індуктивного дроселя носить назву методика нульового наближення, так як $К_{зо}$ – коефіцієнт сповільнення не залежить від частоти і електромагнітна хвиля не володіє дисперсійними властивостями, що не відповідає дійсному.

Більш строга теорія аналізу спіральних хвилеводів показує, що нульове наближення можна користуватись коли:

$$ka\text{ctg}\Psi \geq 3.$$

В даний час відомо декілька строгих методів аналізу електромагнітного поля у сповільнюючих системах виконаних у вигляді спіральних хвилеводів.

Незалежно від того, який метод використовується кінцевий результат аналізу електромагнітного поля в сповільнюючих спіральних структурах, з урахуванням дисперсії хвилі призводить до транцендентного, дисперсійного рівняння, яке має вигляд :

$$(ka\text{ctg}\Psi)^2 = (\gamma\alpha)^2 \frac{I_0(\gamma\alpha)K_0(\gamma\alpha)}{I_1(\gamma\alpha)K_1(\gamma\alpha)}$$

де: $\gamma^2 = \beta^2 - R^2 > 0$ - постійне розповсюдження;

β-повздовжнє хвильове число;

$I_0(\gamma\alpha)K_0(\gamma\alpha)$ – модифікова функція Бесселя;

$I_1(\gamma\alpha)K_1(\gamma\alpha)$ –функція Макдональда.

Для порівняння отриманих результатів по розрахунку параметрів індуктивного дроселя (ФП) у колінеарній антені в таблиці 1 наводяться дані по $К_з$ – коефіцієнту сповільнення. Тут наведено : $К_{зо}$ – коефіцієнта сповільнення по методиці нульового наближення; $К_{зі}$ – коефіцієнт сповільнення по методиці 1-го наближення; $К_з$ – коефіцієнт сповільнення по дисперсійному рівнянні; $К_{зе}$ – експериментальний коефіцієнт сповільнення.

Таблиця 1

$К_з$ / Ψ,град	$К_{зо}$	$К_{зі}$	$К_з$	$К_{зе}$
Ψ=2.6˚, *S*=2,3см	22	20,89	20	20,5
Ψ=3.6˚,*S*=5,2см	16	14,28	13,5	14
Ψ=4.5˚,*S*=4.0см	12,7	12,48	10,5	10,5

Порівняльний аналіз наглядно показує, що найбільш точні результати дає класичне дисперсійне рівняння в порівнянні з експериментальними даними .

Напрямком подальшого дослідження є розробка інженерної методики для параметрів ФП у вигляді індуктивного дроселя.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ільїнов М.Д. Антена базової станції з секторною діаграмою направленості в азимутальній площині / Ільїнов М.Д., Мацаєнко А.Н., Шацький І.О. // Збірник наукових праць ВІТІ НТУУ „КПІ”. – Київ, 2010. – № 1. – С. 5.

2. Бузов А.Л. Антенно-фидерные устройства базовых станций подвижной связи: основные требования и проблеми проектирования / Бузов А.Л.,Романов В.А.,Сподобаев Ю.М. – М. : Радио и связь, 2001.-С. 12-16.

Заїка М.В. (ВІТІ ім. Героїв Крут)
Яцико Ю.О. (ВІТІ ім. Героїв Крут)
к.т.н. Ільїнов М.Д. (ВІТІ ім. Героїв Крут)

ВИКОРИСТАННЯ АНТЕН MIMO ЯК ОДИН ІЗ НАПРЯМКІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЛІНІЙ РАДІОЗВ'ЯЗКУ

Актуальність. Технологія MIMO (Multiple Input – Multiple Output) представляє собою метод просторового кодування сигналу. Він 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. Два важливих завдання, які вирішуються за рахунок застосування технології MIMO:

- підвищення швидкості передачі при застосуванні просторового мультиплексування;
- збільшення якості зв'язку за рахунок просторового, часового- та частотного кодування і (або) формування променів.

Постановка задачі.Провести аналіз конструктивної будови панельної антени MIMO 2x2 та обґрунтувати доцільність її використання у військовій техніці радіозв'язку.

Основні положення. 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 , що зображено на рис. 1.

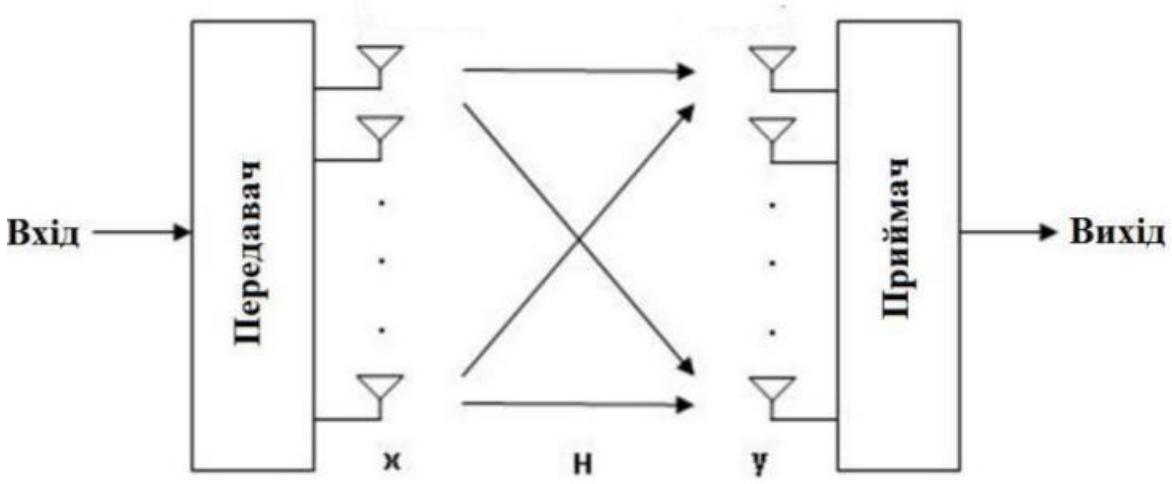


Рис. 1. Реалізація систем MIMO

Властивості MIMO-каналу, що з'єднує n-й передавальний елемент, з m-м приймальним елементом, описуються комплексними канальними коефіцієнтами h_{nm} що утворюють канальну матрицю **H**розміру $N \times M$. Їх значення випадково змінюються згодом через наявність багатопроменевого поширення сигналу. Введемо наступні позначення:

$\vec{s}$ – вектор сигналів, що передаються;

$\vec{z}$–вектор власних шумів прийомних елементів антени;

$\vec{x}$–вектор прийнятого повідомлення,

Тоді сигнал на приймальній стороні записується наступним чином:

$$\vec{x} = \mathbf{H} \cdot \vec{s} + \vec{z}\ ,$$

а матриця **H** вважається нормованою.

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 (рис. 2) 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 4 антени. Для передачі опорних символів кожній із антен виділені певні ресурсні елементи (РЕ). Ці елементи необхідні для оцінки каналів та організації когерентної демодуляції. У результаті 14,3% від усіх РЕ виділено на передачу опорних символів.

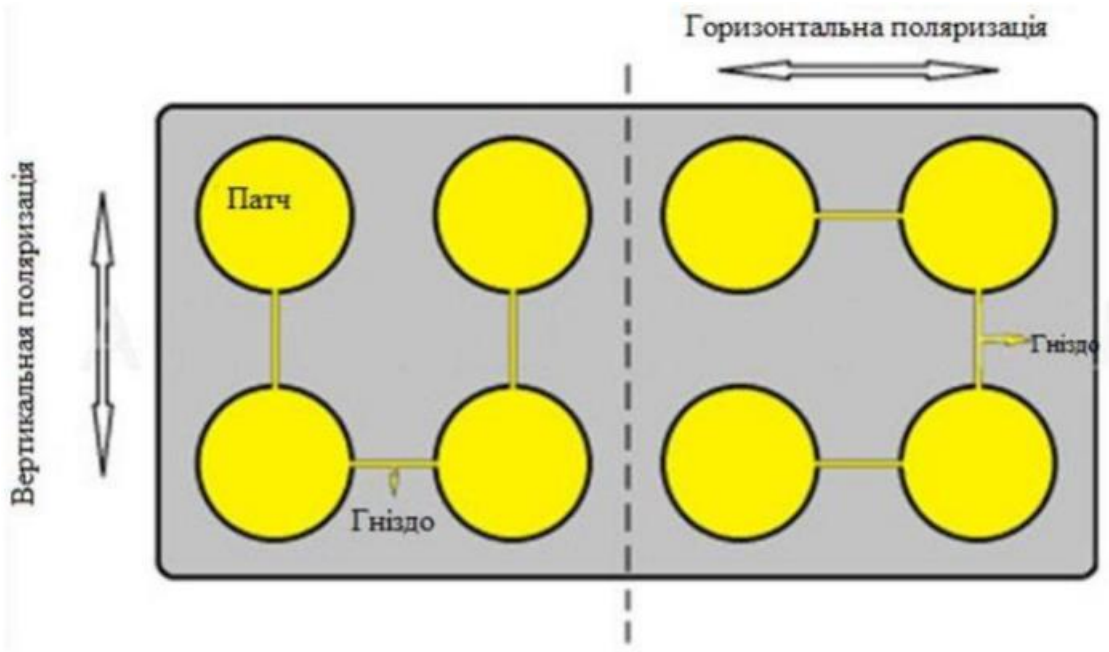


Рис. 2. Панельна MIMO антена 2x2

Висновок. Таким чином, антени для систем MIMO не потребують великих матеріальних затрат на їх виготовлення, а проведений теоретичний аналіз показує, що на практиці їх використання 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.

Заруба О.С. (ВІТІ ім.Героїв Крут)
к.т.н. Гуржій П.М. (ВІТІ ім.Героїв Крут)
Зінченко М.О. (ВІТІ ім.Героїв Крут
Чуйко В.В. (ВІТІ ім.Героїв Крут

ВИЗНАЧЕННЯ ОСНОВНИХ ВИМОГИ ТА РЕКОМЕНДАЦІЇ ПРИ СТВОРЕННІ ПЕРСПЕКТИВНИХ ЗАСОБІВ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ

Актуальність. В сучасних умовах збільшується необхідність у мобільних тропосферних засобах зв'язку з підвищеною пропускною здатністю які будуть задовольнять потребам Збройних Сил у передачі великих обсягів інформації на значні відстані. Створення та модернізацію тропосферних станцій необхідно здійснювати на основі новітніх технологій подвійного призначення та сучасних технічних ідей.

Основні положення.

Основними напрямками створення перспективних засобів тропосферного зв'язку є: застосування цифрових антенних решіток, впровадження технології MIMO; реалізація ефективних алгоритмів обробки кодових сигналів (OFDM, COFDM). Впровадження останніх забезпечить стійку роботу тропосферної лінії та більше співвідношення сигнал-перешкода на вході приймальних пристроїв при одночасному ефективному використанні смуги частот.

Перспективні системи тропосферного зв'язку мають базуватися на створенні високомобільних уніфікованих малогабаритних станцій модульного типу, покращенні характеристик швидкодії, стійкості, скритності, збільшення показників мобільності та рухливості комплексу, а також швидкості передачі даних.

Найбільш привабливою щодо цього є технологія MIMO, варіанти її практичної реалізації можуть передбачати кілька варіантів побудови перспективного комплексу тропосферного зв’язку. З метою реалізації зазначених вище функцій потребує розгляду ускладнена модель опису тропосферної мережі зв'язку, коли окремо взятій системі MIMO здійснюється обробка сигналів кількох інших рознесених в просторі MIMO-систем. У цьому випадку зберігається основна перевага технології MIMO – одночасна робота з усіма користувачами в одній і тій самій смузі частот. Для поділу використовується просторове рознесення приймачів, додатково може застосовуватися часовий, частотний або кодовий поділ користувачів, такі системи називають системами множинного доступу із просторовим поділом (SDMA – Space-Diversity Multiple Access). Аналіз схемотехнічних рішень цифрового сегмента ТРС дозволяє зробити висновок, що використання Digital Signal Processors недоцільне через труднощі підбору прийнятної продуктивності, складності заснованих на DSP багатопроцесорних технологій та необхідності ліцензування їх використання для військових додатків. Поєднання FPGA та масових процесорів Intel може здешевшити розробку ПЗ, та відповідно знизити вартість та час реалізації. При цьому можливий перехід до консептуально нового спрямування розвитку тропосферних систем – обслуговування одним комплектом обладнання кількох тропосферних напрямків. Основні технічними вимогами до станцій тропосферного зв'язку, що створюється, повинні бути: низька собівартість обладнання; забезпечення необхідних характеристик надійності; тривалий життєвий цикл; захист від електромагнітних звад; забезпечення теплового балансу в жорстких умовах експлуатації. При проектуванні серійних систем слід також врахувати деякі фактори, а саме: наявність готового системного та прикладного програмного забезпечення; вимога швидкої готовності до серійного виробництва; наявність кваліфікованих розробників; доступність готових сумісних апаратних та програмних засобів інших виробників; вимоги відкритої архітектури. Для забезпечення висунутих вимог та врахування зазначених факторів пропонується використання технічних рішень на базі стандарту CompactPCI або Open VPX.

Висновки. Зазначені вимоги та рекомендації доцільно врахувати при створенні уніфікованих багатофункціональних тропосферних комплексів з програмною реконфігурацією архітектури та можливістю одночасної роботи з кількома кореспондентами.

Заруба О.С. (ВІТІ ім.Героїв Крут)
Літовщук .І.О. (ВІТІ ім.Героїв Крут)
к.т.н. Гуржій П.М. (ВІТІ ім.Героїв Крут)
Савчук М.В. (ВІТІ ім.Героїв Крут)
Пантась С.О. (ВІТІ ім.Героїв Крут)

ФАКТОРИ ТА ПРИЧИНИ ЩО ВПЛИВАЮТЬ НА НАПРЯМКИ ПОДАЛЬШОГО РОЗВИТКУ ЗАСОБІВ РАДІОРЕЛЕЙНОГО ЗВ'ЯЗКУ

Актуальність.Розвиток засобів радіорелейного зв'язку останнім часом рухається напрямком вдосконалення можливостей та їх технічних характеристик за рахунок розширення частотних діапазонів, впровадження нових видів сигналів, використання багатопозиційних методів модуляції тощо, позначимо основні фактори та причини що впливають на напрямки подальшого розвитку засобів радіорелейного зв'язку.

Основні положення. Загальними передумовами для подальшого розвитку засобів радіорелейного зв'язку є ряд факторів, які можна поділити на три основних: організаційні; технологічні; технічні. Але цей поділ носить досить умовний характер, а всі ці фактори дуже пов'язанні між собою, розглянемо їх більш детально.

Організаційні: необхідність збільшення пропускної спроможності у зв'язку з стійкою тенденцією зростання числа користувачів та підвищення якості надаваємих інфокомунікаційних послуг користувачам; постійно зростаючим обсягом мультимедійних даних та необхідності передачі їх у русі; зменшення частки передачі лише телефонних повідомлень, появою стійкої тенденції до передачі різнорідної інформації (передача даних, відео, голос) у пакетованому вигляді; можливість реалізації поєднання різнорідних ліній зв'язку з метою перерозподілу трафіку на основних інформаційних напрямках; можливість створення розгалужених мереж радіорелейного зв'язку, що адаптивно змінюються в залежності від потреб користувачів та/або під впливом середовища поширення.

Технологічні: можливість впровадження автоматизації в управління процесами встановлення та ведення зв'язку, адаптивного регулювання потужності, зміни режимів роботи, документування, постійного контролю якості зв'язку та його підтримання на заданому рівні, простоти використання обладнання, застосування системи віддаленого керування обладнанням та ін.

Технічні: необхідність пошуку та застосування простих недорогих технічних рішень для доведення різнорідної інформації безпосередньо до кореспондента, у тому числі рухомих, при роботі в умовах міжсимвольної інтерференції та складної радіоелектронної обстановки (застосування сигнально-кодових конструкцій, багаточастотних сигналів OFDM, COFDM); зменшення НВЧ вузлів (для можливості компактного розміщення обладнання в одному малогабаритному контейнері), необхідність забезпечення високої надійності функціонування обладнання та ліній зв'язку шляхом автоматизації управління ним; використанням ділянкової перевірки ліній (мереж) для швидкого пошуку несправностей; дублювання елементів основного обладнання; використання більш сучасної елементної бази; впровадження роботи радіорелейних засобів у більш високих ділянках діапазону НВЧ.

Висновки. Перехід від безперервних до дискретних сигналів дозволив широке використання Digital Signal Processsng (цифрових методів обробки сигналів) в телекомунікаційних засобах в загалі та радіорелейних засобах зокрема, мініатюризація елементної бази техніки та розвиток програмуємих мікропроцесорів дозволяє перейти до Software-Defined Radio реалізації основних вузлів радіорелейного обладнання та відповідно тим самим істотно зменшити масогабаритні характеристики радіорелейного обладнання. Включення до складу радіорелейного обладнання комутаторів та маршрутизаторів дозволяє розглядати засоби радіорелейного зв'язку повноправними елементами мережевої структури.

Зарубенко А.О. (ВІТІ)
Палівода В.С. (ВІТІ)
Хоменко П.В. (ВІТІ)

АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ЗНИЩЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Актуальність. Аналіз досвіду локальних конфліктів 2011 – 2021 років на територіях: Лівії, Сирії, в регіоні Нагірного Карабаху та на тимчасово окупованих територіях України дозволяє відокремити з числа всіх факторів та засобів, які впливають на успішне виконання бойових завдань – застосування безпілотних літальних апаратів (БпЛА). Розвідувально-ударні можливості сучасних БпЛА пов'язані зі стрімким їх розвитком, що в свою чергу потребує відповідного розвитку засобів їх знищення.

Постановка задачі. На сьогоднішній день ЗС України не готові ефективно протистояти розвідувально-ударним діям БпЛА противника, оскільки існуючі засоби протиповітряної оборони (ППО), які призначені для ураження великих повітряних цілей на висотах 2,5 км – 10 км не розраховані для виявлення літальних апаратів малих розмірів. Крім того застосування існуючих активних зенітних засобів ураження повітряних цілей не завжди є економічно доцільним та ефективним.

Метою дослідження є розробка підходів до боротьби з БпЛА різних класів на основі проведеного аналізу сучасних засобів і способів знищення БпЛА провідних країн світу.

Виклад основного матеріалу. Ефективність застосування засобів ППО залежить не лише від дальності виявлення БпЛА, а й від можливості їх розпізнавання (ідентифікації).

Визначення класу БпЛА дозволить прийняти рішення щодо застосування тих зенітних засобів ураження, які будуть як економічно обґрунтованими, так і ефективними.

В таблиці 1 представлено запропоновану в НАТО класифікацію БпЛА.

Таблиця 1 – Класифікація БпЛА

№ з/п	Клас	Категорія	Маса, кг	Висота застосування, м	Радіус дії, км
1	I	Малі, міні, мікро	1 – 150	60 – 1500	5 – 50
2	II	Тактичні	(150-600)	до 5500	до 200
3	III	Ударні	(>600)	10000-20000	до 6000

Для ефективного застосування зенітних засобів незмінним є завдання виявлення та ідентифікації БпЛА. В ЗС України залишається частково не вирішеними питання можливості виявлення та ідентифікації БпЛА I та II класів, а без цього неможливо прийняти рішення щодо ефективного застосування зенітних засобів ураження. Ідентифікація БпЛА залежить від ступеня його помітності, яка визначається величиною його сигнатур в радіочастотному, інфрачервоному і видимому діапазонах, а також сигнатури акустичної. Крім того сучасні БпЛА мають невеликі розміри завдяки застосуванню композитних матеріалів або пластика зі спеціальним фарбуванням і з особливою комбінацією шарів, а їх невеликі бензинові і тим більше електричні двигуни мало випромінюють тепла і працюють майже безшумно.

Для ефективного знищення БпЛА III класу в збройних силах передових країн світу застосовують зенітні ракетні комплекси, які здатні ефективно знищувати як малі, так і великі повітряні цілі на висотах 5 км – 20 км. Для знищення БпЛА I та II класів широкого застосування отримало гарматне озброєння калібрів: 23 мм, 35 мм та 40 мм. Новітні боєприпаси дозволяють створити хмару уламків із сотні вражаючих елементів, що забезпечує ефективне знищення БпЛА. Але розвиток технологій БпЛА ставить перед ЗС

України завдання впровадження новітніх засобів ППО щодо протидій БпЛА. Без повноцінного захисного купола, здатного протистояти будь-якому класу БпЛА, питання безпеки всіх об'єктів та підрозділів не буде виконано.

Покращення показників ефективності знищення малорозмірних БпЛА можливе шляхом розробки новітніх засобів ураження, а також впровадження комплексу спеціальних заходів щодо організації їх знищення активними засобами.

До перспективних засобів знищення БпЛА провідних країн світу, які під час випробувань показали свою ефективність, слід віднести: електромагнітну та лазерну зброю, а також БпЛА-перехоплювачі (БпЛА-камікадзе). До таких зразків слід віднести мікрохвильову гармату "Phaser" компанії Raytheon (США). Зазначена система електромагнітної зброї призначена для знищення БпЛА I та II класів, які переміщуються зі швидкістю від 185 км/год до 370 км/год. Також існують зразки електромагнітної зброї, які забезпечують знищення БпЛА в радіусі 360°. Наприклад система "DroneDome" (Ізраїль) здатна ідентифікувати БпЛА, здійснювати супроводження цілей та автоматичне їх знищення при цьому не створюючи перешкод для інших літальних апаратів. Це досягається завдяки використанню спеціальної направленої антени. Система здатна працювати в будь-яких погодних умовах і може виявляти цілі розміром до 2 квадратних сантиметрів на відстані 3,5 км.

Лідером в розробці лазерної зброї є США. На сьогодні лазерні комплекси та системи як перебувають на озброєнні збройних сил США, так і активно вдосконалюються.

Прикладами таких систем:

– система протиракетної оборони Skyguard і Nautilus яка побудована навколо високоенергетичного тактичного лазера – THEL (Tactical High Energy Laser);

– система LaWS (Laser Weapon System) технологічний демонстратор високоенергетичної лазерної зброї, створеного командуванням морських систем ВМС США;

– лазерний комплекс HEL (High-Energy Laser) компанії Boeing встановлений на бронетранспортер Boxer. Комплекс здатний виявляти, супроводжувати і знищувати цілі – як в повітрі, так і на землі. Потужності досить для знищення безпілотників і ракет малої дальності.

Електромагнітна та лазерна зброя має як переваги, так і недоліки. До переваг використання таких систем озброєння можна віднести вартість та точність пострілу, а до недоліків – залежність від погодних умов, які істотним чинником можуть обмежити дію лазеру та дальність застосування у випадку з електромагнітною зброєю.

Висновок. Боротьба з БпЛА потребує підходу який зводиться до трьох вимог: виявити, розпізнати і знищити. Перші два кроки в цій послідовності на даний момент здебільшого відпрацьовані за рахунок вдосконалення існуючих технологій. В свою чергу знищення БпЛА потребує одночасно як технічних, так і організаційних рішень. До них може бути віднесено:

– створення спеціальних мобільних груп, що включають різнотипні компактні зенітні засоби знищення БпЛА (ЗРК, ПЗРК), з порівняно високими розвідувальними і вогневими можливостями при виявленні та стрільбі по малорозмірних цілям;

– вдосконалення (модернізація) існуючих зразків зенітного озброєння та боєприпасів до них в інтересах підвищення ефективності боротьби з малорозмірними цілями;

– розробку перспективних зразків зенітного озброєння, в тому числі нетрадиційних видів зброї, для вирішення завдань виявлення і знищення малорозмірних повітряних цілей.

Пріоритетами в реалізації програм розробки сучасних вітчизняних засобів знищення БпЛА можна вважати використання засобів перехоплення або знищення БпЛА за допомогою безпілотників-камікадзе, які за своїми вартісними показниками значно нижче чим перехоплювана ціль.

A.Zakharchuk (VITI named after Heroes of Kruty)

ANALYSIS OF FIELD TELECOMMUNICATION NETWORKS OF BROADBAND ACCESS FOR DEPARTMENTAL PURPOSE IN THE TACTICAL CONTROL CHAIN

Topicality. The level of computerization of any country is determined mainly by the development of infocommunications. The basis of infocommunications are information networks, which are essentially based on telecommunications networks. Most new technologies depend on the availability of an Internet source and related services. Internet connection provides an opportunity to develop the potential and competitiveness of the state in the digital world. A very fast connection to the Internet is called broadband access. Therefore, most countries are working to provide their citizens with quality SD. Future mobile communication systems offer a wide range of services - from high voice quality to high quality video, clear wireless channels with high data rates around the world. These include not only mobile phones, but also many new types of communication systems, such as local broadband wireless access systems, LAN millimeter wave networks, intelligent transport systems. Since 2015, digital military communications have already been provided to units of the Armed Forces of Ukraine of foreign production, which is based on modern technologies. The analysis of field telecommunication networks of broadband access for corporate purposes in tactical management has shown that today in the Armed Forces of Ukraine there is a re-equipment of divisions with digital means of communication and automation that allows to provide inhomogeneous qualitative information.

Formulation of the problem. To analyze telecommunication networks of broadband access of departmental purpose in the tactical link of management.

Substantive provisions. The general concept of "telecommunications" is based on the idea of the means that allow you to organize communication between two or more remote points. All network equipment used to build networks can be divided into three levels:• level of subscriber access and service networks; level of switching information flows; level of transport organization.

This distribution is typical of the large number of models offered by hardware manufacturers and software developers for different types of networks.

The access network, namely the broadband access network, serves for the best work of all components. Broadband access - access to the Internet at a data rate that exceeds the maximum possible when using dial-up access using a modem and a public telephone line. If dial-up access has a limit of about 56 Kbps and completely occupies the telephone line, then broadband technology provides many times higher data rates and does not overload the telephone line. The study of field telecommunication networks of broadband access in telecommunication networks of departmental purpose showed that currently the access area uses mainly copper cables (twisted pairs). The bandwidth and channel capacity of such cables do not allow the full implementation of modern multiservice services, ie services for the transmission of speech, data and multimedia traffic, including video information. The provision of new multiservice services requires a certain bandwidth, usually wider than that which can be provided by existing technologies in copper-cable infrastructure. Copper cables are replaced by fiber optic cable. But fiber optic cable is suitable for stationary control points. Therefore, the use of Ubiquty Airgrid M5 HP 27 dbi and NanoBridge M5 25 dBi broadband access stations will be most effective during hostilities. Broadband access stations make it possible to organize binding and communication in the tactical link of management.

Conclusion. After analyzing the use of field telecommunications networks for departmental broadband access, it was found that the main requirement for networks is to provide users with access to the resources of all computers connected to the network. An important task today is the continuous implementation of the current concept of telecommunications development in Ukraine in order to ensure the development of infocommunications. The use of broadband antennas is a necessary condition for the implementation of long-distance transmission of high-speed streams (Gbit / s). Thus, we can say that the above means of SD are available and allow to increase and improve the level of communication in the Armed Forces of Ukraine and in the country as a whole.

к.т.н. Здоренко Ю.М. (ВІТІ ім. Героїв Крут)
д.т.н. Лаврут О.О. (НАСВ)
Злобін О.К. (ВІТІ ім. Героїв Крут)

МЕТОД ВИЗНАЧЕННЯ ЗОНИ РАДІОПОКРИТТЯ В БЕЗДРОТОВИХ AD-HOC МЕРЕЖАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Актуальність. Якість обслуговування кінцевих користувачів в бездротовихad-hoc мережах військового призначення визначається множиною факторів. Сучасні технології, що покладені в основу реалізації таких мереж передачі інформації мають враховувати особливості функціонування такого класу систем та бездротових систем передавання інформації вцілому. Так, для бездротових систем характерним є випадковий характер зміни рівня сигналу в точці прийому. Це пов'язано з наявністю завмирань, які здійснюють вплив на характеристики радіоканалів. За таких умов, відсутність інформації про рівень сигналу, не дозволяє гарантувати доступність обраного маршруту та своєчасне передавання інформації, що, в свою чергу, не дає змогу забезпечити вимоги по якості обслуговування кінцевих користувачів. Тому задача завчасного визначення рівня сигналу в точці прийому в мережах з динамічною топологією є актуальною.

Виклад основного матеріалу.Перспективним напрямком удосконалення сучасних бездротових систем передачі є використання засобів радіозв'язку здатних до адаптації при зміні зовнішніх факторів. Одним з напрямків адаптації є можливість змінювати маршрут передавання інформації в мережі де кожна з радіостанцій може виступати в якості ретранслятора. Вибір маршруту визначається множиною факторів та оснований на протоколах динамічної маршрутизації. В основу таких протоколів має бути покладений розрахунок рівня сигналу для будь-яких окремо взятих радіостанцій.

Об'єктом дослідження є процес визначення можливості забезпечення радіозв'язку між різними вузлами в мережах з динамічною топологією.

Предметом дослідження є методи та засоби автоматизованого розрахунку рівня сигналу в точці прийому для військових ad-hoc мереж.

Метою дослідження є удосконалення процесу визначення маршруту передавання інформації в військових ad-hoc мережах шляхом використання автоматизованих засобів розрахунку рівня сигналу в точці прийому.

Для військових ad-hoc мереж характерною є динамічна топологія та можливість використання кожної радіостанції в якості ретранслятора сигналу. Тому для реалізації перспективного протоколу взаємодії вузлів мережі для передавання інформації необхідно завчасно визначити можливість ведення радіообміну між двома окремими радіостанціями такої мережі. При цьому потрібно врахувати ряд факторів, які здійснюють безпосередній вплив на величину сигналу в точці прийому, а саме: потужність передавача, відстань між станціями, коефіцієнти передачі трактів прийому та передачі радіостанцій, коефіцієнти підсилення передавальної та приймальної антен, характеристики середовища розповсюдження сигналу (рівень вологості повітря, діелектрична та магнітна проникність ґрунтів вздовж траси розповсюдження сигналу, характер рельєфу (забудови) та ін.), висота підйому антен, характеристики перешкод, характеристики сигналу (поляризація, частота).Метод, шо пропонується дозволить здійснювати адаптивний вибір маршруту передавання інформації з врахуванням вимог по пропускній здатності тракту.

Висновок. Таким чином використання запропонованого рішення дозволить завчасно визначати допустимі маршрути передавання інформації в військових ad-hoc мережах та може бути покладено в основу перспективного протоколу динамічної маршрутизації для таких мереж.

к.т.н. Здоренко Ю.М. (ВІТІ ім. Героїв Крут)
Марфін А. К. (ВІТІ ім. Героїв Крут)

МЕТОД АВТОМАТИЗОВАНОГО КОНТРОЛЮ ЕЛЕМЕНТІВ РОЗПОРЯДКУ ДНЯ В ПІДРОЗДІЛІ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

Одним з пріоритетних напрямків забезпечення високої ефективності управлінських рішень є всебічний аналіз умов обстановки та врахування множини факторів. Повсякденна діяльність підрозділів Збройних Сил України, як і будь-яка спеціалізована сфера діяльності, потребує високої оперативності реагування та максимальної точності в прийняті управлінських рішень. Людина, в силу своїх особливостей перед вирішенням задач масштабного характеру, не завжди здатна осягнути всі можливі взаємозв'язки між множиною факторів, які, безперечно, впливають на перебіг подій. Більшою мірою це стосується об’єктів військового призначення з високою оперативністю реагування, таких як контрольно-пропускні пункти військових частин, об’єкти інформаційної діяльності та інші режимні об’єкти. Тому основними напрямками для підвищення ефективності роботи управлінських структур, в тому числі підрозділами ЗС України є забезпечення: точності прийнятих рішень; високої оперативності їх прийняття; всебічного аналізу існуючих факторів.Реалізація цих завдань можлива при автоматизації рутинних завдань повсякденної діяльності. На даний час такі складові повсякденної діяльності військових підрозділів, як перевірка особового складу або контрольні заходи з перевірки кількості особового складу є не досконалими та ґрунтуються на організаційних заходах. Такий підхід змушує концентрувати увагу на діях, які займають багато часу, але без виконання яких, подальші етапи служби є не можливими. Тому актуальною є задача автоматизації цих процесів.

Метою роботи є підвищення ефективності процесу контролю за дотриманням елементів розпорядку дня в підрозділах шляхом використання автоматизованих засобів контролю на основі систем розпізнавання образів з використанням штучних нейронних мереж.

Провівши аналіз керівних документів, що регламентують контроль елементів розпорядку дня в підрозділі, пропонується створити підсистему автоматизованого контролю виконання елементів розпорядку дня особовим складом підрозділу. Її розробку пропонується здійснити з використанням розподіленої архітектури на основі біометричних методів з використанням математичного апарату штучних нейронних мереж. Одним з пріоритетних напрямків біометричної ідентифікації є розпізнавання людських облич. Задача біометричної ідентифікації полягає в визначенні факту володіння об'єктом розпізнавання необхідною множиною властивостей. З точки зору, вирішення задачі розпізнавання облич, необхідно, маючи два електронних зображення визначити, чи належать вони одній людині чи ні [1]. Тобто, чи мають вони множину властивостей, яка визначає належність одній людині.

Пропонується програмна реалізація, що дозволить удосконалити процес перевірки дотримання елементів розпорядку дня, за рахунок автоматизації процесу виявлення, розпізнавання та визначення кількості особового складу на основі використання математичного апарату штучних нейронних мереж.

Запропонований підхід має дозволити значно підвищити рівень оперативності контрольних заходів на об’єктах військового призначення та запобігти несанкціонованій відсутності особового складу. Напрямком подальших досліджень є синтез оптимальної за структурою нейронної мережі для розпізнавання та визначення кількості особового складу підрозділу з її програмною реалізацією.

ЛІТЕРАТУРА

1. Volchenkov M. P. About automatic face recognition / M. P. Volchenkov, I. Y. Samonenko. - Intelligent Systems, № 9.

к.т.н. Здоренко Ю.М. (ВІТІ ім. Героїв Крут)
Самозвон М.О. (ВІТІ ім. Героїв Крут)

ІНФОРМАЦІЙНА ПІДСИСТЕМА ОБЛІКУ ТА ОБРОБКИ ДАНИХ ВІЙСЬКОВОГО ШПИТАЛЮ

Актуальність. Процеси обліку та обробки даних у військово-медичних закладах Міністерства Оборони України є невід'ємною складовою їх повсякденної діяльності.

Дані процеси дозволяють ефективно організовувати діяльність такого закладу, як медичної установи, так і як військової частини. Посадові особи такого кожного дня взаємодіють з даними особових справ всіх категорій працівників, різноманітним чином здійснюють їх обробку та обліковують їх за встановленим порядком. Взаємодія зі службовою інформацією може накладати певні обмеження на коло осіб, які повинні з нею працювати, а взаємодія з медичною інформацією вимагає підвищеної швидкості її отримання та опрацювання, оскільки у критичних ситуаціях з'являється загроза життю пацієнта.

В медичні дані про пацієнтів заноситься вся докладна інформація про їх стан здоров'я. Таким чином в наявних даних можуть міститися як явні, так і неявні причинно-наслідкові зв'язки, що можуть бути використані наприклад в прогнозі обсягів сезонної захворюваності серед пацієнтів найрізноманітніших категорій. Тому задача розробки відповідних механізмів автоматизованої обробки та аналізу медичних даних та будь-яких видів прогнозування на їх основі є актуальною.

Постановка задачі. Провести аналіз сучасних методів обліку, обробки та аналізу даних у військово-медичних закладах Збройних Сил України та вдосконалити їх шляхом розробки інформаційної підсистеми обліку та аналізу даних на основі програмних рішень.

Основні положення. Належним чином організована система збору, накопичення, обробки, групування, узагальнення і реєстрації (фіксації) необхідної інформації або її повних даних, що відображають кількісну чи якісну характеристику подій, явищ, фактів, процесів, об'єктів є необхідною складовою забезпечення обліку та аналізу даних.

Керівництво військово-медичних закладів Міністерства Оборони України має потребу в автоматизації обліку та аналізу службових та медичних даних. Ці дані використовуються для забезпечення повсякденної діяльності військового шпиталю як медичної установи, так, і як військової частини. На сьогоднішній день в таких закладах, частина процесів обліку та обробки інформації все ще забезпечується з використанням паперових носіїв. Використання інформаційних систем з розподіленою архітектурою для автоматизації зазначених процесів дозволить зменшити навантаження на посадових осіб, зменшити витрати сил та засобів на обслуговування архівів необхідних даних та збільшити продуктивність праці медичного персоналу. Визначена архітектура визначає вимоги до організації самої підсистеми. Для рішення задачі пропонується використання сучасних типів розподіленої архітектури, а саме рішення на основі технології «клієнт-сервер». Клієнт-серверна архітектура інформаційної системи дозволить спростити взаємодію з медичними даними одразу декількох користувачів з різними ролями. Таким чином така архітектура інформаційної системи дозволить використовувати розподілені механізми обробки внесених даних. Також замість локального зберігання даних на кожному комп'ютері вони можуть бути оновлені в онлайн-режимі та зберігатимуться на віддаленому виділеному сервері. Крім того в рішенні, пропонується використати модуль аналітичної обробки даних для забезпечення прогнозування важливих медичних показників, що необхідні в управлінській діяльності.

Висновок. Процеси обліку та аналітичної обробки даних військово-медичних закладів Міністерства оборони України пропонується здійснювати за допомогою автоматизованих систем з розподіленою архітектурою. Для цього в подальшому пропонується розробити програмний модуль аналітичної обробки, що дозволить здійснювати прогнозування показників сезонної захворюваності серед військовослужбовців на основі накопичених даних.

к.т.н. Здоренко Ю.М. (ВІТІ ім. Героїв Крут)
Шупер О.А. (ВІТІ ім. Героїв Крут)
к.т.н. Успенський О.А. (ВІТІ ім. Героїв Крут)

АНАЛІЗ І ОЦІНКА ЗВУКОВОЇ ОБСТАНОВКИ В БОЙОВИХ УМОВАХ

Актуальність. Для розпізнавання людського мови існує велика кількість сервісів, таких як PocketSphinx, Google Speech APIта інші. Але жодне з цих рішень не дозволяє здійснювати класифікацію різних за класом звуків, що можуть супроводжувати командира в бойових умовах. До таких класів звуків можна віднести: людську мову, шум двигунів різної техніки, звуки пострілів та вибухів снарядів, крики тварин, музика та інші. Класифікація звуків може бути корисною командиру підрозділу приймати управлінські рішення з високою оперативністю та точністю та надає йому додаткові дані про обстановку в екстремальних умовах, коли природні органи слуху можуть бути пошкоджені. Тому задача створення автоматизованих систем з класифікації звуків на основі методів машинного навчання є актуальною.

Постановка задачі. Розробити програмне рішення для автоматизованого аналізу і оцінки звукової обстановки командиром підрозділу в бойових умовах.

Основні положення.Об’єктом дослідження є процес аналізу та оцінки обстановки в умовах ведення бойових дій. Предметом дослідження є методи та засоби автоматизованого збору даних обстановки та її оцінки на основі програмних рішень аналізу звуків.

Метою дослідження є удосконалення процесу оцінки обстановки в бойових умовах шляхом розробки програмних рішень аналізу та класифікації звуків.

Аудіоаналіз дозволяє здійснювати автоматизоване розпізнавання мови, цифрову обробку сигналів, а також класифікацію звуків за множиною ознак. Зазвичай звуковий сигнал характеризується такими параметрами як: основна частота, смуга частот, рівень сигналу та інші. Необхідний класифікатор звуків пропонується реалізувати на основі механізмів оцінки множини значень вхідних параметрів звукового сигналу на їх відповідність певному класу. На даний момент автоматизована обробка звуків та аналіз аудіоданих не є поширеними для аналізу обстановки у Збройних Силах України, але використання механізмів класифікації звуків дозволить більш точно та комплексно підійти до процесу обробки звукової обстановки у бойових умовах. Початковим етапом такої класифікації є постійний моніторинг звукової обстановки, оцифрування звуків та представлення їх у сучасних та зручних для обробки форматах. Приклади таких форматів: .wav (Waveform Audio File); .mp3 (MPEG-1 Audio Layer 3); .wma (Windows Media Audio).

В подальшому процес обробки звуку має включати вилучення його акустичних характеристик, необхідних для виявлення, класифікації та видачі повідомлень. Для реалізації класифікатора пропонується використати штучну нейронну мережу. Для її навчання та подальшої класифікації необхідно з оцифрованого звуку отримати необхідний набір характеристик для можливих класів звуків. Для цього пропонується виділити спектральні ознаки. Спектральні (частотні) ознаки можна отримати шляхом перетворення звукового сигналу в частотну область за допомогою перетворення Фур'є. До таких ознак відносять: частоту основного тону, частотні компоненти, спектральний центроїд, спектральний потік, спектральну густину, спектральний спад та інші. Для отримання цих ознак необхідно побудова спектрограми з подальшим вилученням необхідних ознак. Отримані таким чином ознаки використовуються як вхідні дані для навченої штучної нейронної мережі.

Висновок. Використання класифікації звуків дозволить більш точно та комплексно підійти до процесу аналізу звукової обстановки. Задачі автоматизованого аналізу та обробки звукі пропонується вирішити на основі використання штучної нейронної мережі, яка приймає вхідні дані у вигляді множини спектральних ознак і дозволяє класифікувати захоплені мікрофоном звуки. Пропоноване рішення спростить оцінку обстановки в бойових умовах.

Зінченко І.А. (ВІТІ)
Зінченко К.А. .(ВІТІ)
Бригадир С.П. (ВІТІ)

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ В СИСТЕМАХ ОЗБРОЄННЯ ТА ВОЄННОЇ ТЕХНІКИ

Актуальність.Методи машинного навчання активно впроваджуються у різні сфери застосування для програм з великими обсягами даних, де явне моделювання системи є складним. Для додатків, де простір добре зрозумілий імає математичний опис, наприклад опис впливу аеродинамічної сили на літак, методи машинного навчання доведено менш корисні, ніж в явному моделюванні.

Постановка завдання. В технічних системах озброєння та військової техніки можливість використання методів машинного навчання поки не має широкого застосування, але потребує додаткового дослідження можливості як такої.

Мета доповіді. Аналіз можлівості застосування методів машинного навачння в системах озброєння та військової техніки.

Результат дослідження. Аналізуючи використання методів машинного навчання у багатьох дослідницьких програмах розроблення зброї, стає зрозумілим, що на разі існує розрив між експериментальними інструментами і випробовуваними в польових умовах системах.

Перш ніж зброя або будь-яка військова система може бути використана, вона повинна пройти широку оцінку, тестування та розгляд єкспертів. Так як системи озброєння спрямовані на заподіяння шкоди, вони природньо можуть спричинити ненавмисну шкоду або нещасні випадки, якщо вони використовуються непередбаченим способом чи в іншій від прогнозованої і попередньо модельованої ситуації. Таким чином, надзвичайно важливо вміти розуміти і передбачати, як система зброї буде себе поводити. Це змушує розробників таких систем використовувати консервативні процеси розробки з широкими процедурами тестування та верифікації бази знань системи.

Станом на зараз хоча методи машинного навчання і виявилися корисними для багатьох галузей, вони ще не знайшли широкого використання в системах зброї. Одна з причин це складність процесу верифікації внутрішньої логіки систем розроблених на основі машинного навчання. Так, Мартін Хагстрьом у своїй роботі «Військові застосування машинного навчання в автономних системах» говорить про те, що проблеми даних систем, як технічного, так і оперативного характеру можна передбачити. До таких проблем автор відносить необхідність зробити зрозумілими системи з оперативної точки зору для їх розпорядників, а тобто військових командирів, але непередбачуваними для їх військових супротивників. Це доповнюється проблемою статистичного характеру методів машинного навчання, адже системи побудовані на даних, які є прозорими і чия когнітивна функція статистично описується. Використання машинного навчання під час зустрічі, військових вимог передбачуваності та здатності розуміти систему поведінки зброї стає викликом.

Окрема увага приділяється і даним, що використовують такі системи для навчання. Пітер Свенмарк та ЛінусЛуоцінен у своїх роботах наголошують на вразливостях роботи з вхідними даними та побудовою моделі даних для навчання систем озброєння. Так, наприклад, не збалансовані вхідні дані у системі при її верифікації, можуть призвести до того, що при бойовому застосуванні противником можуть бути створені такі вхідні дані для системи, що вона просто вийде з ладу, буде оманута противником, тощо.Інші пов’язані з даними проблеми це необхідність врахування Прав людини, даному питанню присвячено доповідь ООН «*WarnsArtificialIntelligenceCanThreatenHumanRights*», окремо гострою стає ця проблема для систем військового призначення та зброї.

Висновок.Отже, останній прорив в областях машинного навчання та штучного інтелекту поступово досягає точки, коли ці технічні рішення можна використовувати для вирішення військових задач, але військові вимоги можуть дуже відрізнятися щодо ризику, якості вхідних даних, юридичних вимог для побудови систем озброєння тощо.

Перспективи подальших наукових досліджень. Аналіз практичного використання машинного навчання у системах озброєння.

Зінченко М.О. (ВІТІ)
Лазута Р.Р. (ВІТІ)
Бородавка А.С. (ВІТІ)
Безносенко С.Ю. (ВІТІ)

РОЗВИТОК ПІДХОДІВ ПРОВІДНИХ КРАЇН СВІТУ ДО ПРОТИСТОЯННЯ В КІБЕРПРОСТОРІ

Актуальність. За даними керівника компанії McAfee, оприлюдненими на Всесвітньому економічному форумі в Давосі ще у 2010 р., вже у 2009 –2010 рр. понад 20 країн планували або здійснювали різноманітні кібероперації. Скільки країн стурбовано створенням і модернізацією власних ківбервійськ станом на 2018 – 2021 роки невідомо. Однак, зважаючи на випадки (висвітлені пресою) застосування кіберозброєнь, можна припустити, що кількість таких країн істотно зросла.

Якщо в 2010 – 2011 роки розвинуті країни лише наблизилися до розв'язання проблеми формування спецпідрозділів, завданням яких є розвідувальна робота в мережі, захист власних мереж, блокування та "обвал" структур противника з використанням можливостей кіберпростору, то в 2012 році кібервійська почали повноцінно функціонувати, і дедалі більше країн розглядали створення таких підрозділів як об'єктивну необхідність. Станом на кінець 2013 року згідно з офіційними заявами військові кіберпідрозділи з виразно захисними функціями вже було створено у США (U.S. Cyber Command); Великобританії (урядовий Cyber Security Operations Centre); Німеччині (Internet Crime Unit та Federal Office for Information Security); Австралії (The Cyber security operations centre); Індії; Ізраїлі та багатьох інших країнах. Активну позицію щодо протидії кіберзагрозам посідають провідні міжнародні безпекові організації й передусім НАТО (Cooperative Cyber Defence Centre of Excellence) та ОБСЄ.

Таким чином, провідні держави світу дедалі більше уваги приділяють розвитку й захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн, що загалом описується як проблема забезпечення кібербезпеки держави.

Метою дослідження є кібератаки, кіберінциденти, кіберзагрози та кібердії: аналіз форм та способів реалізації в провідних країнах світу та застосування цих форм в нашій державі.

Виклад основного матеріалу. Безумовно, США як одна із країн з найбільшим рівнем Інтернет-проникнення в усі сфери життя суспільства чи не найбільше опікується проблемами кібербезпеки, зокрема її військовим аспектом.

Хоча країни ЄС і виявляють певну активність у цьому напрямі, але на тлі запеклих протистоянь щодо тих чи інших нормативно-правових документів, що матимуть вплив на забезпечення кібербезпеки США, активність ЄС є набагато скромнішою.

Лише в лютому 2013 року Європейська Комісія спільно з Верховним представником ЄС у закордонних справах та з політики безпеки представили проект Стратегії з кібербезпеки "Відкритість, безпека та надійність". Стратегія спрямована на поліпшення взаємодії між державним і приватним сектором у подоланні кіберзагроз, створення єдиних баз даних щодо загроз у кіберпросторі тощо.

Аналогічні стратегії створено на рівні окремих країн ЄС, зокрема в Естонії, Фінляндії, Словаччині, Чеській Республіці, Франції, Німеччині, Литві, Люксембургу, Нідерландах, Великобританії, Польщі та Румунії.

Крім упорядкування нормативно-правового поля проблем кібербезпеки, держави ЄС та інші провідні держави готуються до протистоянь у кіберпросторі на суто практичному рівні. Вони беруть участь у навчаннях щодо протидії кібератакам. Із 2006 року США практикують навчання Cyber Storm (наразі під егідою Міністерства внутрішньої безпеки США. Крім того, у США щорічно, починаючи з 2001 року, функціонує Cyber Defense Exercise – турнір між

командами чинних захисників кіберпростору США, зокрема Агентством національної безпеки США та курсантами кількох військових навчальних закладів, що спеціалізуються на кібербезпековій тематиці.

Cyber Europe вперше відбулися в 2010 році. У 2011 році розпочато проведення спільних американсько-європейських кібернавчань Cyber Atlantic 2011, метою яких була перевірка готовності основних безпекових структур до співпраці в протидії кіберзагрозам. Для поліпшення якості таких навчань і моделювання ключових процесів функціонують спеціальні полігони на кшталт Northrop Grumman, що надають можливість виявляти проблемні зони захисту інфраструктури, моделювати можливі інциденти й виробляти типові схеми реагування, поліпшувати міжвідомчу взаємодію тощо.

Навчання, спрямовані на посилення кібербезпеки учасників, здійснює також НАТО. Із 2009 року Центр кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence) допомагає в плануванні, розроблені сценаріїв і тренуваннях у межах Навчання НАТО з кібероборони (NATO Cyber Defence Exercises) – Кіберкоаліція (Cyber Coalition). З поміж учасників навчань є навіть країни, які не є членами НАТО. Зокрема, Україна приєдналася до цих навчань у 2018 році.

Потреба в забезпеченні кібербезпеки та створенні засобів ведення кібервійн наразі спонукає уряди держав переглядати внутрішню політику в кіберсфері, оскільки дедалі частіше трапляються випадки використання розвідувальними службами та спеціалізованими військовими підрозділами можливостей і технічних потужностей транснаціональних кримінальних груп, що спеціалізуються у сфері кіберзлочинності. Звідси і зміни в інформаційній політиці, які, щоправда, стосуються передусім обмежень і цензури як механізмів здійснення внутрішньої політики.

Дедалі активніше застосовується низько-технологічний (low-tech) рівень контролю, до якого відносять бюрократичні, організаційні та обмежувальні методи захисту власного інформаційного та кіберпростору від латентних загроз безпеці даних і заходи, спрямовані на посилення цифрового суверенітету, зокрема на протидію засиллю іноземного програмного продукту.

Висновки. Провідні держави світу дедалі більше уваги приділяють розвитку й захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн, що загалом описується як проблема забезпечення кібербезпеки держави.

При цьому залишаються невирішеними питання, які унеможливлюють формалізацію безпекової політики в кіберпросторі, а саме: досі відсутні системні міжнародні нормативно-правові документи, які б чітко надавали визначення кіберпростору та всім його “безпековим” похідним; не визначено правовий статус кіберпростору; на міжнародному рівні відсутній консенсус щодо правил поведінки в кіберпросторі; відсутні загальноприйняті методології оцінки наслідків кіберзлочинів та їх розгляду як об’єкта міжнародних норм і правил (зокрема щодо визнання кібератаки як акту війни). Тому в провідних країнах світу постійно удосконалюється діяльність по забезпеченню кібербезпеки за двома ключовими напрямами:

удосконалення власного законодавства та об’єднання у відповідні безпекові організації;

створення та нарощування спроможностей власних кібервійськ та національних команд реагування на комп’ютерні інциденти, з одночасним удосконаленням ними форм і способів кібердій в рамках підготовки до кібервійни.

За таких умов, надані пропозиції щодо необхідності нарощування в Україні можливостей військових підрозділів кібербезпеки з функцією постійного удосконалення форм і способів кібердій, з одночасним розвитком національної нормативно-правової бази у сфері кібербезпеки відповідно до вимог міжнародного права.

Калашніков І.А. (ТОВ «Радіо Сатком Груп»)

РОЗВИТОК L3 HARRIS TECHNOLOGIES

L3Harris Technologies є гнучким глобальним новатором у сфері аерокосмічних та оборонних технологій, який пропонує критично важливі потребам клієнтів комплексні рішення. Компанія надає передові оборонні та комерційні технології в повітряних, наземних, морських, космічних і кібер-сферах.

Розробка новітніхтехнологійбезпосередньо стосується і тактичногозв'язку. На сьогоднішній день у L3HARRIS Technologies є ряд новихрозробок, якіздатні задовольнити сучасні вимоги до тактичнихсистем зв'язку.

Покращена радіостанція високої пропускної здатності L3Harris RF-7880NR – це найсучасніша на сьогодні автомобільна радіостанція, що ідеально підходить для використання в мережах MANET. Завдяки підтримці передової технології LTE радіостанція здатна збільшити у вісім разів пропускну здатністьканалу. За рахунок протоколу автоматичного контролю мережі, налаштування, які потребують втручання оператора, зводяться до мінімуму. RF-7880NR швидко адаптується від малих до великих мереж,які можуть містити до 240 вузлів. Захист даних забезпечує алгоритм шифрування AES, а ряд додаткових технологій запобігає подавленню каналів противником.

Одноканальна компактна персональна радіостанція RF-9820S забезпечує зв'язок в наземних тактичних групах, підтримуючи декілька режимів роботи, включаючи широкосмуговий MANET,вузькосмуговий голос і дані PLI. RF-9820S має спрощений інтерфейс, що потребує мінімального часу для освоєння оператором. Для забезпечення експлуатації в суворих умовах і зменшення навантаження на користувача радіостанція виконана в міцному та компактному формфакторі.

Польовий термінал / гучномовець L3Harris RF-7980-ST001 забезпечує дистанційний прийом та передачу голосу за допомогою польового кабелю на відстань до 3 км. RF-7980-ST001 оснащений вбудованим динаміком для чіткого відтворення звуку і дозволяє контролювати голос як за допомогою гарнітури, так і без неї. Виріб сумісний для роботи з радіостанціями Falcon III, які на сьогоднішній день експлуатуються в Збройних Силах України.

Система дистанційного управління RF-9800R дозволяє приймати і передавати дані та голос на відстань до 5 км, що забезпечує скритність фактичного місця управління. Систему можна використовувати як автономно, так і в тандемі з системою інтерком RF-7800I. RF-9800R підтримує сумісну роботу з радіостанціями Falcon II, Falcon III і Falcon IV.

Програмне забезпечення LinkBudgetCalculatorдозволяє адміністраторам мереж оцінити продуктивність радіоканалів при різноманітних сценаріях, конфігураціях обладнання, топологіях мереж і атмосферних умовах. Застосунок являється невід'ємним інструментом при попередньому плануванні та оцінці каналів зони прямої видимості, а також супутникових мікрохвильових каналів.

Наразі, для спрощення експлуатації обладнаннязв'язку персоналом Збройних Силах України,L3Harris Technologies за участю ТОВ «Радіо Сатком Груп» активно проводять роботи над створенням україномовного інтерфейсу для сімейства радіостанцій RF-7800Vта RF-7850M.

Розробка новітніх технологій L3Harris направлена на підтримкуключових пріоритетів потреб армій, а саме цілісності системи зв'язку, підвищення рівня ситуаційної обізнаності, мобільності і живучості.

Камінська А.С. (ВІТІ ім.Героїв Крут)
к.т.н. Сілко О.В. (ВІТІ ім.Героїв Крут)

МЕТОДИКА ОПТИМІЗАЦІЙ МОДУЛЮ САЙТУ ЗА ДОПОМОГОЮ SEO-ТЕХНОЛОГІЙ

Актуальність. Одним з важливих критеріїв вдалої вступної компанії ВВНЗ є доступність та інформативність матеріалів вступу для абітурієнта. Найбільш вагомий процес реалізації вступу – це результативний пошуковий запит в бік зацікавленої навчальної установи.Аналіз вступних кампаній до ВІТІ імені Героїв Крут за останні п'ять років показав, що 18 % респондентів дізналися про виш з офіційного сайту, а 36,1% вважають офіційний сайт інституту найінформативнішим медіа-ресурсом. Такий результат доводить, що незважаючи на використання молоддю соціальних мереж *Instagram, Facebook* та наявності розміщених офіційних сторінок вишу, важливим питанням залишається супровід розділу «Вступникам» на офіційному сайті Військового інституту. Цей розділ повинен мати всю необхідну та розширену інформацію, розміщення цієї інформації має забезпечувати механізми легкого доступу для користування. Ключовим інструментарієм вирішення задачі являється пошукова оптимізація *(searchengineoptimization).*

Постановка задачі. Метою роботи є покращення функціонування механізмів видимість розділу сайту для пошукових систем та сприйняття інформації відвідувачем у розділі «Вступникам» сайту ВІТІ за рахунок впровадження новітніх технологій оптимізації.

Основні положення. Оптимізація сайтузавжди починається з проведення веб-аналітики ресурсу, що включає в себе: аналіз структури та підрозділів розділу «Вступникам» (денна та заочна форма навчання ВІТІ, ВКСС ВІТІ, навчання в докторантурі та ад'юнктурі, підготовка за програмою офіцерів запасу, фаховий курс тактичного рівня, порядок дій та довідник вступника); моніторинг відвідуваності сайту (10469 переглядів профілю); аналіз цільової аудиторії; юзабіліті; визначення технічних недоліків; обчислення пошукових трафіків на сайті (5178 пошукових запитів); валідація веб-сайту (перевірка на коректність *html*-коду).Лише після отримання повної інформації з веб-аналітики можливо застосовувати запропоновані у доповіді етапи методики оптимізації:

Eman 1: збір семантичного ядра (за допомогою *GoogleAdWordsKeywordPlanner* визначаємо «*keywords*» та розподіляємо їх на високочастотні, що йдуть на головну сторінку, середньочастотні – розділи сайта та низькочастотні для самого контенту).

Eman 2: заповнення мета-тегів *«title», «description», «h1».*

Eman 3: збільшення швидкості відповіді сервера, завантаження сторінки - за допомогоюкешування даних.

Eman 4: створенняфайлів*robots.txt* і *sitemap.xml* у форматі, сумісному з пошуковим браузером.

Eman 5: коректна оптимізація*url*за допомогою додаванняключових слів.

Eman 6: за допомогою *GoogleWebmaster*та спеціальних програм *ScreamingFrogSEOSpider*визначення непотрібних дублікатів сторінок, заголовків та мета-тегів.

Eman 7: налаштування внутрішньої та зовнішньої системи перелінкування.

Eman 8: оптимізація контенту підрозділів.

Eman 9: покращення юзабіліті розділу для користувача.

Висновок. Послідовне виконання всіх етапів дозволить значно покращити видимість розділу сайту для пошукових систем та забезпечить відповідний рівень адаптивності сприйняття інформації розділу до вимог користувача. Але варто пам'ятати що,пошукова оптимізація сайту – не застигла комбінація. Вона орієнтована на алгоритми пошукових систем, а ці алгоритми часто змінюються для того, щоб протидіяти методам чорної оптимізації. Тому в подальшому планується вдосконалювати запропоновану методику відповідно до нових алгоритмів та факторів пошукової оптимізації.

Камчатна К. І. (ВІТІ)
Павлюк М. А. (ВІТІ)
Помін А. Г. (ВІТІ)

АНАЛІЗ МЕТОДІВ ВИБОРУ РОБОЧИХ ЧАСТОТ У КОГНІТИВНИХ РАДІОМЕРЕЖАХ

У світовій практиці для кожної радіослужби призначаються певні ділянки частотного діапазону на довгостроковій основі. У межах цих ділянок здійснюється призначення частот окремим радіоелектронним засобам (РЕЗ). Це призводить до неефективного використання радіочастотного спектру в цілому.

Підхід до побудови системи когнітивного радіо, котру ще називають смарт-радіо, є передовою технологією для забезпечення ефективного використання діапазону радіочастот. Когнітивні радіостанції мають можливість динамічно визначати і використовувати діапазон частот для доступу до мережі.

Вони покращують ефективність використання спектру за рахунок того, що вторинні користувачі тимчасово застосовують ліцензовані частини спектру первинних користувачів, які на цей момент не зайняті. Проте, вторинні користувачі повинні звільнити канал, який вони використовували щойно. Для того, щоб забезпечити надійну роботу системи для вторинних користувачів, використовується процедура передачі обслуговування спектру, яка повинна допомогти вторинному користувачу повернути займаний канал первинному, а самому відновити передавання на іншому або на тому самому каналі, але вже після завершення процесу передачі даних первинного користувача.

Вибір ділянки спектру є важливим процесом у мережах когнітивного радіо, який надає можливість вторинному користувачеві вибрати найкращий канал з доступних на певний момент каналів-кандидатів для здійснення передачі даних. Для того, щоб рівномірно розподілити навантаження трафіку від вторинних користувачів цими каналами-кандидатами, система прийняття рішень і вибору спектру повинна ефективно опрацьовувати статистику завантаження кожного каналу всіма можливими користувачами.

Відмінними рисами когнітивного радіо є здатність всіх прийомо-передавачів адаптивно приймати і передавати сигнал при зміні радіочастот, а також типів модуляції, кодування та інших параметрів системи.

У доповіді проведено детальний аналіз методів вибору робочих частот у когнітивних радіомережах. Їх класифікують на дві категорії: методи без балансування навантаження і методи з балансуванням навантаження.. Розглянемо їх докладніше.

1. Вибір частот без балансування навантаження – це метод, при якому вторинний користувач може вибрати свій робочий канал за одним або декількома параметрами каналу (завантаженість каналу, імовірність, того що канал знаходиться в режимі простою, час очікування).

2. Вибір частот на основі ймовірності. Цей метод працює за балансування навантаження вторинних користувачів одразу в декількох каналах когнітивної радіомережі за параметрами ймовірності того, що канал займуть, ймовірності вибору каналу, ймовірності переривання у каналі і т.д.

3. Вибір спектру на основі сканування потребує попереднього сканування всіх каналів-кандидатів, щоб знайти найбільш придатний робочий канал. За цим методом основним параметром, що впливає на тривалість системного часу, є кількість робочих каналів.

Технологія когнітивного радіо є надзвичайно перспективною для використання у системах військового радіозв’язку. Тому перспективним напрямком подальших досліджень є розробка методики вибору робочої частоти у когнітивних засобах військового радіозв’язку в умовах взаємних та навмисних завад різного походження.

Каптьол Є.Ю. (ХНУ ім. В.Н. Каразіна)

АНАЛІЗ КВАНТОВИХ МЕТОДІВ КРИПТОАНАЛІЗУ ПОСТКВАНТОВОГОЕЛЕКТРОННОГО ПІДПИСУ RAINBOW

Актуальність. У зв'язку зі зростаючим інтересом до квантового криптоаналізу, пов'язаного з успіхами в розробці квантового комп'ютера, в межах конкурсу NIST PQC було проведено відбір, за яким до третього раунду було допущено 3 електронних підписи, що претендують на використання в постквантовий період: CRYSTAL-DILITHIUM, FALCON, Rainbow. Так як Rainbow є одним з фіналістів, варто розглянути методи його криптоаналізу, що можуть використати перевагу, надану квантовим комп'ютером.

Постановка задачі. Провести аналіз методів криптоаналізу постквантового електронного підпису Rainbow. Виділити методи, що придатні для застосування з використанням квантового комп'ютера.

Основні положенні. На конкурс NISTPQC було представлено 3 варіанти схеми електронного підпису та кожен з них має свої набори параметрів для різних категорій безпеки, їх варто розглядати окремо. На конкурс було представлено такі варіанти схеми електронного підпису Rainbow: звичайний алгоритм Rainbow, CZ-Rainbow та стислий алгоритм Rainbow.

Набори параметрів для зазначених варіантів електронного підпису відповідають різним категоріям безпеки NIST. Кожен з варіантів Rainbow має 3 набори параметрів: I, III та V. Відповідність наборів параметрів категоріям безпеки NIST наступна: набір параметрів I відповідає категоріям безпеки I та II, набір параметрів III відповідає категоріям безпеки III та IV, набір параметрів V відповідає категорії безпеки V.

Всі відомі атаки, що можуть бути застосовані до Rainbow, є класичними. Проте деякі з них можуть використовувати переваги, що надаються квантовим комп'ютером, шляхом застосування квантових алгоритмів до деяких кроків атаки. До атак на Rainbow можна віднести: атаки знаходження колізій на геш-функції, прямі атаки, атаки MinRank, атаки HighRank, атаки "Rainbow-Band-Separation" (RBS), атаки UOV, атаки на диференціальне поле та квантові атаки «грубої сили».

Серед них використовують квантові методи для пришвидшення наступні методи:

- прямі атаки
- атаки HighRank
- атаки UOV
- квантові атаки «грубої сили».

Прямі атаки. Найбільш прямолінійною атакою на Rainbow вважається пряма алгебраїчна атака, де рівняння $\mathrm{P}(\mathbf{z}) = \mathbf{h}$ розглядається як приклад задачі MQ. Складність вирішення такої системи оцінюється як кількість множень у полі, що наведена у формулі (1), де d_{reg} – це так звана ступінь регулярності системи.

$$\text{Complexity}_{\text{direct; classical}} = \min_k \left(q^k \cdot 3 \cdot \binom{m-k+d_{\text{reg}}}{d_{\text{reg}}} \cdot \binom{m-k}{2} \right) \quad (1)$$

Застосування квантового комп'ютера надає перевагу при використанні «гібридного підходу». Складність оцінюється як кількість множень у полі наведена у формулі (2).

$$\text{Complexity}_{\text{direct; quantum}} = \min_k \left(q^{k/2} \cdot 3 \cdot \binom{m-k+d_{\text{reg}}}{d_{\text{reg}}}^2 \cdot \binom{m-k}{2} \right) \quad (2)$$

Атака HighRank полягає у виявленні змінних, що з'являються найменшу кількість разів у центральних поліномах. Складність цієї класичної атаки оцінюється як кількість множень у полі, наведена в формулі (3).

$$\text{Complexity}_{\text{HighRank; classical}} = q^{O_u} \cdot \frac{n^3}{6}. \quad (3)$$

Застосування квантового комп'ютера дозволяє зменшити кількість множень у полі до кількості наведеної у формулі (4).

$$\text{Complexity}_{\text{HighRank; quantum}} = q^{O_u/2} \cdot \frac{n^3}{6} \quad (4)$$

Атаки UOV. У зв'язку з тим, що Rainbow можна розглядати як продовження добре відомої схеми підписів OilandVinegar, можна стверджувати, що її можна атакувати, з використанням всіх відомих атак UOV. Таким чином, наприклад, може бути застосована атака UOV «Oil Subspace» Кіпніса та Шаміра.Rainbow також можна розглядати як екземпляр UOV з $\upsilon = \upsilon_1 + o_1$ та $o = o_2$.

Складність цієї класичної атаки оцінюється як кількість множень у полі, наведена в формулі (5).

$$\text{Complexity}_{\text{UOV-Attack; classical}} = q^{n-2_{o_2}-1} \cdot o_2^4 \quad (5)$$

Кількість множень у полі, до якої застосування квантового комп'ютера та алгоритма Гровера зменшує складність наведено на формулі (6).

$$\text{Complexity}_{\text{UOV-Attack; classical}} = q^{\frac{n-2_{o_2}-1}{2}} \cdot o_2^4 \quad (6)$$

Квантові атаки «грубої сили». За умови застосування для криптоаналізу квантового комп'ютера, атака «грубої сили» може бути суттєво прискореною шляхом використання алгоритму Гровера. Також в якості квантових методів може бути використано не тільки алгоритм Гровера, а й метод Шора.

Очікується, що використання алгоритму Гровера при проведенні квантового криптоаналізу методом «губої сили» призведе до квадратичного прискорення атаки «грубої сили».

Висновок. Враховуючи відомості про атаки на електронний підпис та оцінки складності атак на набори параметрів можна зробити висновок про наявність можливості реалізації атаки стосовно електронного підпису Rainbow та про можливість застосування квантового комп'ютера для зменшення складності атак.

Проте також слід зауважити, що пришвидшення атак за допомогою квантового комп'ютера є нерівномірним. Через це для різних наборів параметрів оптимальними є різні атаки. Так, наприклад для набору параметрів I найкращою атакою з використанням квантового комп'ютера є атака HighRank, а для наборів параметрів III та V – пряма атака.

Також важливим моментом є те, що повністю квантовою атакою з наведених є лише квантова атака «грубої сили». Інші атаки використовують квантові методи лише для виконання певної частини атаки.

к.т.н. Касім Н.Х.
д.т.н. Хлапонін Ю.І. (КНУБА)
Симоненко О.А. (ВІТІ)

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ LTE ПРИ ВПРОВАДЖЕННІ ІНТЕРНЕТУ РЕЧЕЙ

За підсумками 2020 р. в світових мережах LTE 4,5 млрд підключень - це 57% всіх мобільних підключень. До кінця цього року 4G-мережі охоплять 80% світового населення, а в 2026 році - 95%. Пік попиту на LTE доведеться на 2021 рік, коли число підключень досягне 4,8 млрд, а потім попит на послуги LTE почне плавно знижуватися і до кінця 2026 року становитиме всього 3,9 млрд підключень. Причина очевидна - міграція абонентів на технології 5G [1].

Для ринку мобільного зв'язку 2020 рік став роком технологій п'ятого покоління (5G) - кількість комерційних мереж перевалило за 100, і до кінця року в зоні їх покриття буде жити 15% населення планети. Вже зараз очевидно, що 5G стане найшвидше розвивається технологією, яка за темпами поширення значно випередить стандарти попередніх поколінь. До кінця року оператори наберуть 220 млн 5G-підключень, а в 2026 році - вже 3,5 млрд. Створюються нові сценарії, які використовують ключові переваги технологій 5G: низьку затримку, високу швидкість і надійний захист переданих даних [2].

З розвитком мереж 5G широке поширення отримають сценарії використання, створені на основі критично важливих підключень пристроїв інтернету речей (CriticalIoT). Завдяки розвитку мереж 5G і інтернету речей (IoT) п'ятого покоління з'явиться безліч нових послуг для людей і суспільства в цілому, а зростання сегмента технологічних мереж 5G сприятиме розвитку бізнесу в усіх секторах. Передача даних в гарантований період часу - наприклад, за 50 мілісекунд з гарантією 99,9% - буде необхідна для роботи додатків, призначених для управління пристроями на відстані, а також для розважальних сервісів.

Експерти нарахували чотири типи перспективних сценаріїв використання технологій 5G, для яких необхідне підключення до мережі з гарантованим часом передачі даних [2].

1. Медійні технології в реальному часі - підключення, в яких час передачі даних відіграє ключову роль. Вони дозволяють створювати індустріальні додатки і хмарні ігрові сервіси з використанням технологій доповненої і віртуальної реальності (AR / VR).

2. Управління пристроями на відстані - людина дистанційно управляє машинами та обладнанням, що пересуваються по землі і повітрю. Людям більше не доведеться працювати в складних кліматичних і небезпечних умовах - замість цього вони будуть контролювати автономні пристрої.

3. Промисловий контроль - функції моніторингу та контролю в режимі реального часу будуть застосовуватися для управління розумними мережами, а для роботів стануть доступні технології машинного зору.

4. Мобільна автоматизація - автоматизація циклу управління транспортними засобами і мобільними роботами забезпечить безпечне маневрування безлічі дистанційно керованих пристроїв на одному майданчику.

LTE категорії M1 – еволюційний розвиток LTE, оптимізований під IoT. В той же час, інноваційною технологією Інтернету речей є рішення вузькосмугового (шириною 180 кГц) IoT (Narrow-Band IoT або NB-IoT). Це бездротовий вузькосмуговий різновид глобальних мереж з низьким енергоспоживанням (Low Power Wide Area, LPWA), який в першу чергу призначений для додатків міжмашинної взаємодії (M2M). Перевагами LTE Cat M1 є більш висока швидкість передачі даних, а також мобільність, що дозволить використовувати пристрої для моніторингу рухомих об'єктів. Відносними недоліками є менша зона покриття (порівняно з NB IoT) і досить широкий частотний діапазон (1,08 МГц), що потребує виділення таким пристроям окремих ресурсних блоків. NB IoT має найкраще покриття та суттєво меншу смугу, що дозволяє використовувати захисні інтервали і тим самим ніяк не впливати на ємність LTE-мережі при роботі з підвищеними категоріями. Крім того, деякі

виробники обладнання анонсували, що модернізація мереж LTE для роботи з NB IoT вимагатиме лише оновлення програмного забезпечення, що значно менш витратно для операторів. Мінусом же NB IoT, у свою чергу є обмежена мобільність. Стандарт NB-IoT відкриє компаніям, що спеціалізуються на наданні телекомунікаційних послуг, широкий спектр нових можливостей. Зокрема, істотно збільшить прибутковість операторів від одного абонента (Average revenue per user, ARPU). Технологія NB-IoT займе свою низькошвидкісну нішу в класі рішень, де пріоритетне значення має безперебійна передача даних і низьке енергоспоживання [3].

Nb-IoT- це специфікація стандарту стільникового зв'язку, яка розроблена для обслуговування пристроїв, що генерують невеликий обсяг даних. Технологія відмінно підходить для різних лічильників, датчиків, систем сигналізації та ін.

По своїй фізичній структурі і архітектурі мережу Nb-IoT практично все успадкувала від LTE, тому побудова інфраструктури для Інтернету речей не вимагає нічого, крім оновлення програмного забезпечення на наявних базових станціях. За рахунок простоти системи оператори можуть надавати низькі тарифи для клієнтів Інтернету речей.

Основні характеристики Nb-IoT

Достатня пропускна здатність для більшості IoT-пристроїв.

Можна обмінюватися об'єктами рознесені в часі.

Можливість роботи на більш віддаленій території, ніж 4G на тій же частоті.

Стійкість до шумів.

Неймовірно низьке енергоспоживання (датчики можуть «жити» від однієї батареї близько 10 років).

Знижені вимоги до процесора.

Щоб зрозуміти, як досягаються перераховані властивості, варто трохи заглибитися в технічну складову мережі.

Nb-IoT базується на LTE. Якщо говорити максимально простими словами, то смуга 4G складається з окремих каналів (піднесучих) по 15 кГц. Несуча в LTE ділиться на ресурсні блоки (РБ), кожен з яких складається з 12 піднесучих по 15 кГц. Разом виходить 180 кГц. Кожен ресурсний блок включає 84 ресурсних елемента (сітка 12 на 7). Смуга 5 МГц, на якій може працювати LTE, включає 25 ресурсних блоків.

Для запуску Nb-IoT задіюється тільки один ресурсний блок 180 кГц. Для дальності сигналу його підсилюють на 6 дБ. Це і пояснює, чому мережа Інтернету речей має більш широке охоплення території, ніж LTE, хоча частота використовується однакова.

З розвитком Інтернету речей (Internet of Things, IoT) кількість підключень до мереж мобільного зв'язку операторів збільшиться в рази. За прогнозами Ericsson [3], в 2021 році загальна кількість підключених до інтернету пристроїв в світі складе 28 млрд. З них 1,5 млрд складуть споживча електроніка і розумні автомобілі, які взаємодіють один з одним за допомогою мереж мобільного зв'язку. У найближчі роки кількість міжмашинних підключень (Machine-to-Machine, M2M) буде рости на 25% в рік, більша частина M2M-пристроїв, що поставляються на ринок буде підтримувати стандарт LTE. У міру зростання ринку IoT стає очевидним, що для багатьох варіантів використання таких рішень існуючі технології мобільного зв'язку недостатні у зв'язку з недостатнім покриттям, високою вартістю кінцевих терміналів і малим терміном служби їх елементів живлення.

ЛІТЕРАТУРА

1.https://www.researchgate.net/publication/318509080_3GPP_evolution_on_LTE_connectivity_for_IoT

2.https://halberdbastion.com/sites/default/files/2017-06/Nokia_LTE_Evolution_for_IoT_Connectivity_White_Paper.pdf

3. https://shop-gsm.ua/blog/chto-takoe-set-nb-iot-i-kakovy-ee-osobennosti

д.т.н. Качинський А.Б. (КПІ ім. Ігоря Сікорського)
Кіреєнко О.В. (КПІ ім. Ігоря Сікорського)
Козленко О.В. (КПІ ім. Ігоря Сікорського)

СТОХАСТИЧНА МОДЕЛЬ ПОРУШНИКА ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ОСНОВІ МАРКІВСЬКИХ ПРОЦЕСІВ РОЗМНОЖЕННЯ ТА ЗАГИБЕЛІ

Розробка моделі порушника є одним із перших кроків побудови захищеної інформаційної системи. Постійне протистояння між порушником та стороною захисту і зміна умов (законодавчих, географічних, політичних), в яких воно відбувається потребують нових моделей, здатних враховувати подібні зміни.

На разі при розробці моделі порушника переважають неформальні підходи, що відображають причини та мотиви його дій, знання та можливості, пріоритети у досягненні поставлених цілей: тактика, місце й характер дій, а також шляхи реалізації запланованих кіберзагроз.Адекватна модель порушника гарантує розробку ефективної системи забезпечення кібербезпеки, опираючись на яку можна розробляти відповідні механізми прогнозування й відвертання кіберзагроз.

Розробка математичних моделей порушника для отримання кількісних оцінок збитку є актуальною науково-практичною задачею. На цей час спостерігаються тенденції розширення моделі порушника інформаційної безпеки до більш загальних моделей, що включають інші типи порушників (крадії, вандали та ін.) та інформацію про саму інформаційну систему. Включення подібної інформації дозволяє розробляти більш деталізовані і одночасно з цим спеціалізовані моделі під конкретну систему, а це означає, що єдиного стандартизованого підходу до побудови моделей немає, що створює додаткові труднощі при розробці власної моделі (не можна зробити по аналогії, є проблеми із перенесенням інформації між моделями та інші труднощі). У даному дослідженні до вирішення проблеми розробки моделі порушника пропонується модель, що заснована на марківських процесах розмноження й загибелі. Її характерною рисою є те, що вона описує поведінку зловмисника як випадковий процес з дискретним числом станів, що відбувається в системі *S*.

Такий підхід дає змогу розглядати формалізований опис зловмисника як порушника правил розмежування доступом, що може з будь-якого стану безпосередньо переміститься тільки в один з його сусідніх станів.

Розроблена авторами модель дозволяє:

1. Віднести атаку до одного із чотирьох сценаріїв (атаки на операційну систему, веб-середовище, передачу даних та атаки пов’язані із користувачами).
2. Оцінити середній час перебування порушника на кожному етапі атаки і визначити відповідні збитки.
3. Виявити вплив механізмів захисту на етапи атаки і обрати набір механізмів, що мінімізує збиток або максимізує прибуток (якщо ризик допускає сприятливі та шкідливі зміни в системі).
4. Відображати сформовану модель у вигляді системи диференційних рівнянь Колмогорова, для розв’язку якої можна використовувати доступне програмне забезпечення.

Таким чином, авторами розроблено та запропоновано для використання модель порушника інформаційної системи на основі марківських процесів з безперервним часом.

Відмінністю даної моделі від відомих те, що дії порушника розглядаються як випадковий процес з кінцевим числом станів системи.

Для перевірки адекватності запропонованої моделі були обрані чотири сценарії атаки на інформаційно-комунікаційну систему. Розрахунки сценаріїв здійснювалися на прикладі чотирьох найбільш відомих інцидентів безпеки за останні 5 років. Наступним кроком у дослідженні є застосування запропонованого підходу, у тому числі шляхом модифікації розробленої моделі для отримання результатів можливого прибутку/збитку з урахуванням неповноти та неточності інформації.Textovod = 93%

КіреєнкоО.В. (КПІ імені Сікорського)
КозленкоО.В. (КПІ імені Сікорського)
д.т.н Качинський А.Б.(КПІ імені Сікорського)

СТОХАСТИЧНА МОДЕЛЬ ПОРУШНИКА

Актуальність.Описується модель порушника на основі марківських процесів розмноження та загибелі - математична модель порушника, що містить інформацію про етапи атаки, час перебування в цих станах, та інтенсивності вихідних потоків.

Представлення атаки у вигляді марківського процесу дозволяє співставити із станами етапи атаки, а значення інтенсивностей вихідних потоків залежать від впроваджених механізмів захисту.

Оскільки метою сторони захисту є зниження рівня збитку, кожна послідовність станів аналізується на прийнятність, враховуються не лише витрати, спричинені заданим сценарієм а і вартість механізмів захисту, необхідна для спрямовування порушника саме цим маршрутом.

Постановка задачі. Провести аналіз існуючих кібератак, виявити найбільш розповсюджені типи атак, розробити марківський процес розмноження та загибелі для них. Порівняти із відомими атаками.

Основні положення.Марківський процес розмноження та загибелі можна представити у вигляді орієнтованого зваженого графу. Вершинами графу є стани, що відповідають етапам атаки. З кожним станом пов'язана вартість перебування в даному стані за одиницю часу. Дуги графу відповідають інтенсивності потоків. Чим більша інтенсивність вихідних потоків для даного стану і чим менша інтенсивність вхідних потоків, тим меншим є середній час перебування в даному стані. Будь-який сценарій можна розділити на 2 частини: власне атаку, та відновлення після атаки. Марківський процес розмноження та загибелі допускає існування розгалужень та циклів.

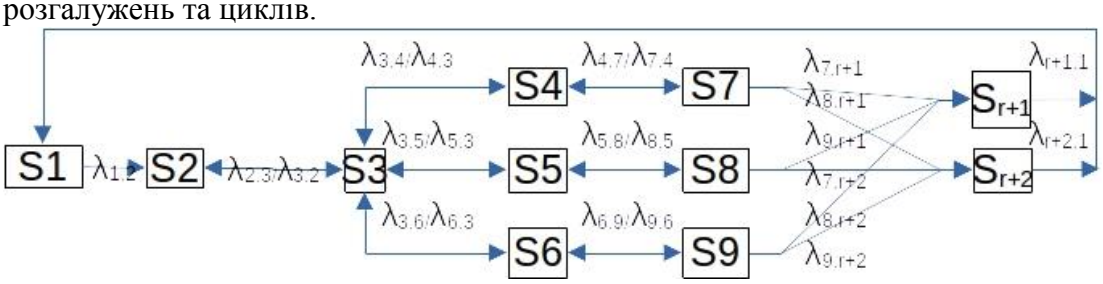


Рис.1 марківський процес для атаки Solorigate

В марківському процесі можуть бути однакові стани, які тим не менш представлені як дві або більше різних вершин графу. Це використовується у випадках, коли порушник може повернутися на попередній етап атаки, але лише тим шляхом, яким прийшов (без переходу з однієї гілки на іншу). Також допускаються стоки - стани із вхідними потоками, але без вихідних. Вони не впливають на отриману систему рівнянь.

Загальними станами для всіх сценаріїв є:

S_0: режим штатного функціонування системи-цілі;

S_1: режим штатного функціонування системи-цілі (відмінність S_1 від S_0 полягає в наявності вхідних дуг);

S_2: підготовка до атаки;

S_3: проникнення в систему та вибір способу атаки;

$S_{(3+i+kn)}$: стани, що відповідають зловмисним діям у системі, де n – кількість гілок розгалуження, k – порядковий номер зловмисної дії атаки, i – порядковий номер гілки розгалуження. При чому $n = 1$, якщо розгалуження відсутні, нумерація k починається з нуля і для i нумерація починається з одиниці. Цим станам відповідають шкідливі дії, які порушник може здійснити в системі після проникнення. Наприклад, це може бути завантаження шкідливого ПЗ (віруси, *ransomware*, *botne*t-клієнт), підвищення повноважень (використання

відомих вразливостей, шел-код), відключення механізмів захисту, припинення запущених в системі прикладних задач, взаємодія із законними користувачами, замітання слідів.

$S_{(r+j+lm)}$: стан відновлення системи, де r – кількість шкідливих дій, j – порядковий номер гілки, l – порядковий номер дії, m – кількість гілок. Тут порядковий номер j починається з одиниці, для l порядковий номер починається з нуля. Ці стани описують способи усунення вразливостей і наслідків атаки, тестування системи перед повторним введенням в експлуатацію.

Переходи між станами відповідають життєвому циклу кібератаки. Для станів $S_{(3+i+kn)}$ це означає виконання наступної зловмисної дії, або виконання тієї ж дії для іншого сегменту системи. Рух в протилежний бік (справа на ліво) означає відміну здійснюваних зловмисих дій, за будь-якої причин (виявлення більш загрозливої атаки, неможливості замітання слідів, помилки, пов'язаної із людським фактором, технічного збою як на стороні порушника, так і в самій інформаційній системі), що примушують порушника розпочинати атаку заново.

Система диференційних рівнянь Колмогорова для сценарію 1 має вигляд:

$$\begin{cases} \lambda_{1,2}P_1 + \lambda_{3,2}P_3 = P_2\lambda_{2,3} \\ \lambda_{2,3}P_2 + \lambda_{4,3}P_4 + \lambda_{5,3}P_5 + \lambda_{6,3}P_6 = P_3\left(\lambda_{3,2} + \lambda_{3,4} + \lambda_{3,5} + \lambda_{3,6}\right) \\ \lambda_{3,4}P_3 + \lambda_{7,4}P_7 = P_4\left(\lambda_{4,3} + \lambda_{4,7}\right) \\ \lambda_{3,5}P_3 + \lambda_{8,5}P_8 = P_5\left(\lambda_{5,3} + \lambda_{5,8}\right) \\ \lambda_{3,6}P_3 + \lambda_{9,6}P_9 = P_6\left(\lambda_{6,3} + \lambda_{6,9}\right) \\ \lambda_{4,7}P_4 = P_7\left(\lambda_{7,r+1} + \lambda_{7,r+2} + \lambda_{7,4}\right) \\ \lambda_{5,8}P_5 = P_8\left(\lambda_{8,r+1} + \lambda_{8,r+2} + \lambda_{8,5}\right) \\ \lambda_{6,9}P_6 = P_9\left(\lambda_{9,r+1} + \lambda_{9,r+2} + \lambda_{9,6}\right) \\ \lambda_{7,r+1}P_7 + \lambda_{8,r+1}P_8 + \lambda_{9,r+1}P_9 = P_{r+1}\lambda_{r+1,1} \\ \lambda_{7,r+2}P_7 + \lambda_{8,r+2}P_8 + \lambda_{9,r+2}P_9 = P_{r+2}\lambda_{r+2,1} \\ \lambda_{r+1,1}P_{r+1} + \lambda_{r+2,1}P_{r+2} = P_1\lambda_{1,2} \end{cases}$$

і відповідна матриця

$$\begin{pmatrix} 0 & \lambda_{1,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_{2,3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_{3,2} & 0 & \lambda_{3,4} & \lambda_{3,5} & \lambda_{3,6} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_{4,3} & 0 & 0 & 0 & \lambda_{4,7} & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_{5,3} & 0 & 0 & 0 & 0 & \lambda_{5,8} & 0 & 0 & 0 \\ 0 & 0 & \lambda_{6,3} & 0 & 0 & 0 & 0 & 0 & \lambda_{6,9} & 0 & 0 \\ 0 & 0 & 0 & \lambda_{7,4} & 0 & 0 & 0 & 0 & 0 & \lambda_{7,r+1} & \lambda_{7,r+2} \\ 0 & 0 & 0 & 0 & \lambda_{8,5} & 0 & 0 & 0 & 0 & \lambda_{8,r+1} & \lambda_{8,r+2} \\ 0 & 0 & 0 & 0 & 0 & \lambda_{9,6} & 0 & 0 & 0 & \lambda_{9,r+1} & \lambda_{9,r+2} \\ \lambda_{r+1,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_{r+2,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Атака Solorigateє прикладом атаки, пов'язаної із користувачем. До цього типу відносять APT-атаки. Характерною ознакою для них є наявність великої кількості дуг спрямованих в протилежну сторону (можливість повернутися до попереднього етапу атаки). На рис. 1 такі дуги позначені як двунаправлені стрілки.

Наступним сценарієм є атаки на операційну систему. Використання відомих вразливостей, для конкретної ОС означає, що причин повертатися на попередній етап у порушника не буде, тому марківський процес для такої атаки схожий на рис 1, але більшість маршрутів спрямовані зліва-направо.

Атаки на веб-середовище є лінійними, так як стани в марківському ланцюзі відповідають за зараження окремих вузлів. Атака на веб-середовище із компрометацією та відновленням сегментів системи є найбільш простою. Відмінність між марківськими ланцюгами, що використовують для моделювання в інших предметних областях є поділ на власне атаку та відновлення після атаки. На межі цих двух марківський ланцюг може відрізнятися (наприклад це може бути єдина пара вузлів графу, для якої немає двостороннього зв'язка). Для систем, що мають велику кількість вузлів, модель можна оптимізувати, розглядаючи компрометацію та відновлення вузлів не по одному, а групами із k. При цьому можна використовувати різні розміри груп для компрометації (наприклад по 10) і відновлення (наприклад по 3 вузла), що відповідатиме особливостям даної організації (кількість кваліфікованих працівників із адміністративними правами, здатними ініціалізувати процес відновлення із резервної копії або кількість вузлів, які можна відключити від системи для обслуговування, поки решта вузлів продовжують функціонувати в скомпрометованому стані через необхідніст вирішення ними прикладних задач).

Останнім четвертим типом атак є атаки на дані під час передачі. Характерною ознакою таких атак є розділ на дві гілки. Перша гілка відповідає прослуховуванню в режимі реального часу, а друга - записуванню інформації на носій з метою подальшого вилучення та вивчення зібраної інформації. Так як у другому випадку порушник забирає обладнання, що використовувалося для прослуховування, в моделі це виглядає як вихід із циклу і завершення атаки стоком.

Після складання системи рівнянь для відомої атаки, сторона захисту розв'язує систему рівнянь будь-яким зручним методом відносно невідомих значень $\lambda_{i,j}$. Ці значення описують ефективність механізмів захисту від порушника, який був відповідальний за дану атаку. Наступним кроком є пошук нового набору значень $\lambda_{i,j}$ при якому величина збитку, обрахована як сума добутків вартості перебування в кожному із станів на тривалість перебування у відповідних станах. Якщо не існує прийнятного набору значень $\lambda_{i,j}$ - від використання системи в її поточній конфігурації потрібно відмовитися. Для наборів, що задовольняють вимоги щодо інтегрального ризику сторона захисту порівнює їх вартість. Ще одним критерієм є прийнятий в організації підхід до ризику: riskaverse | riskneutral. При riskneutral підході значення має лише інтегральна оцінка. Величина збитку на кожному окремому етапі атаки ігнорується якщо якийсь інший етап генерує прибуток (найчастіше це стан S_0 - штатне функціонування системи). Riskaverseорганізації можуть додатково розглядати величину збитків для перших k етапів атаки для довільного значення k, щоб переконатися у відсутності катастрофічних наслідків для системи. Крім цього стороні захисту потрібно зробити вибір між мінімізацією збитку для песимістичного сценарію та максимізацією прибутку для оптимістичного.

Одному механізму захисту можуть відповідати декілька значень $\lambda_{i,j}$, або навіть всі. При цьому залежність не завжди однакова. Зменшення збитку для одного із станів системи може означати його зростання для наступного етапу. Так само зменшення збитку для однієї із гілок може означати, що порушник скористається іншою гілкою, для якої не було передбачено механізмів захисту.

Ефект від сумісної дії механізмів захисту може не відповідати сумі ефектів від даних механізмів, взятих окремо. Можливими є ефект синергії та перешкоджання.

Модель також може використовуватися для обгрунтованого *відключення*вже наявних механізмів захисту за умови їх неефективності та перешкоджанню роботи інших механізмів.

Висновок. Було запропонували використовувати модельмарківських процесів з неперервним часом. Перевагою цього метода стало те, що дії порушника розглядаються як випадковий процес з кінцевим числом станів системи. Для опису використання моделі були обрані 4 сценарії атаки на інформаційно-комунікаційну систему. Розрахунки сценаріїв були продемостровані на прикладі 4 інцидентів за останні 5 років. Наступним кроком для поліпшення цього підходу буде модифікація моделі і отримання результатів можливого прибутку/збитку з урахуванням неповної інформації.

Коваленко В.Р. (ВІТІ ім. Героїв Крут)
к.т.н. Здоренко Ю.М. (ВІТІ ім. Героїв Крут)

МОДУЛЬ АНАЛІТИЧНОЇ ОБРОБКИ ДАНИХ ВІЙСЬКОВОЮ СЛУЖБОЮ ПРАВОПОРЯДКУ

Актуальність. В сучасних інформаційних системах існує ряд невирішених задач, пов'язаних з накопиченням великої кількості різнорідної інформації та необхідністю подальшої її обробки та аналізу. Накопичені дані можуть мати різний ступінь структурованості, що впливає на кінцеві показники оцінки якості їх обробки. Також, в накопичених даних можуть міститися неявні причинно-наслідкові зв'язки, які мають бути використані посадовими особами для підтримки прийняття управлінських рішень. Існуюча інформаційна система обліку та аналізу правопорушень військової служби правопорядку ЗС України потребує удосконалення. Впровадження електронного зберігання даних у підрозділах Військової служби правопорядку ЗС України зумовлено підвищеними вимогами, щодо оперативності опрацювання інформації, спрощенням її пошуку та контролю за виконанням, удосконаленням механізмів узагальнення даних, які надійшли, аналітичного пошуку закономірностей та неявних зв'язків між зафіксованими фактами. Тому актуальною є задача розробки відповідних механізмів обліку та аналізу великих даних в такій інформаційній системі.

Виклад основного матеріалу.

Об'єктом дослідження є процес обліку та аналізу правопорушень військовослужбовців ЗС України. Метою дослідження є удосконалення процесу обліку та аналізу даних про правопорушення військовослужбовців ЗС України шляхом розробки та впровадження автоматизованих систем на основі програмних рішень.

Основна задача полягає в розробці програмного модулю для автоматизованого обліку та аналізу правопорушень військовослужбовців ЗС України. Часткові задачі дослідження полягають в: проведенні аналізу процесу обліку правопорушень в ЗСУ військовою службою правопорядку та виявленні його недоліків; розробці проекту програмного модулю автоматизованого обліку та аналізу правопорушень; здійсненні реалізації програмного модулю за визначеним алгоритмом; дослідженні ефективності впровадження програмного модулю в процес обліку правопорушень.

Керівництво Військової служби правопорядку має потребу в періодичній систематизації та узагальненні накопичених даних за визначений проміжок часу. Така інформація необхідна в процесі прийняття управлінських рішень та прогнозуванні динаміки правопорушень військовослужбовців. Існуючі механізмів аналізу даних в інформаційних системах здебільшого здійснюють їх аналітичну обробку на основі традиційних підходів, які основані на використанні методів статистичної обробки даних, що не завжди дозволяє отримати очікуваний результат. Одним з перспективних підходів пошуку неявних закономірностей в даних є застосування методів інтелектуального аналізу даних, що дає можливість вирішити наступні задачі: асоціації, візуалізації, класифікації, кластеризації, прогнозування; та інші. Використання розподіленої архітектури для реалізації інформаційних систем дозволяє здійснювати накопичення та обробку даних на множині вузлів мережі. Така архітектура інформаційної системи також визначає вимоги до механізмів обробки накопичених даних. Розподілена архітектура інформаційної системи передбачає використання розподілених механізмів обробки даних, замість зберігання даних в одній файловій системі, дані зберігають та індексують на множині вузлів.

Висновки. Таким чином аналітичну обробку данихправопорушень військовою службою правопорядку ЗС України пропонується здійснювати на основі поєднання методів інтелектуального аналізу даних з механізмами розподіленої обробки даних, що дозволить виявляти неявні закономірності в великих обсягах накопичених даних.

Kovalchuk L.V. (NTUU “KPI named by IhorSykorskii”)

USING GENERAL SIDE-CHAIN APPROACH FOR BUILDING A STATE REGISTER

The question of building secure state register, which may combine all particular registers, is very important in current situation. One of the challenge ideas is to use blockchain for it.

One of the serious shortcomings of blockchains, which is at the same time a significant inconvenience, is the low network throughput. For example, according to various estimates, the number of transactions per second in the BTC is estimated in the range from 3 to 7, with the desired speed of up to several thousand.

In the available literature, you can find a plethora of different suggestions on how to increase the throughput. These suggestions can be roughly divided into two types:

1) transition from blockchain to block graph (DAG – directed acyclic graph);

2) use various “add-ons” over the blockchain.

In the papers of the first type the authors announce improvements in both throughput and latency until the transaction is fully confirmed. However, none of these papers contains rigorous proofs of the stated results, at best, semi-empirical reasoning. Some also have serious mathematical errors.Papers from the second type contain more substantiated statements and more rigorous proofs. However, they solve only one of the existing problems—increasing the throughput. The second remains currently unresolved.

The main idea of the second type of papers is that, in addition to the classic “reliable” blockchain with “slow” block generation, which is called MainChain (MC), one can generate additional “separate” blocks or even blockchains that can be produced as quickly as you like (with minimal PoW or PoS). These blocks can refer to each other and/or to the mainchain, and in this case, the mainchain must refer to these additional blocks.

Block B not included in the MC is considered stable (i.e., such in which transactions are irreversible with a probability close to 1) if the block B^* from MC containing the first reference to the block B is stable. I.e., stabilization of a block that is not part of the MC is still a consequence of stabilizing the corresponding block from the MC. Therefore, the time until the block stabilizes remains long.The PoP protocol recently suggested can also be classified as type 2 blockchain. But its main difference from the protocols proposed earlier is that it uses a “foreign” blockchain as an MC, for example, BTC. In this case, communication with the MS should be “two-way.”

The Veriblock (VB) blockchain with PoP consensus refers to blocks from the MC, and the MC must, at certain limited intervals, refer to the VB. The blockchain that is MC is called Security Provided (SP blockchain), and the VB blockchain is called Security Inherited (SI blockchain). This protocol increases the throughput (i.e., tps) significantly, but the transaction confirmation time is still fully determined by SP blockchain.

The PoP protocol uses the properties of the SP blockchain (liveness, consistence) to provide similar properties to the SI blockchain. Hereinafter, we will assume that the SP blockchain is BTC, and the SI blockchain is VB.

Informally speaking, the idea to achieve stability in the SI blockchain using stability in the SP blockchain can be described as follows: block B in the SI blockchain is stable if the block B^* in the SP blockchain is stable, where B^* is the first block in the SP blockchain that refers to the block B. In other words, in order to “cancel” block B in the SI blockchain, one need to perform a long enough fork not only in the SI blockchain but also in the SP blockchain, which is an arduous computational task.

In this work we show how SC-idea can be used for building a state register and how it may achieve security under some conditions. We also show what parameters it should have to be secure.

Когут К. М. (НАДПСУ)
к.т.н. Басараб О. К. (НАДПСУ)
Городиський Р.О. (НАДПСУ)

РАЦІОНАЛЬНИЙ ВИБІР ГЛОБАЛЬНОЇ НАВІГАЦІЙНОЇ СИСТЕМИ ДЛЯ ЗАСТОСУВАННЯ В ДЕРЖАВНІЙ ПРИКОРДОННІЙ СЛУЖБІ УКРАЇНИ

Актуальність дослідження. З розвитком систем супутникової навігації в багатьох сферах оперативно-службової діяльності Державної прикордонної служби України використовуються навігаційні дані, зокрема: в прикордонній службі під час побудови маршрутів руху та моніторингу за пересуванням прикордонних нарядів; при організації та побудові системи зв'язку; в процесі здійснення службово-бойової діяльності тощо. Разом з тим, збільшується залежність органів та підрозділів Держприкордонслужби від наявності та якості навігаційних даних, в результаті чого утворилися ряд ризиків та небезпек. Водночас, розвиток систем супутникової навігації ставить перед нами непросту задачу вибору.

Метою дослідження є раціональний вибір глобальної навігаційної системи для використання в органах та підрозділах Державної прикордонної служби України.

Виклад основного матеріалу. На сьогоднішній день відомі неодноразові випадки про блокування навігаційних сигналів, зокрема, з боку Російської Федерації. Вперше про блокування сигналів стало відомо під час навчань "Захід-2017", які відбулися поруч зі странами Прибалтики, вдруге ситуація повторилася в жовтні-листопаді 2018 року в рамках спільних навчань країн НАТО "Єдиний тризуб" в Норвегії, внаслідок чого в 2018 році Міністерство оборони Норвегії публічно звинуватило Росію в причетності до збоїв в роботі GPS в районі Кольського півострова. Разом з тим, в Держприкордонслужбі України інтенсивно використовуються навігаційні дані саме системи GPS. Близькість Російської Федерації та її безпосередня зацікавленість в конфлікті на сході України лише підвищує статус важливості раціонального вибору системи навігації для застосування в оперативно-службовій, службово-бойовій діяльностях відомства. Глобальна навігаційна супутникова система (ГНСС) – комплексна електронно-технічна система, що складається з сукупності наземного та космічного обладнання та призначена для позиціонування в просторі (місцезнаходження в географічній системі координат) і в часі, а також визначення параметрів руху (швидкості, напрямку та ін.) для наземних, водних та повітряних об'єктів.

Найвідомішими на сьогодні ГНСС є: GPS; ГЛОНАСС; Galileo; Бейдоу. Окремі характеристики зазначених систем представлено в таблиці 1.

Таблиця 1

Порівняльна характеристика ГНСС

ГНСС / Показник	GPS	ГЛОНАСС	Galileo	BeiDou/ COMPASS
Власник	США	Росія	ЄС	Китай
Кількість супутників: вимагається/на орбіті	24/32	24/26	30/28	35/35
Висота орбіти	20180	19130	23222	35 786
Заявлена точність	6-8 м	3-8 м	1 м	3,6 м
Наявність в ДПСУ сумісного з ГНСС обладнання	+	-	-	-

Висновок. Виходячи з розглянутих характеристик, на даний чассистема GPS є найбільш зручною для використання в Держприкордонслужбі України. Точність звичайного навігаційного сигналу дозволяють вирішувати поставленні завдання, а застосування диференційного режиму дає значне покращення точності визначення координат. Проте, заявлена точність, сумісність з обладнанням GPS, географічне положення та геополітичні вподобання власника, дають підставу припускати застосування ГНСС Galileo в перспективі.

Козленко О.В. (КПІ імені Сікорського)
Кіреєнко О.В. (КПІ імені Сікорського)

МОДИФІКАЦІЯ АЛГОРИТМУ ПОБУДОВИ НЕЧІТКОЇ ОНТОЛОГІЇ СЦЕНАРІЇВ ВИТОКУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ Q-АНАЛІЗУ

Актуальність. Описуються модифікований алгоритм Fuzzy Ontology Generation Framework побудови нечіткої онтології сценаріїв витоку інформації на основі Q-аналізу. Онтологія демонструє модель понять більш докладно і формально ніж звичайні визначення та таксономії. Комп'ютерні та мережеві атаки стали постійною загрозою але методи їх опису часто суперечать один одному. Крім того, класифікація та виявлення нападів є складним завданням через сильно збільшену кількість загроз впродовж останніх років. Через це класифікаційні схеми, такі як онтології, є поширеним методом у галузі комп'ютерної та мережевої безпеки.

Постановка задачі. Провести аналіз сценаріїв витоку інформації у інформаційній системі, елементів захисту від данних сценаріїв витоків, провести Q-аналіз для визначення найбільш впливових елементів захисту, модифікувати метод побудови нечіткої онтології Fuzzy Ontology Generation Frameork, побудувати онтологію.

Основні положення. Онтології побудовані в трирівневій архітектурі, що складається з доменної онтології на нижньому шарі, онтології середнього рівня, яка кластеризує та визначає декілька доменів разом, і онтології верхнього рівня, яка визначається максимально універсальною. Аналізуючи існуючі онтології у сфері кіберзахисту можна побачити, що такі популярні онтології як CRATELO, DOLCE, онтологія Мортона-Пловмера є спеціфічними тільки для своїх доменів (такі як SQL-ін’єкції). Хоча онтологія відіграє ключову роль у визначенні області, неоднозначно визначені поняття та взаємозв'язки є одним з головних вузьких місць, яке виникає під час проектування доменних програм і проблема в тому, що сама онтологія є заздалегідь визначеною структурою з чіткими описами понять та міжконцепційними відносинами.

Одним із способів подолання цієї проблеми є "нечітка онтологія" в якій міжконцепційні відносини можуть бути представлені як нечіткі відносини, а не як чіткі асоціації. Таким чином, кожне міжконцепційне відношення розглядається як нечітка асоціація, силу якої можна встановити за параметрами програми. Замість того, щоб шукати точні описи понять, нечітка програма на основі онтології визначає найбільш ймовірне поняття з онтології. ключення неточності в структурі онтологій допомагає вирішити двозначності, що виникають через розбіжності в специфікації вимог користувачів та описах понять. Деякі класичні онтології, такі як NetOps, виявляють різного роду відносини між поняттями. У деяких випадках ці відносини можна віднести до ступенів значень функцій належності.

Побудова нечіткої онтології елементів захисту вимагає визначення основиних множин, зв’язків та елементів ієрархії. Проведений у роботі аналіз допоможе визначити основні елементи взаємодії та характеристики між заходами захисту від витоку інформації та заходами забезпечення належного рівня культури інформаційної безпеки. Для побудови нечіткої онтології будемо використовувати модифікований алгоритм Fuzzy Ontology Generation Framework, який у свою чергу основан на методі FCA. Кожний з елементів захисту буде визначений за допомогою 5 характеристик :

- G — відповідає за порушення властивостей захищенної інформації (цілістність, доступність або/та конфіденційність)
- SM— кількість nелементів захисту, які використовуються для запобігання витоку інформації у системі, також враховується людський фактор, частіше зв’язаний з помилками.
- W - можливі підходи до атаки в залежності від взаємодії на систему.

- R_i — вага, яка визначається за кількістю інцидентів загрози
- R_r — вага, яка визначається за кількістю реалізацій інцидентів загрози

$$R_i = [log_{10}(\sum incidentsamount)]$$

$$R_r = [log_{10}(\sum leaksamount)]$$

Статистика відносно кількості інцидентів та реалізацій отримана з репортов компанії Verizon за 2014-2017 роки.

Загальний ваговий коефіцієнт є визначається за допомогою вищезазначених характеристик:

$$F = W_q * G * W * \left(\frac{R_i}{R_r}\right)$$

W_q – вага впливу елементів захисту. Визначається як

$$W_q = \begin{matrix} 1якщо ecc < 1 \\ 2якщо ecc > 1 \end{matrix}$$

Q-аналіз елементів та їх зв'язків дозволить визначитти найбільш впливові компоненти на загальну структуру системи (ексцентриситету).У разі відсутності зв'язку між елементами сама система буде вразлива до атак. Системний характер досліджуваної області дав змогу визначити Σ – множину загроз та мір захисту, які повязані за допомогою відношення λ і є основою системи. За проведеним аналізом відповідно була побудована матриція інцидентості, на основі якої вже були отримані значення відповідних ексцентриситетів та структурний вектор.

Характеристика відносин між елементами буде мати вигляд :

$$F_r = F * W_p * i(SM), i(SM)\epsilon[0, n]$$

- $i(SM)$ — кількість можливих спільних атрибутів між двома концептами.

W_p— характеритиска залежності від способу, реалізації та мір захисту протидії загрози.

$$W_p = \{(3, objective), (16, secuirtymeasures), (2, establishment)\}$$

Для більш простого прикладу була обрана наступна множина типів сили зв'язків між двома концептами онтології :

$$T = \{weak, medium, good\}$$

s_F залежатиме від мінімальних та максимальних значень Максимальним та мінімальним значенням відповідно буде наступне:

$$s_{Fmin} = numberofelementswithminimumweight * minimumweight$$

$$s_{Fmax} = maximumweight * maximumnumberofattrributes = W_p * max(i_n)$$

Висновки. Пропонуєтьсямодифікованийметод побудови нечіткої онтології Fuzzy Ontology Generation Framework за рахунок Q-аналізу та статистичних даних щодо вдалих та невдалих спроб витоку інформації за 5 років, впровадження критеріїв та визначення ваги для кожного елементу захисту від витоку інформації та протидії помилкам людського фактору, що дозволило більш детально формалізувати область та визначити впливовість зв'язків між елементами.

д.п.н. Козубцов І.М. (НЦЗІ ВІТІ)
Нещерет І.Г. (НЦЗІ ВІТІ)
Терещенко Т.П. (НЦЗІ ВІТІ)

ПОШУК ПІДХОДІВ ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ І КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ЗБРОЙНИХ СИЛ УКРАЇНИ

Постановка завдання. Система захисту інформації і кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України є відносно новою системою, що інтенсивно розвивається. Тому дана система, потребує дослідження (оцінки) її ефективності функціонування, захисту інформації і кібербезпеки. Адже з впровадженням зазначеної системи в практику, керівника або відповідальну особу, буде цікавити відповідь на запитання, в якій мірі системи захисту інформації і кібербезпеки в інформаційно-телекомунікаційних системах ЗС України забезпечує необхідний рівень кібербезпеки.

За результатами аналізу останніх публікацій та досліджень підтверджено відсутність у відкритих джерелах аналогічної методики оцінювання ефективності функціонування системи захисту інформації і кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України.

Виходячи із зазначеного можна сформулювати нове наукове завдання з необхідності розроблення методики оцінювання ефективності функціонування системи захисту інформації і кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України (ЗС України). Перш ніж розробити нову методику необхідно дослідити, які саме можуть бути застосовані підходи до оцінювання ефективності функціонування системи захисту інформації і кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України.

Отже, метою доповіді є висвітлення результатів сучасного стану та вибору найбільш адекватних підходів до оцінювання ефективності функціонування системи захисту інформації і кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України.

Результат дослідження. Для оцінювання ефективності функціонування системи захисту інформації і кібербезпеки відібрані підходи за наступними критеріями:

максимального ефекту; запобігання втрат; кіберзахищеності інформаційно-телекомунікаційних систем Збройних Сил України;

комплексне забезпечення технічними засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту (коефіцієнт укомплектованості засобами; коефіцієнт технічної готовності засобів; коефіцієнт укомплектованості справними засобами);

мінімальний час реакції системи на інциденти;

виявлення активних загроз за результатами penetration testing;

укомплектованість штатних посад системними адміністраторами та обслуговуючим персоналом.

Найбільш показовим є оцінювання ефективності функціонування системи захисту інформації і кібербезпеки за критеріям кіберзахищеності. Решта критеріїв доцільно застосовувати як похідні від прямої або опосередкованої залежності кіберзахищеності системи.

Висновки. Таким чином, провівши зазначене дослідження нами встановлено можливість обрати комплекс підходів, які адекватно оцінять ефективність функціонування системи захисту інформації і кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України, на основі яких за класичною структурою методики вирішиться поставлена задача в майбутніх наукових дослідженнях.

к.т.н. Козубцова Л.М. (ВІТІ)
к.т.н. Бескровний О.І. (ВІТІ)
д.п.н. Козубцов І.М. (НЦЗІ ВІТІ)

СТРУКТУРА МЕТОДИКИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ВИКОНАННЯ ЗАХОДІВ, СПРЯМОВАНИХ НА ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Постановка завдання. В роботі [1] апробовано методика планування заходів, спрямованих на забезпечення їх кібербезпеки організації. Одна на даний час встановлено, що відсутні об'єктивні показники, критерії оцінювання реалізованих заходів та й сама методики оцінювання ефективності. В зв'язку з цим виникла необхідність у обґрунтуванні структури методики оцінювання ефективності реалізованих заходів кібербезпеки організації у розпорядження якої є об'єкти критичної інформаційної інфраструктури.

Мета доповіді. Апробувати структуру методики оцінювання ефективності реалізованих заходів кібербезпеки організації.

Результат дослідження. У відповідності до постановки завдання, авторами запропонована методика оцінювання ефективності виконання заходів, спрямованих на забезпечення кібернетичної безпеки організації реалізовується через показник ризику кібернетичної безпеки. Необхідність в її розробці обумовлена тим, що запропонована в роботі [1, с. 208-210] ідея, щодо побудови методики не реалізовується на практиці.

Методика оцінки ризику кібернетичної безпеки ОКІІ ПЗСУ базується на визначенні ймовірності реалізації кібератак (ДІВ), а також рівнів їх збитку. Розробка та застосування в діяльності системи виміру оцінювання ефективності виконання заходів відбувається за такими основними етапами [3, с. 33-35]:

Етап 1. Розробка системи показників оцінювання ефективності виконання заходів. Цей етап пов'язаний із процесом вибору показників та визначення системи мірил.

Етап 2. Планування процедур збирання необхідних вихідних даних для оцінювання ефективності виконання заходів. На цьому етапі здійснюється підготовка до впровадження системи вимірювання значень показників, з плануванням доступу до необхідних даних, розробкою конфігурації обробки та розповсюдження інформації про значення показників.

Етап 3. Обчислення значення показника ефективності виконання заходів, спрямованих на забезпечення кібернетичної безпеки підрозділів ЗС України. На підставі обраного ідеології обчислення значення показника ефективності виконання заходів, спрямованих на забезпечення кібернетичної безпеки підрозділів ЗС України за показником ймовірність ризику кібернетичної безпеки ОКІІ ПЗСУ.

Етап 4. Інтерпретація значення показника ефективності виконання заходів, спрямованих на забезпечення кібернетичної безпеки підрозділів ЗС України. Цей етап включає практичну роботу з обробки, аналізу та інтерпретації даних для прийняття рішень щодо посилення обраних заходів.

Висновки. Таким чином, подана структура методики оцінювання ефективності реалізованих заходів кібербезпеки організації має логічну структуру.

ЛІТЕРАТУРА

1. Козубцова Л.М. Обґрунтування структури методики планування заходів кібербезпеки об'єктів критичної інформаційної інфраструктури організації // Materials of the XVII International scientific and practical Conference Prospects of world science - 2021 (Sheffield, July 30 - August 7, 2021). Sheffield. Science and education LTDC, 2021. Vol.3. Pp. 87 – 92.

2. Мілих Є.Г. Методика оцінювання заходів забезпечення безпеки об'єктів критичної інформаційної інфраструктури // Актуальні проблеми управління інформаційною безпекою держави: наук.-практ. конф. (26 березня 2021 р.). К.: НА СБУ, 2021. С. 208- 210.

3. Нили Э., Адамс К., Кеннерли М. Призма эффективности: Карта сбалансированных показателей для измерения успеха в бизнесе и управления им. Д.: Баланс-Клуб, 2003. 400 с.

Колодійчук Л.В. (ВІТІ)
Березанський Д.О. (в/ч А-1906)

РОЗРОБКА СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АВТОМАТИЗОВАНОГО РОЗРАХУНКУ РАДІОРЕЛЕЙНИХ ЛІНІЙ

Актуальність. Радіорелейний зв'язок займає важливе місце у системі зв'язку ЗС України. Незважаючи на масштабне розгортання волоконно-оптичних ліній зв'язку, радіорелейний зв'язок, як і раніше, залишається найважливішою складовою частиною транспортних систем різного рівня. За допомогою радіорелейних засобів забезпечується оперативне розгортання ліній прив'язки вузлів зв'язку (ВЗ) пунктів управління (ПУ) до стаціонарної мережі зв'язку.

Постановка задачі. Час готовності радіорелейної лінії прив'язки (РРЛП) багато в чому залежить не лише від готовності засобів зв'язку та навченості особового складу, але й від якісного планування. Саме від вибору місця розгортання радіорелейних станцій (РРС) буде залежати якість зв'язку на лінії прив'язки. Таким чином, під час планування РРЛП необхідно якомога швидше та ефективніше визначити допустимі місця розгортання РРС на основі висновку про коефіцієнт готовності (надійність зв'язку) на лінії.

Виклад основного матеріалу. Розрахунок РРЛП представляє собою типову задачу проектування радіорелейного інтервалу, де одна РРС розгорнута в районі розміщення стаціонарного інформаційно-телекомунікаційного вузла (ІТВ), а друга – в районі польового ВЗ. Можливість зміни місця розгортання РРС складає близько 2-4 км, оскільки на території ПУ заборонено розміщувати засоби радіоелектронного випромінювання.

Існують програмні ресурси, які дозволяють приблизно оцінювати придатність РРІ, зокрема Google Earth Pro (https://www.google.com/intl/ru/earth/versions/earth-pro), Air Link (https://link.ui.com),WiFi Френель (https://play.google.com) тощо. Проте точність побудови профілю місцевості та розрахунку енергетики може виявитися на практиці незадовільною.

Тому у доповіді розглядається розроблений програмний продукт у вигляді файлу MicrosoftExcel, який з урахуванням математичного апарату, наведеного в Рекомендаціях MCE–R P.530–16, MCE–R P.526, MCE–R P.527, MCE–R P.836, MCE–R P.837, MCE–R P.1546–2, дозволяє у напівавтоматичному режимі виконувати розрахунки коефіцієнта готовності РРЛП при введенні координат станцій-кореспондентів, робочої частоти, енергетичних параметрів РРС (потужності передавача, чутливості приймача та коефіцієнтів підсилення антен) та висот підвісу антен. Перепади висот на інтервалі та місцеві перешкоди (будівлі, насадження тощо) необхідно вводити вручну: для побудови профілю РРІ можливо використовувати сучасні топографічні карти масштабу 1:100 000 та 1:50 000, цифрову модель висот (ЦМВ) „Shuttle Radar Topography Mission (SRTM) з розширенням 1", а також і програмний ресурс Google Earth Pro. Усі інші розрахунки та їх графічне відображення здійснюються автоматично (профіль місцевості з урахуванням лінії кривизни земної поверхні, перша зона Френеля, енергетичний розрахунок у вигляді коефіцієнта готовності РРЛП). У випадку значного просвіту запасу по висоті для забезпечення відкритого інтервалу при максимально можливому піднятті антен ПЗ дозволяє оперативно визначити необхідні висоти.

Висновок. Використання розробленого програмного забезпечення для проектування РРЛП з можливістю графічного та енергетичного розрахунку параметрів інтервалу на сучасному етапі застосування РРС зменшує час на проведення розрахунків, порівняно з класичним методом, та дозволяє отримати більш точні результати, порівняно з відомими додатками, що знаходяться у вільному доступі у мережі Internet.

Напрямками подальших досліджень є розробка програмного забезпечення для забезпечення повністю автоматизованого розрахунку. Для цього додатково необхідно вирішити завдання автоматичного розпізнавання програмою висот рельєфу місцевості та перешкод (будівлі, насадження тощо) на інтервалі.

д.в.н.Комаров В.С.(Військова частина А1906)
д.в.н. Ільяшов О.А. (Військова частина А1906)
Даценко І.М. (Військова частина А1906)

ТЕНДЕНЦІЇ РОЗВИТКУ РОБОТОТЕХНІЧНИХ КОМПЛЕКСІВ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ РОЗВІДКИ В СУЧАСНИХ УМОВАХ ВЕДЕННЯ ЗБРОЙНОЇ БОРОТЬБИ

Досвід ведення збройних конфліктів початку XXI століття, а також аналіз програм розвитку озброєння провідних країн світу дає змогу зробити висновок щодо перспективності розвитку робототехнічних комплексів (РТК). Тому питання створення, розроблення основ їх бойового застосування та оснащення Збройних Сил України, зокрема частин (підрозділів) розвідки, сучасними РТК набуває особливої актуальності. У доповіді авторами обґрунтовано необхідність проведення досліджень щодо створення та застосування розвідувальних РТК.

Результати аналізу свідчать, що на сьогодні в Україні робляться лише перші кроки за напрямами створення та впровадження РТК, тому спостерігається значне відставання від рівня оснащеності збройних сил провідних країн світу.

На думку авторів, розвідувальні РТК повинні мати специфічні характеристики, які обумовлені формами застосування та способами дій підрозділів розвідки, а також умовами виконання завдань в сучасних збройних конфліктах. У контексті зазначеного постає нагальна потреба в розробленні нових підходів, формулюванні, теоретичному обґрунтуванні та у подальшій апробації на практиці:

форм застосування та способів дій розвідувальних РТК;

завдань, які можуть вирішуватись розвідувальними РТК;

перспективної структури частин (підрозділів) розвідки, у складі яких планується застосування РТК;

системи озброєння та засобів (комплексів) розвідки, які будуть встановлюватись на РТК.З огляду на зазначене, на думку авторів, розвідувальні РТК необхідно розвивати за такими напрямами:

створення РТК, які здатні формувати бойові (змішані) групи та здійснювати груповий інформаційний обмін розвідувальною інформацією між ними під час виконання завдань в районі бойових дій;

створення РТК, здатних об’єднуватись у саморегулювальні мобільні мережі та виконувати поставлені бойові завдання;

розробка та оснащення РТК обладнанням для розпізнавання “свій–чужий”;

створення оптико-електронних і оптичних засобів розвідки РТК з розрізнювальною здатністю, яка забезпечить ведення розвідки на тактичну глибину;

створення обладнання комунікації для відображення інформації з датчиків (розвідувального обладнання) на станції приймання інформації в режимі реального часу. При цьому, необхідно врахувати можливості підвищення надійності та прихованості обміну розвідувальною інформацією і процесу керування РТК;

створення автоматизованих систем управління РТК, які працюють за модульним принципом. Інтеграція в їх склад інших розвідувальних систем для лазерного цілевказання, ведення радіоелектронної розвідки, оцінювання результатів ураження об’єктів противника, тощо.Створення та застосування РТК у підрозділах розвідки забезпечить:

підвищення рівня бойових (розвідувальних) можливостей частин (підрозділів) розвідки;

зниження рівня бойових втрат серед особового складу;

досягнення безперервності виконання завдань за умов, в яких фізіологічні можливості людей обмежені.

Реалізація цих напрямів значною мірою буде залежати від результатів наукових досліджень щодо стану та перспектив розвитку РТК у збройних силах провідних країн світу.

Коробко Н.В. (ВІТІ ім. Героїв Крут)
к.т.н. Ільїнов М.Д. (ВІТІ ім. Героїв Крут)

БАГАТОВХОДОВІ ПРИЙОМО-ПЕРЕДАВАЛЬНІ АНТЕНИ ДЛЯ БАЗОВИХ СТАНЦІЙ СИСТЕМ МОБІЛЬНОГО РАДІОЗВ'ЯЗКУ

Основним елементом будь-якої системи мобільного радіозв'язку є базова (центральна) станція, яка виконує функцію ретранслятора радіосигналів для збільшення дальності зв'язку між кореспондентами і забезпечує канальну ємність системи в цілому.

Метою роботи є вирішення завдань забезпеченню одночасної незалежної роботи декількох приймачів і передавачів.

Якщо об'єднання декількох приймачів для одночасної роботи вирішується відносно просто, то об'єднання передавальних пристроїв, а також сумісна робота передавачів і приймачів на одну антену, або рознесені антени, являє собою складну технічну задачу. На рис. 1 показані основні способи об'єднання передавачів для одночасної незалежної роботи.

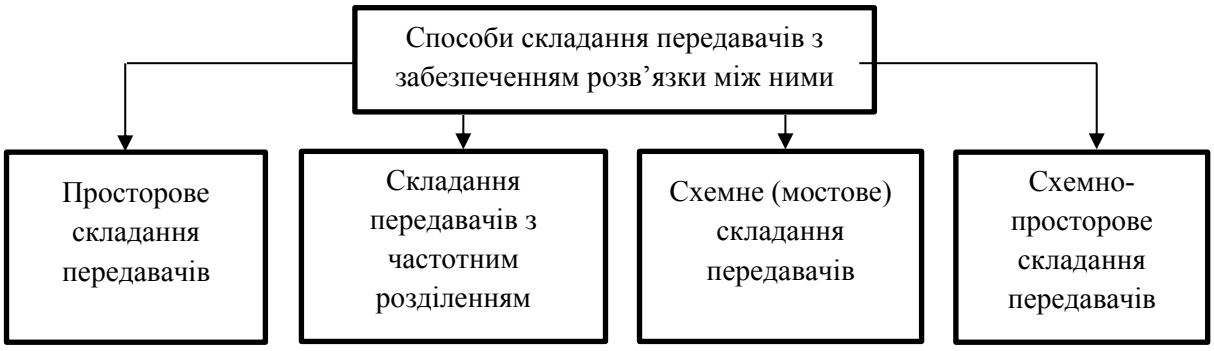


Рис. 1. Способи складання передавачів з забезпеченням розв'язки між ними

По функціональним можливостям найбільший інтерес являє собою схемно-просторовий спосіб об'єднання передавачів, який представляє собою поєднання просторового та схемного складання і передбачає використання багатовходових антен.

Багатовходова антена (рис. 2) являє собою еквідистантну кільцеву антенну решітку (КАР), що збуджується діаграмоутворюючою схемою (ДУС) у вигляді, наприклад матриці Батлера. ДУС має M входів для підключення передавачів і Nвходів для підключення багатовходової антени. M входів ДУС розв'язані між собою і узгоджені. Максимально можливе число входів M дорівнює числу випромінюючих елементів решітки N. Кожному входу M ДУС відповідає незалежна парціальна діаграма направленості (ДН).

Набіг фази ψ_{mn} струму від входу MДУС до n-говипромінювача антенної решітки визначається виразом:

$$\psi_{mn} = m\,(n-1)\frac{360}{N},$$

де $m = 0, \pm1,\ldots, \pm\frac{N-2}{2}, \frac{N}{2}$ — номер моди струму; $n = 1,2,\ldots N$ — порядковий номер випромінювача.

При подачі високочастотних коливань на будь-який вхід m ДУС амплітуди струмів на входах випромінювачів рівні, а відмінність фаз між суміжними випромінювачами постійна і визначається за допомогою виразу:

$$\Delta\psi_m = m\frac{360}{N}.$$

Якщо ширина ДН кожного випромінювача в азимутальній площині вибрана з умови

$$2\Delta\varphi^0_{0,5} = \frac{360}{N},$$

тоді така багатовходова антена забезпечить формування ненаправленого випромінювання в азимутальній площині для *N*-го числа передавачів.

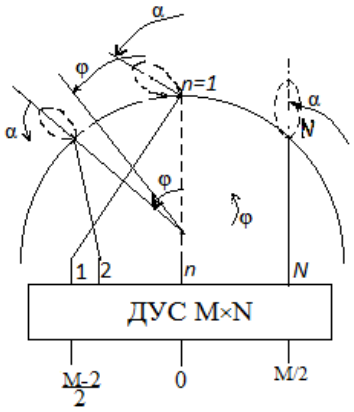


Рис. 2. Багатовходова кільцева антенна решітка

В якості прикладу технічної реалізації схемно-просторового способу складання передавачів для одночасної незалежної роботи на рис. 3 наведена кільцева антенна решітка, вигляд її діаграми направленості представлено на рис. 4.

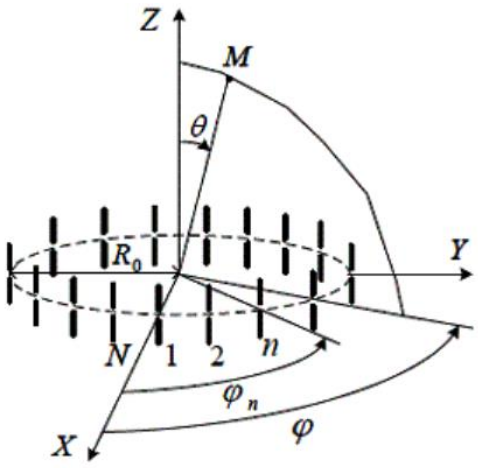


Рис. 3 Схема кільцевої антенної решітки

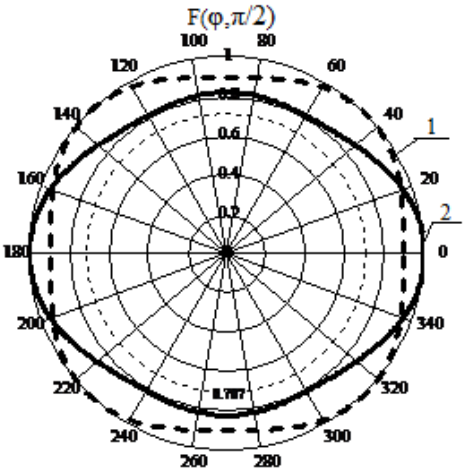


Рис. 4. Діаграма направленості двохвходової антени

Нижче в таблиці наведено амплітудно-фазовий розподіл струмів на виході ДУС.

Вхід	Фаза			
	B1	B2	B3	B4
1	0	90	180	270
2	90	180	90	180

У роботі було проведено теоретичний аналіз електричних характеристик двохвходової антени, скомпільованої на 4-х елементній кільцевій антенній решітці, випромінювачі якої (симетричні вібратори) знаходяться навколо циліндричної поверхні з поперечним елементом $2a = 0{,}002\lambda$, де λ – довжина хвилі. Отримані результати по розрахунку характеристики направленості наочно показують ефективність такої конструкції антени на практиці, що дозволяє формувати ненаправлене випромінювання в азимутальній площині при незалежній роботі декількох прийомо-передавачів.

Практичне значення роботи полягає у можливості використання її результатів при переведенні радіомереж транкінгового зв’язку для роботи у режимі LinkedCapacityPlus для забезпечення одночасної роботи декількох ретрансляторів на одну антену.

Корчомний Р.О. (в/ч А1906)
Ратаніна О.М. (в/ч А1906)
Грінькова Г.В. (в/ч А1906)

ЗАСТОСУВАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ У СИСТЕМАХ КІБЕРЗАХИСТУ

Актуальність. Останнім часом швидкість розвитку кіберпростору вражає як звичайних користувачів, так і досвідчених фахівців в області інформаційних технологій та кіберзахист. Сьогодні не тільки збільшується обсяг обробки даних і кількості підключених кінцевих пристроїв або додатків (сервісів) до мережі, але й розширюються самі концепції й технології. Завдяки цьому більшість комерційних і державних установ переходять в онлайнрежим (дистанційний) функціонування, а з пандемією така тенденція лише прискорюється. Широке застосування високорівневих мов програмування, потужних середовищ розробки, розвитку хмарних середовищ і технологій віртуалізації та "контейнеризації" дають змогу розробляти програмне забезпечення в стислі терміни. З аналогічною швидкістю поширюються кіберзагрози. У зв'язку з цим для забезпечення стійкої роботи інформаційних систем і програмного забезпечення недостатньо розмежовувати доступ та налаштовувати локальні політики безпеки. Слід додатково застосовувати інструментарій, який у своєму складі має засоби машинного навчання. Тому застосування штучних нейронних мереж у системах кіберзахисту є актуальним, оскільки такі мережі базуються на алгоритмах і функціях, здатних до навчання.

Постановка задачі. Проаналізувати роботу окремих алгоритмів штучних нейронних мереж у системах кіберзахисту.

Основні положення. У системах кіберзахисту штучні нейронні мережі застосовуються для виявлення й нейтралізації як зовнішніх, так і внутрішніх загроз. До зовнішніх загроз належить захист персональних даних користувачів за допомогою виявлення (детектування) аномалій на основі зібраних і проаналізованих патернів. До внутрішніх загроз належить виявлення та нейтралізація внутрішніх користувачів (порушників) системи (програмного забезпечення). У цьому разі алгоритми штучної нейронної мережі забезпечують спостереження за діями користувачів і надають адміністратору повідомлення про виявлені аномалії дій окремих користувачів (порушників). Для виявлення й нейтралізації зазначених загроз застосовуються алгоритми з учителем і без нього.Алгоритми з учителем застосовуються в разі, коли відомий повний набір вихідних даних і граничні межі відхилення (аномалій). Недоліком алгоритмів цього типу є необхідність великої кількості відомих вихідних даних і тривалий процес навчання. До алгоритмів цієї групи належать: дерево прийняття рішень (Decisiontrees); опорні вектори SVR (Supportvectorregression); лінійна регресія (Linearregression) і логічна регресія (Logicregression). Найпоширеніший алгоритм з учителем – це "дерево прийняття рішень", яке дає змогу перейти від спостереження за об'єктами, представленимив "гілках дерева", до висновків про цільові значення об'єкта, представлені в "листках дерева". Цей алгоритм широко застосовується в системах фільтрації трафіку прикладного рівня і системах захисту від шахрайства.Алгоритми без учителя застосовуються у випадку, коли є певний набір даних і немає явних вказівок, що з ними робити. Тоді штучна нейронна мережа сама намагається знайти кореляції в даних, отримуючи та аналізуючи корисні ознаки. Недоліком алгоритмів такого типу є складність обчислення точності його результатів, оскільки в даних немає "правильних відповідей" або міток. До алгоритмів цієї групи належать: пошук k-ближніх сусідів (K-NearestNeighbors або K-NN), метод k-середніх (K-Means), алгоритм Баєса, ієрархічної кластеризації (Hierarchical clustering). Найпростішим і найпоширенішим із них є алгоритм ієрархічної кластеризації (Hierarchical clustering), оскільки множина аналізу об'єктів характеризується певним ступенем зв'язності та може бути візуалізована у вигляді дендрограми. **Висновок.** Алгоритми з учителем ідеально підходять для вирішення завдань класифікації об'єктів і регресії. Алгоритм без учителя ідеально підходить для вирішення завдань кластеризації, автоматичного визначення аномалій та асоціативних зв'язків об'єкта з іншими.

к.т.н. Крайнов В.О. (НУОУ)
Коротченко Л.А. (ВІТІ)
Томаля В.В. (в/ч А3796)

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯВІД ЗАГРОЗ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В ПРОЦЕС ЇЇ ФУНКЦІОНУВАННЯ

Неправомірне спотворення або фальсифікація, знищення або розголошування певної частини інформації, рівно як і дезорганізація процесів її обробки і передачі в інформаційно-аналітичних системах наносять серйозну матеріальну і моральну утрату багатьом суб'єктам (державі, ЗС України, юридичним і фізичним особам), що беруть участь в процесах автоматизованої інформаційної взаємодії. Вимоги безпеки можуть змінюватися незалежно від призначення системи, характеру даних, що використовуються, та типу можливих загроз. Проблема забезпечення безпеки носить комплексний характер. Для її вирішення необхідно поєднання законодавчих, організаційних і програмно-технічних заходів. Законодавча база ще відстає від потреб практики. В той же час слід враховувати, що в нашій державі домінує зарубіжне програмно-апаратне забезпечення. В умовах обмеження на імпорт і відсутність міждержавних угод про взаємне визнання сертифікатів, споживачі, що охочі бути абсолютно законослухняними, виявляються по суті в безвихідному становищі – у них немає можливості замовити і отримати "під ключ" сучасну систему, що має сертифікат безпеки. Тому гострота проблеми забезпечення інформаційної безпеки при використовуванні інформаційних і управляючих систем, інформації, що зберігається і оброблюється в них, особливо у воєнній сфері, все більш зростає.

При виробленні підходів до рішення проблеми комп'ютерної, інформаційної безпеки слід завжди виходити з того, що основними реальними та потенційними загрозами інформаційній безпеці автоматизованих інформаційних систем військового призначення є:

- порушення встановленого регламенту збирання, оброблення, зберігання й передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу Україні;
- несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;
- реалізація програмно-математичних заходів із метою порушення функціонування інформаційних систем у сфері оборони Україні;
- перехоплення інформації у телекомунікаційних мережах, радіоелектронне продавлення засобів зв'язку та управління;
- інформаційно-психологічний вплив на населення Україні, у тому числі особовий склад військових формувань із метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби.

Тому забезпечення інформаційної безпеки та захист інформації в автоматизованих інформаційних систем (АІС) військового призначенняє комплексним завданням. Це обумовлено тим, що інформаційне середовище є складним багатоплановим механізмом, в якому діють такі компоненти, як апаратне та телекомунікаційне обладнання, програмне забезпечення та персонал. Для вирішення проблеми забезпечення інформаційної безпеки необхідне використання комплексного підходу до забезпечення безпеки, застосування законодавчих, організаційних і програмно-технічних заходів.Безпечна інформаційна система – це система, яка, по-перше, захищає дані від несанкціонованого доступу, по-друге, завжди готова надати їх своїм користувачам, а по-третє, надійно зберігає інформацію і гарантує незмінність даних. Кінцевою метою забезпечення інформаційної безпеки є захист всіх категорій суб'єктів, прямо або побічно, що беруть участь в процесах інформаційної взаємодії, від нанесення ним відчутного матеріального, морального або іншого збитку в результаті випадкових або навмисних дій на інформацію і

системи її обробки і передачі.

Цьому є цілий ряд об'єктивних причин:

1. Перш за все - це розширення сфери застосування засобів обчислювальної техніки і збільшений рівень довір'я до автоматизованих систем управління і обробки інформації. Комп'ютерним системам довіряють найвідповідальнішу роботу, від якості виконання якої залежить ефективність роботи органів управління. ПЕОМ управляють технологічними процесами обробки та передачі секретної і конфіденційної інформації.

2. Змінився підхід і до самого поняття "інформація". Цей термін все частіше використовується для позначення особливого товару, вартість якого часто перевершує вартість обчислювальної системи, в рамках якої він існує. Здійснюється перехід до ринкових відносин в області створення і надання інформаційних послуг, з властивою цим відносинам конкуренцією і промисловим шпигунством.

3. Проблема захисту автоматизованих інформаційних систем військового призначення стає ще більш серйозною і у зв'язку з розвитком і розповсюдженням обчислювальних сітей, територіально розподілених систем і систем з видаленим доступом до ресурсів, що спільно використовуються.

4. Доступність засобів обчислювальної техніки і, перш за все, ПЕОМ привела до розповсюдження комп'ютерних технологій, що закономірно, привело до збільшення числа спроб неправомірного втручання в роботу автоматизованих систем управління військами як із злим наміром, так і чисто "із спортивного інтересу". На жаль, багато хто з цих спроб має успіх і наносить значну утрату роботі органів управління.

5. Положення усугубляє тим, що практично відсутнє законодавче (правове) забезпечення захисту інтересів суб'єктів інформаційних відносин. Відставання в області створення стрункої і несуперечливої системи законодавчо-правового регулювання відносин у сфері накопичення і використовування інформації створює умови для виникнення і розповсюдження "комп'ютерного хуліганства" і "комп'ютерної злочинності".

6. Ще одним вагомим аргументом на користь посилення уваги до питань безпеки автоматизованих інформаційних систем військового призначення є бурхливий розвиток і розповсюдження так званих комп'ютерних вірусів, здатних скрито існувати в системі і скоювати потенційно будь-які несанкціоновані дії.

7. Особливу небезпеку для автоматизованих інформаційних систем військового призначення, комп'ютерних систем представляють зловмисники, фахівці - професіонали в області обчислювальної технікиі програмування, досконально знаючі всі достоїнства і слабі місця комп'ютерних систем і маючи в розпорядженні найдокладнішу документацію і найдосконаліші інструментальні і технологічні засоби для аналізу і злому механізмів захисту.

Щоб ускладнити зловмисникові доступ до даних, необхідно передбачити самі різні засоби безпеки, починаючи з організаційно-адміністративних заборон і закінчуючи вбудованими засобами мережевої апаратури. Використовуючи багаторівневу систему захисту, важливо забезпечити баланс надійності всіх рівнів. Якщо в мережі всі повідомлення шифруються, але ключі досяжні, то ефект від шифрування нульовий. Або якщо на комп'ютерах встановлена файлова система, що підтримує виборчий доступ на рівні окремих файлів, але є можливість отримати жорсткий диск і встановити його на іншому комп’ютері, то всі переваги засобів захисту файлової системи зводяться нанівець. Порушення політики забезпечення інформаційної безпеки може підвищити уразливість АІС та циркулюючої в ній інформації до неприпустимого ризику. Оскільки найуразливішою складовою будь-якої інформаційної системи є людина, особливого значення набуває виховання чемності співробітників по відношенню до законів і правил інформаційної безпеки. Висновок: найбільшу складність при рішенні питань забезпечення інформаційної безпеки конкретних АІС військового призначення представляє задача визначення реальних вимог до рівнів захисту критичної для суб'єктів інформації, циркулюючої в АІС. Орієнтація на інтереси суб'єктів інформаційних відносин дає ключ до рішення даної задачі для загального випадку.

д.т.н. Кузавков В,В. (ВІТІ)
Болотюк Ю.В. (ВІТІ)

АНАЛІЗ ДІАГНОСТИЧНИХ ОЗНАК ІНФОРМАЦІЙНИХ ПОВІДОМЛЕНЬ В СИСТЕМАХ З ПІДТРИМКОЮ МОДЕЛІ OSI

Модель взаємодії відкритих систем (Open System Interconnection, OSI) визначає рівні взаємодії систем у мережах з комутацією пакетів, дає їм стандартні імена та вказує, які функції має виконувати кожен рівень. У моделі OSI засоби взаємодії поділяються на сім рівнів: прикладний, представницький, сеансовий, транспортний, мережевий, канальний та фізичний. Вона описує лише системні засоби взаємодії, що реалізуються операційною системою, системними утилітами та апаратними засобами. Кожен рівень має справу з певним аспектом взаємодії мережевих пристроїв.

Звичайне повідомлення складається з службової інформації (заголовка) та поля даних. Коли додаток звертається із запитом до певного рівня моделі програмне забезпечення формує повідомлення стандартного формату. Воно повинне містити дані про місцезнаходження файлу та тип операції, яку необхідно виконати. Після формування повідомлення прикладний рівень спрямовує його далі (вниз по стеку) до представницького рівня. Протокол представницького рівня на підставі інформації, отриманої із заголовка прикладного рівня, виконує необхідні дії та додає до повідомлення власну службову інформацію – заголовок представницького рівня, в якому містяться вказівки для протоколу представницького рівня машини-адресата. Отримане в результаті повідомлення передається далі до сеансового рівня, який, у свою чергу, додає свій заголовок. Повідомлення досягнувши нижнього, фізичного рівня, передається лініями зв'язку адресату. До цього моменту повідомлення "обростає" заголовками всіх рівнів.

У стандартах ISO для позначення одиниць даних, з якими мають справу протоколи різних рівнів, використовується загальна назва протокольного блоку даних (Protocol Data Unit, PDU). PDU – загальний блок даних протоколу (корисні дані + службова інформація). Розмір службової інформації напряму залежить від характеристик тих протоколів які використовуються на даному рівні.

Так, IP-пакети (IPv4) складаються з корисного навантаження та заголовка: версія пакета (4 біти); довжина інтернет-заголовка (4 біти); тип обслуговування (8 біт); довжина пакета в байтах (16 біт); тег ідентифікації (16 біт); прапор роздільної здатності фрагментації пакета і прапор дозволу подальшої фрагментації (3 біти); поле для ідентифікації положення фрагмента у вихідному пакеті (13 біт); 8 біт - час життя, яке визначає кількість переходів (через маршрутизатори, комп'ютери та мережні пристрої), дозволених пройти пакету, перш ніж він зникне; 8 біт - тип протоколу (TCP, UDP, ICMP тощо); 16 біт - контрольна сума заголовка, що використовується при виявленні помилок; IP-адресу джерела (32 біта); адреса призначення (32 біта).

Після цих даних можуть бути додані різна кількість необов'язкових прапорів, що змінюються в залежності від протоколу.

Функції фізичного рівня реалізуються апаратно, це забезпечить можливість реєстрації енергетичної складової діагностичного параметру. Зі сторони комп’ютера ці функції виконуються мережевим адаптером або послідовними портами. Протоколом фізичного рівня служить специфікації 10Base-T технології Ethernet.

Таким чином, проведений аналіз свідчить про можливість використання стандартизованих розмірів заголовків для формування часової складової діагностичного параметру та вирішення задач технічної діагностики визначеного класу технічних систем. Сукупність часової та енергетичної складової в діагностичному параметрі за наявністю спеціально побудованої тестової послідовності дозволяють визначити технічний стан не лише апаратної частини об’єкту контролю, а правильність функціонування програмної частини, які функціонують на різних рівнях моделі OSI.

Курінний О.В. (КПІ ім. Ігоря Сікорського)
к.т.н. Яковлєв С.В. (ВІТІ)

ЕКВІВАЛЕНТНІ ФОРМИ ЗАДАЧІ РОЗВ'ЯЗУВАННЯ СИСТЕМИ ЛІНІЙНИХ ЗАБОРОН НАД СКІНЧЕННИМ ПОЛЕМ

Актуальність. Стандартною задачею алгебраїчного криптоаналізу є побудова системи поліноміальних рівнянь, яка описує залежності між відкритими текстами, шифротекстами та ключами. Існує багато апроксимаційних методів розв'язування таких систем, але в загальному випадку всі ці методи потребують експоненційних обчислень, тому виникає необхідність у пошуку альтернативних підходів. Таким підходом може бути відновлення невідомого вектору за частковою інформацією про цей вектор, яка може бути одержана з побічного каналу зв'язку або з особливостей реалізації криптосистеми. Оскільки інформація є частковою, то вона не стосується безпосередньо вектору, але може накладати обмеження на значення деяких лінійних залежностей з цим невідомим вектором.

Мета.Метою роботи є розвиток та уточнення методів розв'язування задачі відновлення невідомого вектора за частковою інформацією, представленою у вигляді певних лінійних залежностей.

Основна частина.Формалізуємо описану вище задачу введенням нотації системи лінійних заборон над скінченним полем. *Системою лінійних заборон над скінченним полем* $\mathbb{F}_{2^k}$ будемо називати систему співвідношень виду:

$$\begin{cases} (a^{(1)}, x) \neq a_0^{(1)} \\ \cdots \\ (a^{(m)}, x) \neq a_0^{(m)} \end{cases},$$

де $a^{(j)} = \left(a_1^{(j)}, \dots, a_n^{(j)}\right) \in \mathbb{F}_{2^k}^n$ та $a_0^{(j)} \in \mathbb{F}_{2^k}$для $j = \overline{1,m}$,$x = (x_1, \dots, x_n) \in \mathbb{F}_{2^k}^n$та під (a, x)позначається скалярний добуток векторів a та x. Будемо також використовувати більш компактний запис цієї системи $A \cdot x \neq a_0$, де $A = \left\{a_i^{(j)}\right\}_{i=\overline{1,n}}^{j=\overline{1,m}}$ та $a_0 = \left(a_0^{(1)}, \dots, a_0^{(m)}\right)$.

У роботі доведено ряд тверджень, в яких сформульовано певні алгоритмічні задачі та доведено їх еквівалентність до задачі розв'язування системи лінійних заборон $A \cdot x \neq a_0$, заданій над полем $\mathbb{F}_{2^k}$. Наведемо перелік цих задач.

1. Розв'язування системи квадратичних рівнянь виду $\Gamma \cdot A \cdot x = \hat{a}_0$ над скінченним полем $\mathbb{F}_{2^k}$, де Γ– це діагональна матриця, яка містить m нових «штучних» змінних, а $\hat{a}_0$– це вектор розміру m, кожна компонента якого в сумі з відповідною компонентою вектору a_0 дорівнює одиниці поля. Зазначимо, що введення «штучних» змінних не додає зайвих розв'язків. В загальному випадку задача розв'язування системи квадратичних рівнянь над скінченним полем є NP-повною задачею.

2. Перевірканалежності полінома

$$F(x) = \left[\left(a^{(1)}, x\right) + a_0^{(1)}\right] \cdot \dots \cdot \left[\left(a^{(m)}, x\right) + a_0^{(m)}\right]$$

ідеалу $I = \left(x_1^{2^k} + x_1, \dots, x_n^{2^k} + x_n\right)$кільця поліномів $\mathbb{F}_{2^k}[x_1, \dots, x_n]$. Цю умову можна переформулювати в термінах подільності поліномів: $F(x)$ буде належати I тоді і тільки тоді, коли його остача від ділення на систему поліномів, які є твірними ідеалу I, дорівнює нулю. Така форма цієї задачі випливає з канонічного гомоморфізму між кільцем поліномів та фактор-кільцем поліномів за ідеалом I.

Висновок. У роботі було сформульовано та доведено твердження, які описують еквівалентні форми задачі розв'язування системи лінійних заборон, яка є формалізацією задачі відновлення невідомого вектора за частковою інформацією. Ці еквівалентні форми надають змогу застосовувати наявні алгебраїчні методи до розв'язування системи лінійних заборон. Отримані результати можуть бути застосовані в алгебраїчному криптоаналізі потокових шифрів та криптосистем на лінійних кодах.

Курило О.М. (ВІТІ)
Мордюк В.І. (в/ч А-1906)

ВИКОРИСТАННЯ СИНФАЗНИХ АНТЕННИХ РЕШІТОК НА НИЗЬКОПРОФІЛЬНИХ ВИПРОМІНЮЮЧИХ ЕЛЕМЕНТАХ В БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСАХ

Актуальність. В даний час розвиток новітніх безпілотних авіаційних комплексів (БАК) є надзвичайно актуальним завданням. Провідні країни світу займаються розробкою БАК протягом останніх десятиліть. Насправді сьогодні ми говоримо про можливість найменшого використання людського ресурсу під час ведення бойових дій, де велику роль відіграють бойові та розвідувальні дрони. Аналіз безпілотних літальних апаратів (БПЛА) показав необхідність удосконалення телекомунікаційних каналів передачі даних між БПЛА та наземним пунктом управління (НПУ), а саме каналу зв'язку та каналу управління БПЛА**.**

Постановка задачі. Якість зв’язку БПЛА та НПУ, дальність зв’язку та швидкість передачі даних в каналі суттєво залежать від вибору антенно-фідерного обладнання. Аналіз електричних та конструктивних характеристик різних видів антен показав, що найраціональнішим рішенням є використання на БПЛА синфазних антенних решіток на низькопрофільних випромінюючих елементах. Такі антенні пристрої представляють собою невеликі за розміром печатні плати. Зручність їх використання, в першу чергу, на БПЛА, а також і на НПУ, полягає у мінімізації розмірів антен, а також у високій ефективності.

Метою дослідження є розробка направленої антени для телекомунікаційних каналів в БАК.

Виклад основного матеріалу. Вибір антенного обладнання для створення телекомунікаційних каналів передачі даних між БПЛА та НПУ ґрунтується на необхідності забезпечення дальності зв’язку на відстані прямої видимості, а також у здатності забезпечити необхідну широкосмуговість для забезпечення можливості ведення онлайн моніторингу систем та датчиків БПЛА.

Розрахунок електричних характеристик синфазних антенних решіток на низькопрофільних випромінюючих елементах здійснюється за допомогою системи комп’ютерної алгебри з класу систем автоматизованого проектування MathCAD 15.6, а також програмного середовища активних проводових та патч-антен MMANA.

Для візуалізації отриманих електричних характеристик розробленої патч-антени було використано середовище моделювання антен та антенних решіток ANSYS HFSS.

Основні характеристики розробленої антени відображені в таблиці 1 та на рис. 1, 2.

Таблиця 1. Характеристики розробленої антени

Параметр	Значення	Одиниці вимірювання
Мінімальна частота	5.71	ГГц
Максимальна частота	5.97	ГГц
Коефіцієнт підсилення	20	дБ
Ширина ДН	24	Градуси
Хвильовий опір	50	Ом
Рівень зворотного випромінювання	-15	дБ
Максимальна дальність зв’язку	40	км

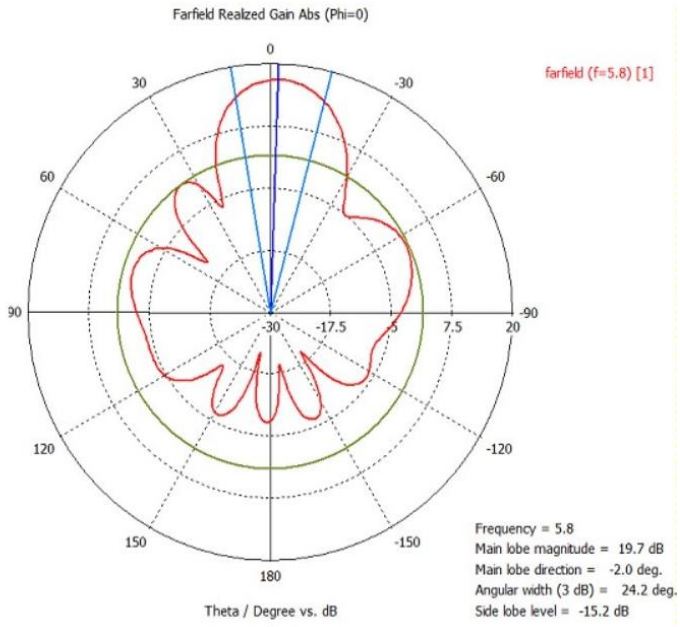


Рис. 1.1.Діаграма направленості в горизонтальній площині

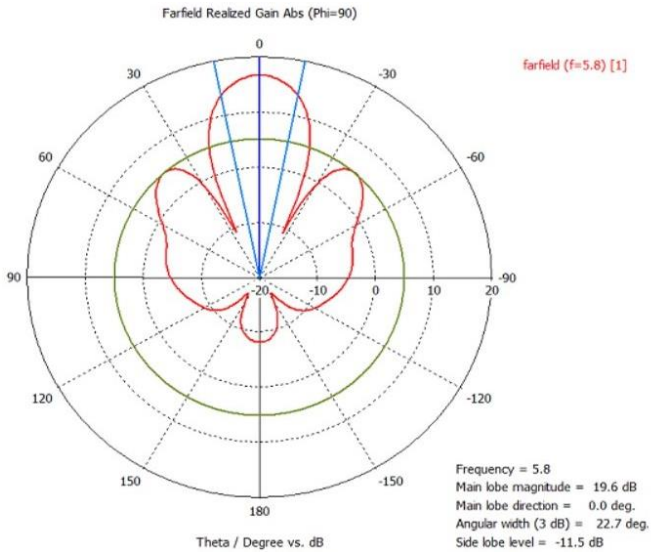


Рис. 1.2. Діаграма направленості у вертикальній площині

На відміну від відомих зразків антенних решіток, розроблена патч-антена має відносно невеликі габарити, а також забезпечує стійкий радіозв’язок в діапазоні 5.71-5.97 ГГц, що в свою чергу дає змогу забезпечити швидкість передачі даних до 95 Мбіт/с на відстані до 35-40 км.

Особливості та переваги розробленої антенної решітки: простота виготовлення подібних антенних решіток; зменшення силуету та потужності випромінюючого елемента антени, що в свою чергу зменшує помітність наземних пунктів управління.

Висновок. Використання розробленої синфазної антенної решітки дає змогу збільшити маневреність та живучість НПУ, а також забезпечити стабільний канал передачі даних з можливістю відстеження та управління БПЛА в реальному часі.

Куцаєв В. В. (ВІТІ)
к.т.н. Орда М.В. (ЦВСД)
Зіборєва О. Б. (ВІТІ)
Головко О. Є. (ВІТІ)
Гришенко Н. О. (ВІТІ)

ЦІННІСТЬ ВІЙСЬКОВОЇ ІНФОРМАЦІЇ

Автори розглядають терміни «інформація» та «цінність інформації» у спеціалізованому визначенні для використання у військовій справі.

Військова інформація (далі – ВІ) у вигляді документів, текстової інформації, повідомлень, пакетів у форматах сучасних протоколів циркулює в інформаційно-телекомунікаційній системі Збройних сил (далі – ЗС) України. Інформація з властивістю «цінність інформації» разом з апаратно-програмними активами та особовим складом підрозділів складають сумарний актив всіх інформаційно-телекомунікаційних систем ЗС України.

Розглянемо комплексну цінність інформації, яка формується з урахуванням сучасних поглядів на оцінку інформації, шляхом аналізу здобутків та втрат, вартості придбання або її перехоплення, експертних висновків фахівців із захисту інформації, експертів спеціальних служб та сучасних підходів до оцінки цінності інформації в бізнесі.

Авторами запропонована комплексна оцінка цінності інформації $Z – \{Z_0, Z_1, Z_2, Z_3, Z_4, Z_5\}$,

де Z_0 – вартість вхідних даних, необхідних для створення нової ВІ;

Z_1 – вартість можливих здобутків або втрат озброєння та військової техніки, особового складу, територій та підприємств, розміщених на цій території, закладені у ВІ;

Z_2 – вартість інсайдерського заволодіння ВІ;

Z_3 – вартість заходів, необхідних для перехоплення ВІ технічними, кібернетичними або криптографічними засобами;

Z_4 – вартість технічного, криптографічного та кібернетичного захисту ВІ;

Z_5 – вартість створення ВІ в інформаційно-телекомунікаційних системах ЗС України.

Постановка завдання в загальному вигляді. Кожна наука має своє специфічне визначення термінів «інформація» та «цінність інформації». Автори розглядають терміни «інформація» та «цінність інформації» стосовно військової справи. Нині зустрічається більше тридцяти визначень поняття інформації, і єдине поняття, яке задовольнило б усі претензії вчених, є поки справою майбутнього. До середини 20-х рр. XX ст. під інформацією (у перекладі з латинської *informatio* – ознайомлення, роз'яснення, викладення) дійсно розуміли відомості та повідомлення, які передаються усно, письмово або іншим способом. Одне з основних універсальних визначень інформації у філософії – це відомості про об'єкти, події та явища, які зафіксовані у різноманітній матеріальній формі [1]. Також одним із найбільш вдалих, на наш погляд, видається визначення інформації, яке запропонував А. Моль: «Інформація – це кількість непередбачуваного, яка міститься в будь-якому змістовному повідомленні» [2]. Важливим є наступне визначення інформації у кібернетиці – це зменшення невизначеності щодо визначеного об'єкту, явища чи процесу [3]. Цінність інформації– це її загальна властивість, яка визначає ступінь досягнення кібернетичною системою мети за допомогою отриманої інформації [4].

В статті автори пропонують розглянути наступні визначення термінів «інформація» та «цінність інформації», притаманні для військової справи:

військова інформація – це опис запланового у часі порядку дій (сценарій), суб'єктів ЗС України, а саме: перелік зразків ОВТ і ОС, територій, локацій та план дій для всіх визначених у ВІ суб'єктів ЗС України у всіх можливих сценаріях подій;

цінність військової інформації – це вартість в доларовому еквіваленті всіх суб'єктів ЗС України та дій з ними, якими маніпулює сценарій, закладений у ВІ. Цінність суб'єктів та дій визначаються методом експертних оцінок (далі – ЕО), зокрема, методом Сааті [5].

Автори пропонують розглянути комплексний підхід для оцінки ВІ. Для зручності використовується вектор Z [6], створений з компонентів актуальних оцінок ВІ, кожний з яких може стати надважливим. Розглянемо вектор компонентів цінності ВІ – $\{Z_0, Z_1, Z_2, Z_3, Z_4, Z_5\}$.

Автори пропонують використовувати наступні компоненти вектора оцінки ВІ:

Z_0 – ЕО вартості вхідних даних для створення ВІ;

Z_1 – ЕО вартості здобутків або втрат під час втілення сценарію, закладеного у ВІ;

Z_2 – ЕО вартості інсайдерського заволодіння, купівлі або викрадення ВІ;

Z_3 – ЕО вартості технічного перехоплення ВІ;

Z_4 – ЕО вартості технічного захисту ВІ;

Z_5 – ЕО вартості створення ВІ.

Розглянемо всі компоненти вектора ВІ – $\{Z_0, Z_1, Z_2, Z_3, Z_4, Z_5\}$, які потрібно розраховувати під час життєвого циклу (далі – ЖЦ) ВІ [7]. Автори пропонують наступну методику розрахунку компонентів ВІ.

Z_0 – *вхідний*компонент вектора ВІ, який визначає витрати, необхідні для отримання вхідної інформації. Вхідна інформація згідно з формулою (1) складається з наступних складових:

$$Z_0 = C_З + C_{РД} + C_{НДР,\ ДКР}, \quad (1)$$

де $C_З$ – кошторис створення задуму;

$C_{РД}$ – кошторис затрат на здобуття розвідданих;

$C_{НДР,\ ДКР}$ – кошторис затрат на проведення НДР та ДКР.

Z_1–*перший* компонент вектора ВІ – це сумарна вартість в доларовому еквіваленті всіх матеріальних ресурсів та дій з ними, які заплановані у ВІ згідно з формулами (2), (3).

Автори пропонують масив інформації $V_{ВІ1}$ визначати описом суб'єктів Збройних сил України та описом запланованих дій з ними за формулою (2):

$$V_{ВІ1} = f\,(ОВТ_n, ОС_S, Км^2, О_l, d_{n,s}). \quad (2)$$

Цінність ВІ – Z_1 визначимо сумою вартості всіх суб'єктів сценарію ВІ та вартості дій з ними в доларовому еквіваленті [8] згідно з формулою (3):

$$Z_1(t) = \sum C_{ОВТn}(t) + \sum C_{\ ОСs}(t) + \sum C_{Км^2}(t) + \sum C_{Ol}(t) + \sum d_{n,s}(t)\,, \quad (3)$$

де $V_{ВІ1}$ – масив ВІ;

t – час здійснення оцінки ВІ;

C – коштовність суб'єктів ВІ;

$ОВТ_n$ – перелік зразків n ОВТ, задіяних у сценарії ВІ;

$ОС_s$ – перелік особового складу s, задіяного у ВІ;

$Км^2$ – обсяги територій, задіяні у ВІ;

$О_l$ – підприємства, розміщені на територіях, задіяних у ВІ;

$d_{n,s}$ – дії з $ОВТ_n$ та $ОС_s$.

Z_2–*другий* компонент вектора ВІ, визначений сучасними підходами до оцінки вартості інформації, придатними для військової справи. Це дуже важливий варіант сценарію, який враховує витрати противника в доларовому еквіваленті, необхідні для інсайдерського заволодіння ВІ згідно з формулою (4):

$$Z_2 = C_{СУ} + C_{ОВД}, \quad (4)$$

де $C_{СУ}$– вартість утримання противником спеціальної установи;

$C_{ОВД}$ – затрати противника на операцію з отримання ВІ.

Z_3–*третій* компонент вектора ВІ визначено необхідністю враховувати загрози технічного, кібернетичного або криптографічного перехоплення ВІ противником. Компонент враховує витрати противника в доларовому еквіваленті, необхідні для заволодіння ВІ технічним шляхом згідно з формулою (5):

$$Z_3 = C_Т + C_К + C_{Кр}, \quad (5)$$

де $C_Т$– вартість технічного перехоплення ВІ;

$C_К$ – вартість кібернетичного перехоплення ВІ;

$C_{Кр}$–вартість криптографічного розкриття перехопленої ВІ.

Z_4–*четвертий* компонент вектора ВІ визначено необхідністю враховувати затрати в доларовому еквіваленті, необхідні на технічний, кібернетичний та криптографічний захист ВІзгідно з формулою (6):

$$Z_4 = C_{ТЗ} + C_{КЗ} + C_{КрЗ}, \quad (6)$$

де $C_{ТЗ}$–вартість технічного захисту ВІ;

$C_{КЗ}$ – вартість кібернетичного захисту ВІ;

$C_{КрЗ}$– вартість криптографічного захисту ВІ.

Z_5 – п’ятий компонент вектору ВІ визначає витрати в доларовому еквіваленті, необхідні для створення ВІ в штабі згідно з формулою (7):

$$Z_5 = C_Ш + C_{ОС} + C_З, \quad (7)$$

де $C_Ш$ – вартість роботи інфраструктури штабу;

$C_{ОС}$ – вартість роботи особового складу штабу;

$C_З$ – вартість збереження ВІ.

На рис. 1 наведено приклад вектора ВІ для різних військових операцій: військовий статут деякої держави; план військової операції «Барбароса – 1941»; план військової операції «Порт-Артур – 1904»; план військової операції «Пірл-Харбор – 1941»; план «виходу з оточення» підрозділу.

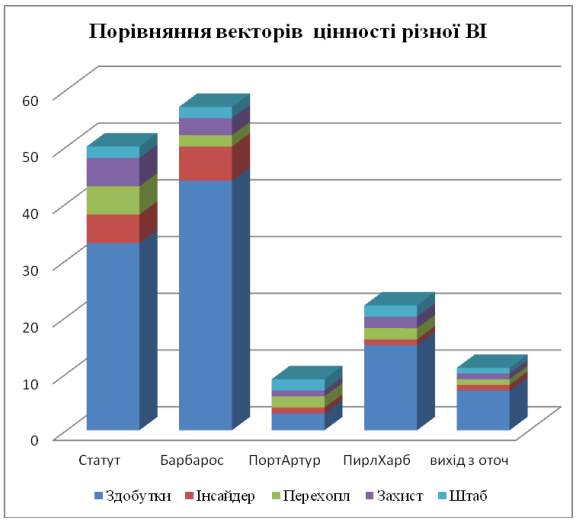


Рис. 1. Порівняння векторів оцінок цінності ВІ для різних операцій

Всі п’ять підходів для оцінки ВІ необхідно враховувати під час ЖЦ ВІ, тому що кожний з них у визначених умовах може стати основною причиною втрати інформації, а також причиною втрати матеріальних та людських ресурсів. Тому автори пропонують розглядати цінність ВД – Z, як вектор оцінок компонентів ЦІВД – $\{Z_0, Z_1, Z_2, Z_3, Z_4, Z_5\}$.

На рис. 2 пояснено, як під час створення ВІ її цінність зростає на 2–3 порядки порівняно з вартістю вхідних даних $\{Z_{01}, Z_{02}, Z_{03}, Z_{04}, \ldots, Z_{0W}\}$.

Якщо ціль досяжна різними шляхами, тоді можливе визначення (V) – цінності ВІ відповідно до зменшення матеріальних або часових втрат завдяки її використанню. Такий метод визначення цінності запропоновано Стратоновичем [9]. Так, наприклад, використання ВІ – «Статут» зберігає ВТО на 7,5 млрд. $ в рік.

Рис. 2. Зміна цінності вхідної інформації

У випадку, коли досягнення мети не обов'язкове, але ймовірно, тоді використовується критерій міри цінності інформації, запропонований М. М. Бонгартом та А. А. Харкевичем [10], вважається:

$$V = \log 2\ (P/p), \tag{8}$$

де p – ймовірність досягнення мети до отримання інформації;

P – ймовірність досягнення мети після отримання інформації.

На рис. 3 показано приріст ймовірності досягнення мети. Приклад, ВІ – «Статут», яка упорядковує всі питання організації життєдіяльності військових підрозділів. Автори вважають, що без використання ВІ – «Статут» військо буде паралізовано та втратить боєздатність. Розглянемо дві попередні оцінки p_0 та P_0. Будемо вважати, що попередня оцінка P_0 відповідає бездоганно налагодженій діяльності під керівництвом ВІ – «Статут». Тоді вважаємо, що $P_0 \rightarrow 0{,}99$ або знаходиться в межах [0,98–0,99].

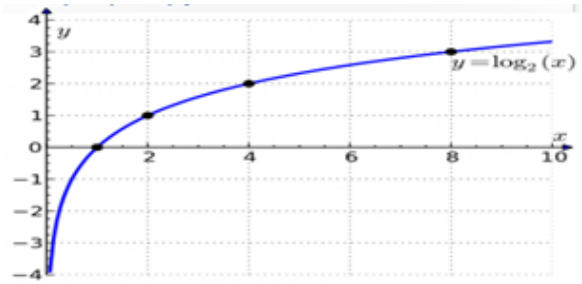


Рис. 3. Приріст ймовірності досягнення мети

Будемо вважати, що попередня оцінка p_0 відповідає діяльності війська без використання ВІ – «Статут». Тоді, згідно з історичними фактами, військо без керівництва – це анархія, отаманщина та безлад, тому військо втрачає боєздатність, хоча й не повністю. Тоді вважаємо, що $p_0 \rightarrow 0{,}5$.

Цінність ВІ – «Статут» визначимо вектором ЕО вартості компонентів $\{Z_0, Z_1, Z_2, Z_3, Z_4, Z_5\}$:

Z_0(вхідні данні) = $C_З + C_{РД} + C_{НДР,\ ДКР}$ ≈ 200 000 $;

Z_1 (здобутки / втрати за рік) = $C_{ОВТ} + C_{ОС} + C_Т + C_О$ ≈ 150 000 000 000 $;

Z_2 (інсайдерське) = $C_{СУ} + C_{ОВД}$ ≈ 10 $;

Z_3 (ТП) = $C_Т + C_К + C_{Кр}$ ≈ 100 $;

Z_4 (ТЗ) = $C_{ТЗ} + C_{КЗ} + C_{Кр3}$ ≈ 100 $;

Z_5 (Ств) = $C_Ш + C_{ОС} + C_З$ ≈ 100 000 $;

$V = V_{Б,Х(ВІ\text{-}Статут)}$ міра покращення Бонгарта ≈ 6,2;

$Z_{Статут}$ – {200 000, 150 000 000 000 $, 10 $, 100 $, 100 $, 100 000, [6,2]}.

На рис. 4 показано зміни цінності кожного компонента вектора під час ЖЦ ВІ.

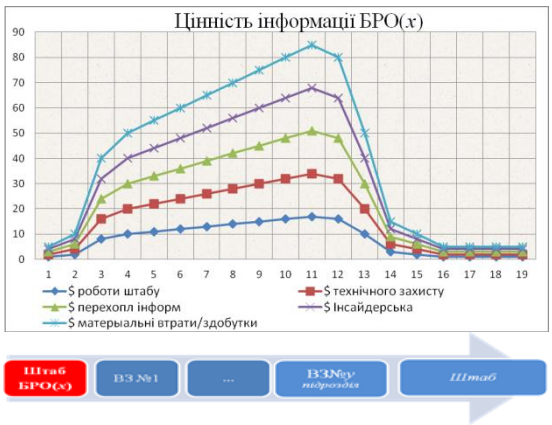


Рис. 4. ЖЦ цінності BI

До початку розробки BI попередня інформація Z_0 коштує ≈ 0,1–2 % від максимальної цінності BI: $Z_{BI} \approx 0{,}015*maxZ_{BI}(t)$.

Інтелектуальна діяльність при розробці BI збільшує цінність Z_{BI} до ≈ $0{,}5*maxZ_{BI}(t)$.

Під час переміщення BI до підрозділу цінність BI – Z_{BI} лінійно зростає з 0,5 до 1.0 $maxZ_{BI}(t)$.

Після використання за призначенням BI повертається до архіву та оцінюється $Z_{BI} \approx 0{,}015*maxZ_{BI}(t)$. Для опису ЖЦ BI автори пропонують використати формулу (9)

$$Z_{BI}(t) = (0{,}5+0{,}5*(t_ч - t) / (t_ч - t_0))maxZ_{BI}(t_ч)]; \quad (9)$$

де $t_ч$ – час застосування сценарію, закладеного у BI.

Висновок. Запропонована авторами методика надає наступні можливості:

контролювати цінність інформації, яка закладена у BI;

контролювати важливі компоненти оцінки BI, які актуальні у різних випадках та сценаріях;

контролювати загальні активи інформаційно-телекомунікаційних вузлів з урахуванням інформаційного активу;

зручно порівнювати активи різних інформаційно-телекомунікаційних вузлів та інформаційних і кібернетичних потужностей різних держав.

В наступних роботах планується розглянути детальну динаміку зміни цінності BI під час її ЖЦ.

ЛІТЕРАТУРА

1. Сучасні означення інформації Т. М. Слінько https://dspace.nlu.edu.ua/bitstream/123456789/14426/1/Slinko_23-29.pdf.
2. Моль А. Социодинамика культуры / Моль А. – М.: Прогресс, 1973. – 150 с.
3. Винер Н. Кибернетика / Н. Винер. – М.: Госкомиздат, 1958. – 220 с.
4. Властивості інформації / П. Зіновій. Кафедра журналістики та засобів масової комунікації НУ «Львівська політехніка». – Львів, Україна. http://ena.lp.edu.ua/bitstream/ntb/38348/1/63_136- 137.pdf.
5. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.
6. Вектор. https://formula.co.ua/uk/content/vectors.html.
7. https://spravochnick.ru/informatika/osnovnye_etapy_zhiznennogo_cikla_informacii/.
8. Раимов А. В. Экономическая оценка конфиденциальной информации организации // Финансы и управление. – 2017. – № 1. – С. 1–9.
9. Стратонович Р. Теория информации. – М.: Сов. радио, 1975.
10. https://pidru4niki.com/1510030647706/informatika/semantichna_pragmatichna_miri_informatsi.

к.т.н. Кучинська Н.В.(ФТІ,КПІ),
Олефір П.Ю(ФТІ,КПІ)

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДІВ ДОДАВАННЯ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ У ФОРМІ ЕДВАРДСА

Еліптичні криві у формі Едвардса над скінченним полем простої характеристики займають особливе місце серед варіативних форм представлення еліптичних кривих та використовуються у сучасних криптографічних алгоритмах та протоколах. Актуальність дослідження ефективності операцій у групі точок кривої Едвардса також визначається введенням у дію нового національного стандарту ДСТУ:9041 «Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених кривих Едвардса».

Відмітимо, що операції в групі точок еліптичної кривої у формі Едвардса є більш ефективним, у порівнянні з іншими формами представлення еліптичних кривих, зокрема Вейєрштрасса та Монтгомері.

Множення точки на скаляр (експоненціювання точки) є найважливішою і затратною операцією для криптосистем на еліптичних кривих. При реалізації криптографічних алгоритмів та протоколів на еліптичних кривих важливо імплантувати операцію скалярного добутку ефективно та безпечно, особливо від атак за побічним каналом. Зазвичай обчислення kP для точки P на еліптичній кривій E над скінченним полем F_q і заданим цілим числом k виконується рекурсивно за допомогою формул додавання та подвоєння точок. Проте даний метод вразливий до атак за побічним каналом, оскільки різниця в часі між реалізацією додавання та подвоєння може виявити інформацію про біти k.

Одним зі способів протидії такому виду атак є метод Монтгомері, який є стійкими до атак за побічним каналом, швидкими та широко використовуються в апаратних реалізаціях. Стійкість до атаки пояснюється тим, що на кожному етапі алгоритму, незалежно від поточного обробленого біта скаляра k, виконується одночасно операція подвоєння однієї точки, а також операція додавання. З кожною ітерацією змінюється лише порядок обчислення бітів.

Нещодавно було запропоновано новий метод реалізації диференціального додавання точок для еліптичних кривих у формі Едвардса, який показав себе рекордно швидким у порівнянні з існуючими методами додавання точок.

Доповідь присвячена оприлюдненню результатів дослідження покращення ефективності обчислення експоненціювання точки кривої Едвардса, шляхом застосування нових інтегральних координат Фарашахі. Також наведено оцінку ефективності для кожного способу додавання точок, використовуючи сходи Монтгомері для протидії атакам за побічним каналом. Було застосовано можливі інтегральні координати Фарашахі до форми еліптичної кривої, яка використовується у стандарті ДСТУ:9041. Також було пораховано кількість операцій для кожного виду координат з використанням сходинок Монтгомері.

Висновки. Швидкий розвиток технологій вимагає покращення криптосистем та стандартів , які відповідають новими вимогами. Наразі застосування нових диференціальних координат до еліптичної кривої у формі Едвардса є найбільш перспективним, бо показує рекордну швидкість та стійкий до атак за побічним каналом.

Лазута Р.Р. (ВІТІ)
Бузаєва К.О. (ВІТІ)
Горбатюк П.М. (НГУ)
Цаплієнко С.Ю. (НГУ)
Дремлюга В.В. (ДССТ)

ОЦІНКА ПРОЦЕСІВ ТА ПРОЦЕДУР ДІЯЛЬНОСТІ СТРУКТУРНИХ ПІДРОЗДІЛАХ ЗБРОЙНИХ СИЛ УКРАЇНИ ТА ІНШИХ ВІЙСЬКОВИХ ФОРМУВАНЬ

Актуальність. Діяльність структурних підрозділівЗбройних Сил України та інших військових формувань ґрунтується на базі українського законодавства та передбачає виконання ряду функціональних завдань. Основними завданнями є: вироблення напрямів реалізації оборонної політики України на основі аналізу воєнних загроз; планування виконання оборонних завдань на короткостроковий, середньостроковий та довгостроковий періоди як у мирний так і у воєнний час; інформування суспільства про діяльність ЗС України та інших військових формувань; вирішення питань міжнародної взаємодії з питань оборони. **Метою дослідження** є поріняльний анліз сучасних методів, які використовуються провідними країнами світу та країнами членів НАТО для оцінки процесів, процедур в структурних підрозділах ЗС України та інших військових формувань.

Виклад основного матеріалу.

На теперішній час в провідних країнах світу та країнах членах НАТО використовується такі методи оцінки: за моделлю CAF;за методом аналізу ієрархій;за методом кластерного аналізу.

Оцінка ефективності якістю за моделлю CAF системи управління під час проведення самооцінювання діяльності за Європейською моделлю удосконалення управління в державному секторі (Common Assesment Framework; далі – CAF) використовується провідними країнами світу та країн членів НАТО. Ця модель побудована за загально прийнятими міжнародними стандартами з урахуванням національних особливостей та менталітету.Загальна схема CAF дає змогу сформувати цілісну картину діяльності та результативності структурних підрозділівЗС України та інших військових формувань під різними кутами зору і надає комплексний підхід до аналізу його діяльності.

Оцінказа методом аналізу ієрархій (далі – MAI) яка розроблена американським математиком Томасом Сааті, являє собою універсальний інструмент арсеналу системного аналізу. MAI дозволяє зрозумілим та раціональним шляхом структурувати складну проблему прийняття рішення у вигляді ієрархій, порівняти та виконати кількісну оцінку альтернативних варіантів.Зазначений метод являє собою математичний інструмент системного підходу до складних проблем прийняття рішень. В його основі полягає компромісне дослідження й вибір найбільш імовірних сценаріїв розв’язання проблем, на які впливають різноманітні фактори.

Оцінкаметодом кластерного аналізу управління якості покладено відомий у науці метод Плюта – як метод кластерного аналізу багатопараметричних об’єктів із визначенням таксономічного показника їх важливості за загальними теоретичними підходами та практичними розрахунками.Оцінка ефективності системи управління якості за даним методом визначається за рейтингом таксономічних показників. Остаточна оцінка ефективності здійснюється за теорією і практикою прийняття рішень на основі багатокритеріальних завдань вкладених скалярних згорток векторного критерію.

Висновки. Проведений аналіз переконує нас що перспективним є метод кластерного аналізу. Цей метод дає змогу в повному обсязі визначити рейтинг структурних підрозділів ЗС України та інших військових формувань. Оцінка системи управління якістю структурних підрозділів ЗС України та інших військових формувань за методом кластерного аналізу може бути визначена за врахуванням наявних значень відповідних критеріїв під час виконання послідовності аналітичних обчислювань за допомогою персонально електронно-обчислювальних машин та методичних рекомендацій.

Лазута Р.Р. (ВІТІ)
Павлюк Д.О. (ВІТІ)
Совік О.В. (ВІТІ)
Кокошинський В.В. (ВІТІ)

ПЕРСПЕКТИВНА АВТОМАТИЗОВАНА СИСТЕМА «LIFERING» ЯК СИСТЕМА БОЙОВОГО УПРАВЛІННЯ ЗБРОЙНИМИ СИЛАМИ УКРАЇНИ

Актуальність. Суть проблеми полягає в перспективі застосування Збройними Силами України програмного забезпечення “LifeRing”в системі автоматизованого управління військами Збройних Сил України. Сумістність данної системи є головною превагою для сумістної роботи з НАТО, що має надавати переваг та можливстей у майбутньому членства України в НОТО з метою тереторіальної цілістності та безпеки. Розробка систем інформаційної інфраструктри, що ведутьяс в секторі безпеки і оборони з елементами автоматизації: ІС “Дзвін-АС”, ТРУК “Кропива”, ІП “Дельта”.

Метою дослідження єудосконалення процесу бойового управління та прийняття рішень у ЗС України за рахунок використання порядку бойового управління та прийняття рішень у ЗС країн НАТО за їх стандартами.

Завдання дослідження єпорівняти існуючі зразки програмного забезпечення, за стандартами НАТО.

Виклад основних матеріалі. Ситема “LifeRing” використовує систему з тонким клієнтом, що дозволяє створювати оперативні шари обстановки, та мати повну картину у реальному часі. ПЗ “LifeRing”, як і «Дельта» використовує систему графічних позначень, що використовуються в НАТО – MIL-STD-2525D JOINT MILITARY SYMBOLOGY та можевикористовуватись для сумісного використання з країнами партнерами НАТО. У НАТО використовують архітектурні підходи до впровадження інформаційних систем. Поняття “C4ISR” визначається як архітектура та концепція взаємодії складових системи бойового управління оперативного та оперативно-стратегічного рівня. У перспективі є доведення мобільних вузлів до кожного військовослужбовця, який знаходиться на полі бою, використання отриманої ним інформації.

Показано, що організація потоків відбувається на тактичному, оперативному та стратегічному рівнях.Досвід минулих військових конфліктів підтверджує, що успішне ведення бойових дій (операцій), буде на боці того, хто швидко приймає рішення та миттєво їх виконує.

Порівняльний аналіз ПЗ “LifeRing” та ІП “Дельта” вказує, що системи є взаємо заміняємі, але функціональні можливості “LifeRing” мають перевагу. Дії в системі можуть фіксуватися для подальшого аналізу. Перераховані можливості дозволяють рекомендувати програмне забезпечення LifeRing для першочергового впровадження.

Пропонується ПЗ “LifeRing” яке надає змогу оперативно володіти важливою інформацією у реальному часі, відображати картографічні знімки, завантажені в пам’ять, перативні дані отримані за допомогою БПЛА. Цінність данного продукту є можливість оперативно приймати рішення за рахунок швидкого збору оперативних даних. Враховуючи те, що LifeRing розробляється в межах допомоги США її розробка не буде обтяжувати бюджет України.

Висновки. Отже, створення автоматизованих систем за стандартами C4ISR підтверджує, що одним з важливих напрямків розвитку України є постійна робота, що до наближення військової інфрастуктури до стандартів НАТО та співробітництва. Відповідно до Воєнної доктрини України, Стратегічного оборонного бюлетеня України, одними з основних завдань є впровадження стандартів НАТО, досягнення сумісності всіх структур ЗС України та їх спецпідрозділів із силами та засобами відповідних структур країн-членів НАТО, інтеграція із системою командування та контролю C4ISR.

д.т.н. Ланде Д.В. (ІПРІ НАН України)
Шнурко-Табакова Е.В. (ГО Рада інформбезпеки та кіберзахисту)

АВТОНОМНІ ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ OSINT

На цей час існують суттєві технічні проблеми, які заважають здійсненню розвідки за відкритими джерелами в різних національних сегментах мережі Інтернет без застосування спеціальних інтегрованих систем контент-моніторингу, які містять у свому складі інтелектуальні пошукові засоби, мережі інформаційних проксі-серверів, засоби взаємодії і зовнішніми агрегаторами мережевих інформаційних ресурсів, інфраструктуру маскування і анонімізації.

Звичайно, на первинному рівні можливо використовувати дані, які доступні через традиційні мережеві пошукові системи, розміщуються на відомих інтеграторах новин. У цьому випадку виникає ряд проблем, що заважають серйозному застосуванню мережевих ресурсів для задач аналітичної роботи:

В національному сегменті доступні далеко не всі ресурси, зокрема, не має доступу до деяких закордонних веб-сайтів і соціальних мереж.

Традиційні пошукові системи не завжди індексують новини, що розміщуються на глибинних рівнях веб-сайтів, не завжди новини індексуються ними своєчасно, погано охоплюються соціальні мережі, спеціальні бази даних, розміщені в Інтернеті.

У деяких випадках при неанонімізованому доступі веб-сайти або соціальні мережі, що приймають участь в інформаційних війнах, можуть видавати первинним користувачам спотворену інформацію, фейки. У деяких випадках доступ до інформації може бути заборонений, хоча ця інформація має статус відкритої для всіх.

Запити, що відповідають інформаційним потребам аналітиків, що передаються у незахищеному вигляді, можуть розкрити ці потреби для зацікавленої сторони - інформаційного противника.

Відсутність розвинених аналітичних засобів.

Для вирішення цих проблем, що стосуються OSINT (open source intelligence - розвідки за відкритими джерелами), мають застосовуватися сучасні інтегровані системи, яким притаманні такі властивості:

Розподілений збір інформації з веб-сайтів і соціальних мереж за допомогою ансамблів інтелектуальних агентів збору, розподілених у хмарному середовищі, що територіально охоплює різні країни. Ці агенти мають взаємодіяти між собою, обмінюватись інформацією, передавати цю інформацію в аналітичну частину системи OSINT.

Агенти добування інформації мають реалізовувати запрограмовані і налаштовані сценарії збору інформації, взаємодіяти із веб-сайтами, соціальними мережами, базами даних глибинного вебу, агрегаторами новин переважно (за можливістю) у анонімному режимі.

Застосування агентів добування інформації як основи системи інформаційних проксі серверів має забезпечувати повноту інформації у випадку блокування окремих агентів, запобігати спотворенню і дублюванню інформації, що передається до баз даних системи OSINT.

Мають застосовуватися засоби анонімізації, маскування, VPN, тощо для недопущення витоку інформаційних потреб аналітиків OSINT при добуванні і обробці даних.

Аналітичні засоби мають обробляти інформаційні потоки у режимі онлайн, реалізовувати процедури інформаційного пошуку, виявлення інформаційних атак, операцій, ранжування факторів впливів, формування і аналізу моделей предметних галузей (онтологій) тощо.

Приклад реалізації автономної програмно – технічної системи з анонімізацією моніторингу інформації та її аналітичною обробкою представлено на мал. 1. OSINT має базуватися на науково – методичному підгрунті, оновлюватися у відповідності до нових викликів та розробок, надавати можливість об’єктивізації висновків за рахунок якості даних,

незалежність результатів сервісу AttackIndex.com від суб'єктивних факторів (думок окремих експертів чи інженерів розробників, їх упереджень, термінологічний популізм), також забезпечує отримання об'єктивних даних, об'єктивну аналітику великих даних, репрезентативність зібраних даних та результатів аналітичної обробки, своєчасне виявлення нових трендів.

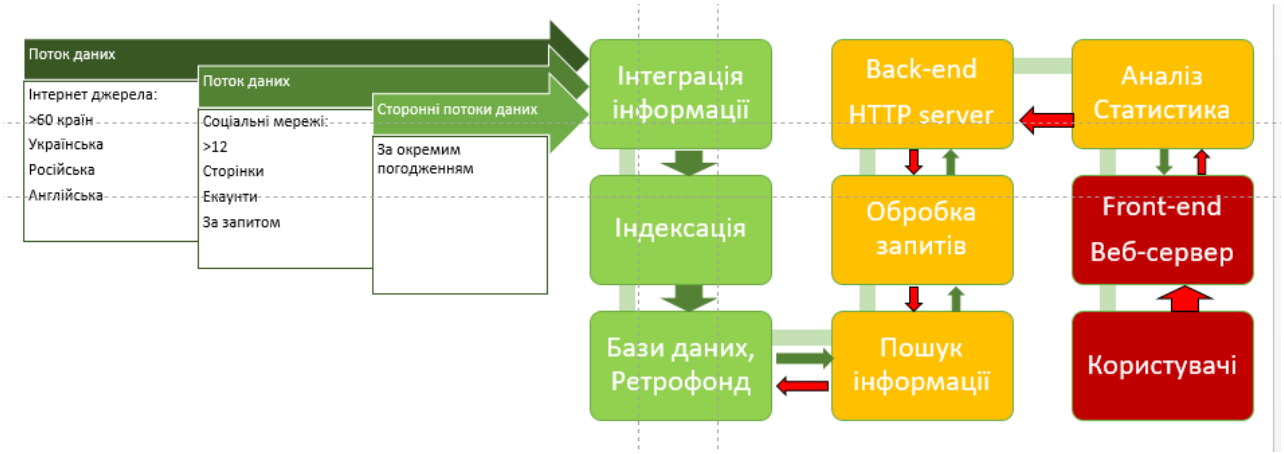


Рис.1 Блок схема ATTACK INDEX SERVER

Висновки

В доповіді представлені основні проблеми і вимоги, що ставляться перед системами OSINT для подолання бар´єрів, притаманних мережевому інформаційному середовищу. На прикладі системи Attack Index показано, що на цей час можливо побудувати систему державного рівня в галузі безпеки і оборони, яка буде реалізовувати завдання OSINT на базі сучасних інтелектуальних технологій.

ЛІТЕРАТУРА

1. Dmytro Lande, Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system // Theoretical and Applied Cybersecurity, 2019. - N. 1. - pp. 103-108.

2. “Army techniques publication no. 2-22.9.” Headquarters Department of the Army Washington, DC, 7 2012. (FMI 2-22.9).

3. Information Operations Recognition. From Nonlinear Analysis to Decision-Making / A. Dodonov, D. Lande, V. Tsyganok, O. Andriichuk, S. Kadenko, A. Graivoronskaya. - LAP Lambert Academic Publishing, 2019. - 292 p.

4. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Компьютерная конкурентная разведка - К.: ТОВ "Інжиніринг", 2021. - 354 с.

5. Lande D.; Subach I.; Puchkov O.; Soboliev A. A Clustering Method for Information Summarization and Modelling a Subject Domain Information & Security: An International Journal 50, no. 1 (2021): 79-86. DOI: doi.org/10.11610/isij.5013

6. Ланде Д.В., Ліненко Ю.О. Мережева модель правових обмежень доступу до Інтернету у світі // Інформація і право, 2019. - N 2 (28). - С. 26-31.

к.т.н. Лебідь Є.В.(ВІТІ)
Скринніков І.І.(ВІТІ)
Дрозд А.В. (ВІТІ)
Антонюк Д.І.(ВІТІ)

ЗАСТОСУВАННЯСИСТЕМ ПОЗИЦІОНУВАННЯ В РОБОТОТЕХНІЧНИХ КОМПЛЕКСАХВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Науково-технічний прогрес, розвитку технологій військового і подвійного призначення забезпечив впровадження Збройних Силах провідних країн світу технології військової робототехніки, що призвело до підвищення ефективності Збройних Сил і зміни характеру, форм і способів ведення збройної боротьби. Технологія військової робототехніки є одним із пріоритетних напрямків створення нових і модернізації існуючих зразків озброєння та військової техніки.

Робототехнічні комплекси (РТК) призначенні для повної чи часткової заміни людини в процесі виконання бойових задач на полі бою. Однак однією з актуальних проблем їх застосування при автономній роботі є орієнтація в просторі і визначення свого місцеположення відносно інших об'єктів, яка дозволить забезпечити ефективне застосування РТК при виконанні задач бойового призначення.

Прикладом визначення місцерозташування (локалізації) робота, є системи позиціонування і визначення координат (ГЛОНАСС/GPS). У даного типу навігації є суттєві недоліки: точність залежить від кількості репітерів в системі, необхідність маяків на визначеній площині, похибка в визначенні координат за рахунок особливостей рельєфу, недоступність сигналу в складних метео- чи магнітних умовах. Крім того, на місцевості зі складним рельєфом чи в приміщеннях GPS сигнал може прийматися нестійко та з завадами.

Альтернативою є локальна радіонавігаційна система дальнього радіусу дії, яка працює в режимі реального часу (RTLS). Дана технологія пов'язана з розвитком сенсорних технологій і алгоритмами, які забезпечують обробку і аналіз сенсорної інформації в реальному масштабі часу.

Архітектура системи RTLS включає в себе передавачі (мітки), які випромінюють сигнали з використанням розширення спектру та фіксовано встановленні пристрої зчитування (рідери). Випромінюючі сигнали приймає та обробляє інфраструктура системи RTLS. Кожен сигнал є коротким повідомленням, що містить тільки ідентифікатор мітки, або телеметричне повідомлення, що містить ідентифікатор мітки системи. Крім того, кожна передача містить слово статусу даних, інформацію про конфігурацію мітки системи, стан джерела живлення і додаткові дані.

Система RTLS є просторово-розподільчою системою, в якій прийомо-передавальні пристрої просторово рознесені, по різним об'єктам. В системі RTLS виникають задачі узгодження форм представлення сигналів від просторово-рознесених прийомо-передавальних пристроїв та синхронізації для можливості їх спільного використання.

Синхронізація пристроїв зчитування є важливим процесом в системах RTLS. Для забезпечення точності позиціонування не більше 1 м часова синхронізація пристроїв зчитування системи RTLS повинна мати порядок 1 нс. Однак існуючі прийомо-передавальні пристрої системи з часовою роздільною здатністю порядку 1 нс збільшують вартість пристроїв системи RTLS, а в процесі синхронізації сигналів виникають не скомпенсовані затримки сигналів в наслідок роботи радіочастотних компонентів прийомо-передавальних пристроїв системи.

Отже, створення системи позиціонування в реальному часі RTLS, яка здатна визначати координати робототехнічних комплексів військового призначення з високою точністю, є актуальною задачею.

Таким, чином застосування сучасних радіонавігаційних систем дальнього радіусу дії, які працюють в режимі реального часу, забезпечуєреалізацію нових принципів управління і ведення бойових дій з застосуванням робототехнічних комплексів військового призначення для вирішення задач в підрозділах Збройних Сил України.

Левченко В.В. (ВІТІ)
Артюх С.Г. (ВІТІ)

АНАЛІЗ ВИКОРИСТАННЯ ПЛАТФОРМ ВІРТУАЛІЗАЦІЇ В ЗАХИЩЕНИХ МЕРЕЖАХ

Актуальність.Сучасна інформаційно-телекомунікаційна система (ІТС) ЗС України характеризується великою кількістю телекомунікаційних послуг та сервісів, що розгорнуті на окремих фізичних серверах.Ефективність використання технологій віртуалізації в ІТС дозволить отримати скорочення витрат на закупівлю додаткового обладнання, зниження витрат на програмне забезпечення, підвищення доступності додатків і забезпечення безперервності роботи організації.

Постановка задачі. Провести порівняльний аналіз існуючих сучасних платформ віртуалізації на основі їх показників, параметрів для визначення можливості подальшого використання в захищених системах та мережах.

Основні положення.Платформа віртуалізації(гіпервізор)допомагаєна одному фізичномусервері розгорнути кілька віртуальних серверів з різними операційними системами. Гіпервізоридозволяють вирішуватизавдання оптимізації розподілу корисного навантаження між серверами, створення середовища віртуальних машин(ВМ),управління центрами обробкиданих, забезпечення використання наявних фізичних пристроїв та міграції додатків між різними фізичними серверами.

Для виконання вимог з безпекив захищених мережах платформи віртуалізації (ПВ)повинні здійснюватиконтроль доступу та збереження цілісності даних, аутентифікацію та перевірку привілеїв, підтримку ключів шифрування та управління правами, а також резервне копіювання даних.

Порівняльний аналіз сучасних ПВ відображено в таблиці 1,проводився на основі визначених параметрів, які забезпечують універсальність, доступність та надійність

Таблиця 1

Порівняння основних параметрів платформ віртуалізації

Параметр	Платформа віртуалізації			
	Citrix	**MS Hyper-V**	**KVM**	**PROXMAX VE**
Центральне управління	так	так	ні	так
Засоби резервного копіювання	ні	так	ні	так
Шаблони ВМ	так	ні	так	так
Підтримка функцій ВМ	так	ні	так	так
Maxmemoryхост/ВМ	4Тб/1 Тб	6 Тб/1 Тб	8 Тб/2 Тб	12 Тб/ 4Тб
Max CPU хост/ВМ	320/128	320/64	480/64	680/128
Міграція між хостом	так	так	так	ні
Автоматична міграція між хостом	так	ні	так	так
Моніторинг трафіка	так	так	так	так

ПВ ProxmaxVEмає можливість інтегрувати інший гіпервізор KVM та контейнери Linux (LXC), використовувати програмно визначені сховища та функціональні можливості мережі на одній платформі.Завдяки інтегрованому веб-інтерфейсу користувача здійснюється керування віртуальними машинамита контейнерами, а також інтегрованими інструментами аварійного відновлення.

ГіпервізорProxmaxVEмає можливість взаємодіяти з пристроями різних виробників, забезпечує моніторинг трафіку в мережі та регулярно оновлюється.

Висновок. Проведений порівняльний аналізсучасних платформ віртуалізації дозволяє обрати перспективним рішенням гіпервізорProxmaxVE для розгортання в захищених мережах, про те питання повноцінного застосування ProxmaxVEпотребує подальшого вивчення та дослідження.

Легкобит В.С. (ВІТІ ім. Героїв Крут)
Гавриленко Р.В. (ВІТІ ім. Героїв Крут)

МЕТОД АНАЛІЗУ ІЄРАРХІЙ ПРИ ВИРІШЕННІ ЗАДАЧ ПОВ'ЯЗАНИХ З РОЗРАХУНКОМ ПОКАЗНИКІВ ПРІОРИТЕТНОСТІ ЛОГІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ ЗСУ

Поступова трансформація ІТ-інфраструктури державних установ, яка відбувається під впливом низки еволюційних, інтелектуальних, інноваційних факторів та випадкових подій, обумовили необхідність застосування нового підходу до організації системи планування забезпечення підрозділів Збройних Сил України (ЗСУ) всіма видами матеріальних ресурсів. Таким новим підходом, який базується на принципі інтегрованості всіх процесів, які формують рух матеріальних засобів від постачальників до споживачів, є логістичний підхід.

Реалізація логістичного підходу в управлінні потоками матеріальних засобів вимагає відповідності та збалансованості управлінських рішень як між усіма суб'єктами логістичної діяльності, так і в забезпеченні логістичних потреб підрозділів. Практична реалізація визначених принципів логістичної діяльності можлива лише при умові наявності достатніх професійних компетенцій всього персоналу, який прийматиме управлінські рішення та реалізуватиме логістичні функції та операції. На основі вищезазначеного одним із напрямків роботи системного аналітика в сфері логістичного забезпечення є формулювання гіпотез та наукових задач для подальшого прогнозування пріоритетності логістичного забезпечення відділів, сил та служб ЗСУ. Наразі складність полягає в опрацюванні великого обсягу вхідних даних тому актуальним є створення інформаційно-вимірювальних систем підтримки прийняття рішення при вирішенні задач розрахунку показників пріоритетності логістичного забезпечення.

Метою роботи є практичне застосування програмної реалізації математичного апарату методу аналізу ієрархій при вирішенні задач пов'язаних з розрахунком показників пріоритетності логістичного забезпечення підрозділів ЗСУ.

Провівши дослідження та зробивши порівняльний аналіз показників пріоритетності логістичного забезпечення обрано метод аналізу ієрархій для удосконалення логістичного забезпечення ЗСУ. Основною перевагою даного методу є висока універсальність.

Метод може застосовуватися для вирішення найрізноманітніших завдань: аналізу можливих сценаріїв розвитку ситуації, розподілу ресурсів, складання рейтингу постачальників, прийняття кадрових рішень тощо. Метод в найбільшій мірі підходить для тих випадків, коли основна частина даних заснована на перевагах особи, яка приймає рішення в процесі вибору найкращого варіанту рішення з безлічі існуючих альтернатив[1].

Метод аналізу ієрархій реалізується через наступні етапи [2]:

1. Структурування завдання у вигляді ієрархічної структури (мета; критерії (k), субкритерії (С), альтернативи (а)).

Постановка завдання в процесі застосування методу аналізу ієрархій: нехай є безліч альтернатив (варіантів рішень): $a_1, a_2, \dots a_n$ Кожна з альтернатив оцінюється списком критеріїв: $k_1, k_2, \dots k_n$. Потрібно визначити найкраще рішення.

2. Попарне порівняння альтернатив за важливістю за дев'ятибальною шкалою зі складанням відповідної матриці (таблиці) розміру (n × n). В процесі заповнення матриці якщо елемент і важливіше елемента j, то клітина (i, j), відповідно рядку і і стовпцю j, заповнюється цілим числом, а клітина (j, i), відповідно рядку j і стовпцю і, заповнюється зворотним числом (дробом).

При розрахунках даних будуть використані наступні формули:

Визначимо середнє геометричне значення кожної строки матриці попарних порівнянь (1):

$$a_i = \sqrt[n]{k_{ij}^1 * k_{ij}^2 * \dots * k_{ij}^n} (1)$$

де a_i – середнє геометричне значення критеріїв кожної строки;

k_{ij} – значення критеріїв;

n – кількість критеріїв;

Наступним етапом є визначення ваги критерію – компоненти нормалізованого вектора пріоритетів (НВП) (2):

$$\text{НВП}_n = \frac{a_i}{\sum a_i} \quad (2)$$

Отримані локальні пріоритети перевіримо на узгодженість, використовуючи такі формули:

власне значення матриці (3):

$$\lambda_{max} = \sum_{j=1}^{n} k_{ij} * \text{НВП}_n \quad (3)$$

індекс узгодженості (ІУ) (4):

$$\text{ІУ} = \frac{\lambda_{max} - n}{n-1} \quad (4)$$

зв'язаність узагальненої узгодженості (УУ) (5):

$$\text{УУ} = \frac{\text{ІУ}}{\text{ПВУ}} \quad (5)$$

де ПВУ – показник випадкової узгодженості для позитивної зворотно симетричної матриці випадкових оцінок розміру n×n, який визначається при умові, що оцінки в матриці надані випадково; ПВУ залежить лише від розміру матриці. Розмір матриці залежить від обраної кількості критеріїв (n).

Останнім етапом є перевірка достовірності рішення, що включає розрахунок узагальнюючого відношення узгодженості:

Рішення вважається достовірним, якщо УУ $\leq$ 10%, в іншому випадку потрібно коригувати матриці порівняння варіантів за критеріями.

Алгоритм застосування розглянутої моделі можна реалізувати за допомогою інструментарію серверної частини веб-системи платформи Node.js. Основною мовою програмування для розроблення системи буде JavaScript. Клієнтську частину системи можна реалізувати за допомогою бібліотеки React та HTML, CSS і JavaScript. Обмін інформацією між мікросервісами і клієнтською частиною програми відбуватиметься за допомогою REST API.

Таким чином, використовуючи метод аналізу ієрархій можна провести розрахунки пріоритетність досягнення цілей для забезпечення високої ефективності логістичної системи Збройних Сил України в межах визначеної логістичної стратегії. Запропонований до використання метод передбачає, по-перше, структурування мети шляхом ранжування критеріїв за порядком зменшення їх значущості, по-друге, визначення критеріїв, кожен з яких визначеним чином впливає на мету, по-третє, побудову матриці попарних порівнянь та розрахунок пріоритетів [3].

Проведене дослідження пропонує до використання конкретний інструментарій стратегічного управління, а саме: метод аналізу ієрархій для формування пріоритетності логістичного забезпечення Збройних Сил України, що зможе забезпечити високу ефективність логістичної системи в межах визначеної логістичної стратегії. Запропонований підхід дозволить значно підвищити ефективність існуючих систем логістичного забезпечення військових частин.

Список використаних джерел:

1. Новікова М. М. Побудова логістичної стратегії підприємств / М. М. Новікова, Н. О. Кондратенко // Науковий вісник Чернівецького університету: збірник наукових праць. – Чернівці: ЧНУ, 2014. – Випуск 717 Економіка. – С. 78-81.

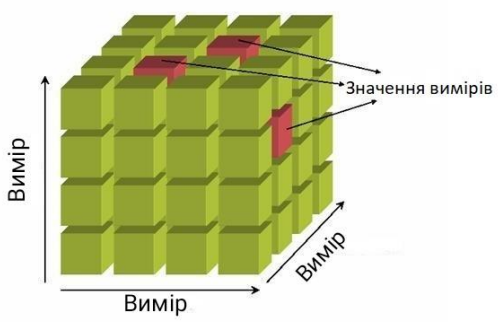
2. Сааті Т. Прийняття рішень. Метод ааналізу ієрархій / Т. Л. Сааті. – М.: Радіо та зв'язок, 1993. – 278 с.

3. Редька В. С. Сутність та основні види логістичних стратегій та їхнє місце у системі управління підприємством / В. С. Редька // Вісник національного університету «Львівська політехніка». – 2012. – №735. – С. 187-191.

Легкобит В.С.(ВІТІ ім.Героїв Крут)
Мірошниченко А.О. (ВІТІ ім.Героїв Крут)

КОНСОЛІДАЦІЯ ДАНИХ В СИСТЕМАХ OLAP НА ОСНОВІ APACHE DRUID

Важко переоцінити важливість аналізу даних в сучасному суспільстві, особливо у військовій сфері. Враховуючи стрімко зростаючі темпи та обсяги генерації тих самих даних, надзвичайної важливості набувають методи їх аналітичної обробки, особливо в режимі реального часу.



Функціональність OLAP характеризується динамічним багатовимірним аналізом консолідованих даних, що підтримують аналітичну та навігаційну діяльність. Консолідація передбачає агрегування даних, які можуть бути накопичені та обчислені в одному або кількох вимірах. Ядром будь-якої системи OLAP є куб, який складається з числових фактів, які називаються мірами, що класифікуються за розмірами. Метадані куба зазвичай створюються на основі схем із зірочкою або сніжинкою таблиць у реляційній базі даних. Показники виводяться з записів у таблиці фактів, а розміри — з таблиць вимірювань.

В будь-якому випадку швидкість отримання знань з консолідованих наборів даних є пріоритетним показником. Що стосується аспектів технічної реалізації, то застосування високопродуктивних, масштабованих, з можливістю паралельної обробки потоків даних з декількох конвеєрів, серверів баз даних існує декілька підходів, одним з яких – застосування ApacheDruid.

Серед особливостей ApacheDruid важливо виділити наступні:

- миттєва видимість даних або підтримка високого рівня паралельності;
- передача даних з шин повідомлень, таких як Kafka і AmazonKinesis , і файлів пакетного завантаження з озер даних, таких як HDFS і Amazon S3;
- поєднання нових ідей зберігання, структур індексації, а також точних та приблизних запитів, щоб отримати більшість результатів менш ніж за секунду;
- стовпчиковий формат зберігання передбачаєвикористання сховища, орієнтованогона завантаження лише точних стовпців, необхідних для конкретного запиту;
- використанняRoaring або CONCISE стиснені растрові індекси для забезпечення швидкої фільтрації та пошук у кількох стовпцях;
- можливість застосування алгоритмів апроксимації для збільшення швидкості обробки даних нехтуючи точністю.

Серед сфер застосування найбільш ідентичні до військової:

- аналітика Clickstream (веб- та мобільна аналітика);
- аналітика мережевої телеметрії (моніторинг продуктивності мережі);
- постачання даних до графічних інтерфейсів аналітичних додатків;
- як бекенд для висококонкурентних API, які потребують швидкої агрегації;

Таким чином застосування ApacheDruid буде більш ефективним у випадках коли частота записів дуже висока, але оновлення трапляються рідше, більшість запитів спрямованих на агрегацію та формування звітів, дані мають пряму залежність від часових показників та термін отримання результатів запитів наближений до 100 мс, в таблицях використовуються високонавантажені стовпці, які потрібно швидко оцінити й обробити. Отже сучасний рівень розвитку апаратних і програмних аналітичних засобів створив передумови для впровадження їхз метоюзабезпечення діяльності органіввійськового управління в контексті обробки великих обсягів даних, якімістять у собі великі потенційні можливості звитягу корисної аналітичної інформації, на основі якої можна виявляти приховані тенденції, будувати стратегію розвитку та знаходити нові рішення.

Легкобит В.С. (ВІТІ ім. Героїв Крут)
Дацков Д.О. (ВІТІ ім. Героїв Крут)

ТЕХНІЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ ПРОЦЕСІВ ETL В КОНТЕКСТІ МІНІМІЗАЦІЇ НЕОБХІДНИХ РЕСУРСІВ ШЛЯХОМ ЗАСТОСУВАННЯ СИСТЕМИ CHANGEDATACAPTURE (CDC)

Необхідність отримання максимально повних, актуальних, однорідних наборів даних є необхідною умовою для їх подальшого якісного аналізу та прийняття зважених рішень. Тому робота з даними повинна бути організована належним чином для отримання бажаного результату. Серед багатьох інструментів, які можуть допомогти нам побудувати відповідний робочий процес, ETL (Extract, Transform, Load) виступає як відсутня частина головоломки.

Щоб забезпечити найефективнішу роботу процесів ETL необхідно в першу чергу позбутися непотрібних даних, тому що кількість даних напряму впливають на швидкість і якість їх обробки. По друге необхідно застосовувати паралельну обробку шляхом виконання декількох одночасних ітерацій. Також варто приділяти особливу увагу застосуванню інструментів фіксації, аналізу та виправлення помилок.

При розробці процесів ETL важливо звертати увагу на наступні технічні аспекти:

- забезпечення ведення журналу подій, що дозволить відстежувати причини виникнення помилок;
- забезпечення гнучкості роботи з різними джерелами структурованих і неструктурованих даних;
- створення відмовостійкої системи, яка матиме можливість відновлення у разі виникнення непередбачуваних проблем без втрати чи пошкодження даних;
- розробка системи сповіщень для забезпечення аналітики в режимі реального часу;
- підтримка інкрементного завантаження шляхом застосування CDC (change data capture) для забезпечення синхронності даних.

CDC це підхід до інтеграції даних, заснований на ідентифікації, реєстрації та доставці змін, внесених у корпоративні джерела даних, у зовнішні системи. CDC часто зустрічається в середовищах, де зберігаються дані, оскільки захват і збереження даних є однією з основних функцій сховищ даних. CDC відстежує операції DML, які застосовуються до таблиць БД. Це робить деталі змін доступними в легко засвоюваному реляційному форматі. Інформація про стовпці та метадані, необхідні для застосування змін до цільового середовища, фіксуються для змінених рядків і зберігаються в таблицях змін, які відображають структуру стовпців вихідних таблиць.

Рішення CDC, засновані на файлах журналів транзакцій, мають наступні переваги:

- мінімальний вплив на базу даних (особливо, якщо для обробки журналів на виділеному хості використовується доставка журналів).
- відсутність необхідності вносити програмні зміни в додатках, користуючись базою даних.
- низька затримка при отриманні змін.
- цілісність транзакцій: сканування журналу може створити потік змін, який відтворює вихідні транзакції в порядку їх фіксації. Такий потік змін включає в себе зміни, зроблені у всіх таблицях, які беруть участь у загальній транзакції.

Отже, враховуючи всі особливості CDC, застосування даної системи дозволяє усунути необхідність масового завантаження під час оновлення даних. Реалізація поетапного завантаження або потокової передачі змін даних у сховище даних передбачає використання даного інструменту для аналізу великих даних , заповнення інформаційних панелей BI в реальному часі, синхронізації даних між географічно розподіленими системами та полегшення міграції баз даних без простоїв. Дозволяючи виявляти, фіксувати та передавати змінені дані, CDC скорочує час, необхідний для зберігання даних, і витрати на ресурси, забезпечуючи безперервну інтеграцію даних.

Легкобит В.С. (ВІТІ ім. Героїв Крут)
Коваленко А.С. (ВІТІ ім. Героїв Крут)

АНАЛІЗ ЕФЕКТИВНОСТІ ЕКСПЛУАТАЦІ ВЕБ-ДОДАТКІВ НА ОСНОВІ ТЕХНОЛОГІЇ PROGRESSIVEWEBAPPS

Динаміка розвитку сучасних інформаційних технологій вражає своїми темпами та масштабами, не винятком залишається і розробка веб-додатків. Однак за результатами проведеного аналізу досвіду інженерів у визначеній галузі було виявлено декілька проблемних питань, що суттєво впливають на ефективність процесу розробки:

застосування новітніх технологій та підходів не гарантують конкурентної переваги, у зв'язку з тим, що нові речі також часто не перевірені, непередбачувані та просто занадто ризиковані, щоб їх впроваджувати в реальні проекти. Натомість використання одних і тих же технологій з року в рік без вивчення нічого нового також є занадто консервативним підходом.

застосування немасштабованих архітектур допомагає швидше розгортати невеликі проекти, але як тільки з'являться нові вимоги, виникають додаткові витрачати часу не лише на те, щоб підтримувати цю архітектуру в робочому стані, а й на розширення можливостей.

часто веб-розробники забувають про пакети та мініфікацію та запускають код ранньої розробки у продакшн. Такий код працює повільніше, довше завантажується і вимагає більше трафіку.

Поверхнева компетентність відносно нових фреймворків, бібліотек та підходів до розробки, суттєво може вплинути на процес розробки. Тому варто докладати максимум зусиль для більш детального їх вивчення.

Враховуючи вищезазначене доцільно звернути увагу на позитивні тенденції щодо веб-розробки, а саме PWA (Progressive Web Applications).

PWA в першу чергу визначають нативність поведінки веб-додатків, характеризуються можливістю запуску в автономному режимі та високим рівнем захищеності, ресурси клієнта зберігаються локально, а через мережу передається тільки той контент що змінюється. Технології на яких базується PWA:

- Service Worker - серце PWA. Це проксі-рівень між інтерфейсом і бекендом у браузері. Через нього проходять усі запити браузера. Такий поділ на два незалежні рівні максимально полегшив перехід від звичайного веб-сайту до PWA.Концептуально Service Worker являє собою javascript файл, який підключається в коді сторінки. Service Worker чудово пишеться руками, і це потрібно, щоб добре розуміти і контролювати логіку роботи веб-додатку.
- HTTPS. PWA вимагає, щоб усі ресурси сайту передавались по протоколу HTTPS.
- Application Shell. Суть полягає в тому, що оболонка програми зберігається на клієнті та завантажується при запуску додатків, а потім уже в неї завантажується з мережі динамічна інформація.

Для багатьох установ, особливо тих, хто створює додатки для внутрішнього використання, витрати на розробку, тестування та підтримку кросплатформних додатків є невиправданими. Gartner прогнозує, що до наступного року до 20% користувачів можуть відмовитись від нативних додатків. Натомість вони вважають, що PWA стане більш життєздатною альтернативою їм. Застосування у ЗСУ може знайти дана технологія наприклад для розробки підсистем інтерактивного психологічного тестування для визначення когнітивних здібностей осіб, які планують вступати на військову службу. В будь-якому випадку технічна реалізація масштабних проектів, орієнтованих на достатньо велике коло користувачів, неодмінно міститиме в собі прогресивні веб-технології. Якщо вже такі транснаціональні гіганти як Google та Microsoft активно інвестують у проекти на основі PWA, то можна зробити висновок, що продуктивність, безпека та надійність PWA у поєднанні з розширеними можливостями дозволять ще декілька років використовувати створені нами додатки будь-де, на будь-якому пристрої.

Легкобит В.С. (ВІТІ ім. Героїв Крут)
Фисун А.С. (ВІТІ ім. Героїв Крут)

АНАЛІЗ ПІДХОДІВ ДО ДИНАМІЧНОЇ ВІЗУАЛІЗАЦІЇ ВМІСТУ .DOCX ФАЙЛІВ ЗА ДОПОМОГОЮ БІБЛІОТЕК JAVASCRIPT

У висококонкурентному середовищі, такому як цифрове, важливо передбачити зміни та навчитися адаптуватися до них. Ще в 2002 році Стюарт Морріс розробив перший у світі одно сторінковий веб-додаток. Це надихнуло веб-розробників на створення таких фреймворків, як Angular, Node, React тощо. Інновації в ідеях веб-розробки не зупинилися, і щодня з'являються нові тенденції та технології, які дають можливості веб-додаткам бути більш динамічними, інтерактивними та швидкими. Успішні керівники установ не розглядають технології просто як спосіб автоматизації рутинних процесів, а натомість використовують їх, щоб відкрити нові можливості для досягнення успіху. Progressive Web Apps (PWA), Accelerated Mobile Pages (AMP), Single Page Application (SPA) технології, які набули популярності завдяки своїй доступності та надійності, забезпечують високу продуктивність та якість відображення контенту. Тестування автоматизаціїдозволить спрямувати зусилля на максимізацію продуктивності та мінімізацію витрат. Застосування безсерверних архітектура є результатом дослідження можливості уникнути перевантаження систем, втрати даних і перевитрат на апаратне забезпечення. Враховуючи поточний стан справ, переважно у Державних установах, в контексті реалізації документообігу, на перший план виходить застосування застарілих методів реалізації даного процесу. Зрозуміло, що стрімкого переходу та впровадження сучасних технологій не варто й чекати. Це пов'язано в першу зі значним об'ємом накладних витрат. Але реалізація певного симбіозу між необхідністю обробляти формалізовані документи в паперовому вигляді та необхідністю у найкоротші терміни передавати та візуалізувати їх в електронному виглядає більш ніж реальною.

Документи Word є скрізь і використовуються для незліченних завдань повсякденної діяльності, і ЗСУ не виключення, тому нам може знадобитися підтримка їх створення у нашому веб-додатку або на веб-сторінці, це може включати завантаження рапортів, довідок, звітів, які клієнт може роздрукувати або надіслати електронною поштою.

Існує достатня кількість JavaScript DOCX Builder Libraries, серед них:

- *easy-template-x* дозволяє створювати документи docx із шаблонів у Node або в браузері.
- *carbone* Швидкий, простий і потужний генератор звітів. Дозволяє створювати PDF, DOCX, XLSX, PPTX документи.
- *docx* дозволяє створювати файли .docx за допомогою JS/TS з гарним декларативним API. Працює для Node і в браузері.
- *Docxtemplater* дозволяє генерувати docx, pptx та xlsx із шаблонів, із Node.js, браузера та командного рядка.
- *Officegen* автономний генератор Open XML файлів Microsoft Office 2007 і новіших версій.
- *generate-docx* генерує .docx з шаблону та даних.
- *docx-builder* модуль NPM для створення або об'єднання файлів .docx
- *docxtemplater-ie11* генератор docx і pptx, що працює з шаблонами та даними.

Таким чином застосування бібліотек для створення, модифікації та пересилання формалізованих документів стає необхідним у розробці веб-додатків орієнтованих на забезпечення потреб документообігу. У поєднані з впровадженням сучасних технологій веб-розробки ми маємо можливість отримання ряду суттєвих переваг в оптимізації витрат, як часових так і фінансових, що істотно вплине на досягнення успіху у забезпеченні потреб життєдіяльності підрозділів ЗСУ.

д.т.н. Лисенко О.І. (КПІ ім. Ігоря Сікорського)
к.т.н. Явіся В.С. (КПІ ім. Ігоря Сікорського)
к.т.н. Новіков В.І. (КПІ ім. Ігоря Сікорського)
аспірант Сушин І.О. (КПІ ім. Ігоря Сікорського)

ЗАСТОСУВАННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ НА БАЗІ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У ВІЙСЬКОВИХ ЦІЛЯХ

Нині бездротові сенсорні мережі (БСМ) є невід'ємною частиною телекомунікаційних систем, що використовуються у військовій сфері. Головною перевагою використання БСМ в умовах бойових дій – швидке, просте та недороге впровадження інфраструктури на території без покриття. Ці мережі формуються на ad-hoc основі, тому їм не потрібно заздалегідь задана структура.Критичним аспектом цієї концепції є потреба у великій кількості релевантної інформації з поля бою, яка доставляється на об'єкт у режимі реального часу для підтримки систем прийняття рішень у центрах управління.

Мережі бездротових датчиків складаються з великої кількості дешевих статичних датчиків, які розкидані на певній географічній області. Датчики здійснюють моніторинг навколишнього середовища та збирають конкретну інформацію, таку як: виявлення руху противника, ідентифікація сил противника, захист кордону, місцезнаходження снайпера тощо [1]. Вони забезпечують інформаційну підтримку для координації, планування та розгортання дій сил, які здійснюють захист території.

Датчики в польових умовах можуть бути мобільними. Мобільні датчики можуть безпосередньо зв'язуватися один з одним по високошвидкісних каналах зв'язку і мають більшу обчислювальну потужність. У військових цілях для перенесення датчиків ефективніше використовувати транспортні засоби, ніж людей. Безпілотні літальні апарати (БПЛА) – мобільні та відносно дешеві пристрої, які ефективно покривають великі площі місцевості з великої висоти. БПЛА використовуються в бездротових сенсорних мережах як основні елементи мережі або для модернізації мережі, що складається з фіксованих сенсорних вузлів. У другому випадку БПЛА можна використовувати як головний вузол кластера, який виконує агрегацію даних, зібраних із сенсорних вузлів, або навіть як базову станцію, яка виконує збирання даних із усієї мережі.

БПЛА в БСМ можна використовувати на різних рівнях мережі: рівень базової станції, рівень головного вузла, рівень сенсорного вузла. На найнижчому рівні БПЛА можуть грати роль мобільних сенсорних вузлів, основним завданням яких є зчитування різноманітних даних з поля та пересилання їх до центру обробки. Використання БПЛА на цьому рівні розширює поле зондування. Крім того, ця концепція може забезпечити додаткове та більш точне зондування, коли це необхідно.

Статичні датчики на полі бою зазвичай розгортаються за допомогою літака, і їх позиції погано сплановані, тому БСМ є мережею зі змінною щільністю, що означає, що деякі частини мережі є щільними, а деякі частини мережі розріджені. Можливо, що частина мережі статичних датчиків буде повністю вилучена через відключення живлення або несправність датчика. Тому окремі ділянки території можна залишити без нагляду. Але, деякі дуже важливі місця потребують додаткових датчиків. У цих ситуаціях використання БПЛА є найефективнішим способом якнайшвидшого відновлення зони, в якій припинено зондування (рис. 1).

Якщо БПЛА використовуються на другому рівні БСМ, тоді весь зв'язок з БС здійснюється через БПЛА (рис.3). Зондування на землі все ще виконується статичними датчиками, які розташовані та згруповані випадковим чином.

БСМ зазвичай мають ієрархічну структуру. Вся мережа організована у вигляді кластерів. Кожен кластер має свій власний головний вузол (ГВ), який здійснює весь зв'язок з базовою станцією (БС), яка розташована у віддаленому захищеному місці. Ієрархічна

організація мережі дає можливість формувати кластери і обирати ГВ за допомогою одного з відомих алгоритмів [2].

Бездротова сенсорна мережа, яка утворена лише статичними датчиками, являє собою одновимірну мережу, де будь-які перешкоди можуть назавжди або тимчасово припинити з'єднання або ускладнити його. Затінений датчик несе втрати не тільки своїх даних, а й усіх даних, що були створені іншими датчиками в кластері, які пересилаються до кінцевого пункту через нього. Поєднання статичних та мобільних сенсорних вузлів надає ряд можливостей для покращення доступності та функціональності бездротових сенсорних мереж, що використовуються у військових цілях.

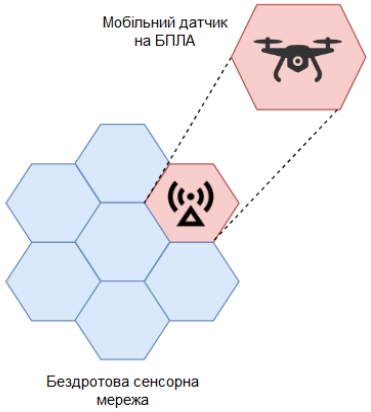


Рис. 1 Відновлення області без зондування

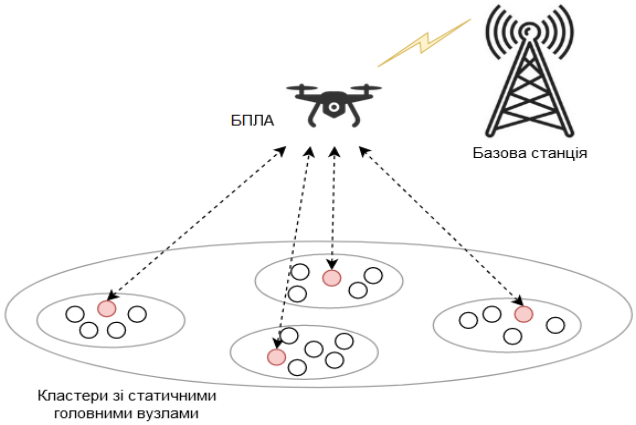


Рис. 2 Взаємодія між БПЛА та кластерами в ієрархічній БСМ

Використання БПЛА на третьому рівні бездротових сенсорних мереж означає, що в мережі є БПЛА, який виконує роль базової станції. Цей БПЛА збирає всі дані на місцях і встановлює прямий зв'язок із системами управління, де дані обробляються.

Незважаючи на всі переваги, додавання БПЛА в БСМ має деякі проблеми. Основною потенційною проблемою для функціонування такої системи є погодні умови, які можуть значно погіршити або повністю вивести мережу зв’язку з ладу. Цей тип мережі потребує більш ефективного управління ресурсами та механізмів безпеки. Зв'язок БПЛА-БС часто пов'язаний з відносно великою відстанню, тому можуть підтримуватися лише послуги, які можуть допускати затримку. Необхідно враховувати, що датчики в мережі мають буди охоплені в періоди часу, коли частина БПЛА повинна буде покинути зону обслуговування через підзарядку акумулятора. У цей період службовий пробіл необхідно заповнити сусідніми БПЛА зі збільшеною потужністю передачі або відкоригувати положення БПЛА. З цієї причини було б добре мати БПЛА на сонячних батареях як базовий або як резервний варіант. Отже, БСМ відіграють важливу роль у різноманітних військових застосуваннях. Проте впровадження цих мереж на місцях, де проводяться воєнні дії, є проблематичним. Тому потрібно враховувати усі нюанси ще на етапах планування мережі. Використання БПЛА на різних рівнях бездротових сенсорних мереж значно сприяє гнучкості, безпеці, надійності та підключенню до мережі, а також зменшенню споживання енергії в мережі.

ЛІТЕРАТУРА

1. M. Winkler, K.D. Tuchs, K. Hughes, G. Barclay, Theoretical and practical aspects of military wireless sensor networks, Journal of Telecommunications & Information Technology,2008.

2. G. Popovic, G. Djukanovic, Cluster formation techniques in hierarchical routing protocols for Wireless Sensor Networks, Journal of Information Technology and applications , 2016.

д.т.н. Лисенко О.І. (КПІ ім. Ігоря Сікорського)
к.т.н. Явіся В.С. (КПІ ім. Ігоря Сікорського)
Сушин І.О. (КПІ ім. Ігоря Сікорського)

ПІДХІД ДО ПОБУДОВИ СИСТЕМИ СТАБІЛІЗАЦІЇ МУЛЬТИКОПТЕРНИХ ДРОНІВ

Сьогодні мультикоптерні дрони широко використовуються для ведення повітряної розвідки і видачі даних цілевказання. Імовірність виконання покладених на мультикоптерні дрони завдань напряму залежить від спроможності забезпечити його рух по визначеній траєкторії. Центральне місце при реалізації цього завдання належить способу побудови системи стабілізації – основної складової системи управління мультикоптерного дрону [1].

Пропонуються наступні основні етапи методики формування системи стабілізації мультикоптерних дронів [2, 3]:

а). Етап аналітичного дослідження включає:

- обґрунтування й вибір способів забезпечення аєронавігації мультикоптерних дронів;
- лінеаризацію рівнянь руху мультикоптерних дронів як об'єкта керування;
- вибір найбільш критичних моментів часу по програмі польоту, для яких проводиться інша робота на цьому етапі;
- обґрунтування й вибір параметрів керування;
- обґрунтування й вибір типів вимірювальних елементів;
- одержання кінематичних співвідношень між вимірюваними параметрами й параметрами керування;
- компонування функціональної схеми системи;
- поділ системи рівнянь руху на окремо інтегруємі групи (поздовжній рух, бічний рух, обертання, крен) і розробка відповідних структурних схем;
- обґрунтування схем, що описують рух близько центру маси й центру маси відносно траєкторії, що задається;
- вибір значень коефіцієнтів передачі контурів керування за критерієм точності;

б). Етап моделювання динаміки системи включає:

- уточнення обраних аналітично параметрів за критеріями точності й стійкості;
- вибір закону керування з урахуванням необхідної форми перехідних процесів;
- уточнення результатів попереднього етапу при змінних параметрах системи;
- остаточне (на етапі розробки) уточнення всіх алгоритмів і параметрів системи;
- облік впливу нелінійностей у виконавчих органах і інших ланках системи;
- аналіз точності системи з урахуванням дії на її входах збурень випадкового характеру.

Запропонований шлях формування системи стабілізації мультикоптерних дронів дозволяє підвищити загальну точність системи управління за рахунок використання сигналів аеронавігації, а відповідно – забезпечити високу імовірність виконання покладених на мультикоптерні дрони завдань.

ЛІТЕРАТУРА

1. Явіся В.С. Методи забезпечення стійкої роботи сенсорних мереж на базі безпілотних літальних апаратів // Десята міжнародна науково-технічна конференція «Проблеми телекомунікацій». Матеріали конференції. – К.: НТУУ «КПІ». – 2016. – С. 498-500.

2. Лебедев Р. К. Стабилизация летательного аппарата бесплатформенной инерциальной системой. – М.: Машиностроение, 1977. − 144 с.

3Явіся В.С., Вакуленко О.В., Могилевич Д.І. Методика формування системи стабілізації безпілотних літальних апаратів // IX Науково-практична конференція «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв’язку та автоматизації в АТО». Збірник тез. – К.: ВІТІ. – 2016. – С. 207.

д.т.н. Лисенко О.І. (КПІ ім. Ігоря Сікорського)
к.т.н. Явіся В.С. (КПІ ім. Ігоря Сікорського)
Сушин І.О. (КПІ ім. Ігоря Сікорського)

СПОСІБ ЗАБЕЗПЕЧЕННЯ СТІЙКОГО УПРАВЛІННЯ ДРОНАМИ

Сьогодні за допомогою мультикоптерних дронів малих розмірів з електродвигунами можна контролювати технічний стан об'єктів, їх безпеку та режими функціонування, дрони можна використовувати з метою аерофотознімання для картографування, безпілотні комплекси дозволяють підвищити показники телекомунікаційних мереж (живучість, пропускну здатність), вони можуть доставляти вантажі і т.п.

Як правило, будь-яке застосування дронів передбачає, що одержувана з їхньою допомогою інформація й сигнали управління безпосередньо дронами повинні передаватися в реальному часі, що вимагає забезпечити передачу великого обсягу даних при заданих смузі пропускання й імовірності бітової помилки.

Для підвищення пропускної здатності необхідно використовувати спектрально-ефективні методи модуляції, що змушує забезпечити більш високе відношення сигнал/шум (ВСШ) на вході приймача [1].

Дрони як правило використовуються на відстанях до 10 км, тому обмежень, пов'язаних з «прямою видимістю» для них не існує, оскільки при висоті польоту 50 м і висоті наземного комплексу управління (НКУ) 1,5 м (за умови його знаходження в руках оператора), дальність прямої видимості, яка визначається формулою [2]:

$$D_{\text{км}} = 4{,}12(\sqrt{h_1} + \sqrt{h_2}),$$

де h_1, h_2 – висоти дрону й НКУ відповідно, складе більше 30 км.

При використанні діапазону 2,4 ГГц загасання сигналу на зазначеній відстані досягає 120 дб [1], таке загасання можна перекрити при використанні достатньо розповсюджених передавачів з посиленням близько 30 дб та приймачів з чутливістю порядку –90 дб.

Однак, для забезпечення ймовірності помилки порядку 10^{-6} при використанні QAM32 на вході приймача необхідне ВСШ на рівні 18 дб [2]. Враховуючи втрати у фідері приймача й передавача (усього близько 3 дб), стає зрозумілим, що енергетика переданого сигналу в реальних умовах повинна бути збільшена не менш ніж на 21 дб.. Розв'язати таке завдання можна шляхом використання спрямованих антен.

Для параболічної антени коефіцієнт підсилення розраховується за формулою [2]:

$$G = 10\lg(k(\pi D/\lambda)^2 \cos\varphi) \quad (1)$$

де: G – коефіцієнт підсилення; k – ефективність або коефіцієнт використання поверхні антени (для більшості антен рівний приблизно 0,55); D – діаметр дзеркала; λ – довжина хвилі; φ – кут приходу хвилі.

Відповідно до виразу (1) при діаметрі дзеркала 0,5 м, точно спрямованій антені на дрон ($\varphi = 0$), у діапазоні 2,4 ГГц коефіцієнт підсилення складе лише 19,4 дб. Подальше підвищення коефіцієнта підсилення може бути здійснене за рахунок збільшення діаметра дзеркала, що важко реалізувати для носимих НКУ. Зрозуміло, що рівень сигналу повинен бути підвищений «із запасом» приблизно на 5 дб, що можна забезпечити за допомогою спрямованої антени на борті дрону.

Управління напрямком максимального посилення бортової антени може здійснюватися декількома способами [3]: установка антени на опорно-поворотному пристрої; використання багатоелементної антенної решітки з керованою діаграмою спрямованості; використання декількох антен, що перемикаються.

При установці антени на опорно-поворотному пристрої необхідне створення обертового переходу. Він може бути розміщений у різних місцях: перед антеною після підсилювача потужності; після передавача перед підсилювачем потужності й антеною; передавальний пристрій, підсилювач потужності й антена розміщуються на поворотному пристрої, через багатоканальний обертовий перехід передаються сигнали та живлення.

Загальними недоліками використання опорно-поворотного пристрою є:

- висока вартість обертового коаксіального НВЧ переходу;

- при розміщенні гостроспрямованої антени будь-якого типу на опорно-поворотному пристрої, більша частина поверхні поворотної платформи залишається невикористованою.

- переміщення антени в горизонтальній площині приводить до переміщення центру ваги дрону, а отже до дестабілізації його просторового положення;

- значні витрати потужності на роботу електропривода.

При реалізації другого способу для створення антенної системи з керованою діаграмою спрямованості може бути використана кільцева антенна решітка.

Однак, для одержання посилення кільцевою антенною решіткою необхідно збільшувати число елементів, що у зв'язку з ваго-габаритними обмеженнями неприйнятно для мультикоптерних дронів з електроприводом.

Третій спосіб передбачає використання декількох антен, що перемикаються, тоді просторові напрямки по азимуту розбиваються на сектори.

Для його реалізації пропонується розмістити на борту дрона шість антен типу «хвильовий канал». З урахуванням ваго-габаритних обмежень конструкція однієї антени буде складатися лише із трьох елементів. Габаритні показники можна визначити використовуючи рис. 1.

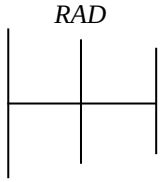


Рис. 1. Типова трьохелементна антена типу «хвильовий канал».

Для обраного частотного діапазону $\lambda = 0{,}125$ м, тому одна антена має габарити приблизно 7х7 см, конструкція із шести антен вписується в окружність радіусом $R_6 = 2l + l\sin 60 \approx 2{,}87l \approx 9$ см, а її вага складе близько 120 грам. Коефіцієнт підсилення трьохелементної антени типу «хвильовий канал» – 5,5 дб .

Таким чином, при використанні запропонованого варіанта побудови антенної системи для дронів загальне посилення приймально-передавального тракту може досягти 55 дб, що забезпечить на віддаленні 10 км ВСШ на вході приймача 22 дб, а відповідно – можливість реалізації складних алгоритмів модуляції. Високе значення ВСШ також може забезпечити стійке управління дронами, навіть при впливі навмисних завад, коли за рахунок використання простих алгоритмів модуляції: BPSK, QPSK, забезпечується пропускна здатність, достатня для передачі сигналів управління.

ЛІТЕРАТУРА

1. Явіся В.С., Лисенко О.І. Спосіб підвищення якості каналу управління дронами // Чотирнадцята міжнародна науково-технічна конференція «Перспективи телекомунікацій». Матеріали конференції. – К.: КПІ ім. Ігоря Сікорського. – 2020. –С. 281-284. ISSN (print) 2663-502X, ISSN (online) 2664-3057. 13-17 квітня 2020 року.

2. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение, Изд. 2-е, испр.: Пер. с англ. / Б. Скляр. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

3. Лисенко О.І., Явіся В.С. Технічні засоби забезпечення стійкого управління дронами // V Міжнародна науково-практична конференція «Відкриті еволюціонуючі системи». Збірник праць. Таврійський національний університет імені В. І. Вернадського. – К: ФОП Маслаков, 2020. – С. 254-256.

4. Гончаренко И.А. Антенны КВ и УКВ. Часть 3. Простые КВ антенны. М.: РадиоСофт, 2015. – 288 с.

к.т.н. Ліщинська Х.І. (НАСВ)
к.ф.-м.н. Сеник А.П. (НУЛП)
Хобор О.Р. (НУЛП)
Северинeнко Д.Ю. (НУЛП)

ПРОГНОЗУВАННЯ МЕТЕОРОЛОГІЧНИХ РИЗИКІВ ЗМІНИ САМОПОЧУТТЯ ВІЙСЬКОВОСЛУЖБОВЦІВ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Багато людей при найменшій зміні погоди відчувають нездужання: спека, раптове похолодання чи шалена злива – будь-яка зміна в природі раптом перетворюється на справжнє випробування для здоров'я. Так організм дає зрозуміти, що людина є метеозалежна. Відомо, що природні фактори відчутно впливають на самопочуття людини. Атмосферний тиск, температура повітря, вологість, геомагнітна обстановка або ж спалахи на сонці мають прямий вплив на виникнення найрізноманітніших неприємних симптомів. Таку реакцію організму на погодні зміни називають метеочутливістю особи.

Відповідно до інформаційних джерел, близько третини чоловіків і майже 50% жінок страждають підвищеною чутливістю до зміни погодних умов. Безпосередньо метеочутливість не загрожує будь-якими важкими наслідками. Проте погіршення самопочуття є серйозною проблемою для дорослої людини, коли під час зміни погоди особа не може зосередитися на роботі, не здатна належним чином виконувати складні завдання і приймати відповідальні рішення.

Для військовослужбовців, більшість з яких є практично здоровими молодими людьми, відповідно до інформаційних джерел, найбільш біотропним, тобто таким, що має найбільший вплив на організм, фактором є атмосферна температура. Причому, всупереч поширеним уявленням, не різкі її стрибки, а плавні зміни з періодом в декілька днів – приблизно стільки кожна місцевість зазвичай перебуває під впливом циклону або антициклону. І слідом за цими хвилями зміни температури змінюється і середній рівень артеріального тиску, особливо систолічного. Наприклад, похолодання взимку від +5 до -15 градусів може проявитися як зміна середнього рівня систолічного артеріального тиску від 105 до 120 мм рт.ст., тобто на 15 одиниць. І, швидше за все, це позначиться на самопочутті і працездатності людини, яка звикла до своїх 105 мм рт.ст. Зауважимо, що, якщо особа з такими скаргами прийде до лікаря, він в результаті огляду, швидше за все, скаже, що показники залишаються в межах загальнолюдської фізіологічної норми.

На підставі наведеного вище актуальним є створення інформаційної веб-орієнтованої платформи для прогнозування метеорологічних змін і відповідних ризиків погіршення самопочуття особи. Така інформаційна веб-орієнтована платформа допоможе людям з метеозалежністю бути готовими до будь-яких метеорологічних аномалій. Це, в свою чергу, сприятиме певній захищеності, оскільки особа буде знати, наприклад, що очікується відхилення від норми атмосферної температури чи атмосферного тиску, вона підготується до певного типу загроз.

В мережі Інтернет наявні і доволі активно використовуються сервіси Dark Sky Forecast, Open Weather API, ApiMedic, які пропонують розширений метеопрогноз та належну медичну діагностику симптоматики окремих осіб.

В роботі наведена структура та алгоритм дії інформаційної веб-орієнтованої платформи, яка може бути застосована для передбачення та відстеження метеозалежних ризиків. Використовуючи мову програмування Python, інтегроване середовище розробки PyCharm by JetBrains, фреймворк Django, створено інформаційну веб-орієнтовану платформу для прогнозування та попередження метеорологічних ризиків. В результаті виконання роботи, розроблено, у вигляді веб-орієнтованого додатку, інформаційну платформу для передбачення та застереження метеорологічних ризиків зміни самопочуття.

к.т.н., Любарський С.В. (ВІТІім. Героїв Крут)
Михайлов В.Р. (ВІТІім. Героїв Крут)

МАТЕМАТИЧНА МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОЗРОБЦІ ІНФОРМАЦІЙНИХ СИСТЕМ НА ПЛАТФОРМАХ MERN, DJANGO-FLASK СТЕКІВ

Актуальність дослідження обумовлена необхідністю вдосконалення системи захисту інформації офіційного вебпорталу Збройних сил України та покращити підхід до оцінки поняття захищеності інформаційної системи.Інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів власників інформаційних систем.В основному це пов'язано зі стрімким розвитком сучасних інформаційно-телекомунікаційних технологій, зв'язку та інформатизації, тому данеінформаційне поле має все більший вплив на наше суспільне життя.Зі збільшенням кількості користувачів інформаційних систем світова спільнота отримала не лише оптимізацію своєї діяльності, а й цілу низку проблем , зумовлених збільшенням вразливості інформаційної сфери, щодо стороннього кібервпливу. Тому закономірним є моніторинг та контроль з подальше регулювання відповідних відносин, шляхом негайного створення надійної системи кібернетичної безпеки.

Мета дослідження полягає у підвищення ефективності механізмів визначення необхідних засобів та методів, які потрібно використатипри забезпеченні інформаційної безпеки інформаційної платформи.Це дозволить зменшитинеобхідні ресурси при реалізації даної системи безпеки зі збереження швидкодії, шляхом виконання**наступних часткових завдань дослідження**: аналіз особливостей застосування систем захисту інформації, як невід’ємної складової інформаційної системи; аналіз сучасних наукових підходів у застосуванні систем захисту інформаціїна основі використання програмно-технічного, технологічного та мережевого методівдля виконання задач підвищення ефективності механізмів забезпечення інформаційної безпеки при розробці інформаційних систем на платформах MERN та Django/Flaskстеків; вдосконалення існуючої моделі, з урахуванням її недоліків та обмежень; автоматизація процесів захисту інформаціїза рахунок розробки програмного модулюаналізу вразливостей ІСз використанням комплексних методів розвитку та моделювання.

Виклад основного матеріалу.Існуючий метод дослідження зв'язків використовується як звичайний метод аналізу рівня інформаційної безпеки. Ці методи розкривають причинно-наслідковий зв’язок між загрозами та небезпеками, шукають причини, які стають першопричинами та спричинили актуалізацію тих чи інших чинників небезпеки, та формулюють заходи щодо їх усунення. Такими методами причинності є: метод подібності, метод відмінності, метод комбінації подібності та відмінності, метод супутніх змін і метод залишків.Основну увагу слід звернути на метод супроводжувальних змін, оскільки він дозволяє порівнювати залежність змін супутніх обставин, можна виділити обставину, що спричинило дане явище. Спираючись на роботи таких науковців, як Петрова та ЮєранаЧжо та всесвітньої організації OWASP ,що досліджували сферу оптимізації виявлення вразливостей інформаційної системи можна виділити, такі невиключні атрибути інформаційної безпеки: цілісність, конфіденційність та достовірність. Ці основні параметри накладають певні обмеження на роботу системи захисту інформаційної системи. Серед таких обмежень є продуктивність, обмеження доступу до інформації відповідно до наданих прав користувача та швидкість виявленнявразливостей.Для подолання даних обмежень пропонується розробка математичної моделі виявленнявразливостей системи захисту інформаційної системи з подальшою реалізацією програмного модулю виявлення вразливостей.**Висновки.** Отже, в роботі запропоновано використання методівсупутніх змін та комплексного для створення математичної моделі забезпечення інформаційної безпеки на основі, якої буде спроектовано архітектуру програмного модулю виявлення вразливостей, які виникають під час розробки на платформах Django/Flask та MERNстеків.

к.т.н. Любарський С.В. (ВІТІ)
Михайлов М.Р. (ВІТІ)

ПІДВИЩЕННЯ ШВИДКОСТІ ВЗАЄМОДІЇ З ОГЛЯДАЧАМИ МОБІЛЬНИХ ПЛАТФОРМ САЙТУ ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність дослідження обумовлена необхідністю вдосконалення системи інтерактивної взаємодії з сайтом Збройних Сил України клієнтами мобільних платформ.

Серед широкого спектру вимог до сучасних веб-орієнтованих it-рішень важливим фактором виступає швидкість отримання інформації з додатку і зручність подання цієї інформації для задоволення інформаційних потреб користувачів. Сайт Збройних Сил України, що представлений веб-ресурсом на домені *http://www.zsu.gov.ua*,не є виключенням.

Аналіз алгоритмів впливу на швидкість отримання даних з веб-ресурсів та організації ефективного прикладного інтерфейсу свідчить про актуальність цієї задачі, особливо в контексті проектування профілю користувача сайту на основі мобільної платформи.

Мета дослідження полягає у підвищення швидкості взаємодії з користувачами мобільних платформ сайту Збройних Сил України, за рахунок вдосконалення його архітектурної будови і буде вимагати виконання **наступних часткових завдань дослідження**:

– аналізу особливостей реалізації мобільних додатків;

– аналізу сучасних інструментальних бібліотек для крос-платформної реалізації програмних додатків;

– вдосконалення алгоритмів підвищення ефективності подання інформації для користувачів мобільної платформи за рахунок підвищення інтерактивності прикладних інтерфесів it-рішення.

Виклад основного матеріалу. Аналіз результатів тестування існуючої системи щодо висвітлення перед суспільством напрямів діяльність Збройних Сил України користувачами мобільних платформ виявив суттєві обмеження у швидкості завантаження переглядаємого інформаційного контенту в веб-оглядачі (очікування перевищувало інтервали часу у 2 хвилини, що є неприпустимим в умовах, коли пропускна здатність каналу зв’язку є достатньо високошвидкісною).

Вирішення задачі подолання обмежень у швидкості завантаження інформаційного контенту сайту Збройних Сил України лежить в підході опрацювання архітектурної будови платформи сайту і у виборі раціонального варіанту засобів розробки, що будуть враховувати особливості реалізації програмної логіки мобільних клієнтів. В аналіз таких засобів розробки потрапили наступні бібліотеки створення мобільних застосунків:

– Flutter–комплект засобів розробки та фреймворк з відкритим вихідним кодом для створення мобільних додатків під Androidта iOS, а також веб-додатків з використанням мови програмування Dart, розроблений та розвивається корпорацією Google;

– React Native–це крос-платформний фреймворк з відкритим вихідним кодом для розробки нативних мобільних та настільних додатків на Java Scriptта Type Script, створений FacebookInc. React Native підтримує такі платформи як Android, iOS, дозволяючи розробникам використовувати можливості бібліотеки Reactпоза браузером для створення нативних програм, що мають повний доступ до системних API-платформ;

– Xamarin–це фреймворк для крос-платформної розробки мобільних програм з використанням мови C#. В розробці можна застосовувати LINQ, лямбда-вирази, Generic та Async. При цьому надається повний доступ до всіх можливостей SDK-платформи та рідного механізму створення UI.

Висновки. Перевага у виборі раціонального варіанту засобів розробки віддається бібліотеці Fluttерчерез її продуктивність, високий рівень взаємодії з нативною частиною пристрою, а також її продуктивність в порівнянні з іншими бібліотеками. Для даного застосунку вже написано публічну API для отримання даних з сайту Збройних Сил України.

к.т.н. Любарський С.В. (ВІТІ)
Уставицький Р.А.(ВІТІ)

РЕАЛІЗАЦІЯ МОДУЛЮ ПОШУКУ КОНТЕНТНО-ЗАЛЕЖНОЇ ІНФОРМАЦІЇ В WEB-ОРІЄНТОВАНОМУ ПОРТАЛІ MOODLE

Актуальністьрозробкиобумовленавідсутністю пошукового модулю для web-орієнтованого інформаційного порталуmoodle.

Web-орієнтований інформаційний портал moodlestворено для підвищення ефективності навчання, покращення умов навчання та підвищення рівню організації навчальних занять навчальних закладів. Система має відкитий код, що дозволяє вносити зміни в її роботу. Але одним з обмежень системи є відсутність модулю пошуку контекстно-залежної інформації в величезних обсягах навчальної інформації, що налічує система.

Мета дослідження полягає у підвищення ефективності в організації проведення навчальних занять та самостійної підготовкиза рахунок надання ефективних важелів у оперативному пошуку навчального матеріалу в насичених сховищах системи. Виконання цієї задачі передбачає реалізацію **наступних часткових завданьдослідження**:

– аналіз вимог до сучасних інформаційно-пошукових систем;

– аналіз архітектурної будови сучасних інформаційно-пошукових систем та вибір раціонального варіанту реалізації для модульної структури moodle;

– оцінка адекватності обраної моделі інформаціно-пошукового механізму на основі результатів тестування програмної реалізації.

Виклад основного матеріалу.Використання інформаційно-пошукових систем значно полегшує та підвищує ефективність пошуку матеріалу та інформації в Інтернеті. Пошукові модулі інтегруються, яку потужні internet-платформи(Google), так і в різнобічні вузько спеціалізовані it-рішення (портали новин, освітньої діяльності, портали ведення комерційної діяльності тощо).

Архітектурнабудова інформаційно-пошукових систем передбачає:

– клієнт-серверний принцип будови;

– наявність механізму індексації веб-орієнтованого контентусторінок;

– механізм каталогізації проіндексованих сторінок;

– механізмотримання інформаційного запиту від кінцевих користувачів, пошук контекстно-залежної інформації в каталогізованих архівах і формування релевантних результатів пошуку.

В роботі Сухого О.Л. визначено основні вимоги до інформаційно-пошукових систем, що безперечно повинно бути забезпечено за результатами проектування:

– повнота –представляє собою відношеннякількостізнайденихдокументів до загального числа документів в базіданих, яківідповідаютьданомузапиту;

– наочність –ступіньвідповідностізнайденихдокументівзапитукористувача;

– швидкістьпошуку, щотіснопов’язана з йогостійкістю до навантажень.

Проектна робота за напрямком дослідження буде передбачативизначення залежності між повнотою та точністю пошуку в moodle-системі.Підвищення точності веде до підвищення шуму і, навпаки, при зменшенні шуму знижується точність виданих результатів.

Всі існуючі системи та продукти мають відповідати певним стандартам, що визначається результатами тестувань як машинами так і людьми. Пошукові системи не виняток, тож до них застосовують методи тестування такі як: тестування продуктивності; навантажувальне тестування; тестування стабільності.

Висновки.Раціональний варіант архітектури інформаційно-пошукового модулю навчальної системи moodleповиненвідповідати зрізу вимог до подібного класу систем і забезпечувати належний рівень повноти та точності контекстно-залежних даних.

Ляшенко В.Р. (ВІТІ ім.Героїв Крут)
Османов Р.Н. (ВІТІ ім.Героїв Крут)

АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЗАВАДОЗАХИЩЕНОСТІ РАДІОРЕЛЕЙНИХ ІНТЕРВАЛІВ У ТАКТИЧНІЙ ЛАНЦІ УПРАВЛІННЯ

Актуальність теми: В сучасних світі невід'ємною складовою операції і бою є радіорелейний зв'язок. Створення особистої мережі для збройних сил України дає змогу незалежно працювати в мережі і не орендувати канали у приватних чи державних компаній за кошти держави. Дає змогу незалежно використовувати мережу за службовим призначенням.

Хоча радіорелейний зв'язок зазвичай відносять до резервного зв'язку за певних факторів, який ми розглянемо в цій роботи. Але він відіграє велику ролі в організації і ведення управляння військами. Тому завадозахищеність є одним із основних вимог до організації військового зв'язку. Так радіорелейні апаратні розміщують в тилах і вони не такий захищений від радіоелектронної боротьби противника, як наприклад радіозв'язок, але радіорелейний зв'язок є надійним, бо працює інтервально з мінімальним випроміненням в різні сторони.

Мета:Захист сигналу від завад противника є одним із основних аспектів для забезпечення якісного зв'язку. В радіорелейному зв'язку це може досягатися не потраплянням під дію наших антен, завади противника і правильно підібраний рельєф місцевості для уникнення потрапляння шумів від противника та не перешкоджаючи нам встановлювати якісний зв'язок з іншою станцією.

Способи розташування радіорелейних станцій на місцевості є ключовим в побудові радіорелейних інтервалів. Завдяки правильному розташуванню забезпечується якісний сигнал і дезорієнтування противника для уникнення на нас завад які противник може завдати.

Викладення основного матеріалу: Проблематика захисту сигналу від будь яких завад які впливають на антену і радіорелейний інтервал. Зокрема від апаратури радіоподавлення противника. Бо з природними завадами ми можемо впоратися наприклад: встановити антену в інше місце, або підвищіти потужність сигналу, а ось якщо противник буду в пливати на наш сигнал і виявить нас, то особовому складу загрожує небезпека з позицій противника.

Найкращій спосіб завадозахищеності радіорелейних інтервалів це сховати антену від позицій ворога. Щоб противнику не вдалося діяти на наш сигнал. Радіорелейну лінію розміщаємо глибоко в тилу. Інтервал прив'язки які дають ресурс до лінії розмежування розташовуємо кінцеву антену до 1000-600 метрів А зв'язок до лінії розмежування розгортаємо за допомогою польових кабельних ліній.

Також в цифрових радіорелейних станціях, які зараз знаходяться на озброєні в Збройних силах України застосовується технологія MIMO (MultipleInputMultipleOutput), яка дозволяє передавати інформацію в різних поляризаціях (вертикальній і горизонтальній) наприклад в радіорелейній станції Р-425С3 є режими роботи 1+1. При цьому режимі станція працює на два передавачі, на різних частотах і має різну площину поширення хвиль.

Висновок: Отже, радіорелейних зв'язок дуже вразливий до завад і подавити корисних сигнал просто. Але за допомогою правильно підібраної місцевості і правильних налаштувань ми можемо протидіяти і захистити сигнал.

По-перше за допомогою правильно підібраної місцевості. Щоб рельєф місцевості нам був сприятливий та не заважав і захищав від противника.

По-друге працювати в двох поляризаціях с передачею і прийомом на різних частотах.

Ляшенко Г. Т.
Черниш Ю.О.
Шемендюк О.В.

РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Вступ

Сучасний стан розвитку інформаційного суспільства вимагає захисту інформаційних ресурсів та критичних даних на найвищому рівні. Безпрецедентні вимоги до програмно-апаратних засобів, технологій організації сучасних інфраструктур, тощо характеризуються різким зростанням попиту державних та суспільних відносин в використанні системи надання надійних і якісних ІТ послуг (послуг інформаційних технологій) різних класів.

Захист від цілеспрямованих атак невизначеного класу залишається одним із найбільш актуальних питань у сфері інформаційної безпеки. Протягом останнього року кількість кібератак в Україні збільшилася в десять разів. Майже кожен знайомий з такими виразами: «таргетована (цільова) атака», «вразливість нульового дня», «0-day» або навіть Advanced Persistant Threats (ATP). Дані теми можна сміливо назвати головним трендом в сфері інформаційної безпеки. Добре відомі атаки з шифруванням є одним з підвидів перерахованих загроз. «Пісочниці» (SandBox) – це єдині засоби, які дозволяють боротися з вище згаданими загрозами. Такі засоби захисту проводять динамічний і статистичний аналіз файлів у віртуальному середовищі і блокують різноманітні атаки при необхідності.

Це дозволяє оцінити поведінку підозрілих файлів і наслідки запуску таких файлів. При цьому головна мета не на виявлення шкідливого коду за допомогою сигнатур, а на оцінку дій, які виконуються кодом, безпеку і коректність в даному середовищі. Атаки нульового дня є серйозною загрозою безпеки інфраструктури практично кожної організації. Традиційний набір засобів захисту інформації не здатний протистояти не визначеним класам загроз. Технологія «пісочниця» є найефективнішим механізмом виявлення загроз нульового дня.

Метою дослідження створення математичної моделі захисту інформаційної системи спеціального призначення від атак «0 дня», що буде використовувати ймовірнісні ранжування станів даної системи в умовах невизначеності. Тобто апріорі невідомо, що саме є деструктивним впливом на систему, тому необхідно використовувати процедури мережевої пісочниці.

Виклад основного матеріалу дослідження

Щоб виявити і запобігти реалізації найвитонченіших або, що ще складніше, раніше невідомих атак на периметрі, потрібні сучасні методи безпеки. Такі методи реалізовані компанією Check Point. Check Point SandBlast Zero-Day Protection – технологія, яка являє собою сукупність двох ключових компонентів: SandBlast Threat Emulation – компонент, який є новим видом організації «пісочниці» від Check Point (Check Point Sandbox).

Новизна полягає в тому, що виявлення атак здійснюється на двох рівнях архітектури: рівні операційної системи (OS level) – як і у традиційних «пісочниць», і на рівні центрального процесора (CPU level); SandBlast Threat Extraction – компонент, що дозволяє проаналізувати файли, які передаються по мережі, видалити з них весь небезпечний вміст, реконструювати файли і надати ці файли користувачеві вже чистими.

Враховуючи характерні відмінності атак «0 дня», а також з метою синтезу нового методу виявлення загроз цього класу на тлі мережевої пісочниці, необхідно сформувати математичну модель методу на базі багатоальтернативного підходу до кількості можливих типів атак. Зазначений підхід характеризується тим що сторона, яка є ціллю атаки, не має апріорних даних про тип, параметри та час здійснення атаки на критичні дані власника інформаційних ресурсів. Таким чином, загальний підхід до моделювання загрози на інформаційні ресурси будемо розглядати в контексті побудованої моделі аналітичного ряду. При цьому слід враховувати дискретні стани та безперервний час імовірнісного ранжування вхідних потоків з метою розрахунку необхідних параметрів та характеристик функції впливу

(загрози). З метою коректності та спрощення аналітичного представлення, використаємо функціональний ряд з врахуванням динамічної послідовності випадкових станів (потік подій), що виникають у системі з урахуванням вразливостей інформаційних ресурсів. Враховуючи особливості класу атак «нульового дня», оберемо експонентний розподіл часу нагнітання частоти загроз процедури здійснення атаки через вразливості системи.

Оскільки моделюється серія загроз, в формуванні аналітичної моделі доцільно враховувати послідовність вразливостей інформаційної системи (або ресурсів), які використовуються порушником. Відмінність проблематики формування моделі для атак «нульового дня» полягає в тому, що в аналітичній моделі ряду не буде враховуватись кореляційний взаємозв'язок між загрозою та відповідною вразливістю. У відповідності до визначених досліджень, введемо обґрунтоване припущення, що інцидент створюється двома класами відповідних параметрів несанкціонованого впливу на інформаційну систему. Ці параметри наступні: за інтенсивністю впливу загроз різного класу за часом, а також на основі помилок реалізації програмних засобів при виявленні інцидентів й усуненні уразливостей.Згідно визначеного підходу можна сформувати аналітичну модель системної функції визначення процедури виявлення інцидентів будь-якої складності.

В дослідженнях визначено, що для адекватності представленої моделі існують базові реалістичні обмеження, що стосуються розглянутої проблеми моделювання загрози атаки «0 дня», а саме:

- модель системи з дискретними станами і безперервним часом коректна в загальному випадку, якщо з кожного стану системи при випадковому процесі не санкціонованих впливів, виходять всі N вхідних потоків подій з інтенсивністю Q_i, $i=1,\ldots, N$.

- у загальному випадку для моделювання станів системи при загрозах атак «0 дня» повинно використовуватися розрахунки на базі моделі ряду з нескінченним числом дискретних станами і безперервним часом.

В рамках визначених обмеженьтака модель підлягає обчисленню та застосовується для математичного моделювання інформаційних систем. Запропонована модель характеризується можливістю одночасного виникнення в системі двох і більше несанкціонованих зовнішніх впливів. Модель ймовірнісного ранжування станів системи застосована для математичного моделювання атак «0 дня» з врахуванням інтенсивності потоків впливу. Оскільки при моделюванні використовується достатня кількість можливих наборів атак або потоків впливу, можна обґрунтовано використати нормальний закон розподілу випадкових подій впливів на систему. Враховуючи характеристики атак «0 дня», необхідно врахувати ймовірність виникнення в системі одночасно кількох несанкціонованих подій. Тобто, одночасний вплив кількох подій на вразливості одного типу на фіксованому інтервалі часу. Запропонований підхід до моделювання інформаційної системи з урахуванням впливу атак типу «0 дня» дозволяє об'єктивно оцінити базові параметри і характеристики загрози.

Висновки

1. Розроблено аналітичну модель, що враховує різні стани системи, ймовірність переходу між цими станами, та їх частоту. Це дозволяє виявляти підозрілу та потенційно небезпечну активність, навіть якщо раніше загрози подібного виду ніколи не спостерігались.

2. Створення математичного опису процедури виявлення загроз дозволяє адаптувати систему до різних вимог, не змінюючи її ядро. Завдяки цьому запропонована модель є досить універсальною, але в той же час дозволяє проводити досить глибокий аналіз активності в реальному часі. При цьому використовувались деякі підходи штучного інтелекту, але без використання конкретних методологій.

3. Зазначену модель доцільно використовувати в системах захисту інформації в інформаційних системах спеціального призначення з метою ідентифікації атак нульового дня. Напрямками подальших досліджень слід вважати розробку удосконалених процедур виявлення загроз з меншою обчислювальною складністю, для можливості здійснення аналізу загроз в режимі реального часу.

Макаренко О.О. (ВІТІ)
Петрова Д.В.(ВІТІ)

ПЕРЕСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ "БЛОКЧЕЙН" У СФЕРІ ОБОРОНИ

В даний час блокчейн та інші технології розподілення привертають увагу дослідників через їх потенційну можливість застосування поза межами фінансової сфери, де вони виникли. Блокчейн є, по суті, децентралізованою одноранговою (peer-to-peer – P2P) мережею транзакцій без потреби підтверджень центрального органу або посередника. Комп'ютери в мережі ("вузли") використовують криптографічні алгоритми та смарт-контракти для підтвердження транзакцій, які потім записуються в "блоки". "Ланцюги" таких блоків утворюють журнал транзакцій, який згодом може сформувати узагальнену книгу. Коли відбуваються транзакції, записи про власність (активи та їхні значення) постійно реєструються в бухгалтерських книгах. Це робить корумпованість книги надзвичайно складною, надаючи цій технології високий рівень "незмінності", що також робить її сильною альтернативою традиційним централізованим базам даних. Теоретично немає потреби в підтвердженні транзакції з боку уповноваженого централізованого посередника, а отже й немає потреби в центральній базі даних або сховищі операцій і записів. Цей механізм призводить до децентралізованої/розподіленої бази даних бухгалтерських книг із показником операцій, який постійно зростає. Основні характеристики технології блокчейн показані на рис. 1

Ключові особливості блокчейну	Недоліки блокчейну
Відсутність центру. Рівноправність і розгалуженість системи робить її злам і пошкодження практично неможливими. Кожен окремий учасник є незалежним сервером	Кожна операція безповоротна, тому якщо транзакція пройшла навіть помилково, змінити і повернути її неможливо
Відкритість. Відомості про операції, укладені угоди і контракти зберігаються у вільному доступі. Проте змінити їх неможливо – тільки переглянути. Дані про учасників – закриті! Кожен користувач блокчейну має унікальний ключ (комплект криптографічних записів, що упереджує можливість підміни інформації та ризик хакерської атаки), який служить гарантією надійності системи	«Атака 51%» – якщо більше половини потужностей будуть належати одному пристрою, цілісність ланцюга порушується
Необмеженість ланцюга блоків. Теоретично ланцюг може доповнюватися безкінечно, що стимулює аналогії блокчейну із суперкомп'ютером	Відсутність законодавчого регулювання роботи блокчейну. Немає встановлених стандартів та рівнів відповідності. Доки технологія не досягне певних рамок, це буде істотно обмежувати її впровадження. Як тільки проясняться правила гри і будуть вироблені законодавчі норми, в індустрію почне заходити крупний капітал, стане простіше виконувати операції з конвертації криптовалюти у фіатні гроші, ринок зблизиться з класичним ринком цінних паперів
Ефективність і надійність. Ланцюг записує тільки транзакції, що пройшли перевірку, і гарантує захист від збоїв та підміни хешу (функція запису операції, шифратор)	Блокчейн передбачає застосування потужної обчислювальної техніки, що збільшує витрати на переобладнання і відсікає значну кількість потенційних користувачів

В результаті блокчейнові мережі не тільки зменшують ймовірність загрози з боку атаки противника, але суттєво збільшують витрати супротивника на її створення.

Новий підхід, який створює блокчейн, може призвести до нових знахідок, придатних для застосування у оборонній галузі. Зокрема, в таких напрямках як інформаційна безпека,

автентифікація, цілісність та стійкість даних та інших. Технологія блокчейн має чотири основні характеристики: перша - децентралізація. Технологія блокчейн використовує розподілений облік і зберігання, не покладається на сторонні управляючі організації і відсутній централізований контроль. Будь-який учасник блокчейна є вузлом, і кожен вузол має рівні права. Другий – відкритість. В основі технології блокчейн лежить відкритий вихідний код, за винятком того, що особиста інформація сторін транзакції зашифрована, дані блокчейна відкриті для всіх, а вся системна інформація прозора. Третій – автоматизація. Блокчейн заснований на узгоджених специфікаціях та протоколах, і вся система може автоматично та безпечно перевіряти та обмінюватись даними, не покладаючись на третю сторону. Четверта – анонімність. Оскільки всі вузли можуть працювати автоматично в «ненадійному» середовищі, ідентифікаційна інформація кожного блокового вузла не потребує розкриття чи перевірки, і цю інформацію можна передавати анонімно. У військовій сфері децентралізація, масштабованість, міжмережевий розподіл та надійне шифрування блокчейна можуть ефективно підвищити безпеку та живучість бойових мереж, а також значно підвищити гнучкість та відмовостійкість бойових систем. З постійним оновленням методів мережевих атак, проблеми, що стоять перед безпекою мережі, збільшуються з кожним роком. Провідні хакери незаконно вторгаються в мережеві інформаційні системи, очищають журнали дозволів і іноді приховують сліди незаконного доступу до пристроїв. Блокчейн може постійно записувати динаміку бази даних, конфігурація кожного компонента у системі може бути записана, а захист постійно відстежується у базі даних. Будь-які незаконні зміни конфігурації можуть бути практично негайно виявлені системою, що може ефективно запобігти вторгненню хакерів, а мережеві журнали можуть бути розподілені між кількома пристроями, щоб мінімізувати ризик атаки. Мережа з кількома вузлами блокчейна працює через механізм консенсусу, і кожен вузол зберігає всі дані в ланцюжку блоків. Навіть якщо хакери атакують один вузол, це не вплине на роботу системи блокчейн вцілому. Очікується, що блокчейн здійснить перетворення механізму довіри від особистої довіри та інституційної довіри до машинної довіри, що має велике значення для реалізації нової моделі управління та контролю «людина-машина / машина-машина», яка відповідає операціям із застосуванням безпілотних комплексів. Безпілотний рій є технологією блокчейн, і з його механізмом консенсусу він може ефективно запобігати зловмисним вузлам від імітації або обманних мережевих атак, підтримувати надійне з'єднання та забезпечувати стабільність та ефективність операцій безпілотного рою.

У галузі військового управління механізм машинної довіри блокчейна може зменшити невизначеність та складність, спричинені людськими факторами у процесі військового управління. Наприклад, в галузі управління обладнанням на основі блокчейну для побудови повноцінної системи управління інформацією за участю розробників, виробників та користувачів, а також взаємного контролю, відстеження всього процесу управління, проектуванням обладнання, дані випробувань, стан бойової техніки та записи про технічне обслуговування та іншу інформацію для підвищення ефективності та результативності управління обладнанням. У галузі логістичної підтримки використання технології блокчейн для управління важливими даними військової логістики, такими як потреби користувачів, складування товарів, навантаження та транспортування, а також розподіл та транзит. В галузі людських ресурсів зберігання історії служби військовослужбовців, звітів про нагороди та покарання та іншу інформацію у формі блокчейну може ефективно запобігти втраті архівної інформації та штучному втручанню. Враховуючи її високий потенціал, технологія блокчейн є перспективною темою для досліджень. Впровадження технології блокчейн у військову сферу певною мірою змінить майбутні моделі ведення бойових дій і навіть вплине на результат війн. В даний час застосування технології блокчейн у військовій галузі все ще знаходиться на стадії дослідження, і великі проекти ще не реалізовані. Однак, як тільки технологія блокчейн буде успішно застосована у військовій галузі, вона перевершить традиційну систему військового управління та викличе революційні зміни у військовому будівництві та методах ведення бою.

к.т.н. Макарчук О. М. (ВІТІ ім.Героїв Крут)

КОМБІНОВАНИЙ МЕТОД ПОШУКУ ЕКСТРЕМУМУ МУЛЬТИМОДАЛЬНИХ ФУНКЦІЙ

Актуальність. При розв'язанні багатьох задач необхідно знайти екстремум функції, яка залежить від декількох параметрів. Якщо функція одномодальна (тобто у неї один екстремум) і має часткові похідні, то розв'язок можна одержати за допомогою методу градієнтного спуску. Перевагою методу є наявність добре розробленого математичного апарату, хороша сходимість і швидкодія. Але для мультимодальних функцій з декількома локальними екстремумами цей метод дозволяє знайти тільки певний локальний екстремум, який в загальному випадку може бути далекий від глобального.

Зараз немає методу, який би гарантував знаходження глобального екстремуму для мультимодальних функцій. Однак існує ряд методів, які дозволяють отримати кращі наближені розв'язки, ніж градієнтні методи. Серед них широкого поширення набули стохастичні методи (випадковий пошук, метод пчіл, метод рою частинок). Стохастичні методи за рахунок розширення області пошуку можуть знайти декілька локальних екстремумів, з яких вибирається кращий. Однак вони також не гарантують досягнення глобального екстремуму. Крім того, ці методи мають повільну сходимість в області екстремуму і тому працюють повільніше, ніж градієнтні.

Постановка задачі. В зв'язку з вищевказаним виникає ідея об'єднати переваги стохастичного і градієнтного методів шляхом їх комбінації. Комбінований метод проводить пошук екстремуму в два етапи:

- на першому етапі стохастичний метод формує множину околиць точок-кандидатів на можливі точки екстремуму;
- на другому етапі градієнтний метод досліджує околиці точок-кандидатів на екстремум і вибирає з них оптимальну.

Основні положення. Для оцінки ефективності комбінованого методу проведена серія порівняльних експериментів з градієнтним методом найшвидшого спуску і стохастичним методом рою частинок для знаходження екстремуму мультимодальних функцій. В якості тестових функцій використовувались відомі функції Химмельблау і Стибінського-Танга. Ці функції часто використовуються для оцінки ефективності методів пошуку екстремуму мультимодальних функцій.

Функція Химмельблау двох змінних має один глобальний максимум і чотири локальні мінімуми. В експериментах на пошук мінімуму градієнтний метод найшвидшого спуску виявився кращим в 22% експериментів, метод рою частинок – в 33% і комбінований метод – в 45%.

Функція Стибінського-Танга має один глобальний мінімум і декілька локальних мінімумів. Для цієї функції можна змінювати кількість вхідних параметрів. З ростом числа параметрів збільшується і кількість локальних мінімумів. Це призводить до зниження ефективності при пошуку глобального мінімуму всіх методів, а особливо градієнтного. Для 4-х вхідних параметрів градієнтний метод знайшов глобальний мінімум в 43% експериментів, метод рою частинок – в 68% і комбінований метод – в 82%. Для 8-ми вхідних параметрів відповідні цифри 23%. 51% і 63%.

Швидкодія всіх методів залежить від розмірності цільової функції, а методу рою частинок і від розміру рою. За швидкодією, як і очікувалось, градієнтний метод в 5-50 разів переважає метод рою частинок. Комбінований метод займає проміжне становище.

Висновки. Результати проведених експериментів показали, що комбіноване використання стохастичного методу рою частинок і градієнтного методу найшвидшого спуску дозволяє знайти більш ефективні наближені значення екстремумів мультимодальних функцій, ніж використання кожного з цих методів окремо.

Мартиненко А.Г. (ВІТІ)
Лукашенко Є.О.(ВІТІ)

АНАЛІЗ ЗАСТОСУВАННЯ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність. Для ефективної обробки інформації, проведення і планування операцій з використанням інформаційних систем ЗСУ.

Мета. Проаналізувати можливості обробки інформації з використанням ГІС в інформаційних системах ЗСУ.

Основні положення. Інтенсивне впровадження інформаційних технологій у ЗСУ надає нові можливості зі збору, обробки, аналізу, графічної візуалізації та зберігання просторових даних і пов'язаної з ними інформації про місцевість і конкретні об'єкти, розташовані на цій місцевості. Для можливості відображення, аналізу та обробки даних широко використовують ГІС системи.

Інформація, що включає просторову складову, становить значну частину всіх даних, з якими мають працювати при проведенні чи плануванні операцій. Тому сьогодні геоінформаційні системи вже давно вийшли за рамки поняття системи, що обробляє, власно, просторові дані. Сучасні ГІС дозволяють працювати не тільки з різними картами та атрибутами об'єктів на них, але і з різними типами документів (текстових, графічних, мультимедійних), пов'язаних з певними об'єктами, здійснювати складні запити до баз даних та перетворювати їх результати у карти, картограми чи діаграми, прив'язані до певних територій та багато інших операцій.

До задач, які вирішують геоінформаційні системи відноситься:

1. Обробка матеріалів польових вимірювань та спостережень, оформлення їх у вигляді карт та схем;
2. Зберігання картографічних даних різних типів;
3. Відображення окремих картографічних даних та різних комбінацій даних;
4. Підготовка карт різних типів до друку;
5. Пошук даних за їх положенням, атрибутами, розташуванням відносно заданого об'єкта чи групи об'єктів;
6. Аналіз місцезнаходження об'єктів, топологічних відношень, наявності та щільності розподілу об'єктів;
7. Аналіз атрибутів об'єктів карт, класифікація даних;
8. Аналіз та відображення змін даних у часі;
9. Робота з різними типи баз даних по пошуку та виборці інформації, пов'язаної з певною територією чи об'єктами, формування звітів;
10. Побудова графових структур, мережевий аналіз, вирішення транспортних задач;
11. Моделювання рельєфу, місцевості, розвитку певних подій на місцевості;
12. Оформлення результатів аналізу даних у вигляді різних типів карт, картограм, діаграм, мультиплікацій;
13. Вирішення задач проєктування об'єктів та територій;
14. Обмін даними з іншими ГІС та інформаційними системами.

Висновок. Одна з головних переваг застосування ГІС, при проведенні операції полягає у забезпеченні можливості відображення змін тактичної обстановки і характеристик елементів місцевості у реальному масштабі часу. Таким чином, дані системи можуть використовуватись для ефективної роботи з геопросторовими даними з мінімальними зусиллями для впровадження й підтримки з боку розробників та використання з боку кінцевих користувачів.

Мартинюк В.В. (ВІТІ)
Мальцева І.Р. (ВІТІ)
Бондаренко Т.В. (ВІТІ)

АНАЛІЗ ВИКОРИСТАННЯ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ У СУЧАСНИХ ОПЕРАЦІЯХ

Успіх у сучасних операціях і бойових діях в значній мірі визначається ефективним застосуванням усіх видів озброєння та військової техніки, що в свою чергу залежить від стійкої роботи систем управління військами та зброєю, технічну основу яких складають радіоелектронні системи.

Коло військових завдань, які вирішуються за допомогою радіоелектронних систем дуже широке:

ведення комплексної технічної розвідки;

підготовка інформації і рекомендацій для прийняття рішень командирами на ведення бойових дій;

передача даних, повідомлень, команд та сигналів управління військам;

забезпечення навігації (літаків, кораблів, танків та інших);

наведення (самонаведення) засобів ураження;

захисту військових об'єктів і військ від розвідки та засобів ураження, тощо.

Сучасний етап розвитку теорії і практики збройної боротьби характеризується: підвищенням ролі високоточної зброї, комплексною автоматизацією систем управління військами (силами) і зброєю, удосконаленням сил і засобів розвідки і радіоелектронної боротьби. Створюються передумови завоювання і утримання однією з воюючих сторін переваги в управлінні військами (силами) та зброєю. В сучасних операціях (бойових діях) дезорганізація управління, а тим більше втрата управління військами (силами) однією із сторін може мати для неї непередбачувані наслідки.

Все це обумовлює зростання ролі радіоелектронної боротьби, як одного з видів забезпечення у сучасній збройній боротьбі.

Еволюція засобів радіоелектронної боротьби (РЕБ) та стрімкий розвиток інформаційних і телекомунікаційних технологій обумовили зміни ролі радіоелектронної боротьби, розгляд її в якості складової частини інформаційного протиборства в технічній сфері. Але це не призвело до втрати радіоелектронною боротьбою своєї провідної ролі. Незважаючи на широке впровадження в системи військового управління телекомунікаційних і комп'ютерних систем, і в сучасних умовах основою систем управління зброєю є засоби радіолокації, а основою систем управління – засоби зв'язку. При цьому засоби радіоелектронної боротьби історично орієнтовані на порушення функціонування саме цих засобів. Досвід локальних конфліктів початку XXI століття показав, що саме РЕБ є основою дестабілізуючого впливу на підсистеми зв'язку систем військового управління противника.

Системи радіоелектронної боротьби вирішують завдання щодо подавлення радіолокаційних засобів проти повітряної оборони і прикриття бойових порядків авіації, дезорганізації всіх підсистем управління військами і зброєю противника в сучасних операціях. Від ефективності заходів з РЕБ, які починають проводитись напередодні і на початковому етапі операцій, безпосередньо залежить ефективність зниження бойового потенціалу противника.

Досвід локальних війн та збройних конфліктів останнього часу свідчать про неухильну залежність ходу та результату збройної боротьби в тому числі й від можливостей щодо дезорганізації управління військами та зброєю протиборчої сторони. Значний внесок при цьому вносять частини та підрозділи радіоелектронної боротьби. Радіоелектронна боротьба поступово набирає риси специфічної форми бойових дій, що має за мету досягнення переваги або недопущення переваги противника в інформаційній компоненті збройної боротьби, яка забезпечується радіоелектронними засобами (РЕЗ). В сучасних

умовах сили і засоби радіоелектронної боротьби залучаються до вирішення завдань усіх рівнів.

У збройних конфліктах останніх десятиріч інтенсивно розвивається теорія і практика РЕБ, випробовуються нові зразки техніки радіоелектронної боротьби. Задля досягнення переваги у всьому радіочастотному просторі вдосконалюються існуючі та досліджуються нові форми та способи застосування сил та засобів РЕБ. На заміну існуючим засобам та комплексам РЕБ приходять нові автоматизовані та багатофункціональні комплекси радіоелектронної боротьби.

Аналізуючи особливості ведення радіоелектронної боротьби у збройних конфліктах сучасності постають основні причини підвищення ролі РЕБ:

зростання ролі оперативного управління військами (силами) і зброєю в ході бойових дій;

зростання масштабів використання різних за призначенням РЕЗ;

здатність практично миттєво за допомогою засобів РЕБ дезорганізувати управління противника;

збільшення ролі засобів радіоелектронної боротьби у боротьбі із високоточною зброєю противника.

На розвиток РЕБ впливає велика кількість чинників, до основних з них належать:

масштаб завдань військ, до вирішення яких залучаються сили й засоби радіоелектронної боротьби;

склад і належність сил та засобів; масштаби маневру силами і засобами РЕБ у ході бойових дій;

просторовий розмах дій;

час реакції на зміну радіоелектронної обстановки;

масштаб стримування дій противника у ході ведення систематичних дій з РЕБ;

детальність розвідки сигналів і параметрів РЕЗ.

Результати аналізу бойових дій в Європі і на Близькому Сході, показують, що системи і засоби радіоелектронної боротьби повітряного базування залишаються одними з ключових елементів в досягненні переваги над супротивником і, як наслідок, в забезпеченні успіху інформаційних операцій, що проводяться.

Сучасний воєнний конфлікт є комплексним, його основними складовими є політична, воєнна, економічна, інформаційна і міжнародно-правова. Воєнно-стратегічною метою сучасного воєнного конфлікту є територіальний розподіл та формування нових більш залежних країн. Сценарії розвитку сучасних воєнних конфліктів мають багато схожих рис, їх імплементація і розвиток є керованим процесом. Воєнна сила не є вирішальною у сучасному воєнному конфлікті, мета досягається в першу чергу оптимальним поєднанням економічної, інформаційної і воєнної складових.

Таким чином, ефективність виконання бойових завдань частинами та підрозділами РЕБ у сучасних операціях і бойових діях за досвідом збройних сил країн членів НАТО забезпечує зниження бойового потенціалу противника шляхом дезорганізації систем управління військами противника. Так як системи управління військами постійно модернізуються та змінюються, має місце подальше дослідження у даній сфері для підвищення ефективності застосування сил та засобів радіоелектронної боротьби в операціях (бойових діях).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Порядок оперативного планування в органах військового управління НАТО : навч. посіб. / [А.М. Сиротенко, В.М. Тарасов, С.М. Салкуцан та ін.]. – К. : НУОУ імені Івана Черняховського, 2019. – 232 с.

2. Куртсеітов Т.Л., Салій О.Я. Особливості ведення радіоелектронної боротьби за досвідом війни на сході України /Т.Л. Куртсеітов, О.Я.Салій// Труди університету: збірник наукових праць. – К.: НУОУ ім. Івана Черняховського. – № 1 (146). – 2018. – С. 60-65.

к.т.н. Масесов М.О. (ВІТІ)
Новицький Д.В. (ВІТІ)
Шугалій О.О. (ВІТІ)
Пономаренко З.М. (ВІТІ)

ПЕРСПЕКТИВИ РОЗВИТКУ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Для резервування стаціонарних ліній зв'язку в тактичній, оперативній і стратегічній ланках управління використовуються засоби радіорелейного зв'язку, станції супутникового зв'язку та засоби тропосферного зв'язку.

За результатами аналізу досвіду організації та забезпечення зв'язку в ході виконання завдань в операції Об'єднаних сил та антитерористичній операції на сході України, використання застарілих засобів тропосферного зв'язку радянського парку виявилося неефективним. В той же час, забезпечення зв'язком службових осіб на пунктах управління у випадках виходу з ладу стаціонарної компоненти системи зв'язку Збройних Сил України залишається проблемним питанням.

Саме тому, на теперішній час залишається актуальним завдання забезпечення Збройних Сил України новітніми зразками тропосферного зв'язку. Основними перспективами розвитку зазначеного роду зв'язку є впровадження малогабаритних (в тому числі – переносних) станцій у тактичній ланці управління, мобільних радіорелейно-тропосферних станцій в оперативній та стратегічній ланках управління, модернізація існуючих тропосферних станцій з урахуванням сучасних телекомунікаційних технологій, а також використання найбільш вдалих технічних рішень іноземних виробників обладнання, виробництво яких на території України не є економічно доцільним (ефективним).

В будь-якому разі, залишається головна мета розвитку системи зв'язку Збройних Сил України, а саме – створення єдиного інформаційно-телекомунікаційного середовища на основі впровадження сучасних інформаційно-телекомунікаційних технологій, протоколів обміну інформацією, комплексів, систем та засобів зв'язку спеціального призначення, що дасть можливість забезпечити обмін усіма видами інформації між органами й пунктами управління (всіх ланок) з відповідною пропускною спроможністю, достовірністю та надійністю.

Сучасний стан та результати науково-технічної діяльності фахівців наукових установ та підрозділів, а також представників Командування Військ зв'язку та кібербезпеки Збройних Сил України, дозволяють стверджувати про наявність переходу на нову модель (стратегію), яка передбачає планування, реалізацію та впровадження проектів розвитку, що є вкрай актуальним і необхідним рішенням. Зазначений підхід представляється природною реакцією щодо створення тропосферних радіорелейних систем нового покоління з використанням новітніх радіотехнологій на екологічно безпечних і ресурсозберігаючих принципах.

За результатами проведеного аналізу застосування тропосферних засобів у розвинутих країнах світу слід зазначити, що найбільш доцільним є перехід на принципово нові телекомунікаційні технології, які б з одного боку дозволили забезпечити передавання зростаючих обсягів інформації, а з іншого здійснювали б це на екологічно безпечному рівні для особового складу із урахуванням вимог щодо перешкодозахищеності та розвідзахищеності зв'язку.

Впровадження зазначених перспектив та використання тропосферних (радіорелейно-тропосферних) станцій нового покоління дозволить створити передумови подальшого розвитку системи військового зв'язку з метою забезпечення функціонування системи управління Збройними Силами, що постійно розвивається.

Михайлюк С.С. (ВІТІ)

РЕЗЕРВУВАННЯ ОБ'ЄКТІВ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ І МЕРЕЖ ЗАГАЛЬНОГО ТА СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З КОМПЛЕКСНИМ ВИКОРИСТАННЯМ НАДЛИШКОВОСТІ

При створенні сучасних засобів зв'язку спостерігаються протиріччя між значними потенційними можливостями телекомунікаційних систем і їхньою реальною ефективністю, які обумовлені недостатнім рівнем їхньої експлуатаційної надійності. Усунення цього протиріччя шляхом забезпечення необхідної надійності телекомунікаційних систем у процесі тривалої експлуатації - одна з найактуальніших проблем сучасної техніки, на розв'язання якої спрямовані зусилля вчених, конструкторів, інженерів.

Основи надійності й експлуатації засобів зв'язку є необхідною умовою правильного розуміння сутності проблеми й обґрунтованого підходу до вибору шляхів і методів підвищення експлуатаційної надійності.

Необхідною умовою підвищення надійності системи є введення надлишковості. Використання надлишковості в поєднанні з контролем підвищує надійність телекомунікаційної системи.

Надлишковість – властивість більшості існуючих технічних об'єктів (систем) виконувати більше функцій, чим потрібно, і мати ресурси вище, ніж необхідно для виконання лише необхідних функцій. Надлишковість – це наявність у технічному об'єкті можливостей понад тих, які мінімально необхідні для забезпечення його нормального функціонування. З діалектичного погляду надлишковість є однією з умов переходу кількості у нову якість.

Резервування – метод забезпечення надійності, який полягає в застосуванні додаткових засобів і можливостей з метою збереження працездатності об'єкту резервування при відмові одного або декількох його елементів або порушення зв'язків між ними. Найбільш часто резервування використовують в тих випадках, коли інші методи виявляються недостатніми або ними можна скористатися в повній мірі через обмеження, що виникають при проектуванні і експлуатації систем.

Таким чином резервування – спосіб створення надлишковості, заснований на введенні в систему додаткових елементів, які не потрібні для її роботи в штатному режимі.

Для того, щоб введення надлишковості призводило до резервування, слід дотримуватися ряду додаткових умов і заходів. Зокрема: проведення контролю працездатності та технічного стану апаратури і обладнання; установки перемикачів резерву, які відповідають певним вимогам за часом спрацьовування і надійності; динамічного перерозподілу функціонального навантаження елементів при зміні структури системи, забезпечення можливості паралельних робіт в системах з паралельною структурою; включення до складу систем алгоритмів і засобів реконфігурації (перебудови структури), які б дозволили організувати ресурси для виконання завдання.

Ускладнення системи (об'єкту) спонукає виробника до підвищення ціни усього устаткування та створення додаткових елементів контролю та автоматичного перемикання. Тому такий спосіб підвищення надійності доцільно використовувати лише на об'єктах критичної інфраструктури, відмова елементів якої може спричинити техногенні (екологічні) катастрофи.

Напрямком подальших досліджень є дослідження надійності об'єктів телекомунікаційних систем і мереж загального та спеціального призначення з комплексним використанням надлишковості та з урахуванням не тільки стійких відмов, а також збоїв обладнання, оскільки збої грають суттєву роль у порушенні нормального функціонування мереж зв'язку.

д.т.н. Міночкін А.І. (ВІТІ)
Єрмаченков А.В. (ВІТІ)
Живило Є.О. (НУОУ)
Плугова О.Б. (ВІТІ)

РОЗРОБКА ПІДХОДІВ ДО ВИЗНАЧЕННЯ СКЛАДОВИХ КІБЕРОБОРОНИ, ЯК СИСТЕМИ ОРГАНІЗАЦІЇ ТА ВЕДЕННЯ КІБЕРДІЙ

Актуальність. За результатами вивчення підходів держав-членів НАТО щодо реагування на загрози в кіберпросторі, а також за досвідом проведення Антитерористичної операції та операції Об'єднаних сил на території Донецької та Луганської областей, найбільш сучасною і одночасно перспективною формою реалізації державної політики за напрямом забезпечення кібербезпеки у воєнній сфері вважається створення та забезпечення ефективного функціонування системи кібероборони, як організованої сукупності суб'єктів і об'єктів кібероборони з визначеними зв'язками між ними, об'єднаних єдиним керівництвом.

Метою дослідження є розробка підходів до визначення складових кібероборони, як системи організації та ведення кібердій в нашій державіза результатами вивчення підходів держав-членів НАТО щодо реагування на загрози в кіберпросторі.

Виклад основного матеріалу. Основним змістом ведення кібероборони є сукупність узгоджених і взаємопов'язаних за метою, завданнями, об'єктами, місцем та часом одночасних і послідовних заходів в кіберпросторі та через кіберпростір щодо запобігання, виявлення, стримування, активного реагування на агресію противника та мінімізації наслідків від його кібервпливу, які готуються та проводяться за єдиним замислом і планом силами та засобами Збройних Сил України із залученням необхідних можливостей інформаційної інфраструктури та ресурсів держави у взаємодії із військовими формуваннями та правоохоронними органами інших складових сил оборони держави, відповідно до їх компетенції.

Ураховуючи комплексний характер підготовки та ведення кібероборони, з метою розподілу та узгодження практичних заходів діяльності органів військового управління та дій військ (сил) в Міноборони та Збройних Силах пропонується визначити організаційну, інституалізаційну, функціональну, виконавчу,просторову та часову складові системи кібероборони.

Організаційна складова кібероборони випливає із нормативного визначення сутності кібероборони та включає сукупність заходів, розподілених на політичні, економічні, соціальні, військові, наукові, науково-технічні, інформаційні, правові, освітні, організаційні та інші заходи.

Інституалізаційна складова кібероборони реалізується шляхом створення, розвитку та функціонування органів управління, військ (сил), окремих військових частин (підрозділів), установ, організацій з визначеними завданнями та повноваженнями щодо підготовки та ведення кібероборони.

Ураховуючи інноваційний характер набуття Міноборони та Збройними Силами необхідних спроможностей з кібероборони, зазначене потребує створення та функціонування принципово нових організаційних одиниць органів управління та військ (сил) за напрямом кібербезпеки, у т.ч. наукових, навчальних, експериментальних, навчально-бойових, випробувальних тощо, включаючи формування інтегруючого роду військ для забезпечення кібербезпеки.

До функціональної складової кібероборони доцільно віднести:

запобігання (англійською – "Prevention") – заходи щодо завчасного виявлення, уникнення, стримування, запобігання можливих (потенційних) кіберзагроз чи кібератак, припинення підготовки до них;

захист (англійською – “Protection”) – заходи щодо забезпечення випереджувального захисту від можливих кібератак (кібервпливу) противника, в першу чергу в інтересах всебічного та стійкого забезпечення у кіберпросторі процесів управління власними військами та зброєю;

попередження (англійською – “Mitigation”) – заходи щодо безпосереднього виявлення, відвернення загрози, зменшення можливих втрат (збитків, пошкоджень) у разі безпосередньої загрози проведення кібератак. При певних умовах в межах зазначеного можуть проводитися випереджувальні (зустрічні) заходи активного кіберзахисту;

реагування (англійською – “Response”) – заходи комплексного реагування та впливу на противника, у т.ч. шляхом активного кіберзахисту в умовах безпосереднього проведення ним кібератак з одночасним проведенням заходів захисту власної інфраструктури, особового складу, ресурсів тощо від впливу противника;

відновлення (англійською – “Recovery”) – заходи, направлені на відновлення інформаційної та іншої інфраструктури, яка стала об’єктом кібератак противника, стабілізацію ситуації та ліквідації інших негативних наслідків.

Виконавчу складову кібероборони пропонується реалізовувати через Національний координаційний центр кібербезпеки при Апараті Ради національної безпеки та оборони України відповідно до завдань та повноважень Міноборони та Збройних Сил.

Іншими складовими ведення активної кібероборони є необхідні заходи в межах здійснення розвідувальної діяльності, радіоелектронне придушення роботи телекомунікаційних та інших засобів, фізичний вплив (вогневе ураження) на об’єкти інформаційної інфраструктури, здійснення кіберзахисту (у т.ч. активного кіберзахисту) власної інформаційної інфраструктури (засобів рухомого зв'язку, як апаратної, так і контентної складових, додатків та сервісів зв’язку, інших інформаційно-телекомунікаційних систем та об’єктів інформаційної діяльності суб’єктів оборони держави) від кібератак та кібервпливу противника, що забезпечує необхідний рівень інформаційного забезпечення управління військами та зброєю, інші дії в кіберпросторі тощо. Зазначені заходи можуть проводитися як складова частина кібероборони або як окремі самостійні заходи під час підготовки та застосування військ (сил), їх участі в проведенні операції Об’єднаних сил, Антитерористичній операції тощо.

Часова складова кібероборони на теперішній час розглядається стосовно умов мирного часу, у випадку воєнної агресії проти України або загрози нападу на Україну (в особливий період, під час воєнного стану (в умовах правового режиму воєнного стану), у воєнний час), а також в умовах правового режиму надзвичайного стану, під час проведення операції Об’єднаних сил та заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях. В межах зазначеного заходи кібероборони розподіляються на заходи завчасної підготовки, безпосередньої підготовки кібероборони та власне заходи ведення кібероборони.

Врахування наведених складових кібероборони в ході створення системи кібероборони дозволить підвищити ефективність її функціонування в інтересах досягнення цілей, які визначені перед Міноборони та Збройними Силами під час виконання військами (силами) завдань за призначенням.

Висновки. Найбільш сучасною і одночасно перспективною формою реалізації державної політики за напрямом забезпечення кібербезпеки у воєнній сфері вважається створення та забезпечення ефективного функціонування системи кібероборони, як організованої сукупності суб’єктів та об’єктів кібероборони з визначеними зв’язками між ними та об’єднаних єдиним керівництвом.

Ураховуючи комплексний характер підготовки та ведення кібероборони, з метою розподілу і узгодження практичних заходів діяльності органів військового управління та дій військ (сил), в інтересах Міноборони та Збройних Сил вперше запропоновані підходи до визначення організаційної, інституалізаційної, функціональної, виконавчої,просторової та часової складових системи кібероборони.

к. т. н. Міхєєв Ю. І. (ЖВІ ім. С.П. Корольова)
Носова Г. Д.(ЖВІ ім. С.П. Корольова)
Павленко М. М. (ЖВІ ім. С.П. Корольова)

АВТОМАТИЗАЦІЯ ПРОЦЕСУ ВІДСЛІДКОВУВАННЯ ДИНАМІКИ ПОШИРЕННЯ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В МЕРЕЖІ ІНТЕРНЕТ

Актуальність. Аналіз воєнно-політичної обстановки навколо України та суспільно-політичної в самій країні свідчить про те, що держава з дня своєї незалежності стала об'єктом зосередженого деструктивного інформаційно-психологічного впливу (ІПсВ), який Росія протягом останніх шести років здійснює у поєднані із політичними та військовими діями. Можливість здійснення ефективного ІПсВ забезпечується шляхом використання противником електронних засобів масової інформації, які мають високий рівень доступності до визначеної цільової аудиторії.

Постановка задачі. Отже, одним із актуальних завдань, яке виникає під час протистояння гібридній агресії з боку Росії є створення відповідної системи протидії зовнішнім інформаційним загрозам. Така система насамперед повинна передбачати появу деструктивного ІПсВ, визначати ступінь його загрози та надавати пропозиції щодо подальшого розвитку ситуації органам військового управління. В умовах постійного збільшення обсягів даних, які циркулюють у мережі Інтернет, забезпечити виконання функцій такої системи можливо лише через автоматизацію основних етапів її роботи. Тому **метою** наукового завдання обрано автоматизацію процесу відслідковування динаміки поширення деструктивного ІПсВ в мережі Інтернет, як першочергового етапу роботи системи попередження та захисту від зовнішніх інформаційних загроз.

Основні положення. На сьогодні існуючі системи попередження та захисту від зовнішніх інформаційних загроз переважно базуються на семантичних методах із використанням якісних показників впливу. У доповіді запропоновано використання кількісних індикаторів для підвищення оперативності виявлення деструктивного ІПсВ і прогнозування ситуації щодо динаміки його поширення. Запропонований підхід використаний для розроблення відповідного прототипу спеціалізованого програмного забезпечення (СПЗ), яке дозволяє автоматизувати процес відслідковування динаміки поширення ІПсВ у мережі Інтернет. Особливість СПЗ полягає у використанні клієнт-серверної архітектури, реалізованої у вигляді Web-додатку. Під час розроблення СПЗ використано методи машинного навчання для інтелектуального оброблення інформаційних повідомлень.

Основними функціональними можливостями СПЗ є:

організація багатокористувацького режиму роботи СПЗ з можливістю збереження налаштувань програми окремо для кожного користувача;

синхронізація даних під час сумісної роботи користувачів;

забезпечення контекстного пошуку у масиві вихідних даних за різними параметрами та їх фільтрації;

створення класифікаторів повідомлень та автоматизованої рубрикації контенту;

присвоєння категорії важливості/терміновості інформації в ручному (автоматизованому) режимі;

створення календаря подій з можливістю його відображення за визначений період часу;

відображення статистичних даних результатів обробки інформації (числових даних) за інформаційними приводами (подіями) та джерелами.

Висновок. Використання розробленого СПЗ спеціальними підрозділами Збройних Сил України дозволило автоматизувати процес збору, оброблення, узагальнення та аналізу інформації у мережі Інтернет та збереження результатів моніторингу в єдиній базі даних; автоматизувати процес визначення тематики текстових повідомлень та їх емоційного забарвлення з впровадженою функцією аналітичного оброблення текстових повідомлень.

д.т.н. Могилевич Д.І. (ВІТІ)
Сінько В.В. (ВІТІ)

МОДЕЛІ НАДІЙНОСТІ ОБ'ЄКТІВ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ МЕРЕЖІ ВІЙСЬКОВОГО ЗВ'ЯЗКУ

До основних особливостей мереж військового зв'язку (МВЗ) слід віднести перш за все те, що вони являють собою складні технічні комплекси, в склад яких входить різноманітні програмні засоби (ПЗ), утворюючи функціональне та системне програмне забезпечення (ПЗ). Програмне забезпечення є найбільш розвинутою за структурою та функціональними зв'язками складовою частиною телекомунікаційного обладнання (ТКО), яка поряд з апаратною (технічною) частиною має помітний вплив на надійність функціонування МВЗ, оскільки відмови та збої програмних засобів часто призводять до не менш тяжких наслідків, ніж відмови техніки. Тому актуальним є підхід, при якому надійність ПЗ оцінюється за ступенем впливу відмов та збоїв програмних засобів на узагальнені показники надійності ТКО, що має у своєму складі велику кількість різноманітних програмних засобів.

Предметом теоретичного дослідження є процеси функціонування об'єктів ТКО в умовах обмеженої надійності програмних засобів з метою побудови моделей надійності об'єктів з урахуванням використання непоповнювальним часовим резервом для компенсації наслідків різних типів відмов.

Під об'єктом ТКО розуміється апаратно-програмний комплекс (АПК) – сукупність взаємозалежних технічних та програмних засобів, за допомогою яких здійснюється процес обміну інформацією між абонентами в МВЗ. До технічних засобів належать апаратура каналоутворення, пристрої комутації та маршрутизації, сервери, апаратура IP шифрування, кінцеве та інше обладнання. У складі програмних засобів «software» АПК зазвичай виділяють три частини: математичне забезпечення (сукупність математичних моделей, методів та алгоритмів), інформаційне забезпечення (сукупність баз даних із системами управління, файлових структур з каталогами, констант та інших елементів) та програмне (системне, функціональне, інструментальне) забезпечення.

Результатом побудови надійності об'єктів ТКО з непоповнювальним резервом часу є отримання аналітичних моделей, що встановлюють зв'язок між показниками надійності функціонування об'єктів, характеристиками відмов програмних засобів та їх наслідків, а також сукупністю технічних параметрів об'єкта, що визначають умови його функціонування, з урахуванням тимчасових обмежень, зумовлених використанням резервів.

За характером наслідків всі відмови програмних засобів можуть бути розділені на три групи: незнецінюючі, частково знецінюючі та повністю знецінюючі попередній наробіток. Відмову вважають незнецінюючою, якщо об'єкт із резервом часу після відновлення працездатності може відновити роботу з того самого місця, на якому вона була перервана. При цьому все напрацювання між сусідніми відмовами є корисним. У разі повністю знецінюючої відмови програмних засобів доводиться всю роботу, виконану на момент відмови, виконувати заново. Весь наробіток до виникнення відмови виявляється марним, якщо він менший за задану величину, і повинен бути включений у втрати робочого часу. Корисною є лише та частина напрацювання, яка не переривалася відмовами. Можливі проміжні випадки, коли знецінюється лише частина виконаної роботи. Частково знецінюючі відмови характерні для об'єктів з безперервним або періодичним контролем працездатності, у яких періодично фіксуються та зберігаються проміжні результати роботи. В об'єктах можуть виникати у певних пропорціях і всі три розглянуті типи відмов.

Таким чином, запропоновано аналітичні моделі надійності об'єктів телекомунікаційного обладнання, в яких можуть виникати зазначені типи відмов програмних засобів.

Nasibov Yashar (PhD student)
Armed Forces War College of the Azerbaijan Republic,

ONE-STOP DATA INFRASTRUCTURE: BUILDING SMART CITIES IN DEVELOPING COUNTRIES

ABSTRACT:

While the emergence of cities dates back to ancient times, especially to the 18th century, the process of urbanization was further accelerated by the industrial revolution. The rapid growth of the population has led to an increase in various problems in areas such as planning, management, security, transport and regulation. As a result, there is a need for future urban planning and smart solutions, and therefore the need to improve people's quality of life. As a result of all these developments, the concept of smart city has emerged.

"Smart city", which improves the quality of life of people with environmentally friendly physical, digital and technological systems; offering a modern, competitive, functional and sustainable future; they are cities supported by advanced life technologies.

The article gives various definitions of "Smart City", discusses the need and benefits of its creation, and examines its application in Azerbaijan and around the world.

KEY WORDS: Smart city, smart village, Geographic Information Systems (GIS), Azerbaijan, World

MAIN:

The ever-increasing number and quality of technological developments and innovative approaches have a strong transformative impact on city life. Described as a 'smart city', the transformation aims to enable the city to govern itself with future forecasts based on information and experience without the need for human intervention by building strong networks and interconnecting them with the city's ecosystem stakeholders. With the ability to turn the information it offers into economic, social and environmental benefits, Smart City benefits in the areas of sustainable development, competitiveness and environmental sustainability. For this reason, the "smart city" attracts the attention of countries, and countries make special efforts to understand the concept of "smart city", to be prepared for changing conditions, to adapt and guide this dynamic process.

The need for cities to compete in an interconnected economy on a global scale and to sustain the wellbeing of their inhabitants is forcing countries and cities to consider new technologies and innovative approaches. This motivation, the complexity and speed of the change brought about by the above technologies and approaches, highlights the need for a unified and systematic approach to urban solutions. The goal of a smart city is to make the current and future expectations of the city, as well as its problems a driving force in all spaces and systems, to be able to combine physical and social and digital planning, to predict, identify and solve problems in a systematic, efficient and sustainable manner to provide integrated services by providing connectivity and to unleash the potential of innovation.

CONCLUSION

Smart cities with their ability to harness technology to improve planning and the efficiency of service delivery, and their governance and effective urban management are key to achieving a green, resilient, and sustainable future for all. In many cities, especially in developing countries, the lack of evidencebased planning and decision-making is necessary for the implementation of livable urban environments.

Improving the quality, safety and efficiency of services provided in the cities and villages of Azerbaijan, the application of information technology in their provision, as well as ensuring the effective use and management of available resources for these services are among the main priorities of sustainable development in urban and rural areas.

Нерознак Є.І.(ВІТІ імені Героїв Крут)
Меркотан Д.Ю. (ВІТІ імені Героїв Крут)
д.т.н., с.н.с. Сова О.Я. (ВІТІ імені Героїв Крут)

МЕТОДИ ТА АЛГОРИТМИ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В КЛАСТЕРНИХ СИСТЕМАХ НА ОСНОВІ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ

На теперішній час існують певні проблемні питання пов’язані з розподілом навантаження на серверні системи, які слід вирішувати ще на ранній стадії планування та розвитку будь-якої інформаційної системи. Відмова сервера або вузла кластеру, що зазвичай відбувається несподівано, а також у відповідальний момент часу, тягне за собою серйозні наслідки, що особливо актуально для систем спеціального призначення.

Проблеми недостатньої продуктивності сервера (вузла) у зв'язку зі зростанням навантаження можна вирішувати шляхом нарощування потужності сервера, або оптимізацією використовуваних алгоритмів, програмних кодів і т.д. Але рано чи пізно настає момент, коли ефективність цих заходів виявляється низькою, особливо з урахуванням коштів, які інвестуються в розвиток серверної інфраструктури. Іншим способом підвищення продуктивності серверів є їхнє об'єднання в кластер, у якому навантаження розподіляється між серверами (вузлами) за допомогою комплексу спеціальних методів та алгоритмів балансування навантаження. Крім вирішення проблеми високих навантажень, технологія кластеризації допомагає також забезпечити резервування серверів, ефективність якого знову ж таки залежить від того, як розподіляється (балансується) навантаження між вузлами кластера.

Метою дослідження є обґрунтування доцільності застосування елементів штучного інтелекту в процесі балансування навантаження в кластерних системах.

Балансування навантаження може здійснюватися за допомогою апаратних і програмних інструментів та може бути реалізоване на мережевому, транспортному та прикладному рівнях моделі OSI. Балансування навантаження кластерної системи на **мережевому** рівніпередбачає таке підключення сервера до мережі, за якого його кожна IP-адреса (в тому числі віртуальна) обслуговується різними фізичними серверами (вузлами кластера).. Балансування навантаження кластерної системи на **транспортному** рівніпередбачає розподіл трафіка за сокетами елементів даної системи.

Балансування навантаження на **прикладному** рівні передбачає використання відповідних протоколів, зокрема HTTP і SMTP, для прийняття рішень про розподіл трафіку на основі фактичного вмісту кожного повідомлення.

На сьогодні існує певна кількість різних алгоритмів і методів балансування навантаження. Обираючи той чи інший алгоритм, потрібно чітко розуміти особливості конкретного проекту, у рамках якого планується використання серверних кластерів, та цілі, які потрібно досягти.

З-поміж цілей, для досягнення яких, використовується балансування, потрібно виділити наступні:

- справедливість: потрібна гарантія того, що на обробку кожного запиту буде виділена достатня кількість системних ресурсів і не виникне ситуацій, коли один запит обробляється, а всі інші чекають своєї черги;

- ефективність: полягає у тому, що всі сервери, які обробляють запити, повинні бути навантажені, тобто не допускати ситуації, коли один з серверів простоює в очікуванні запитів на обробку (на практиці ця мета досягається не завжди);

- скорочення часу виконання запиту: потрібно забезпечити мінімальний час між початком обробки запиту (або його постановкою в чергу на обробку) і його завершенням.

Разом з тим алгоритм балансування повинен мати такі властивості як:

- передбачуваність: потрібно чітко розуміти, в яких ситуаціях і при яких навантаженнях алгоритм буде ефективним для вирішення поставлених завдань;

- рівномірне використання ресурсів системи;

- масштабованість: алгоритм повинен зберігати працездатність при зміні топології системи, тобто додаванні нового чи виведення існуючого вузла з кластеру.

Розглянемо найпоширеніші на сьогодні алгоритми балансування навантаження.

Round Robin, або метод кругового обслуговування, являє собою перебір закруговим циклом: перший запит передається до одного сервера, потім наступний запит передається іншому і так до останнього сервера, після чого цикл починається спочатку.

Weighted Round Robin - вдосконалена версія алгоритму Round Robin суть якого полягає в наступному: крім виконання умов алгоритму Round Robin, кожному серверу присвоюється ваговий коефіцієнт відповідно до його продуктивності і потужності. Це допомагає розподіляти навантаження більш гнучко, тобто сервери з більшим ваговим коефіцієнтом обробляють більшу кількість запитів. Однак усіх проблем з відмовостійкістю не вирішує.

Least Connections. При балансуванні навантаження за алгоритмами Round Robin та Weighted Round Robin абсолютно не враховується кількість активних підключень до сервера в поточний момент часу. Описану проблему можна вирішити за допомогою алгоритму Least Connections. Цей алгоритм враховує кількість активних підключень, підтримуваних серверами в поточний момент часу. Кожен наступний клієнтський запит буде передаватись серверу з найменшою кількістю активних підключень.

Weighted Least Connections являє собою удосконалений варіант попереднього алгоритму та призначений в першу чергу для використання в кластерах, що складаються з серверів з різними технічними характеристиками і різною продуктивністю. Цей алгоритм враховує при розподілі навантаження не тільки кількість активних підключень, а й ваговий коефіцієнт серверів.

У алгоритмі **Sticky Sessions** запити розподіляються залежно від IP-адреси користувача. Sticky Sessions припускає, що запити від одного клієнта будуть направлятися на один і той самий сервер, а не перерозподілятися між серверами. Запити клієнта можутьспрямовані на інший сервер тільки в тому випадку, якщо первинний призначений сервер буде недоступний.Виходячи з вищезазначеного, слід розуміти, що вибір та застосування якогось одного алгоритму в майбутній або існуючій системі, особливо розподіленій, не в повній мірі зможе забезпечити надійне та відмовостійке функціонування системи, що в подальшому призведе до порушення роботи як окремих модулів, так і всієї системи в цілому. Тому виникає актуальна задача пов’язана з розробкою комплексного підходу до проектування розподілених інформаційних систем та застосування різного роду методів та алгоритмів балансування навантаження, здатних приймати рішення з урахуванням множини різнорідних параметрів стану кластерної системи та за умов непередбачуваності навантаження на її елементи.

Окрім того, необхідно враховувати і людський чинник та часову прострацію. Це пояснюється тим, що людині потрібен певний проміжок часу на переналаштування або реорганізацію системи при виникненні різного роду ситуацій, особливо нештатних. Якщо говорити про передбачення поведінки системи за умов різкої зміни середовища функціонування, то людині також буде потрібно затратити значну кількість часу на відновлення функціонування, а також здійснити передбачення поведінки системи буде досить складно за умов неповноти інформації про систему чи відсутності достатньої кваліфікації у фахівця.

Вирішення вищезазначеної задачі може бути виконане шляхом інтелектуалізації процесів балансування навантаження на основі використання елементів штучного інтелекту, зокрема нейронних мереж.

Роль та місце нейронної мережі можна пояснити наступним чином: нейронна мережа повинна здійснювати контроль за вказаними параметрами кластеру та реагувати на зміни, які відбуваються шляхом оцінювання параметрів системи та вибору оптимального на поточний момент часу алгоритму балансування навантаження. Разом з тим, нейронна мережа також

повинна здійснювати процеси пов'язані з передбаченням поведінки системи, тобто здійснювати аналіз попередніх інцидентів та на їх основі робити прогнозування на предмет виникнення нових інцидентів.

Також, в залежності від поставлених завдань, з використанням нейронної мережі можна організувати як систему підтримки прийняття рішень на балансування навантаженням, тобто автоматизувати рутинний процес збору даних для аналізу стану системи, так і систему управління навантаженням на серверний кластер, яка буде приймати рішення на застосування того чи іншого алгоритму балансування навантаження та переналаштування інфраструктури без участі адміністратора.

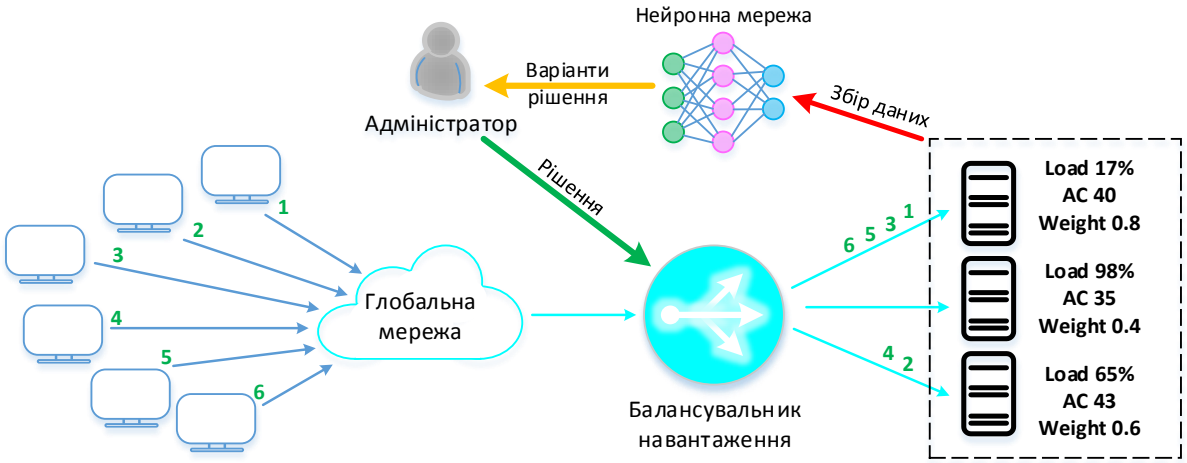


Рис. 1. Схема системи підтримки прийняття рішень на балансування навантаження

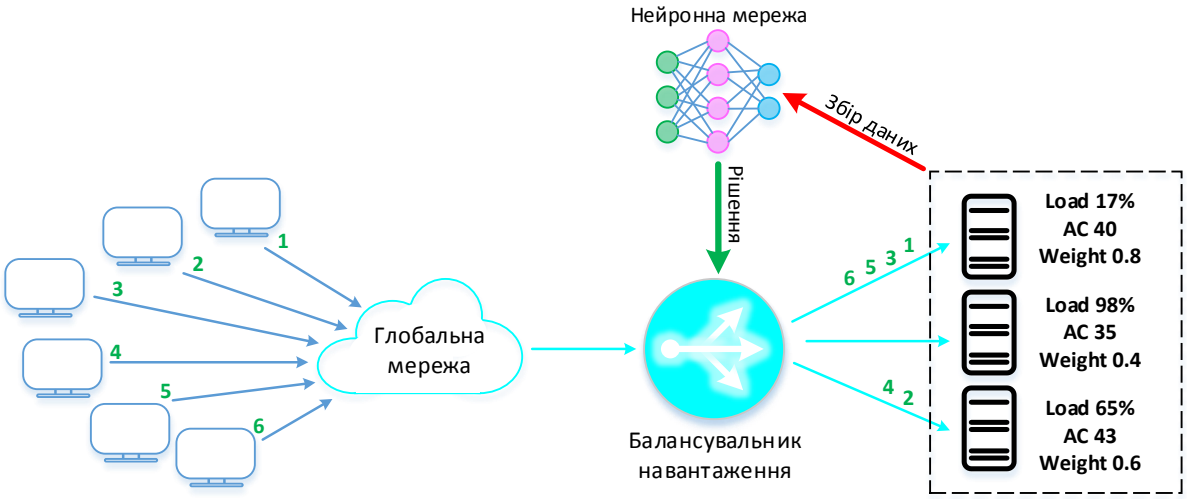


Рис. 2. Схема автономної системи балансування навантаження на основі нейронної мережі

Таким чином, використання нейронної мережі для реалізації систем балансування навантаження на кластерні системи надасть можливість забезпечити більш високу живучість та стійкість різного роду розподілених інформаційних систем до динамічної зміни середовища функціонування шляхом підбору оптимального алгоритму балансування в поточних несприятливих умовах, разом з тим ефективність управління потоками даних та раціональність розподілу ресурсів розподілених систем буде значно вищою. Вищезазначені процеси можливо реалізувати при правильному виборі типу нейронної мережі та найбільш оптимального методу її навчання.

Подальші дослідження будуть спрямовані на розробку моделі нейронної мережі для балансування навантаження в розподілених інформаційних системах спеціального призначення.

к.т.н. Нестеренко М.М. (ВІТІ)
Кулікова О.С. (ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ ПОБУДОВИ РЕЙТИНГУ КУРСАНТІВ ФАКУЛЬТЕТУ ВВНЗ НА ОСНОВІ ПЛАТФОРМИ NODE.JS

Основна мета та завдання вищих військових навчальних закладів (ВВНЗ), його структурних підрозділів (факультетів) це підготовка фахівців за відповідними спеціальностями (спеціалізаціями) та галузями для забезпечення якісного виконання ними обов'язків за посадою під час проходження служби у ЗС України. Для представлення більш повної картини про майбутніх офіцерів та зменшення часу на збір та обробку персональних даних необхідно автоматизувати процес побудови рейтингу курсантів. Це в свою чергу, дозволить більш ефективно розподіляти кадри на первинні посади з урахуванням реальних знань, морально-ділових якостей та практичних навичок. Отже, актуальними завданням є удосконалення процесу визначення рівня підготовки фахівця (курсанта ВВНЗ) за відповідною спеціальністю шляхом автоматизації побудови рейтингу курсантів в рамках факультету.

Більш того, рейтинг – це відносна чисельна величина, що формується на основі показників якості засвоєння матеріалу та набуття необхідних навичок у вигляді оцінок за навчальними дисциплінами. Беручи до уваги, що навчальними дисциплінами є як предмети за фахом та спеціальністю, так і предмети загальні для військових вишів та в цілому для закладу вищої освіти, пропонується ввести коефіцієнти важливості конкретної дисципліни для груп з різних спеціальностей. Складання рейтингудуже важливий етап у навчально-виховному процесі на факультеті, так як формується конкуренція та мотивація серед курсантів.

Підсистема побудована за принципами трьохрівневої архітектури, яка складається з таких компонентів: клієнт, сервер і база даних. Для цього було обрано стек MERN, що включає в себе СКБД MongoDB, базову платформу Express.js, бібліотеку React та програмну платформу Node.js., що приведено на рис. 1.

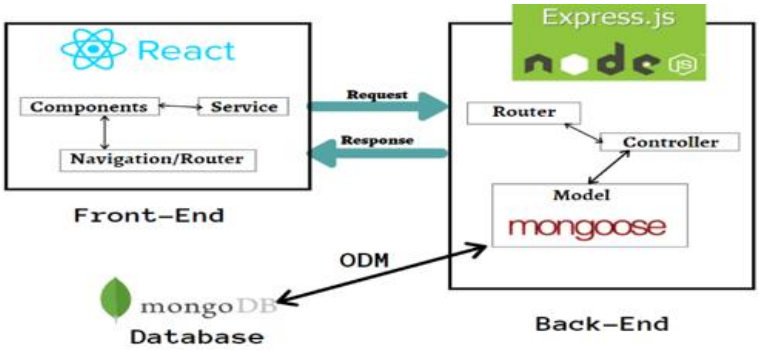


Рис. 1. Архітектура підсистеми побудови рейтингу курсантів факультету ВВНЗ

Для написання програмного модулю було обрано мову програмування JavaScript, яка дозволяє реалізувати і клієнтську і серверну частину підсистеми на основі бібліотеки React та платформи Node.js. Всі дані зберігаються в нереляційний базі даних MongoDB. Особливістю доступу до даних є використання ODM системи mongoose, яка надає зручний інтерфейс маніпулювання даними. Застосування даного програмного модулю повинно зменшити число помилок, пов'язаних з людським фактором, а також підвищити ефективність обробки даних.

Висновки. Провівши аналіз технологій розробки програмного забезпечення було визначено: вимоги до функціональності підсистеми рейтингу курсантів факультету ВВНЗ; застосування трьохрівневої клієнт-серверної архітектури; використання мови програмування JavaScript та СКБД MongoDB.

к.т.н. Нестеренко М.М. (ВІТІ)
Сорока Д.В. (ВІТІ)

ПІДСИСТЕМА РОЗРАХУНКУ НАВАНТАЖЕННЯ НАУКОВО-ПЕДАГОГІЧНИХ ПРАВЦІВНИКІВ ВВНЗ НА ОСНОВІ СТЕКУ ТЕХНОЛОГІЙ MERN

Оптимальне планування навчального процесу є актуальним питанням для будь-якого вищого начального закладу і має велике значення для забезпечення ефективної роботи науково-педагогічних працівників (НПП) та підвищення якості надання освітніх послуг. Попри існування низки програмних рішень, спрямованих на автоматизацію розрахунку навантаження, мають місце особливості у ході розрахунку навантаження для НПП у вищих військових навчальних закладах (ВВНЗ), що не дозволяють їх прямого використання. У зв'язку з цим, метою роботи є розробка підсистеми розрахунку навантаження ВВНЗ на основі стеку технологій MERN.

Розподіл навчального навантаження затверджується начальником ВВНЗ у наказі про організацію освітньої та службової діяльності на новий навчальний рік. Навантаження НПП розраховується відповідно до визначених норм часу та видів занять (робіт), специфічних видів занять і службових завдань.

В основу розробки підсистеми покладено компоненти стеку MERN (MySQL, Express, React, Node), який застосовується для створення web-додатків та їх легкого масштабування у ході реалізації багатокористувальницьких систем. Крім того, наведені технології дозволяють створювати клієнтську і серверну частини за допомогою однієї мови програмування, а неблокуючий I/O платформи Node.js – обробляти велику кількість запитів одночасно. Зважаючи на роботу з великим набором структурованих даних та підтримку транзакцій, для досягнення мети підсистеми застосовується СКБД MySQL, що містить повний обсяг даних про науково-педагогічних працівників ВВНЗ.

Архітектура модуля розрахунку базується на класичному патерні проєктування MVC (Model-View-Controller), що представлено на рис. 1.

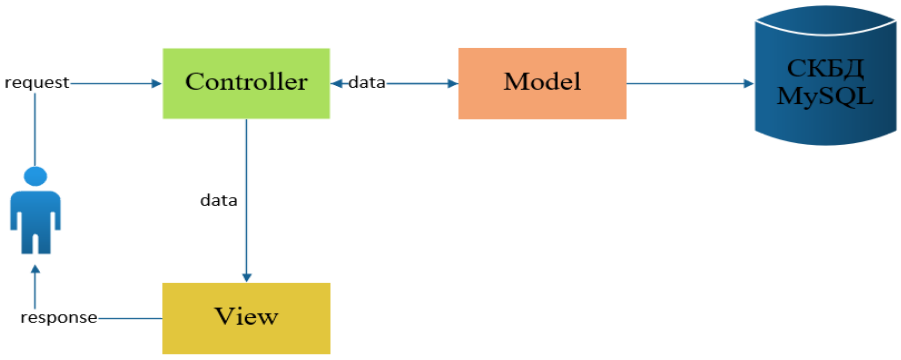


Рис. 1. Архітектурний патерн підсистеми розрахунку навантаження НПП ВВНЗ

Роботу серверної частини модуля забезпечують фреймворк Express.js та Node.js, а клієнтської частини – бібліотека React. Відповідно до приведеної схеми, користувач подає запит на сервер (Controller), який за допомогою моделі (Model) доступається до відповідних даних у СКБД MySQL. На основі програмної логіки (формул і числових значень для розрахунку навантаження), закладеної в контролері та отриманих даних, контролер формує кінцеву відповідь користувачу у вигляді HTML-шаблону, тобто представлення (View).

Отже, в рамках даної роботи було розроблено підсистему розрахунку навантаження НПП ВВНЗ на основі стеку MERN та архітектурного патерну MVC. Застосування функціоналу перерахованих web-технологій забезпечить зручний інтерфейс користувача, масштабованість і модульність підсистеми, що дозволить в подальшому розширяти функціонал та полегшити процес розрахунку навантаження НПП.

к.т.н. Нестеренко М.М. (ВІТІ імені Героїв Крут)
Степаненко С.Ю. (ВІТІ імені Героїв Крут)
Ковальчук Д.О. (ВІТІ імені Героїв Крут)

ПРОГРАМНО-АПАРАТНИЙ МОДУЛЬ ПІДСИСТЕМИ ВИЯВЛЕННЯ АВАРІЙНИХ СИТУАЦІЙ НА ОБ'ЄКТАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ НА ОСНОВІ ТЕХНОЛОГІЇ WEB OF THINGS

На теперішній час на об'єктах військового призначенням виникають аварійні (нештатні) ситуації, що призводять до жахливих наслідків, наприклад займання боєприпасів на артилерійських складах, тощо. Існуючі програмно-апаратні комплекси не в повній мірі дозволяють вирішити питання, щодо збору даних про технологічні процеси та оперативного реагування на дані інциденти, в режимі реального часу. В зв'язку цим, виникає актуальне завдання, щодо розробки програмно-апаратного модулю підсистеми аварійних ситуацій на об'єктах військового призначення на основі сучасних інформаційних технологій.

Для цього пропонується розглянути сучасні архітектури та протоколи *Internet of Things (IoT) та Web of Things (WoT)*. Дані технології дозволяють інтегрувати різнорідне обладнання, масштабувати систему та гнучко налаштовувати необхідний функціонал шляхом додавання відповідного програмного модулю.

В свою чергу, архітектура *IoT* має чотири рівні: прикладний рівень (ідентифікація, обробка, візуалізація даних отриманих із множини сенсорів та датчиків); рівень підтримки (забезпечення місця зберігання та обчислювальної потужності для пристроїв з обмеженими ресурсами на основі хмарних сховищ); мережевий рівень (комунікаційний канал для передачі даних на основі різних мережевих технологій *Z-Wave, LoRa, Wi-Fi, Bluetooth* та ін.), рівень сприйняття (сенсори, радіочастотні ідентифікатори RFID, датчики та бездротові мережі, наприклад: WSAN, ZeBee та інші).

Сучасні *IoT*-системи працюють у режимі реального часу, мають розподілену клієнт серверну архітектуру та зазвичай складаються з мережі «розумних пристроїв» та хмарної платформи. В рамках концепції *IoT* протоколи розділяють на групи, в залежності від ділянки мережі: сенсорний вузол – сенсорний вузол (найпоширеніший протокол *Data Distribution Service,DDS*), сенсорний вузол – сервер (*Constrained Application Protocol, CoAP*; *Message Queue Telemetry Transport, MQTT*; *Extensible Messaging and Presence Protocol, XMPP*; *Simple Text Oriented Message Protocol, STOMP*), сервер – сервер (*Advanced Message Queuing Protocol, AMQP*).

Для вирішення проблем взаємодії різнорідних платформ *IoT* було створено технологію *Web of Things,* якадопомагає спростити розробку додатків, підвищує гнучкість системи та сумісність з існуючими стандартами. Метадані пристрою *IoT*, включаючи всю інформацію необхідну для дотримання загальної абстракції, задокументовані в так званому описі речей *WoT– Thing Description (TD***).** *TD* – відкрита інформаційна модель з форматом представлення на основі *JSON*. Вона забезпечує: уніфікований спосіб опису можливостей пристрою (або служби) *IoT* з його запропонованою моделлю даних та функціями; використання протоколу обміну; а також механізм безпеки, який використовується для контролю доступу.

Висновки. Для розгортання та тестування програмно-апаратного модулю підсистеми виявлення аварійних ситуацій доцільно використовувати апаратну обчислювальну платформу *Arduino* в якості системи для збору даних із датчиків, *Ethernet shield* для міжмережевої взаємодії (*HTTP*, також *XMPP* та *MQTT)*, а мікрокомп'ютер *Raspberry Pi* – сервер додатків (збір, обробка, візуалізація даних).*Sketch* щодо збору поточних значень із датчиків та порядку передачі даних по мережі було реалізовано за допомогою *IDE Arduino* (*C/C++*). Додаток обробки статистичних даних на серверній частині реалізовано на мові програмування *Python*.

к.в.н. Олексіюк В.В.,
Військова частина А1906
к.в.н. Балик І.В.,
Військова частина А1906
Касалапов А.Д.,
Військова частина А1906

ЗАВДАННЯ РОЗВІДКИ РОБОТОТЕХНІЧНИХ КОМПЛЕКСІВ ЗА ДОСВІДОМ ЇХ ЗАСТОСУВАННЯ У СУЧАСНИХ ЗБРОЙНИХ КОНФЛІКТАХ

Кінець XX – початок XXI ст. характеризується інтенсивним розвитком інформаційних технологій і практичним впровадженням їх переваг у сферу збройної боротьби. Вони реалізовані під час створення високоточної зброї, інформаційних систем, комплексів і засобів військового призначення, робототехнічних комплексів (РТК) тощо.

Результати аналізу розробок РТК в Україні свідчать, що на сьогодні спостерігається значне відставання від рівня оснащеності збройних сил провідних країн світу відповідними РТК. Тому питання створення, розроблення основ їх бойового застосування та оснащення Збройних Сил України, зокрема частин (підрозділів) розвідки, сучасними РТК набуває особливої актуальності.

На думку авторів, зростання ролі розвідувальних РТК у сучасних збройних конфліктах визначається такими основними їх перевагами:

підвищення рівня бойових (розвідувальних) можливостей частин (підрозділів) розвідки;

зниження рівня бойових втрат серед особового складу;

досягнення безперервності виконання завдань за умов, в яких фізіологічні можливості людей обмежені.

доступність (дешевизна) виробництва порівняно зі звичайним озброєнням та військовою технікою;

зменшення витрат на їх бойове розгортання;

можливість адаптації РТК до виконання завдань в різних умовах бойової обстановки.

У контексті зазначеного та за результатами аналізу досвіду застосування РТК у збройних конфліктах, у доповіді визначено основні розвідувальні завдання, які на них покладались та покладатимуться у майбутньому:

викриття системи вогню, засобів вогневого ураження та розвідки;

визначення координат, кількості, характеру й типу об’єктів (цілей) противника для їх вогневого ураження;

виявлення оптичних та оптико-електронних засобів (засобів збору інформації) противника;

дорозвідка результатів вогневих ударів, визначення ступеня поразки об’єктів;

передача розвідувальних даних про цілі (об’єкти) для їх відображення на електронних картах командирів (штабів) з метою ефективного ураження в реальному масштабі часу;

ведення радіаційної, хімічної, бактеріологічної розвідки;

виявлення інженерних загороджень, насамперед мінно-вибухових, в умовах урбанізованої місцевості;

виявлення завалів та руйнувань у межах міста, можливі шляхи їх обходу та найбільш доцільні способи подолання.

Застосування РТК для вирішення розвідувальних завдань збереже особовий склад частин (підрозділів) розвідки та підвищить ефективність їх виконання.

Ольшанський В.В. (ВІТІ)
Поляк І.Є. (ВІТІ)
Хижий О.І. (НУОУ)

РОЗПОДІЛ ЧАСТОТНОГО РЕСУРСУ ПРИ РОБОТІ РАДІОМЕРЕЖ ТЛУ В РЕЖИМІ ППРЧ

Для ефективного управління підрозділами в тактичній ланці управління (ТЛУ) ЗСУ під час виконання завдань за призначенням необхідно використовувати сучасні військові радіозасоби КХ та УКХ радіозв'язку з високим рівнем розвід- та завадозахищеності.

Тому при побудові мереж радіозв'язку використовуються режими роботи з псевдовипадковою перебудовою робочих частот (ППРЧ). Для ефективного використання частотного ресурсу при плануванні даного режиму роботи необхідно раціонально розподіляти просторово-частотний ресурс системи радіозв'язку між усіма радіомережами.

Можливо застосувати три основних підходи для частотного планування радіомереж, які потенційно можуть створювати взаємні завади одна одній:

1) увесь частотний ресурс спільно використовується усіма кореспондентами;

2) кожній радіомережі призначається власна смуга частот, яка не перетинається з іншими;

3) декілька радіомереж може спільно використовувати декілька частотних смуг, які можуть прилягати одна до одної, або бути розосередженими.

Очевидно, що з позиції розвідзахищеності переважають перший та третій способи, а з урахуванням необхідності максимізації швидкості передачі даних та/або дальності зв'язку – третій. При цьому, зменшення взаємних завад між радіомережами, що працюють у спільній смузі частот може бути досягнуте наступними способами:

1) різним радіомережам призначаються різні номінали частот у межах однієї смуги (як реалізовано, наприклад, у радіозасобах виробництва "Aselsan");

2) номінали частот можуть співпадати для декількох радіомереж у межах однієї спільної для використання смуги. Мінімізація взаємних завад досягається, по-перше, збільшенням кількості можливих для використання номіналів частот, по-друге – застосуванням псевдовипадкових послідовностей з з мінімальними значеннями рівня взаємної кореляції.

Очевидно, другий спосіб хоч і не забезпечить повної відсутності взаємних завад, але є значно ефективнішим стосовно протидії розвідці противника.

У доповіді запропоновано алгоритм розподілу частотного ресурсу для системи радіозв'язку з ППРЧ. Вихідними даними для розподілу частотного ресурсу є наступні: кількість радіомереж; кількість радіомереж та відповідних їм кореспондентів у кожній ділянці (ділянка – смуга частот, в межах якої буде працювати одна або декілька радіомереж); кількість ділянок; загальна кількість піддіапазонів (піддіапазон – відношення частотного ресурсу до кількості радіомереж, частотний ресурс – загальний діапазон робочих частот радіостанцій); середній час роботи одного кореспондента на одній частоті; допустимий рівень взаємних завад.

Основними принципами, реалізованими в процесі розподілу частотного ресурсу є: використання оптимальних смуг частот в залежності від характеристик антенних пристроїв; рівномірний розподіл кореспондентів (радіомереж) по всьому частотному діапазону з урахуванням пріоритетності радіомереж вищого рівня управління; мінімізація рівня взаємних завад між сусідніми радіомережами з урахуванням взаємних впливів на гармоніках та, в першу чергу, взаємного впливу радіозасобів різних радіомереж, що встановлені поряд у одному транспортному засобі або на пункті управління.

Запропонований спосіб розподілу частотного ресурсу для радіомереж ТЛУ дозволить автоматизувати призначення частот та підвищити оперативність планування та налаштування.

д.т.н. Орлов В.В., ВА (м. Одеса)

ПАСИВНІ СИСТЕМИ ЗВУКОЛОКАЦІЇ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

В даний час активні системи радіолокації не володіють достатнім помехозахистом від засобів радіоелектронної боротьби і малоефективні в умовах проведення високотехнологічних терактів із зяастосуванням безпілотних літальних апаратів (БпЛА). При цьому має місце низька ефективність виявлення малих БпЛА. Вони невидимі для радарів, внаслідок малої поверхні, що відбиває і низьку висоту польоту. Відеозасоби моніторингу також малоефективні внаслідок апріорної невизначеності щодо направлення і часу появи БПЛА противника.

Актуальним напрямком є застосування пасивних систем звуколокації, захищених від засобів радіоелектронної боротьби. В даний час широко застосовуються звукометричні розвідувальні комплекси, які належать до класу високоточних засобів ведення війни й призначенні для визначення координат снайперів, вогневих артилерійських позицій. Однак вони неефективні при локації рухомого транспорту та не визначають координати в трьохвимірному просторі. Малі БПЛА, що рухаються зі швидкості до 50 м/с, випромінюють безперервні звукові сигнали, що виникають у результаті роботи гвинтів та двигуна. Тоді на просторово разнесені датчики надходять сигнали з різними допплерівськими частотами, що швидко змінюються під час польоту залежно від геометрії цілі – датчики в трьохмірному просторі. У зв’язку з апріорною невизначеністю щодо різних доплерівських частот сигналів, що знімаються з рознесених у просторі датчиках, виникають суттєві труднощі визначення координат цілі в тривимірному просторі, які на даний час не вирішено. Тому необхідна розробка алгоритмів цифрової обробки сигналів для побудови багатоканальних доплерівських систем просторової спектрально-часової обробки безперервних сигналів.

Метою доповіді є ефективність визначення координат і розпізнавання класів вогнепальної зброї та літальних апаратів, як джерел звукових сигналів.

Для проведення фізичних експериментів розроблений стенд 16-канального запису 12-розрядних сигналів з частотою дискретизації до 44 кГц. В даний час вивчені записи акустичних сигналів, визначені характеристики ряду БпЛА, дронів і літаків. Проблема розв'язана шляхом побудови багатоканальних систем не лише у просторово-часовій області, а також в області доплерівських частот. Розроблені алгоритми обробки сигналів, які показали принципові можливості локації в тривимірному просторі, а також розпізнавання літальних апаратів з урахуванням відмінностей за спектральними характеристики. Розроблено програмне забезпечення призначене для вибору конфігурації системи в залежності від вимог до розміру зони контролю і точності визначення координат. Визначення координат засновано на розрахунках кореляцій від між датчиками, що рознесено на площині або в просторі, для оцінювання часових затримок сигналів від джерел випромінювання. Для спрощення розрахунків координат об'єктів на земній поверхні застосовується дискретизація карти і попередній розрахунок відповідності тимчасових затримок для кожної дискретної точки в декартовій системі координат. Це дозволяє виключити необхідність вирішення системи гіперболічних рівнянь в реальному часі.Створений макет звуколокатора, що призначений для розміщення на наземному роботизованому комплексі, містить 5 датчиків мікрофонного типу.

Встановлено, що для контрольованої зони 500 метрів помилка визначення координат джерела, що рухається, може досягати до 10 метрів. Помилки координат нерухомих джерел імпульсних сигналів приблизно в 2 рази менше. Цього достатньо для подальшого супроводу БпЛА засобами відеомоніторингу.

Остапчук В.М. (ВІТІ ім. Героїв Крут)
Величко В.П. (ВІТІ ім. Героїв Крут)
д.т.н. Сова О.Я. (ВІТІ ім. Героїв Крут)

УДОСКОНАЛЕНИЙ МЕТОД ОБРОБКИ СИГНАЛІВ У БАГАТОАНТЕННИХ СИСТЕМАХ ВІЙСЬКОВОГО РАДІОЗВ'ЯЗКУ

Вступ

Ущільнення частотного діапазону виділеного для роботи спеціальних користувачів, підвищення технологічних можливостей засобів радіозв'язку, зростаючі вимоги до швидкості передачі інформації – все це обумовлює пошук нових рішень для підвищення ефективності використання радіоресурсу. Одним з напрямків підвищення ефективності систем радіозв'язку є застосування методів просторової обробки сигналів у системах радіодоступу, зокрема технології "багато входів-багато виходів" (*Multiple-Input Multiple-Output* – MIMO). Проте мають місце недоліки, пов'язані зі складністю виготовлення багатоантенних систем. Велика кількість радіочастотних трактів в таких системах призводить до збільшення їх розмірів, енергоспоживання та вартості. Складність радіочастотного тракту пропорційна кількості антен. Одним з напрямків вирішення зазначеного питання є застосування методів просторово-часового кодування, що дозволяють сформувати оптимальну кількість логічних каналів в системі MIMO.

Метою дослідження є підвищення оперативності обробки сигналів у багатоантенних системах військового радіозв'язку.

Виклад основного матеріалу дослідження

Метод обробки сигналів в багатоантенних системах військового радіозв'язку складається з наступної послідовності дій:

1. Введення вихідних даних. Вихідними даними є параметри системи MIMO і каналу (кількість передавальних та приймальних антен, кількість ітерацій обробки, розмірність ансамблю сигналів, тривалість кадру на виході демодулятора, канальна матриця).
2. Визначення методу попереднього кодування. Визначається ступінь надлишковості інформації в кожному антенному каналі та виконується процедура зворотнього декодування.
3. Перевірка інформації про кореляційну матрицю каналу. На даному етапі відбувається перевірка наявної інформації про кореляційну матрицю. У разі коли кореляційна матриця відома то відбувається оцінка стану каналу за методом середньоквадратичного відхилення. Якщо ж кореляційна матриця не відома, то відбувається ініціалізація базової кореляційної матриці, оцінка інформаційних символів на кожному кроці та оцінка кореляційної матриці на кожному з кроків.
4. Визначення помилки оцінювання. Відбувається визначення різниці між отриманими значеннями та еталонними.
5. Виведення результатів. Формування кінцевої оцінки стану каналу та формування керуючих впливів.

Висновки

Завадостійкість приймання сигналів в системі MIMO суттєво залежить від вибору методу обробки сигналів на приймальному боці. Існуючі методи обробки сигналів, які забезпечують задану якість передачі інформації, мають високу обчислювальну складність, тому виникає необхідність удосконалення цих методів. Запропоновано удосконалений метод обробки сигналів в системах MIMO, сутність якого полягає у врахуванні характеристик методу попереднього кодування, забезпеченні можливості роботи з відомою та невідомою кореляційною матрицею, розбитті прийнятих сигналів на групи і оцінці кожної групи з урахуванням помилки оцінювання. При обробці сигналу в демодуляторі на кожній ітерації враховується не тільки оцінка, отримана на попередньому кроці, але й ступінь точності оцінювання символів.

Остапчук В.М. (ВІТІ ім.Героїв Крут)
Рудніцька А.А. (ВІТІ ім.Героїв Крут)

АКТУАЛЬНІ ПИТАННЯ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ВІДЕОКОНФЕРЕНЦЗВ'ЯЗКУ НА РІЗНИХ ЛАНКАХ УПРАВЛІННЯ

Актуальність. XXI сторіччя характеризується високою динамічністю та необхідністю прийняття важливих рішень у найкоротші терміни. Світова пандемія COVID – 19 наклала великі обмеження на пересування та спілкування людей, проведення різнобічних заходів, нарад, конкурсів, Хакатонів, зустрічей тощо відбувається у online – режимі. Проблематика даного питання не обігнула й Збройні Сили України. Найбільш ефективним варіантом вирішенням цієї задачі стає організація захищеного відеоконференцзв'язку, що дозволяє не тільки зменшити витрати на організацію відряджень для військовослужбовців, але й відповідно заощадити їх час, який, як ми знаємо, є дуже цінним ресурсом. Сучасна система відеоконференції у військах зв'язку та кібербезпеки Збройних Сил України будується на базі телекомунікаційного обладнання Cisco за підтримки фахівців компаній «Восток». Однією з основних задач даного проєкту є підвищення ефективності роботи.

Мета. Аналіз варіантів організації захищеного відеоконференцзв'язку на різних ланках управління.

Основна частина. Відеоконференцзв'язок є комплексом телекомунікаційних послуг, що дозволяє організувати спілкування великих і малих груп людей, які знаходяться на великій віддаленості. Системи відеоконференцзв'язку використовуються великими приватними та державними компаніями (організаціями) для побудови максимально ефективної системи комунікацій. ВКЗ має велику кількість переваг, та ці переваги активно застосовуються у багатьох сферах життя.

Відеоконференцзв'язок може бути реалізовано як програмними, так і апаратними засобами. Система зв'язку Збройних Сил України є складною та високотехнологічною. Вона має дев'ять взаємопов'язаних складових у польовому і стаціонарному сегменті, які здатні забезпечувати стійке, завадозахищене управління частинами та підрозділами в умовах застосування противником засобів радіоелектронної протидії. Впровадження систем відеоконференцзв'язку у ЗСУ сприяють активному зростанню динамічності та гнучкості управління військами, оптимізації процесу управління на всіх ланках системи управління ЗСУ. Відеоконференцзв'язок у ЗСУ, в першу чергу, призначен для забезпечення управління військами (силами) у повсякденної діяльності та в системі бойової підготовки. Аналіз застосування комплексів відеоконференцзв'язку в системі управління ЗСУ дозволяє виділити такі рівні їх використання: стратегічний, оперативний, тактичний.На стратегічному рівні використовуються комплекси для організації та реалізації функцій управління та забезпечення методом «ланцюга»: МО України →Генеральний штаб ЗСУ →Головний Командний центр ЗСУ→ Озброєння ЗСУ, Логістика ЗСУ, оперативне забезпечення ЗС, Командування видів ЗС та Сил спеціальних операцій. Оперативний рівень системи управління використовує комбінацію стаціонарного та мобільного сегменту відеоконференцзв'язку. Мобільний сегмент відеоконференцзв'язку необхідний органам управління для виконання завдань в польових умовах. Для доведення наказів, розпоряджень, постановки завдань нижчій ланці. застосовуються в першу чергу бездротові технології передачі даних. На тактичному рівні системи управління ЗСУ відеоконференцзв'язк реалізований здебільшого на основі мобільних комплексів.

Висновок. Аналіз основних напрямків розвитку і впровадження комплексів відеоконференцзв'язку в інтересах профільних органів державного управління на прикладі системи управління ЗСУ показує, що система відеоконференцзв'язку здійснює значущий вплив на: швидкість прийняття рішень, якість управління, систему підтримки прийняття рішень в кризових ситуаціях та беззаперечно здійснює значущий вплив на якість функціонування сектору безпеки та оборони України.

Острянська Є. В. (АТ «ІІТ»)
Кандій С.О. (ХНУ ім. В.Н. Каразіна, АТ «ІІТ»)

ГЕНЕРАЦІЯ ЗАГАЛЬНОСИСТЕМНИХ ПАРАМЕТРІВ ДЛЯ СХЕМИ ЕЛЕКТРОННОГО ПІДПИСУ RAINBOW

Актуальність. Однією з основних проблем сучасної криптографії є створення криптографічних схем, які були б безпечними у постквантовий період, тобто були б захищені як від квантових, так і від класичних атак. На даний момент у світі зусилля багатьох дослідників зосереджені на відкритому конкурсі NIST PQC [1], основною ідеєю якого є знаходження такого алгоритму шифрування, який би був стійким до квантових атак і тому міг бути прийнятим у якості нового стандарту. Фіналістами третього етапу конкурсу NIST PQC стали три схеми ЕП: Crystals-Dilithium, Falcon, на основі алгебраїчних решіток та Rainbow на основі багатовимірних перетворень. У даній роботі особлива увага була приділена схемі електронного підпису Rainbow.

Постановка задачі. Розглянути схему електронного підпису Rainbow, а саме проведення первинного аналізу відомих атак і встановлення обмежень та розробка алгоритмів генерації загальносистемних параметрів для 384 і 512 біт безпеки.

Основні положення. Rainbow є узагальненням структури UOV [5].Теоретична безпека Rainbow базується на тому, що вирішення набору випадкових багатовимірних квадратичних систем є NP-складною проблемою [6]. Rainbow заявляє стійкість EUF-CMA. Далі розглянемо основні атаки на схему Rainbow.

Прямі атаки. Найбільш прямолінійною атакою на багатовимірну схему Rainbow, є пряма алгебраїчна атака, в якій загальновідоме рівняння $\mathrm{P}(\mathbf{z})=\mathbf{h}$ розглядається як проблема MQ. Оскільки Rainbow – це невизначена система з $n\approx 1.5\cdot m$ рівнянь, найефективнішим способом вирішення цієї системи є фіксація $n-m$ змінних для створення детермінованої системи. Можна очікувати, що отримана детермінована система має рівно одне рішення. Складність вирішення такої системи з m квадратних рівнянь у m змінних можна оцінити (1)

$$\mathrm{Complexity}_{\mathrm{direct;classical}}=\min_k\left(q^k\cdot 3\cdot\binom{m-k+d_{reg}}{d_{reg}}^2\cdot\binom{m-k}{2}\right), \tag{1}$$

де d_{reg} – це так звана ступінь регулярності системи.

Атака MinRank. Під час атаки MinRank криптоаналітик намагається знайти лінійну комбінацію загальновідомих поліномів мінімального рангу. У випадку з Rainbow така лінійна комбінація рангу υ_2 відповідає лінійній комбінації центральних поліномів першого рівня. Таким чином, знаходячи o_1 цих лінійних комбінацій низького рангу, можна ідентифікувати центральні поліноми першого рівня та відновити еквівалентний секретний ключ Rainbow. На сьогодні найбільш ефективний метод вирішення проблеми MinRank був запропонований у [4], в результаті якого отримуємо складність (2)

$$\mathrm{Complexity}_{\mathrm{MinRank}}=3\cdot\left(\left(\left(o_2+1\right)\cdot\binom{n'}{r}\right)^2\cdot\left(r+1\right)\cdot\left(o_2+1\right)\right). \tag{2}$$

Атака HighRank. Метою атаки HighRank [5] є виявлення (у лінійному представленні) змінних, що з'являються найменшу кількість разів у центральних поліномах (вони відповідають Oil-змінним останнього рівня Rainbow, тобто змінним x_i з $i\in O_u$). Складність цієї атаки можна оцінити за допомогою (3)

$$\mathrm{Complexity}_{\mathrm{HighRank;\ classical}}=q^{o_u}\cdot\frac{n^3}{6}. \tag{3}$$

*UOV атака.*Оскільки Rainbow можна розглядати як продовження добре відомої схеми підпису Oil та Vinegar [2], її можна атакувати, використовуючи всі відомі атаки UOV [6].

Можна розглядати Rainbow як екземпляр UOV з $\upsilon = \upsilon_1 + o_1$ та $o = o_2$. Метою даної атаки є пошук попереднього відображення так званого Oil підпростору O афінного перетворення T, де $\mathrm{O} = \left\{ \mathbf{x} \in \mathrm{F}^n : x_1 = \cdots = x_\upsilon = 0 \right\}$. Знаходження цього простору дозволяє відокремити Oil від змінних Vinegar та відновити закритий ключ. Складність цієї атаки можна оцінити за допомогою (4) множень у полі

$$\mathrm{Complexity}_{\text{UOV-Attack; classical}} = q^{n-2o_2-1} \cdot o_2^4 . \tag{4}$$

*RBS атака.*Атака RBS [7] спрямована на пошук лінійних відображень S і T, що перетворюють загальновідомі поліноми в поліноми форми Rainbow. Для цього криптоаналітик повинен вирішити кілька нелінійних багатовимірних систем. Складність цього кроку визначається складністю вирішення першої (і найбільшої) з цих систем, яка складається з $n+m-1$ квадратних рівнянь з n змінними і можна оцінити як (5), де $\mathrm{M}_{\alpha,\beta}$ позначає кількість одночленів (α, β)

$$Compl_{RBS} = \min_{\alpha,\beta} 3 \cdot \mathrm{M}_{\alpha,\beta}(t,s)^2 \cdot (n_x + 1) \cdot (n_y + 1). \tag{5}$$

Генерація параметрів для 384 та 512 біт стійкості. В результаті аналізу наведених вище атак під час вибору параметрів керувалися наступними умовами:

- Кількість рівнянь, що нам необхідна, залежить від складності прямої атаки та атаки на геш-функцію;
- Кількість змінних залежить від складності атак RBS, UOV та HighRank.

Тож, якщо підсумувати вище сказане, то знайти параметри υ_1, o_1, o_2 при $q = 256$, тобто $GF(q) = GF(256)$ можливо з умов (1)-(5). На основі цього було розроблене програмне забезпечення, з використанням якого були згенеровані параметри υ_1, o_1 та o_2 для схеми ЕП Rainbow для 384 та 512 біт безпеки, що наведені в таблиці 1.

Табл. 1 Основні загальносистемні параметри Rainbow для 384, 512 біт безпеки

Безпека	υ_1	o_1	o_2	$GF(q)$
384	192	48	136	$GF(256)$
512	272	120	128	$GF(256)$

Висновки. В результаті було зроблено висновки, що головним недоліком Rainbow є великий розмір відкритих ключів, а перевагою – дуже малі підписи лише в кілька сотень бітів. Також було розглянуто низку атак на схему ЕП Rainbow. Хоча пряма атака є атакою підробки підпису, яка повинна виконуватися для кожного повідомлення окремо, атаки MinRank, HighRank, UOV та RBS є ключовими атаками відновлення. Після відновлення секретного ключа Rainbow за допомогою однієї з цих атак криптоаналітик може виробляти підписи так само, як законний користувач. Також нами були запропоновані набори загальносистемних параметрів для 384 та 512 біт безпеки: (GF(256), 192, 48, 136) та (GF(256), 272, 120, 128) відповідно.

Список використаних джерел.

1. PQC Standardization Process: Third Round Candidate Announcement. July 22, 2020.
2. A. Kipnis, J. Patarin, L. Goubin: Unbalanced Oil and Vinegar schemes. EUROCRYPT 1999, LNCS vol. 1592, pp. 206-222. Springer, 1999.
3. Rainbow Signature/Ding J.,anoth.2020.P.6-21.//–Режим доступ: https://www.pqcrainbow.org/.
4. Algebraic attacks for solving the Rank Decoding and MinRank problems without Groebner basis / M. Bardet, and other. 2020. CoRR abs/2002.08322.
5. D. Coppersmith, J. Stern, S. Vaudenay: Attacks on the birational signature scheme. CRYPTO 1994, LNCS vol. 773, pp. 435-443. Springer, 1994.
6. A. Kipnis, A. Shamir: Cryptanalysis of the Oil and Vinegar signature scheme. CRYPTO 1998, LNCS vol. 1462, pp. 257-266. Springer, 1998.

Паламарчук С.А. (ВІТІ)
Паламарчук Н.А. (ВІТІ)
Фіненко Ю.І. (ПрАТ Укртелеком)

ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ КАНАЛІВ КІБЕРЗАГРОЗ

Наразі спостерігається новий і небезпечний тренд: все більше і більше шкідливого програмного забезпечення (ПЗ) та засобів кібершпигунства вдаються до використання стеганографії для приховування каналів кіберзагроз. На сьогоднішній день, більшість антивірусних систем не захищають від стеганографії або захищають слабко, між тим, потрібно розуміти, що кожен заповнений контейнер може бути небезпечним.

У ньому можуть бути приховані дані, які ексфільтруються шпигунським ПЗ, він може містити комунікацію шкідливого ПЗ з командним центром або нові модулі шкідливого ПЗ. Серед інструментів для проникнення у внутрішню мережу часто використовуються точкові розсилки фішингових листів з стеганографічними вкладеннями, вразливості RDP підключень, тощо.

Відомо, що середньостатичний час отримання повного контролю над захищеною мережею – до 10 хвилин.

При розслідуванні кіберінцидентів, важливо знати якими каналами потрапила в систему загроза, що спричинила збій в роботі, чи потрапила прихована кіберзагроза взагалі, які деструктивні дії вона здатна виконати, та ін.

Одним з таких прихованих каналів є зображення, як носій шкідливого коду, який не ідентифікується системою захисту. Спільне використання методів стеганографічного аналізу і машинного навчання дозволить ефективніше виявляти приховані загрози інформаційним системам. Пристосованість існуючих методів та алгоритмів пошуку і аналізу прихованих кіберзагроз до методів машинного навчання є невеликою, відповідно, тематика дослідження є актуальною.

Для вирішення завдання ефективного захисту перспективним вбачається використання потенціалу інтелектуальних систем підтримки прийняття рішень (СППР) або експертних систем (ЕС). СППР і ЕС здатні в достатній мірі взяти на себе рутинні завдання, особливо при аналізі великого об’єму інформації в різнорідних базах даних і файлових сховищах, коли мова йде про слабоструктуровані ознаки загроз і кібератак.

Побудова надійної системи захисту інформації часто залежить від правильного виявлення (розпізнавання) та оцінки кіберзагроз, з подальшою актуалізацією більш вразливих з точки зору кібербезпеки. Одним з найбільш перспективних підходів для виявлення факту існування та передачі прихованих кіберзагроз є підхід, який представляє процес приховування шкідливого вкладення, та полягає в дослідженні статистичних закономірностей природних контейнерів. При цьому підході аналізуються статистичні характеристики послідовностей, що досліджуються та визначаються чи схожі вони з характеристиками природних контейнерів, якщо так, то прихованої інформації немає або навпаки.

Класифікатори, що використовуються при аналізі вхідних даних, будуються на основі машинного навчання з бази даних, що містить велику кількість інформації, яка попередньо класифікована за наявністю в ній прихованої інформації.

Стеганографічний аналіз є одним з підвидів статистичних моделей аналізу кіберзагроз, і який може входити як складова частина в СППР і ЕС. Імовірнісний характер статистичних методів стегоаналізу не є істотним недоліком, так як на практиці ці методи часто видають оцінки ймовірності існування кіберзагрози, що відрізняються від одиниці або нуля на нескінченно малі величини. Звернемо увагу, що всі методи аналізу кіберзагроз не виносять бінарного вердикту “містить цей контейнер приховану кіберзагрозу”, замість цього визначається приблизний % прихованої кіберзагрози.

В ході досліджень великої кількості класифікованих об’єктів (2000 природних зображень) з різним ступенем наповненості прихованої інформації виявлено закономірність, яка полягає в тому, що чим більший % заповнення контейнера прихованою інформацією, тим статистичні характеристики (математичне очікування, дисперсія, середньоквадратичне відхилення) істотно відрізняються від математичного аналогу природного зображення (дослідження проводились методом LSB, заповнення глибиною 1 та 2 біт та з % заповнення 1-100%).

Наразі, проводяться дослідження можливості виведення більш кращого математичного аналогу наближеного до природного зображення, при цьому, використовується навчання нейронної мережі.

Висновки. Аналіз кіберзагроз це динамічно змінний процес. Через щоденне збільшення інформації та знань, виявлення та нейтралізація прихованих кіберзагроз стає все більш складною задачею.

На допомогу у вирішенні задачі аналізу великих об’ємів інформації приходять методи машинного навчання та штучного інтелекту. Результати, отримані на даному етапі дослідження, дозволяють зробити припущення про те, чи наявні приховані загрози в інформаційних системах, і відповідно, зменшити ймовірність помилкового спрацювання систем захисту в комплексі з іншими методами аналізу/захисту.

В подальшому, доцільно провести дослідження стеганозображень за статистичними характеристиками, більш точного навчання нейронної мережі та відповідно, удосконалення механізму виявлення прихованих каналів кіберзагроз.

.

Пантась І.О. (ВІТІ ім. Г. Крут)
Масесов М.О. (ВІТІ ім. Г. Крут)

ВИБІР ПОКАЗНИКІВ ТА КРИТЕРІЇВ ЖИВУЧОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Для проектування або оптимізації існуючих телекомунікаційних систем та мереж висувається сукупність вимог – критеріїв ефективності ТКМ та ТКС, тобто умов, згідно яких приймається рішення щодо ефективності функціонування мережі. Дані критерії поділяються на три групи – критерії якості і надійності функціонування, економічні критерії, критерії живучості.

У випадку телекомунікаційних систем та мереж спеціального призначення, в функціонуванні яких в першу чергу є важливим забезпечення гарантованої роботи в складних умовах та непередбачуваних несприятливих впливах, першочерговою є група критеріїв, по яким проводяться розрахунки живучості даних систем та мереж.

До основних показників живучості можна віднести такі:

показник ймовірності того, що мережа збереже свій стан відновлення протягом заданого часу;

показник невразливості;

умовний закон невраження, який характеризує динаміку збереження системою працездатного стану при кількості впливів рівному деякому параметру;

умовний закон невраження структури, який характеризує динаміку збереження системою працездатного стану при послідовному видаленні елементів;

кількість впливів, при якій система втрачає можливості;

середня кількість видалених з структури елементів, при якому вона втрачає стан працездатності.

Основні критерії живучості:

критерій відповідності мережі заданим показникам якості й оцінки ступеню її функціонування;

критерій оцінки ефективності реконфігурації й оптимального перерозподілу ресурсів;

критерій динаміки відновлення після збоїв;

критерій, який характеризує зміни продуктивності та швидкості передачі інформації в мережі при виконання різноманітних дій в умовах деградації мережі;

критерій структурної живучості;

критерій функціональної живучості.

Забезпечення необхідного рівня живучості є однією з найважливіших та актуальних умов при вирішенні задач щодо проектування, реконфігурації телекомунікаційної системи або мережі та при перерозподілі ресурсів в них. Вибір критеріїв, згідно яких будуть проводитись подальші розрахунки живучості, напряму залежить від задачі, яку необхідно розв’язати.

Особливу увагу необхідно звернути на динаміку змін характеру і якості несприятливих впливів, які з часом змінюються, модернізуються та приймають абсолютно нові форми.

Виходячи з вищезазначеного, в теперішній час необхідно приділити увагу удосконаленню методів та методик розрахунку живучості ТКС та ТКМ спеціального призначення з врахуванням активної модернізації підходів до організації зв’язку, самої техніки зв’язку, широкого розповсюдження такого класу техніки як БПЛА, а також з врахуванням сучасних несприятливих впливів – кібератаки, шкідливе програмне забезпечення, електромагнітна зброя.

Парнюк І.О. (ВІТІ)
Дем’яненко А.Д. (ВІТІ)
Тітаренко А.В. (ВІТІ)

АНАЛІЗ МАСШТАБОВАНОСТІ ELASTICSEARCH ПРИ ВИКОРИСТАННІ ВЕЛИКИХ МАСИВІВ ДАНИХ У ВІЙСЬКОВИХ АСУ

Актуальність. Необхідність масштабованості при обробці дійсно великих масивів даних у військових АСУ.

Мета. Проаналізувати можливість масштабованості ELASTICSEARCH при використанні великих масивів даних.

Основні положення. Як би ми не намагалися оптимізувати структури даних та алгоритми пошуку, коли мова заходить про справді великі масиви даних і справді велику кількість запитів, необхідно задуматися про можливість вплинути на продуктивність системи шляхом збільшення апаратного ресурсу. Простіше кажучи, ми хочемо мати можливість додати пам’яті, ЦП та дискового простору, щоб усе діяло швидше. Ми можемо назвати це масштабованістю.

Найпростіший варіант – додати обладнання на сервер. Таке масштабування називається вертикальним.

Другий варіант – розділити наші завдання на групу серверів. У цьому випадку ми теж збільшуємо апаратний ресурс, але ми розподіляємо його у площині, тобто горизонтально.

Схема зберігання даних

Те, які дії з даними ми будемо визначати схему їх зберігання:

- швидше за все пошукова система повинна буде швидко проводити пошук;
- запис та видалення можуть не відрізнятися високою швидкістю, в системах пошуку, вважається, цим можна знехтувати;
- структура даних інтенсивно змінюватиметься і сховище може заповнюватися з кількох незалежних джерел.

Уявіть ще раз, скільки атрибутів може мати публікація і скільки пов’язаних з нею об’єктів. Автор, категорія, спільнота, геомітки, медіафайли, теги, пов'язані публікації. Цей перелік можна продовжувати до вичерпання фантазії. Якщо ми зберігаємо це у звичній реляційній базі, то маємо мільйон зв’язків і мільярд атрибутів. Це чудово підходить для структурованого зберігання довгі роки, але не дуже в’яжеться із вимогами швидкого пошуку.

А якщо ми захочемо додати пару інтеграцій із зовнішніми системами? Доведеться реалізувати додаткові таблиці або навіть бази. Нам завжди потрібно щось додати або змінити в об’єктах доступних для пошуку.

Висновок.

1. Вертикальний спосіб гарантує нам швидкий результат, але, як довго ми можемо збільшувати ресурс окремого сервера? По-перше, дешевим способом це буде тільки на самому початку, далі оплата одного сервера буде коштувати як кілька АРМів. По-друге, критичний збій в одній машині спричинить збій усієї системи. На відміну від вертикального способу, горизонтальний не накладає таких явних обмежень, ми можемо додавати сервера скільки завгодно, зв’язуючи їх мережею. Звичайно, це спричинить мережеві витрати – низьку швидкість передачі в мережі (у порівнянні з обробкою на одній машині), мережевий оверхед. Але разом з тим мережа має одну дуже важливу властивість – велику стійкість до відмов.
2. Набагато швидше читати з об’єктів, що містять все необхідне тут і зараз. І набагато простіше вносити зміни до неструктурованої схеми даних. Ці об’єкти ми можемо сприймати як окремі сторінки, файли, картки, це можна назвати деякими документами. Тому така модель зберігання даних називається документоорієнтованою.

Пивоварчук С.А. (ВІТІ ім. Героїв Крут)
Стовба Є.М. (ВІТІ ім. Героїв Крут)

ОРГАНІЗАЦІЯ ЗВ'ЯЗКУ СУЧАСНИМИ ЗАСОБАМИ В ТАКТИЧНІЙ ЛАНЦІ УПРАВЛІННЯ З УРАХУВАННЯМ ДОСВІДУ В ООС

Локальні війни, воєнні конфлікти і бойові дії різної інтенсивності протягом останніх років, які відбувалися в різних куточках земної кулі, свідчать про зростання динамічної зміни обстановки в зоні ведення бойових дій та необхідність жорсткого виконання вимог щодо стійкого, безперервного, оперативного і скритого управління військами під час виконання ними бойових завдань. Виконання вказаних вимог неможливо без удосконалення процесу зв'язку та інформаційних систем під час підготовки та проведення операцій і пов'язано з необхідністю обробки значних обсягів різнорідної інформації в стислі терміни.

Таким чином, розвиток системи зв'язку Збройних Сил України, з урахуванням впровадження в наше життя сучасних ІТ-технологій, є складним процесом.Тому сучасні системи управління навіть на даному етапі відчувають необхідність у розвитку та модернізації, а також забезпечення виконання вимог щодо своєчасності, достовірності та безпеки інформаційного обміну.

Можливості цифрових засобів зв'язку, сучасних інформаційних технологій, які використовувалися та використовуються у Збройних Силах передових країн світу, розгляд етапів застосування цих засобів, технологій та тенденцій їх впровадження в Збройних Силах України дозволили виокремити основні найбільш доцільні напрямки їх подальшого впровадження під час побудови сучасної системи управління військами Збройних Сил України. З початку операції Об'єднаних сил (раніше – АТО) керівництвом Збройних Сил України прийнято рішення щодо використання комплексних апаратних зв'язку для забезпечення зв'язку, автоматичної комутації та маршрутизації цифрових потоків між комплексними апаратними вузлів зв'язку пунктів управління, вузлами зв'язку пунктів управління вищестоящих штабів і підпорядкованих підрозділів, для організації (розгортання) абонентських мереж телефонного зв'язку і передачі даних, управління мережею зв'язку, надання телекомунікаційних послуг оперативному складу на пункті управління всіх ланок управління Збройних Сил, інших військових формувань і правоохоронних органів спеціального призначення в усіх видах бою, спеціальних операціях, а також в умовах мирного часу по каналах, які утворюються різними засобами зв'язку.

Особливості та основні тактико-технічні характеристики обладнання комплексних апаратних зв'язку відповідають встановленим вимогам щодо забезпечення зв'язку.

Позитивний досвід:

функціонування автоматизованих робочих місць (оператора комплексної апаратної зв'язку і оператора управління системою зв'язку), обладнаних засобами телефонного та службового зв'язку а також ПЕОМ з відповідним програмним забезпеченням;

розгортання проводових ліній зв'язку з інтерфейсами G.703;

розгортання проводових ліній зв'язку стандарту SHDSL;

розгортання ліній зв'язку з використанням польового волоконно-оптичного кабелю;

розгортання відкритої телефонної мережі;

розгортання закритої телефонної мережі (МОСІ, ЗСОІ);

розгортання мереж передачі даних для подальшої організації відкритого (СІДО) і засекреченого (МОСІ, ЛАВИНА) зв'язку;

об'єднання та підтримка функціонування локальних обчислювальних мереж на пункті управління (КШМ, намети, штабні машини, бронеоб'єктів);

маршрутизацію потоків даних, об'єднання автоматизованих робочих місць в локальну обчислювальну мережу.

забезпечення захищеного відеоконференцзв'язку.

Також залежно від побудови системи управління підрозділами, особливості їх дій та інших факторів підрозділи тактичної ланки управління забезпечуються наступними

радіозасобами УКХ радіозв’язку Harris − RF-7800V-HH, RF-7800M-MP, RF-7850M-HH, RF-7800V-VS511, RF-7800V-VS501 тощо. Основним режимом роботи цих радіозасобів є режим передачі даних для відображення обстановки, що склалась, обміну командами управління, функціонування системи управління в режимі реального часу.За допомогою радіостанцій RF-7800H-MP (потужністю 20 Вт), а також RF-7800H-MP потужністю 150 Вт, організується радіозв’язок з вищим штабом від батальйону і вище. У випадку застосування противником засобів радіоелектронної боротьби канали мережі транкінгового зв’язку Mototrbo, можуть бути легко придушені. Тому КХ зв’язок за допомогою радіостанцій RF-7800H-MP у режимі ППРЧ може залишитись єдиним можливим способом забезпечення зв’язку. Однією з переваг цих радіостанцій є можливість отримання багатьох функцій і сервісів в одному компактному корпусі і можливість виконати роботу, для якої раніше вимагалося декілька радіостанцій.

В інтересах підрозділів, які виконують завдання в районі проведення операції об’єднаних сил на пунктах управління знайшло широке використання станцій супутникового зв’язку, що є на даний час основною складовою польової системи зв’язку тактичної ланки управління.Застосування системи “Tooway” дозволяє забезпечити ефективні, захищені, інтерактивні лінії зв’язку високої якості за технологією Ethernet з віддаленими пунктами управління.

Переносні станції супутникового зв’язку дозволяють організувати:

первинний канал передачі даних;

розгортання локальної мережі до трьох автоматизованих робочих місць;

підключення двох телефонних апаратів.

Затребуваність супутникового зв’язку підрозділами пояснюється його загальними перевагам такі, як:

велика пропускна здатність;

можливість обслуговування абонентів у важкодоступних районах;

забезпечення зв’язку між станціями розташованих на дуже великих відстанях; можливість побудови мережі без фізично реалізованих комутаційних пристроях.

Ця можливість пов’язана зі значним економічним ефектом, який може бути отриманий в порівнянні з використанням звичайної несупутникової мережі, заснованої на численних фізичних лініях зв’язку і комутаційних пристроях.

Також, під час проведення ООС знайшли широке використання комплекси УКХ транкінгового зв'язку компанії “Motorola”, які характеризуються високою якістю і функціональними можливостями. Ефективність застосування цих засобів пов’язана, насамперед, з невеликими габаритами і стійкістю до перешкод, можливістю технічного маскування під час ведення радіообміну.Система Mototrbo відповідає європейському стандарту DMR. В ній реалізована технологія TDMA, яка забезпечує високу ефективність використання радіочастотного ресурсу шляхом створення двох логічних розмовних каналів (два часових слоти) в межах одного фізичного каналу.

Основні функціональні можливості цифроаналогової системи радіозв’язку Mototrbo:

блокування радіостанції (будь-яка радіостанція може бути дистанційно заблокована, наприклад, у разі крадіжки);

телеметрія (передача телеметричних даних);

телефонні виклики (напівдуплексні виклики абонентів телефонної мережі);

сканування (сканування як цифрових, так і аналогових каналів);

передача GPS координат (радіостанція має вбудований GPS-приймач, координати передаються по радіоканалу);

програмування через радіоефір (віддалене програмування радіостанцій та ретрансляторів);

оповіщення про виклик (індикація та тонове оповіщення про вихідний виклик);

шифрування (може бути використаний один з видів шифрування: базовий, розширений чи AES);

системні рішення (IP site connect, capacity plus, linked capacity plus, connect plus).

D. Pishenina (Viti named Heroes of Kruty)

ANALYSIS OF THE OPPORTUNITY OF APPLICATION OF THE CORPORATE NETWORK ON THE BASIS OF PON TECHNOLOGY

Actuality. Optical access networks in the last few years have become one of the most actively developed segments in the field of telecommunications.

There are many reasons for this, ranging from the fact that they mean working with the provision of operator services to a large number of subscribers. Technologies in this area are improving year by year, as well as technical solutions - all in order to meet the growing demands of customers.

If many people have already switched to "optics" in the field of transport networks, access networks are still lagging behind in terms of the degree of innovation implementation. However, the existing infrastructure of the Network does not lag behind the growing demands of consumers. If we want to clarify this issue, we must first determine how much information we want to convey to users, and what it will look like.

Formulation of the problem. To analyze the construction of a corporate network based on PON technology.

Substantive provisions. Today, laying OK for the organization of the access network has become profitable when upgrading the old, and when building new access networks. There are many options for choosing fiber-optic access technology. Along with traditional solutions based on optical modems, optical Ethernet, Micro SDH technology, new solutions have emerged using the architecture of passive optical networks PON.

A passive optical network (PON) is a fiber-optic network that uses a point-to-multipoint topology and an optical connection to deliver data from a single transmission point to multiple user endpoints. In this context, the liability refers to the unprotected state of the fiber and its components.

The main idea of the PON architecture is to use only one transceiver module in the central OLT node to transmit information to multiple ONT subscriber devices and receive information from them. The number of ONT subscriber nodes connected to one OLT transceiver may be as large as the power budget and maximum speed of the transceiver allow.

To transmit a stream of information from OLT to ONT - direct stream, usually using a wavelength of 1550 nm. On the contrary, data streams from different subscriber nodes to the Central node, together forming a reverse (uplink) stream, are transmitted at a wavelength of 1310 nm. OLT and ONT have built-in WDM multiplexers that separate output and input streams.

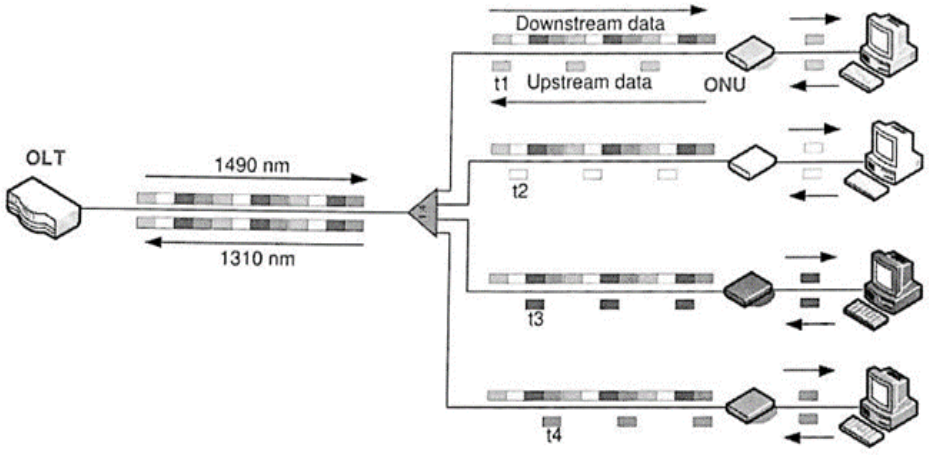


Figure 1 Principles of PON technology

Direct flow at the level of optical signals is broadcast. Each subscriber node

ONT, reading the address fields, selects from the total flow assigned only to him part of the information. In fact, we are dealing with a distributed demultiplexer;

In order to calculate the amount of use of cable, dividers, subscribers, welded joints, it is necessary to develop an analysis of the graphical position of subscribers.

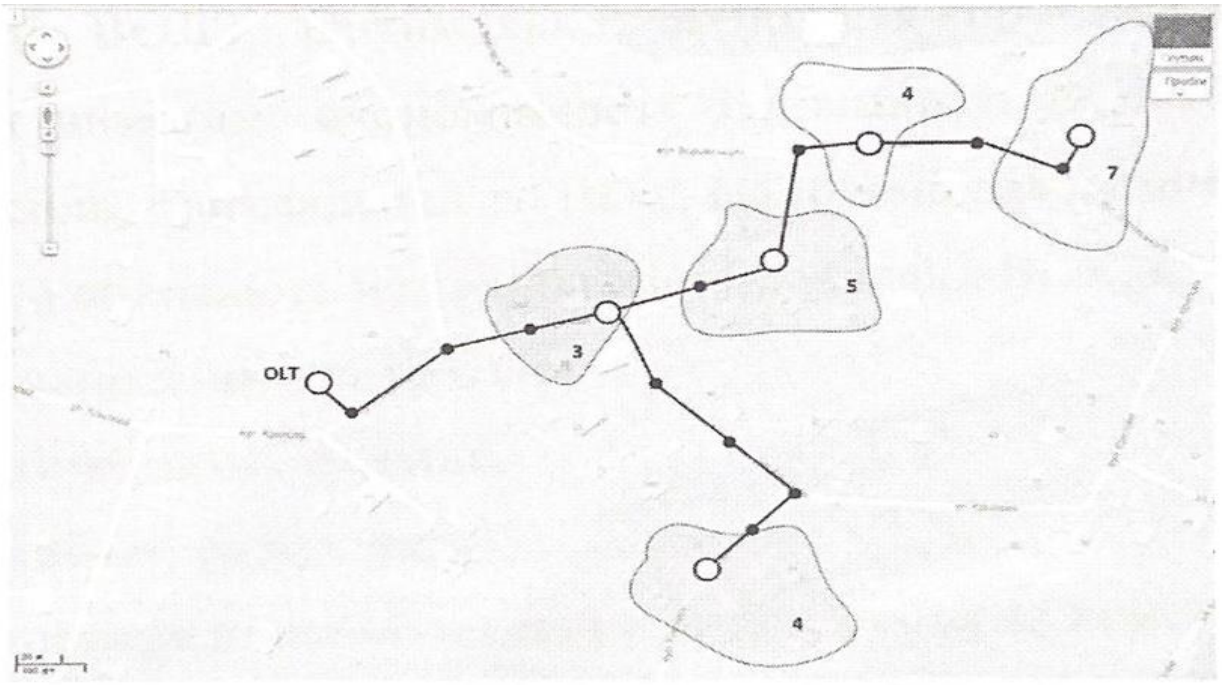


Figure 2 Geographical location of subscribers

Calculation of the loss budget for each subscriber terminal taking into account the losses in all elements of the chain, comparing it with the dynamic range of the system. Due to the fact that the subscribers are at a different distance from the main station, then, with a uniform distribution of power in each splitter, the power at the input of each ONU will be different. The selection of splitter parameters is associated with the need to obtain at the input of each subscriber terminal network approximately the same level of optical power, ie to build a so-called balanced network. If you need to determine the losses of splitters with a large number of output or use at other partition coefficients, you can use the estimation formula:

$$A_i = 101_g\left(\frac{100\%}{D\%}\right) + log2(N-1)\cdot 0{,}4 + 0{,}2 + 1{,}5\cdot \lg(\frac{100\%}{D\%}),\ [\text{дБ}]$$

where D% is the percentage of power output to this port,%; N is the number of output ports; and - source port number.

Now it is possible to pass to a choice of coefficients of division of splitters for the concrete project and calculation of the budget of losses. Losses between OLT and ONT For each optical line we present all losses in the line as the sum of the attenuated all components:

$$A_\Sigma = (1_1 + +1_1)\cdot\alpha + N_p\cdot A_p\cdot + N_c\cdot A_c + (A_{\text{раз}} + A_{\text{раз}}),[\text{дБ}]$$

where AΣ - total losses in the line (between OLT and ONU), dB; li- length of i-section, km; n is the number of plots; a - attenuation coefficient of the optical cable, dB / km% 3 NP - the number of detachable connections; AR - average losses in the detachable connection, dB;

NC - number of welded joints; AS - average losses in the welded joint, AB3B ARAZ and - losses in the i-optical splitter, dB;

The first term refers to the total losses in the optical cable, the second - to the losses in the connectors, the third - to the losses in welding, and the fourth loss in the splitters. After that, the attenuation is calculated for each circuit (from OLT to ONU) for the first three terms and the splitter distribution coefficient is selected so that the attenuation in each circuit is approximately the same. The calculation of the loss budget must prove that for each chain the total amount of losses (including stock) does not exceed the dynamic range of the system, ie:

$$P = P_{\text{ВИХ}_{min}} - P_{\text{ВХ}} \geq A_{\Sigma} + P_{\text{ЗАП}}$$

where P is the dynamic diameter PON, dB; RVIH min - minimum output power of the OLT transmitter, dBm; RVH - allowable power at the input of the receiver ONU, dBm; A2 - total line loss (between OLT and ONU), dB; RZAP-operational stock PON, dB.

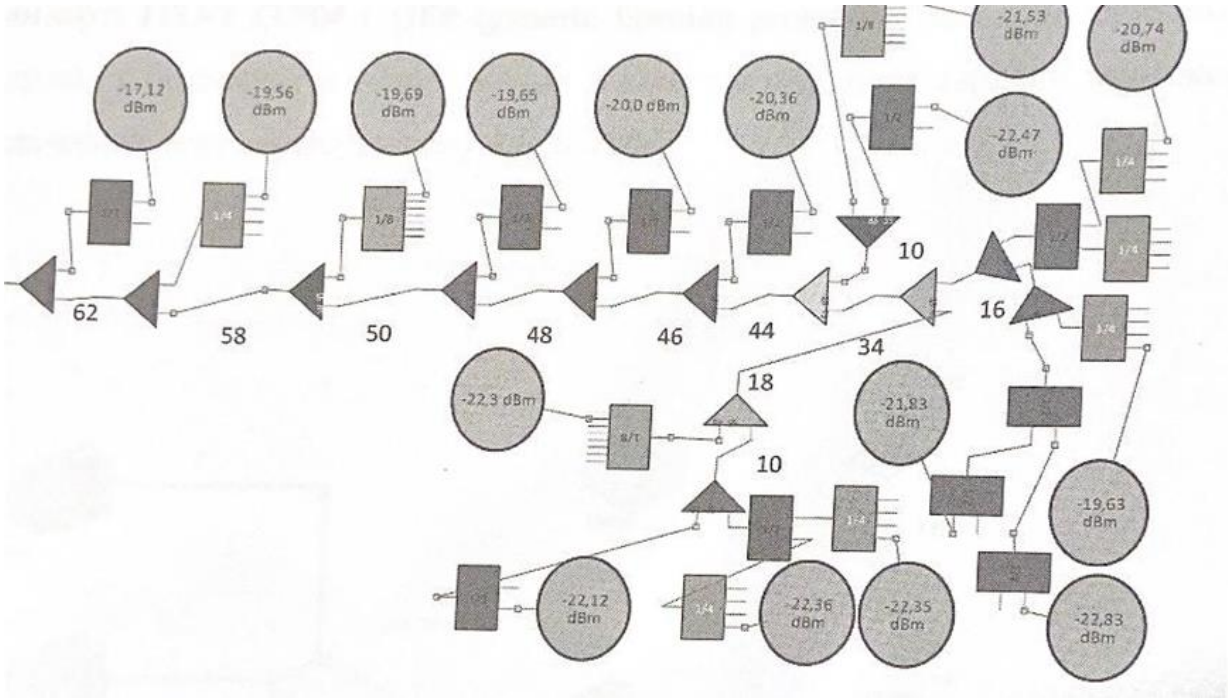


Figure 3 Option to build a network

The figure shows a schematic network RON whose power budget is divided into 64 subscribers, when using measuring devices, network attenuation is a difference of 5dBm, which provides data transmission in the network.

Conclusion. Fiber-optic transmission has become one of the most exciting and rapidly improving areas in telecommunications. In fact, it is a relatively simple technology. Compared to cable, microwave and radio communication systems, fiber optic communication systems are much easier to design and build.

Погребняк С.В. (ВІТІ ім. Героїв Крут)
Яровий В.С. (ВІТІ ім. Героїв Крут)

ХІМІЧНІ ПРОЦЕСИ В ЕЛЕКТРОЛІТИЧНИХ КОНДЕНСАТОРАХ БЛОКІВ ЖИВЛЕННЯ СУЧАСНОГО ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

Актуальність.ВЗбройних Силах України активно здійснюється перехід на новітні зразки озброєння та військової техніки, які відповідають стандартам країн-НАТО. На озброєння надходять зразки іноземного виробництва. Особливо це стало відчутно на прикладі систем зв'язку та автоматизації управління військами. Епоха цифрового зв'язку та найрізноманітніших "розумних" мереж управління обумовлена концепцію створення С4ISR. При цьому потрібно розуміти, що елементна база подібного устаткування постачається вузько профільними виробниками з усього світу в умовах конкуренції та економічної доцільності (вигоди). Це однозначно відбивається на якості устаткування.

До складу телекомунікаційного обладнання обов'язково входить блок живлення (джерело перетворення промислової напруги, стаціонарноїелектромережічи автономних джерел електроенергії).Основусучасного блоку живлення становить імпульсна схема перетворювача напругі і складається з пасивних радіоелектронних компонентів (трансформатори, котушки індуктивності, резистори та конденсатори) та активних компонентів (біполярних і польових транзисторів, напівпровідникових схем).

Постановка задачі. Проведені дослідження та зібрані статистичні дані за період проведення антитерористичної операції та операції об'єднаних сил вказують на стійкий тренд виходу з ладу малонадійних компонентів: напівпровідникові діоди Шотки та електролітичні конденсатори. При чому переважна більшість (70-80%) всіх зареєстрованих відмов радіоелектронної апаратури пов'язані з експлуатацією понад встановлені часові показники,що спричиняє підвищення нормальної робочої температури до критичних і навіть понад критичних значень.

Основні положення. Наслідком підвищення експлуатаційної температури радіоелектронних компонентів стають теплові та лавиноподібні пробої. Як відомо однією з основних негативних характеристик діодів Шотки є підвищені зворотні струми, які зростають з підвищенням температури кристала і мають незворотні наслідки для цього радіоелектронного компоненту.Не винятком є і електролітичний конденсатор який так само піддається впливу температури. Критичні значення температурних показників для електролітичних конденсаторів варіюються від декількох десятків до сотень градусів в залежності від типу конденсатора. Робота спрямована на дослідження впливу температури на хімічні процеси в електролітичних конденсаторах, визначення їхнього технічного стану безконтактними методами неруйнівного контролю. Відомо що ряд основних характеристик електролітичного конденсатора має пряму залежність від температури серед них температурний коефіцієнт ємності (ТКЄ), еквівалентний послідовний опір (ESR) та струм витоку. (R_{LEAK}). Один з найважливіших ТКЄ — це параметр, який характеризує залежність ємності конденсатора від температури. Практично ТКЄ визначають як відношення зміни ємності конденсатора при зміні температури на 1°С. Це обумовлено неоднорідністю протікання хімічних процесів в електролітах та діелектриках за різних температур. Розглянемо більш докладно ці залежності.Закон Джоуля – Ленца дає кількісну оцінку теплового впливу електричного струму:

$$dQ = I^2\,Rdt;$$

деdQ – кількість тепла яка виділяється за одиницю часуdt; I – струм пульсації конденсатора, а $R = ESR$.Виходячи з викладеного саме параметр ESR сприяє виділенню основної кількості тепла під час експлуатації конденсатора. В свою чергу саме тепло знижує надійність конденсатора через висихання електроліту і їх деградацію через порушення в ізолюючому оксидному шарі. В розчинах електролітів процес дисоціації протікає не безповоротно тому до нього може бути застосовано закон діючих мас. Як відомо з курсу електрохімії всі

електроліти поділяються на дві великі групи “сильні” та “слабкі”. Різниця між ними полягає в ступені дисоціації. Ступінь дисоціації – це відношення кількості молекул, що розпалися на іони до загальної кількості молекул електроліту до дисоціації.

Якщо кількість дисоційованих молекул позначити літерою n, а загальну кількість молекул у розчині – N, то ступінь дисоціації α (альфа) можна обчислити за формулою:

$$\alpha = \frac{n}{N} \text{або} \quad \alpha = \frac{n}{N} * 100\%;$$

електроліти зі ступеню дисоціації від від 0,3 до 1 називаються “сильним”, електроліт зі ступеню дисоціації меншим 0,3 називають “слабким”.

Якщо в якості електроліту в електролітичних конденсаторах використовуються “сильні” електроліти (в розчинах сильних електролітів в наслідок їх повної дисоціації концентрація іонів максимально велика) то вони здатні до кращої провідності. Однак зворотнім наслідком використання “сильних” електролітів є їх підвищена схильність до впливу температури. Властивості таких розчинів будуть суттєво залежати від взаємодії іонів між собою, а також взаємодії іонів з полярними молекулами розчинника. Взаємодія іонів в “сильних” електролітах буде призводити до того що катіони та аніони будуть відчувати взаємне притяжіння, а іони одного знаку відштовхуватись. Тому в електролітичних розчинах кожний довільно обраний іон буде в середньому часі переважно оточений протилежно зарядженими іонами, як наприклад в іонних кристалах. Однак енергія теплового руху іонів в рідких розчинах значно більша ніж в твердих кристалах тому іони взаємодіючі з сусідніми іонами будуть утворювати не кристалічну решітку а розміщуватись у вигляді сфери. Таку сферу прийнято називають іонною атмосферою (Рис. 1).

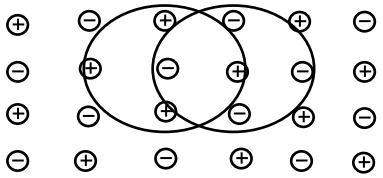


Рис. 1Двовимірна модель іонної атмосфери електролітів

Іонні атмосфери володіють наступними характеристиками: до їх складу входять катіони та аніони, однак переважають іони протилежні за знаком заряду центрального іона. Сумарний заряд іонної атмосфери дорівнює за величиною заряду центрального іона і протилежний йому за знаком. Всі іони в розчині рівноправні тому кожний з них одночасно є і центром власної іонної атмосфери і входить до складу периферії атмосфери сусідніх іонів. За рахунок теплового руху іони які входять до складу іонної атмосфери постійно міняються місцями з іонами які знаходяться за її межами тобто іонна атмосфера носить динамічний характер. Замість практично нереалізованого розрахунку енергії взаємодії окремих іонів в розчинах електролітів її відображають як функцію сумарної взаємодії всіх іонів котрі входять до складу його іонної атмосфери. Енергія цієї взаємодії залежить від щільності заряду іонної атмосфери і її середнього радіуса. Вивільнення енергії під час розривання цих зв’язків є екзотермічною реакцією і призводить до вивільнення тепла і як наслідок підвищення температури електроліту. Підвищення ж температури електроліту призводить до погіршення основних характеристик електролітичного конденсатору. Для більш точного визначення цієї енергії було введено поняття активності α. Для визначення коефіцієнту активності електролітів γ зазвичай приймають як середньогеометричне значення активностей формуючих його іонів. Так для електроліту $A_n B_m$ справедливий вираз:

$$\gamma\pm = \sqrt[n+m]{\gamma_A^n + \gamma_B^m}$$

Висновки. Внутрішні хімічні процеси в електролітах разом із зовнішніми чинниками що впливають на конденсатор визначають його основні характеристики час життя (час безвідмовного функціонування). Виробники електролітичних конденсаторів не вказують який саме електроліт використовується в тих чи інших конденсаторах. Тому розробка методики визначення технічного стану електролітичних конденсаторів з урахуванням фізіко-хімічних процесів в них є актуальною і практично значущою.

аспірант Подгайко В.О. (ХНУ ім. В.Н. Каразіна)
д.т.н., проф. Рассомахін С.Г. (ХНУ ім. В.Н. Каразіна)

АНАЛІЗ АЛГОРИТМІВ ІДЕНТИФІКАЦІЇ У СИСТЕМАХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

Актуальність. У наш час все більше застосовуються різні системи ідентифікації особистості. З ними ми стикаємось під час електронних розрахунків, для отримання доступу до об'єктів з обмеженим доступом, в системах з авторизацією особистості та ін.

Зараз, як ніколи раніше, важлива проблема коректної ідентифікації та аутентифікації особистості. А що може бути особистого, як не індивідуальні біометричні ознаки людини, такі як голос, сітківка ока, хода, індивідуальний відбиток пальця і, звісно, ДНК. Все це об'єднує термін «біометрія». На сьогодні, ідея використання біометричних засобів аутентифікації та ідентифікації дуже актуальна. Більш того, майже кожен з нас стикається з нею – для розблокування екрану телефону своїм відбитком пальця, або з використанням так званого «Face ID», тобто ідентифікатора обличчя. Також біометричні механізми використовуються у паспортах нового типу – закордонних та громадян України. Але, на жаль вже названі мною, та особливо більш складні методи працюють не зовсім коректно. Наприклад «Face ID» може розблокувати екран, якщо до його сканеру піднести лише фотокартку людини. А відбиток пальця не спрацьовує, коли пальці вологі або щось інше ускладнює доступ до папілярного рисунку.

Такі системі потребують більш детального вивчення, всепоглинаючого поліпшення та подальшого розвитку, щоб уникати хибних спрацьовувань та досягнути повністю коректного процесу ідентифікації та аутентифікації, в яких помилка може «коштувати» дуже і дуже дорого.

Постановка задачі. Провести аналіз потенційно кращих алгоритмів ідентифікації та визначити напрямки подальшого їх розвитку для вирішення існуючих проблем:

1) конфіденційності і розмежування (дані, отримані під час біометричної реєстрації, можуть використовуватися з метою, на які зареєстрований індивід не давав згоди (не був обізнаний);

2) небезпеки для власників захищених даних (є можливість замаху на носія біометричних ідентифікаторів з метою отримання доступу);

3) можливість відміни біометричних даних (перевага паролю над біометрією є можливість його зміни). Головним чином скасування біометрії – це спотворення біометричного зображення або властивостей до їх узгодження.

Основні положення. Всі ці, зазначені проблеми намагаються вирішити кілька основних напрямків розвитку біометрії – алгоритм на основі абстрактно-мінуативних циліндричних кодів та алгоритм з використанням нечітких екстракторів. Вони є найбільш використовуваними в біометрії для забезпечення високої ймовірності вірного спрацьовування ідентифікації.

Мінуатівні ціліндрічні коди.

Абстрактно-мінуативні циліндричні коди засновані на дрібних деталях дескрипторів відбитків пальців, які враховують найдрібнішу інформацію на зображенні відбитка пальця для зіставлення відбитків. Мінуція – це унікальні для кожного відбитку ознаки, що визначають пункти зміни структури папілярних ліній (закінчення, роздвоєння, розрив та ін.), орієнтацію папілярних ліній та координати в цих пунктах. Кожен відбиток може містити до 70 й більше мінуцій. Саме завдяки їх порівнянню відбувається порівняння за локальними ознаками.

Алгоритм за мінуативними циліндричними кодами використовує тривимірні структури даних, звані циліндрами, де кожен циліндр орієнтований у напрямку центральної мінуції за всім зображенням. Розташування дрібниць – це просторові точки, в яких орієнтація, частота та енергія мають більш високий диференціал змін.

Зображення орієнтації, обчислене за допомогою STFT-аналізу, відрізняється від традиційних орієнтаційних зображень, розрахованих з використанням простих похідних. За винятком точок ядра і дельти, будь-яка місцева область зображення відбитка пальця забезпечує послідовну інформацію про текстуру за методом STFT. У традиційній градієнтній оцінці орієнтації це не так.

Підхід, за допомогою якого воно створюються, називається функцією за замовчуванням, де не кожна клітинка в циліндрі буде накопичувати зазначений внесок. Так, осередки, які лежать за межами дійсної маски території, вважаються недійсними, а осередки без сусідів – мають нульовий внесок. Циліндр зберігається або викидається відповідно до обмежень дійсності. Ці обмеження включають в себе мінімальну кількість сусідів навколо центральної мінуції при постійному радіусі, відсотках від загальної кількості дійсних осередків. Тільки справжні циліндри будуть частиною шаблону відбитка.

Недоліком такого підходу є складність математичних обчислень значної кількості мінуцій та значна кількість циліндрів, які опрацьовуються, але відкидаються через ту чи іншу причину (вважаються недійсними).

*Нечіткі екстрактори***.**

Нечіткий екстрактор – це система (об'єкт, алгоритм), яка перетворює біометричні дані в випадкові послідовності, що надають можливість застосувати шифрувальні методи для біометричної безпеки. Вони використовуються, щоб зашифрувати та підтвердити справжність користувача транзакцій. При цьому біометричний вхід розглядається як ключ. Слово “нечіткий” в назві екстрактора має на увазі, що значення отриманої послідовності мають вигляд досить близькій до оригінального та можуть підтвердити справжність персоналії.

Алгоритм з використанням нечітких екстракторів – спосіб, який дозволяє однозначно відновлювати секретний ключ з неточно відтворюваних біометричних даних за участю допоміжних даних, які є відкритими. Відповідно алгоритму виконується послідовність дій:

- ініціалізація, де задається параметр безпеки, що визначає довжину відкритого і секретного ключів, та поріг спрацьовування, на основі чого алгоритм породжує секретний майстер-ключ і публічні параметри;
- екстракція, де задається конкретна особистість та секретний майстер-ключ, а сам алгоритм опрацьовує ці дані та повертає секретний ключ користувача;
- шифрування, де за даними секретного ключа користувача, його особистості та закладеним повідомленням алгоритм повертає шифротекст;
- розшифрування, де за секретним ключем та шифротекстом, що зашифрований за допомогою особистості, алгоритм повертає повідомлення в разі, якщо дані особистості підтверджені, або зупиняє роботу в іншому випадку.

Надалі проводять оцінювання стійкості такого алгоритму з точки зору силових атак типу: повний перебір, створення колізій тощо, а за умови отриманої стійкості до них – переходять до аналізу його стійкості від аналітичних атак.

Недоліком такого підходу є складність математичного апарату обробки даних за наявністю значної кількості помилок та неможливість забезпечити необхідну точність за умови необхідності виправляти ці помилки.

Висновок. Таким чином, найбільш важливими та перспективними напрямами для подальших досліджень є ті, що стосуються некоректної роботи нечітких екстракторів та абстрактно-минутивні коди, які вирішують питання коректної ідентифікації та аутентифікації особистості. Застосування ідентифікації на основі синтезу “найсильніших сторін” обох алгоритмів надасть можливість нівелювати їх окремі недоліки.

Привар А. В. (ВІТІ ім.Героїв Крут)
к.т.н. Залужний О. В. (ВІТІ ім.Героїв Крут)

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ МОДУЛЯЦІЇ В СИСТЕМАХРАДІОЗВЯЗКУ БЕЗ ЗВОРОТНОГО КАНАЛУ

Сучасні тенденції розвитку телекомунікаційних систем, в основному, направлені на підвищення швидкості передачі данихта ефективності використання частотного ресурсу. Проте длясистем радіоуправління, телеметрії, моніторингу віддалених об'єктів та оповіщення основним завданням є максимізація надійності і достовірності доведення інформації, що особливо критично при використанні їх в умовах проведення спеціальних операцій, для охорони підприємств, установ і організацій, що можуть стати об'єктом терористичних атак та ін.

Для покращення електромагнітної сумісності різних засобів, зменшення енергоспоживання, масогабаритних показників, затрат на розгортання та експлуатацію обладнання, а також, що особливо важливо, з метою приховати місце знаходження кореспондента, особливе місце у вказаних системах, як вітчизняного так і зарубіжного виробництва знаходитьодностороння радіопередач. Її недоліками є відсутність інформації про факт посилки корисного сигналу і можливості адаптації до сигнально-завадової обстановки. Обмеженим є вибір оптимальних методів модуляції і способів прийому та обробки сигналів, завадостійкого кодування, що зумовлено обмеженим частотним, часовим, енергетичним ресурсом і необхідністю функціонуванням в умовах високого насичення радіоефіру та впливу засобів радіоелектронної боротьби противника.

У зв'язкуз цим важливим завданням є проведення порівняльного аналізу методів цифрової модуляції (маніпуляції), що використовуються у системахрадіозв'язку без зворотного каналу (СРЗ без ЗК)за критерієм мінімуму середнього значення ймовірності помилки на біт – $p_{\text{біт}}$, при довільно складній завадовій обстановці.У багатьох наукових публікаціях наведені формули, що дозволяють проводити такі дослідження, в тому числі і в реальних каналах (напр. –релеєвський, райсівський канал), проведені відповідні розрахунки,проте відсутній узагальнений аналіз для застосування в СРЗ без ЗК.

Відомо, що вLPWAN (Low-powerWide-areaNetwork) технологіяSigfox, яка підтримує як односторонню так і двосторонню радіопередачу,використовується двійкова відносно фазова маніпуляція (DBPSK - DifferentialBinaryPhase-ShiftKeying) та гаусівська маніпуляція з мінімальним частотним зсувом (GFSK - GaussianFrequency-ShiftKeying). При DBPSK більш ефективно використовується смуга частот ніж при GFSK. Крім того DBPSK забезпечує кращу завадостійкість.

Технологія Weightless-N повністю базується на односторонній радіопередачі висхідною лінією. Всі пристрої відправляють повідомлення на центральну базову станцію без синхронізації та підтвердження. В системі використовується DBPSK модуляція.

Відповідно до MIL-STD-188-110Dв стандартизованих модемах, що використовуються врадіостанціях КХ діапазону, в складній завадовій обстановці при відношенні сигнал/шум (ВСШ) від – 1 до 11 дБ застосовуються BPSK в поєднанні зі згортковим кодуванням (швидкість коду 1/2 – 3/4). Коли ВСШ більше або дорівнює 14дБ застосовуєтьсяквадратурна фазова маніпуляція (QPSK –QuadraturePhaseShiftKeying).

В результаті проведених досліджень виявлено, що найбільшу потенційну завадостійкість мають сигнали з фазовою або відносно фазовою (когерентною чи некогерентною) видами модуляції. Перехід від BPSK до когерентного DBPSK призводить до погіршення завадостійкості, яке стає все суттєвішим із зменшення ВСШ (при $p_{\text{біт}} = 0{,}1$ енергетичний програш становить 2 дБ). При $p_{\text{біт}} = 0{,}1$використання когерентного DBPSK у порівнянні з некогерентним дає енергетичний виграш менше 1-го дБ.

Перехід від BPSK до когерентного DBPSK в релеєвському каналі призводить до

погіршення завадостійкості приблизно на 2 – 2,5 дБ. Втрати при переході від когерентного DBPSK до некогерентногоDBPSK зменшуються при погіршенні завадової обстановки і становлять менше 1-го дБ при $p_{\text{біт}} = 0.1$.

Варто зазначити, що сигнали зBPSK мають найкращу завадостійкість, при умові використання складних схем оцінки фази, які б забезпечили когерентний прийом та мінімізували можливість виникнення явища зворотної роботи. В іншому випадку доцільно використовувати DBPSKсигнали, які допускають, як когерентну так і некогерентну обробку. Якщо початкова фаза елементів сигналу, що приймається – невідома і не може бути оцінена за передісторією сигналу то когерентний демодулятор просто непрацездатний. Тоді найкращої завадостійкості слід очікувати тільки при використанні некогерентного прийому сигналів з DBPSK, який до того ж відрізняється простотою реалізації.

Перехід від сигналів з 2-х позиційною до сигналів з 4-х позиційною фазовою маніпуляцією дає незначний програш по $p_{\text{біт}}$, проте це справедливо тільки при незмінній швидкості передачі. Застосування коректуючих кодів для компенсації втрат при багатопозиційній модуляції є обмеженим, бо в умовах складної завадової обстановки їм властиве розмноження помилок. Можливим виходом є застосування мажоритарного принципу кодування, який по своїй суті не призводить до виникнення вказаного явища. Результати проведених досліджень свідчать про те, що використання такого способу завадостійкого кодування дозволяє підвищити завадостійкість навіть в критичній завадовій обстановці ($p_{\text{біт}} = [0{,}3; 0{,}2; 0{,}1; 10^{-1}; 10^{-2}]$), проте із зменшення $p_{\text{біт}}$ виграш зменшується. Недоліком мажоритарного кодування є збільшення надлишковості інформації, яке пропорційне кількості повторень одного і того ж повідомлення (біта), аналогічно зростають і витрати часу на передачу всього блоку. Останнє особливо критично для радіоліній з обмеженою швидкістю передачі.В радіосистемах передачі сповіщень вона, як правило, складає 1 – 10 кбіт/с. В системах радіозв'язку, які працюють в режимі EMCON (EmissionControl – "радіомовчання"), за протоколом АСР 142 або АСР 142 (А), швидкість передачі в радіоканалі може складати, в окремих випадках, 75 біт/с, в ультра-вузькосмуговихLPWAN швидкість передачі, як правило не перевищує 100 біт/с.

Таким чином варто підкреслити, щоу випадку використання систем радіозв'язку без зворотного каналу та при функціонуванні їх в умовах апріорної невизначеності стану каналу зв'язку доцільно використовувати сигнали з двох позиційною фазовою чи відносно фазовою видами модуляції.

Застосування методів завадостійкого кодування можливе тільки за рахунок зменшення швидкості передачі повідомлень і ні в якому разі шляхом збільшення ансамблю сигналів. При його використанні необхідно враховувати максимально допустимий час для передачі повідомлень.

к.т.н. Прокопенко Є. В. (НАДПСУ)
к.т.н. Мул Д. А. (НАДПСУ)

УПРОВАДЖЕННЯ СТАНДАРТІВ НАТО В СИСТЕМІ ОРГАНІЗАЦІЇ ЗВ'ЯЗКУ ОРГАНІВ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ

Актуальність. В умовах збройної агресії з боку Російської Федерації проти України консолідація міжнародної підтримки залишається одним із ключових завдань зовнішньої політики України. В свою чергу в Конституції України зафіксовано «…стратегічний курс держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору». Впровадження стандартів НАТО у складові сектору безпеки та оборони України, є одним із пріоритетних завдань визначеним законодавством, зокрема, Законом України «Про національну безпеку України» та стратегічними оборонними документами України – Стратегією національної безпеки України, Стратегічним оборонним бюлетенем, Воєнною доктриною України, тощо.

Державна прикордонна служба України щорічно є виконавцем заходів річної національної програми під егідою комісії Україна – НАТО. Дежприкордонслужба залучена до реалізації 6 трастових фондів НАТО з питань:логістики та стандартизації; переходу з військової кар'єри на цивільну; управління, контролю, зв'язку та комп'ютерів; медичної реабілітації;кібербезпеки; протидії саморобним вибуховим пристроям.

Метою дослідження є розробка науково-обґрунтованих рекомендацій, щодо впровадження стандартів НАТО з питань організації зв'язку на всіх рівнях системи управління Державної прикордонної служби України,за рахунок виконання **наступних завдань:**

селекція та каталогізаціястандартів НАТО рекомендованих до запровадження в систему зв'язку органу охорони державного кордону з науковими коментарями;

опрацювання науково-обґрунтованих етапів та механізмів впровадження стандартів НАТО в системі організації зв'язку на всіх рівнях системи управління;

розробка практичних рекомендації щодо впровадження стандартів НАТО з питань організації зв'язку в системі управління органів та підрозділів охорони державного кордону.

Виклад основного матеріалу. Система зв'язку органу охорони державного кордону є складовою частиною системи управління та повинна забезпечувати своєчасний і скритий інформаційний обмін між пунктами управління з високим ступенем достовірності при повному використанні технічних можливостей різних засобів зв'язку та забезпечувати високу захищеність каналів зв'язку від несанкціонованого доступу.

В органі охорони державного кордону будується єдина система зв'язку, що досягається централізованим плануванням і використанням усіх сил і засобів для забезпечення управління. Визначна роль системи зв'язку та її вплив на функціонування системи управління частин (з'єднань) в мирний час, при розгортанні передових пунктів управління, так і під час загострення військово-політичної обстановки потребує її постійного удосконалення і доведення її готовності до стандартів НАТО.

Висновки. Отже, було окреслено роль системи зв'язку в системі управління органу охорони державного кордону та описано основні етапи впровадження стандартів НАТО, реалізація яких можуть бути використані на етапі реформування системи управління Державної прикордонної служби України у відповідності до стандартів в частині що стосується функціонування системи зв'язку.

Проскуріна М.М. (ВІТІ)
Боголій С.М. (ВІТІ)
к.т.н. Жук О.Г. (ВІТІ)

АНАЛІТИЧНА МОДЕЛЬ ВЗАЄМОДІЇ ЛІНІЇ РАДІОЗВ'ЯЗКУ ТА ПОСТАНОВНИКА НАВМИСНИХ ЗАВАД

Фізичний зміст процесу функціонування системи радіозв’язку (СРЗ) в умовах організованих завад являє собою радіоелектронний конфлікт, в якому приймають участь з одного боку СРЗ, а з іншого – система радіоелектронного подавлення (РЕП), до складу якої, в загальному випадку, входять станція радіотехнічної розвідки та, безпосередньо, постановник завад (ПЗ).

У роботі запропоновано підхід до формалізованого опису зазначеного радіоелектронного конфлікту.

Лінія радіозв'язку, що функціонує в умовах радіоелектронного подавлення, в моделі розглядається як об'єкт управління, що знаходиться під впливом двох суб'єктів, які нею керують, а саме системи управління радіолінією і системи управління засобами РЕП. Їх інтереси протилежні (антагоністичні): система управління радіолінією прагне максимізувати ефективність свого функціонування (наприклад – ймовірність доставки пакета за встановлений час), а система РЕП прагне її мінімізувати. Тому доцільним є вибір для формального опису досліджуваного об'єкта апарату теорії ігор і опис розглянутої взаємодії як антагоністичної гри з двома гравцями. Залежно від реалізованих в апаратурі радіозв'язку і РЕП алгоритмів управління стратегії гравців можуть бути як динамічними, так і статичними.

Взаємодію лінії радіозв'язку та станції РЕП ймовірного противника в запропонованій моделі представлено у вигляді графа функціональної взаємодії, що відображає цикли управління гравців і показник ефективності функціонування системи.

Радіолінія в кожен момент часу t знаходиться в одному зі станів $s(t)$ з множини станів S. Стан в кожен момент часу характеризується значенням показника ефективності $q(t)$, фізична суть якого повинна бути заздалегідь обґрунтована, а розрахункові співвідношення для його чисельного визначення Q заздалегідь встановлені: $s(t) \rightarrow q(t)$. Стани об'єкта можуть змінитися, як внаслідок впливів від системи прийняття рішень на управління радіолінією (СПРУ), так і від системи прийняття рішень на подавлення (СПРП), яка є складовою частиною станції РЕП.

СПРУ в процесі функціонування може змінювати технічні характеристики радіолінії: модуляцію, кодування та інше, реалізуючи тим самим стратегію функціонування радіолінії. СПРП, у свою чергу, змінює частоти, шпаруватість завади та інше, реалізуючи тим самим стратегію постановки завад. І СПРУ і СПРП мають обмеження ступенів свободи вибору стратегій, які обумовлюються спеціальним чином. Так СПРУ може мати обмеження щодо вибору типів сигналів, кодів, швидкостей передачі, енергетиці радіолінії. СПРП, як правило, має обмеження по енергетиці завади, також може мати обмеження по швидкості реакції, типам формованих завад та інше.

СПРУ приймає рішення на основі інформації, яку вона отримує з каналу спостереження, та реалізує свої рішення через канал управління. Ці канали характеризуються: часом затримки в них станів, що спостерігаються, а також операторами перетворення вхідних станів у вихідні. СПРП приймає рішення на основі спостереження, які вона отримує з каналу розвідки, і реалізує свої рішення через канал подавлення. Ці канали характеризуються: часом затримки в них станів, які спостерігаються, а також операторами перетворення вхідних станів у вихідні.

Запропонована модель дозволяє формалізувати опис радіоелектронного конфлікту “радіолінія – система РЕП” та проводити оцінку ефективності радіоліній в умовах радіоелектронного подавлення для заздалегідь визначених вихідних даних.

Раєвський О.В. (ВІТІ)
Кравченко А.О. (ВІТІ)
Панкратова А.А. (ВІТІ)

АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ANSIBLE ДЛЯ ВИКОРИСТАННЯ У ВІЙСЬКАХ ЗВ'ЯЗКУ ТА КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність. Для ефективного використання та конфігурації великої кількості мережевого та серверного обладнання, що нарощується в інформаційно-телекомунікаційних вузлах та центрах інформаційних систем.

Мета.Зменшення часу, що витрачається на виконання завдань з налаштування та розгортання мережевого та серверного обладнання.

Основні положення. Ansible — програмне забезпечення, що надає засоби для управління конфігурацією, оркестровки, централізованої установки застосунків і паралельного виконання типових завдань на групі систем. Сирцевий код Ansible, написаний мовою Python і розповсюджується під ліцензією GPLv3.

З особливостей Ansible можна відзначити просту і легко читану мову управління конфігурацією, підтримку розпаралелювання робіт, відсутність необхідності установки на віддалені системи спеціальних програм-агентів (всі операції ініціюються централізовано по SSH, або за допомогою інших плагінів, як-то winrm), можливість роботи без прав root. Система Ansible не така ускладна, як CFEngine, Puppet, або Chef, але при цьому надає досить широкі можливості та високу гнучкість управління віддаленими АРМ, мережевими пристроями, серверами, тощо. Користувач, що використовує в своїй роботі Ansible, створює так звані "плейбуки" у форматі YAML з описом необхідних штатних керованих систем. "Плейбук" — це опис стану цільової ресурсної системи, в якому вона має перебувати у конкретний момент часу, включаючи встановлені системні пакунки, запущені служби, створені файли та багато іншого. Ansible перевіряє, що кожен із ресурсів системи знаходиться в очікуваному стані і запитує та виправляє стан ресурсу, якщо він не відповідає очікуваному. "Плейбуки" Ansible - індемпотентні, тобто завдання, яке описано не буде виконано повторно. Наприклад, в "плейбуці" описаний процес встановлення певного програмного забезпечення (unzip-архіватор). При повторному використанні даного "плейбука" не буде виконуватись видалення та повторне встановлення, Ansible пропустить цей крок, повідомивши користувача, що дана дія вже виконана.Для виконання завдань використовується система модулів. Кожне завдання становить собою назву завдання, модуль що використовується і список параметрів, які описують завдання. Ansible підтримує змінні, фільтри (за допомогою бібліотеки Jinja2), умовне виконання завдань, паралелізацію, шаблони файлів. Адреси та налаштування цільових систем містяться в статичних файлах "інвентарю" (inventory), або ж визначаються динамічно через «плагіни інвентарю». Підтримує групування. Для реалізації набору подібних завдань існує система ролей, а для поширення уніфікованих наборів контенту, як-то плейбуків, різних типів плагінів і ролей, є Ansible Collections — формат пакунків, які зберігаються у публічному реєстрі ansible-galaxy, які можна завантажити на сервер або АРМ, з якого буде здійснюватися керування.

Висновок. Отже, за допомогою такого ресурсу як Ansible, створюється спроможність до внесення одночасних та паралельних змін в конфігураційних файлах кінцевих пристроїв, без необхідності повторення цих процедур на кожному пристрої окремо, кількість яких постійно зростає із викликом часу. Функціонал даного ПЗ забезпечує перебування різних за архітектурою віддалених систем у тому стані, який описаний в «плейбуках», завдяки різноманітним модулям залежностей, які дозволяють виконувати ті чи інші операції, в залежності від архітектури кінцевого пристрою. Таким чином, оволодівши навичками використання даного ПЗ, війська зв'язку та кібербезпеки покращать швидкість змін до конфігурацій обладнання від моменту прийняття рішення до моменту потрібного стану кінцевої системи, уніфікують типові конфігурації мережевого обладнання, та матимуть здатність до оперативного внесення змін до всіх керованих засобів кібербезпеки.

Рибаченко І.І. (ВІТІ ім. Героїв Крут)
Голуб О.Д. (ВІТІ ім. Героїв Крут)
к.т.н. Ільїнов М.Д. (ВІТІ ім. Героїв Крут)

СПОСОБИ ЗМЕНШЕННЯ ГЕОМЕТРИЧНИХ РОЗМІРІВ НИЗЬКОПРОФІЛЬНИХ АНТЕН

Актуальність. Малогабаритні низькопрофільні антени (НПА) знаходять широке застосування в різних радіоелектронних пристроях і системах завдяки їх мініатюрності і високій технологічності. Інтерес до них обумовлений перспективами їх використання в системах супутникової навігації, в системах радіозв'язку з використанням БПЛА, в радіотехнічних приладах, де масо-габаритні параметри являються головною вимогою до апаратури.

Постановка задачі. Метою роботи єпроведення аналізу способів мініатюризації низькопрофільних антен, та пошук нового технічного рішення по зменшенню геометричних розмірів та масо-габаритних показників антен.

Основні положення. Нині існує ряд способів щодо зменшення геометричних розмірів низькопрофільних антен, класифікація яких показана на рис. 1.

Рис. 1 - Класифікація способів мініатюризації низькопрофільних антенних випромінювачів

Класичним способом зменшення розмірів НПА являється використання діелектричного матеріла для заповнення об'єму між пластинами. Тоді розміри антени (А) зменшуються в $\sqrt{\varepsilon}$ раз у відповідності до наведеного виразу

$$A \approx \frac{\lambda}{2\sqrt{\varepsilon}},$$

де λ – довжина хвилі; ε – відносна діалектрична проникність.

Одним із способів мініатюризації антен класичних форм можна розглядати перехід від напівхвильових випромінювачів до чвертьхвильових. Така зміна конструкції дозволяє скоротити її габаритний розмір майже вдвічі в порівнянні з напівхвильовою антеною. На рис. 2 показана чвертьхвильова НПА, яка дозволяє зменшити розміри антени в два рази.

Нижче представлена низькопрофільна антена, згорнута в площині випромінюючого елемента (рис. 3), зменшення розмірів якої досягаються за допомогою щілин, виконаних у верхній пластині, які збільшують шлях струму, пройденого від одної кромки пластини до другої.

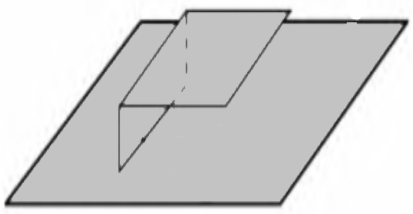
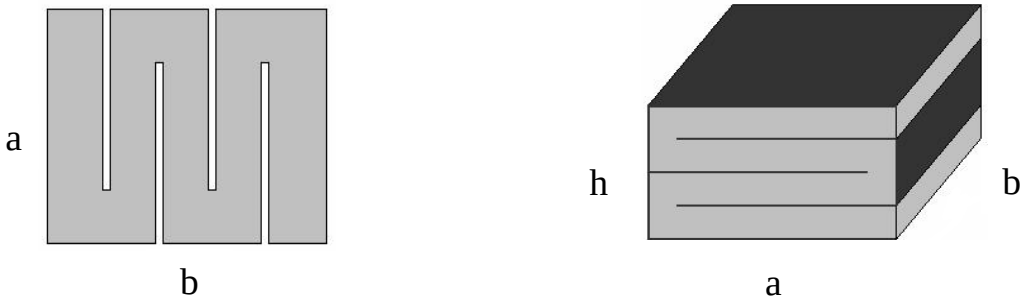


Рис. 2 - Чвертьхвильова низькопрофільна антена

В такому разі розміри верхньої пластини вибираються згідно виразу $a + (n+1)b = \frac{\lambda}{2\sqrt{\varepsilon}}$, де n – кількість щілин. Реалізація згорнутої низькопрофільної антени по висоті показана на рис 3-б. В цьому випадку розмір визначається згідно формули $(a+h)n = \frac{\lambda}{2\sqrt{\varepsilon}}$.



а)б)

Рис. 3 - Згорнуті низькопрофільні антени

Нове технічне рішення по зменшенню масо-габаритних показників показані на рис. 4, де зменшення геометричних розмірів досягається за допомогою зміни конфігурації верхньої та нижньої (екрана) пластин.

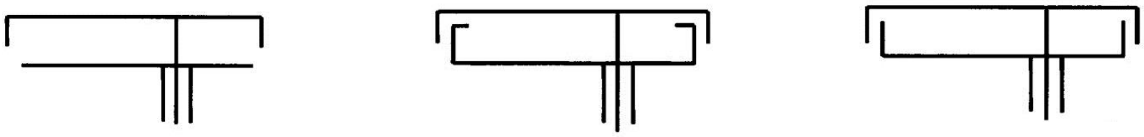


Рис. 4 - Компактні мікросмужкові антени

Висновок. Таким чином компактні, малогабаритні НПА, не потребують великих матеріальних затрат на їх виготовлення, можна зменшити по габаритам, використовуючи розглянуті вище способи. Отже аналіз досвіду розробки малогабаритних антен показує, що на практиці доцільно використовувати комбіновані принципи мініатюризації антен, виходячи із основних вимог до радіотехнічних об’єктів.

к.т.н. Романов О. М.
Військова частина А1906

МОДЕЛЬ ПОСТУ РАДІОМОНІТОРИНГУ ЯК СИСТЕМИ МАСОВОГО ОБСЛУГОВУВАННЯ

Стрімкий розвиток і широке використання систем зв'язку та передачі даних обумовлює необхідність моніторингу їх роботи. Ефективність постів радіомоніторингу (РМ) через ймовірність виявлення сигналів за заданий час і час пошуку із заданою ймовірністю вже оцінювалась автором у [1]. Оскільки ефективність РМ для заданої радіоелектронної обстановки (РЕО) обмежується наявними ресурсами (кількістю постів РМ та можливостями комплексів РМ), для подальшого дослідження ефективності постів РМ їх доцільно розглянути як систему масового обслуговування (СМО) [2, 3].

Нехай на вхід посту РМ із інтенсивністю λпоступає стаціонарний потік сигналів, моніторинг яких необхідно провести, – заявок на обслуговування, який виражається законом Пуассона. Пост РМ представимо як *n*-канальну СМО з відмовами, що має дискретні стани і безперервний час.

Оскільки кількість джерел заявок *M* значно більше, ніж каналів обслуговування *n:M>>n,* інтенсивність вхідного потоку не залежить від кількості одночасно занятих каналів СМО, а джерела заявок в СМО не входять і не аналізуються, модель посту РМ розглядатимемо як розімкнену СМО.

Середній час обслуговування однієї заявки $\bar{t}_{обсл}$ визначається характеристиками комплексу РМ. Час обслуговування вважатимемо випадковою величиною, розподіленою за показниковим законом з параметром $\mu = \frac{1}{\bar{t}_{обсл}}$.

Така СМО може бути представлена графом (рис. 1).

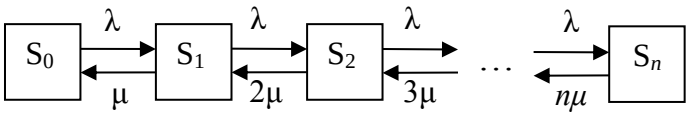


Рис. 1. Граф станів посту РМ як багатоканальної СМО з відмовами

Рівняння ймовірностей станів такої СМО визначаються формулами Ерланга:

$$P_k = \frac{1}{k!}\left(\frac{\lambda}{\mu}\right)^k P_0,\ k = 1,2,\ldots,n;\ P_0 = \left[\sum_{k=0}^{n}\frac{1}{k!}\left(\frac{\lambda}{\mu}\right)^k\right]^{-1},$$

де P_k – ймовірність того, що зайнято k каналів обслуговування, P_0 – ймовірність того, що всі канали вільні.

Вихідними даними для оцінки ефективності посту РМ є інтенсивність заявок на пошук λ, кількість каналів на посту *n*, середній час обслуговування однієї заявки $\bar{t}_{обсл}$.

Ефективність функціонування посту РМ оцінимо через ймовірність відмови у обслуговуванні чергової заявки, що надійшла, $P_{відм}$ та середню кількість занятих каналів $\bar{k}$. Для цього можна застосувати такі формули:

$$P_{відм} = P_n = \frac{1}{n!}\left(\frac{\lambda}{\mu}\right)^n\left[\sum_{k=0}^{n}\frac{1}{k!}\left(\frac{\lambda}{\mu}\right)^k\right]^{-1};$$

$$\bar{k} = \sum_{k=1}^{n} kP_k = \sum_{k=1}^{n} \frac{1}{(k-1)!}\left(\frac{\lambda}{\mu}\right)^k P_0 = \frac{\lambda}{\mu}\left(1 - P_{відм}\right).$$

Ймовірність обслуговування заявок (відносна пропускна здатність) обчислюється за формулою $P_{обсл} = 1 - P_{відм}$, а абсолютна пропускна здатність $A = \lambda \cdot P_{обсл} = \lambda\left(1 - P_{відм}\right)$. Коефіцієнт занятості каналів обчислюється за формулою $k_з = \frac{\bar{k}}{n}$.

Побудовані залежності відносної пропускної здатності посту РМ та середньої кількості занятих каналів від приведеної інтенсивності потоку заявок $\rho = \frac{\lambda}{\mu}$ при кількості каналів обслуговування *n* від 1 до 25 наведені на рис. 2 і 3 відповідно.

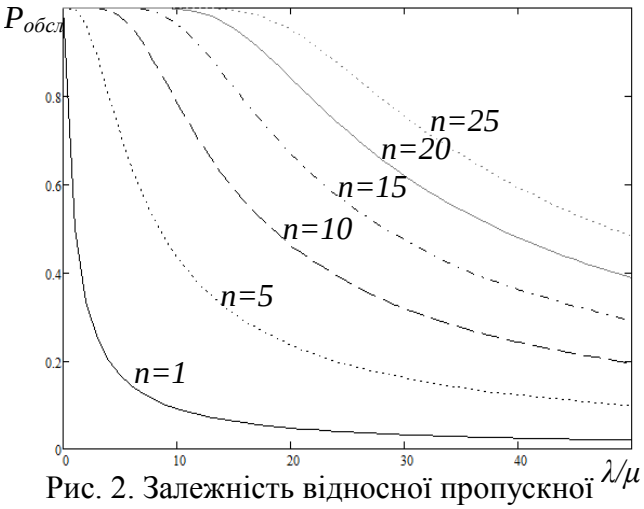


Рис. 2. Залежність відносної пропускної здатності посту РМ від приведеної інтенсивності потоку заявок

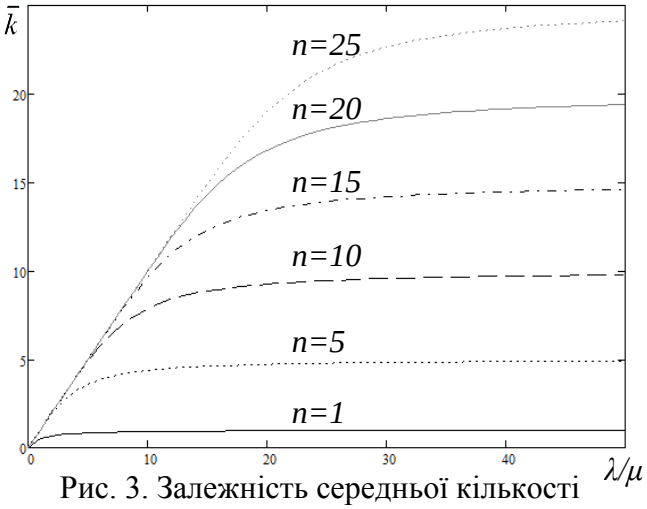


Рис. 3. Залежність середньої кількості занятих каналів посту РМ від приведеної інтенсивності потокv заявок

З побудованих графіків видно:

із збільшенням інтенсивності потоку сигналів, моніторинг яких необхідно провести, при фіксованому середньому часі обробки одного сигналу відносна пропускна здатність посту РМ зменшується;

для забезпечення бажаної відносної пропускної здатності посту РМ при заданій інтенсивності потоку сигналів, моніторинг яких потрібно провести, необхідно збільшувати кількість каналів обробки або зменшувати середній час обробки сигналів;

збільшення кількості каналів при фіксованій приведеній інтенсивності потоку заявок дозволяє зменшити коефіцієнт занятості каналів.

Таким чином, представлення посту РМ як СМО дозволяє оцінити достатність наявних ресурсів для ведення РМ при заданій РЕО, а за необхідності – розрахувати на скільки їх потрібно збільшити шляхом зменшення середнього часу обслуговування або збільшення кількості каналів обслуговування.

Список використаних джерел

1. Erokhin V. F. Determining The Effectiveness of Signals Detection During Search / Erokhin V. F., Romanov O. M., Nikolaev S. N. // 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2020, pp. 148–153.

2. Taha H. A. Operations research: an introduction / Hamdy A. Taha. – 8th ed. – New Jersey : Prentice Hall, 2007, 813 p.

3. Вентцель Е. С. Прикладные задачи теории вероятностей / Е. С. Вентцель, Л. А. Овчаров // М. : Радио и связь, 1983. – 416 с.

д.т.н. Романюк В.А. (ВІТІ)
Веремійчук В.Є (ВІТІ)

АНАЛІЗ DoS АТАК НА БЕЗПРОВІДНІ СЕНСОРНІ МЕРЕЖІ

Розглянуто особливості побудови та функціонування безпровідних сенсорних мереж (БСМ) військового призначення: значна розмірність (сотні, тисячі вузлів), обмеженість ресурсів вузлів (енергії батареї, продуктивності процесора, пам'яті, потужності передавача, пропускної спроможності радіоканалу тощо), концентрація трафіка навколо шлюзу, використання радіо середовища тощо. Визначено їх вплив на захищеність БСМ, на реалізацію захисних механізмів та протоколів, на ефективність та специфіку атак на дані мережі.

Визначені основні впливи DoS атак: порушення функціонування всієї мережі або її частини, зниження продуктивності мережі (за рахунок збільшення кількості спам-повідомлень, перенаправлення трафіка, тощо), збільшення часу передачі або втрата пакетів і їх підтверджень, підвищення витрат ресурсів вузлів тощо.

Розглядаються методи DoS атак на безпровідні сенсорні мережі, проведена класифікація даних атак по рівню стеку протоколів OSI на які проводиться атака (табл. 1).

Таблиця 1

Рівень OSI	**DoS атака**
Фізичний	Jamming, Interference, Node tampering and destruction
Канальний	Collision, Exhaustion, Unfairness
Мережевий	Sybil, Selective forwarding, Sinkhole, Hello flooding
Транспортний	Flooding, Desynchronization
Прикладний	Overwhelming sensors or sensor overload, Path based attack

Атаки фізичного рівня направлені на перешкоджання передачі, глушіння сигналу чи створення завад, які перешкоджають передачі пакетів, також, знищення чи перезапис керуючої інформації вузла через прямий фізичний доступ до вузла.

DoS-атаки на канальному рівні використовують недоліки механізмів підключення та розподілу канального ресурсу при передачі пакетів для втручання в роботу мережі.

Атаки на мережевому рівні відбуваються шляхом оперування даними полів пакетів, фальсифікації маршрутної інформації та, як правило, направлені на порушення структури сенсорної мережі, створення помилкових маршрутів передачі, втрату інформації що передається між вузлами, створення масштабних збоїв у роботі системи.

Атаки на транспортному та прикладному рівні, я правило, направленні на збільшення енерговитрат системи.

Проведена оцінка небезпеки даних атак, на які вразливості системи вони направлені, зазначено потенційні наслідки проведення атаки. Розглянуто механізми, заходи та протоколи які дозволяють послабити, завадити або запобігти даним атакам, запропоновано нові методи які дозволяють ускладнити деякі типи атак на безпровідні сенсорні мережі, або повністю запобігти їм.

Захист та запобігання визначеним атакам пропонується здійснювати за допомогою протоколів шифрування або встановлення граничних обмежень на прийом, передачу повідомлень, час роботи вузла чи тривалість з'єднання. Оскільки найбільш захищені протоколи шифрування вимагають досить високих енергозатрат, в безпровідних сенсорних мережах перевага надається більш простим протоколам, які забезпечують відносну безпеку, проте, витрачають менше енергії при роботі, а недостача криптографічного потенціалу компенсується організаторськими методами, які дозволяють ускладнити атаку чи зменшити її вплив, тим самим підвищуючи ефективність інших протоколів захисту.

Ротань Б.К. (ВІТІ)
Стоцький І.В. (ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ ПЕРЕДАЧІ ШИФРОВАНОГО ТЕКСТУ ТА ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ МЕТОДІВ СТЕГАНОГРАФІЇ

Актуальність теми. Проблема безпеки інформації вирішується на протязі всієї історії людини. Ще в давні часи відокремилось два основні напрямки захисту інформації: криптографія та стеганографія. Криптографія заблоковує несанкціонований доступ до інформаційних даних за допомогою шифрування. Стеганографія приховує сам факт існування конфіденційних та даних та їх передачі. Через наявність обмежень на використання криптографічних засобів та надзвичайну актуальність проблеми захисту інтелектуальної власності, стеганографія стає предметом зростаючого інтересу й активних наукових досліджень. Законом України "Про основи національної безпеки України" серед загроз національним інтересам і безпеці України в інформаційній сфері зазначені: комп'ютерні тероризм та злочинність; розголошення таємної чи конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; маніпулювання суспільною свідомістю, зокрема, шляхом поширення недостовірної інформації.

На сьогоднішній день нерідко виникає необхідність конфіденційне повідомлення, але для використання складних криптографічних систем безкоштовно простому користувачеві неможливо, оскільки безкоштовні рішення є не надто конфіденційними, а на інші варіанти потрібні і кошти і ресурси, яких у користувача може і не бути. Нині існує і розвивається комп’ютерна стеганографія (КС), предметом вивчення якої є методи, що приховують інформацію в потоках оцифрованих сигналів із використанням комп'ютерної техніки та програмного забезпечення. Цей новий напрямок наукових досліджень поєднує в собі останнідосягнення криптографії, теорії інформації, торії ймовірностей і математичної статистики, цифрової обробки сигналів і зображень, теорії дискретних Фур’є і вейвлет – перетворень, кодування і стиснення даних.

Завдання КС – захистити інформацію від несанкціонованого використання за допомогою розміщення (вбудовування) одних даних (секретних повідомлень) в інші (контейнер) таким чином, щоб візуальний або технологічний доступ до повідомлень був неможливий. Інформація, яка має цифровий вигляд повинна бути надійно захищена від багатьох загроз: несанкціонованого доступу та використання, витоку, підробки, знищення та ін. Для забезпечення конфіденційності інформації коли це потрібно, необхідна наявність модулю, який реалізує відповідні функції, розробка якого і є **метою** даного дослідження.

Для досягнення мети дослідження у роботі сформульованого наступні **завдання**:

- обґрунтувати необхідність криптографічного та стеганографічного захисту інформації для військовослужбовців ЗС України;
- проаналізувати принципи забезпечення криптографічної безпеки інформації у цифровому вигляді;
- розробити програмний модуль передачі шифрованого тексту на зображень за допомогою методів стеганографії.

Виклад основного матеріалу. Головним завданням модуля є забезпечення стеганографічного захисту шифрованого тексту та зображень. Стеганографічний алгоритм виконаний за допомогою мови програмування Python. Створений модуль дозволяє користувачам передавати шифрований текст за допомогою методів стеганографії та забезпечити конфіденційність факту передачі зашифрованої інформації.

Висновки. Таким чином, в роботі розроблено прикладний програмний інтерфейс модулю передачі шифрованого тексту та зображень за допомогою методів стеганографії. Даний модуль реалізує технологічний підхід забезпечення принципів безпеки при передачі інформації, з використанням досвіду сучасних криптографічних систем.

Руденко В.І. (ВІТІ)
Лазута Р.Р. (ВІТІ)
Макарчук В.І. (ВІТІ)
Атаманенко М.В. (ВІТІ)

МОДЕЛЮВАННЯ НЕНАДІЙНОГО ВУЗЛА БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ НЕОДНОРІДНОЮ МЕРЕЖЕЮ МАСОВОГО ОБСЛУГОВУВАННЯ ДЛЯПІДВИЩЕННЯ НАДІЙНІСТІ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ВСЕБІЧНОГО (ЛОГІСТИЧНОГО) ЗАБЕЗПЕЧЕННЯ ВІЙСЬКОВИХ ПІДРОЗДІЛІВ ЛАНКИ “БАТАЛЬЙОН – РОТА”

Актуальність. Сучасні бездротові сенсорні мережі (БСМ) зазнають розвиток саме як мережі спеціального призначення. Вони мають гнучку конфігурацію, яка може змінюватися залежно від поточного положення в просторі та можливостей енергопостачання.

Конфігурація системи із множини бездротових інформаційних вузлів, розміщених у просторі і маючих змогу працювати в недружньому середовищі, є найбільш доцільною для організації інформаційної підтримки всебічного (логістичного) забезпечення військових підрозділів ланки “батальйон – рота” в залежності від зміни тактичної обстановки. З цього приводу автори вважають за актуальне дослідження характеристик БСМ, аналізу їх властивостей та розробці методів оцінки основних характеристик для пошуку оптимальних управлінських рішень у військовій ланці “батальйон – рота” в залежності від зміни тактичної обстановки.

Метою дослідження є моделювання БСМ, що відповідає позиціонуванню сил і засобів інформаційної підтримки логістичного забезпечення військових підрозділів при виконанні ними завдань за призначенням.

Завданнями дослідження є:

- формалізований опис конфігурації бездротової сенсорної мережі, що відповідає позиціонуванню сил і засобів військової ланки “батальйон – рота”, процесів, які відбуваються у БСМ в залежності від зміни тактичної обстановки;
- визначення основних режимів роботи БСМ та аналіз “вузьких” місць за для підвищення надійності функціонування мережі в процесі зміни тактичної обстановки.

Авторами показано, що інформаційна підтримка у військовій ланці “батальйон – рота” через GPS зв’язок, дрони автоматизованої технічної розвідки і т. ін. може бути організована як бездротова сенсорна мережа і можуть бути змодельовані як мережі масового обслуговування.

Виклад основних матеріалів. Зміна технічної обстановки при виконанні військовими підрозділами завдань за призначенням обумовлюють наявність ненадійних вузлів відповідної сенсорної мережі. Для організації інформаційної підтримки всебічного (логістичного) забезпечення військових підрозділів “батальйон – рота” та підвищення ефективності функціонування БСМ ненадійного вузла сенсорної мережі змодельований неоднорідною мережею масового обслуговування.

За результатами дослідження математичної моделі були визначені такі стаціонарні характеристики мережі массового обслуговування як математичне очікування числа вимог, час реакції мережі обслуговування, час перебування вимог в системі, математичне очікування числа загублених пакетів.

Висновки. Таким чином, приведені аналітичні залежності дозволяють дослідити функціонування ненадійного вузла, провести аналіз “вузьких” місць та зробити пропозиції щодо пошуку оптимальних управлінських рішень у військовій ланці “батальйон – рота” в залежності від зміни тактичної обстановки та, як наслідок, підвищити надійність інформаційної підтримки всебічного (логістичного) забезпечення військових підрозділів ланки “батальйон – рота”.

к.т.н. Самойлов І.В. (ІСЗЗІ КПІ ім. Ігоря Сікорського)
к.т.н. Конотопець М.М. (ІСЗЗІ КПІ ім. Ігоря Сікорського)

ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ З ВИКОРИСТАННЯМ КОМПОНЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ

Актуальність. На сьогодні актуальною науково-технічною проблемою є створення систем оцінки захищеності інформаційних систем від загроз, які можуть опрацьовувати нечітку інформацію. Дані систем дозволяють визначати, які дії ефективні для мінімізації та попередження загроз. На основі аналізу захищеності можна прогнозувати можливий збиток від реалізації загрози, його оцінку та рекомендувати необхідні дії. Для формалізації експертної інформації при моделюванні причинно-наслідкових зв'язків, зручно використовувати теорію нечітких множин.

Постановка задачі. Нехай відомо: множина вхідних змінних $X = (x_1, x_2, ..., x_n)$; $x_i \in [\underline{x_i}, \overline{x_i}], i = \overline{1,n}$; множина вихідних змінних $Y = (y_1, y_2, ..., y_m)$; $y_j \in [\underline{y_j}, \overline{y_j}], j = \overline{1,m}$; множина загроз $D = (d_1, d_2, ..., d_n)$, де загроза d_i, $i = \overline{1,n}$, інтерпретується як нечіткий терм, що описує змінну x_i; множина збитків $S = (s_1, s_2, ..., s_m)$, де збиток s_j, $j = \overline{1,m}$, інтерпретується як нечіткий терм, що описує змінну y_j; відношення між загрозами і збитками $R \subseteq D \times S$. Задача оцінки захищеності може формулюватись у формі оберненого логічного виведення наступним чином. Знайти вектор $X = (x_1, x_2, ..., x_n)$, який задовольняє обмеження $x_i \in [\underline{x_i}, \overline{x_i}]$, $i = \overline{1, n}$ і забезпечує найменшу відстань між експериментальними і теоретичними виходами об'єкта: $F_{II}(X) = \sum_{j=1}^{m} \left[y_j - f_j^{II}(X) \right]^2 = \min_X$, де $f_j^{II}(X)$ – оператор зв'язку „входи-виходи" для нечіткої системи II типу.

Основні положення. Моделювання зв'язків „загрози–збитки", здійснюється шляхом інтерпретації композиційного правила виведення Заде ($\tilde{B} = \tilde{A} \circ \tilde{R}$), в якому носієм інформації є матриця нечітких відношень, що зв'язує вектор мір значимості загроз і вектор мір значимості збитків. З цього правила слідує система рівнянь нечітких відношень $\mu^{\tilde{s}_j} = \coprod_{i=\overline{1, n}} (\prod(\mu^{\tilde{d}_i}, \mu_{ij}^{\tilde{R}})), j = \overline{1, m}$. У зв'язку з відсутністю загальних аналітичних прийомів розв'язання рівнянь нечітких відношень, пропонується числовий метод розв'язання таких систем на основі комплексного використання генетичних алгоритмів і нейронних мереж.

Розв'язання системи рівнянь нечітких відношень I типу зводиться до задачі оптимізації, яка розв'язується шляхом комплексного використання генетичного алгоритму і нейронної мережі. Генетичний алгоритм забезпечує грубе влучення в область глобального мінімуму нев'язки між теоретичними і експериментальними мірами значимості збитків по мірі переходу від однієї загрози до наступної. Нейронна мережа, ізоморфна рівнянням нечітким відношенням I типу, використовується для on-line уточнення результатів оцінки захищеності і їх адаптації по мірі зміни параметрів стану об'єкта або параметрів моделі.

Для розв'язання рівнянь нечітких відношень II типу використовується послідовний підхід. Цей підхід означає, що пошук розв'язку рівнянь нечітких відношень II типу здійснюється не з нуля, а використовує результати розв'язання рівнянь нечітких відношень I типу. Підстройка розв'язку здійснюється за допомогою нейро-нечіткої мережі, ізоморфною рівнянням нечітких відношень II типу.

Висновок. Таким чином пропонується числовий метод розв'язання рівнянь нечітких відношень на основі комплексного використання генетичних алгоритмів і нейронних мереж, що дозволить оцінити вплив невизначеності на точність розв'язання задачі оберненого логічного виведення і отримати початковий розв'язок для розв'язання рівнянь нечітких відношень II типу.

Сергієнко А.В. (ВІТІ)
Бондаренко О.Є. (ВІТІ)
Коротков М.М. (ВІТІ)
Івченко М.М. (ВІТІ)

ПОРЯДОК ФОРМУВАННЯ ОПТИМАЛЬНОГО ВАРІАНТУ ПЕРСПЕКТИВНОГО ШТАТУ ПІДРОЗДІЛУ ВИДІВ (РОДІВ) ВІЙСЬК (СИЛ) ЗБРОЙНИХ СИЛ УКРАЇНИ НА ОСНОВІ КРИТЕРІЇВ “РЕЗУЛЬТАТ/ВАРТІСТЬ”

Актуальність. В умовах збройної агресії Російської Федерації проти України обумовлюється потреба в послідовному продовженні оборонної реформи, створення оптимального штату підрозділу видів (родів) військ (сил) ЗС України та цілеспрямованому розвитку необхідних спроможностей з урахуванням принципів і стандартів НАТО.

Мета. Визначення порядку формування оптимального варіанту перспективного штату підрозділу видів (родів) військ (сил) ЗС України на основі критеріїв “результат/вартість”.

Основна частина. Розробка варіанту перспективного штату підрозділу видів (родів) військ (сил) ЗС України передбачає створення робочої групи (далі – РГ), що повинна відповідати меті та масштабу заходу.

Для формування перспективного штату підрозділу видів (родів) військ (сил) Збройних Сил України проводяться наступні заходи: Визначення сценаріїв застосування перспективного підрозділу видів (родів) військ (сил) Збройних Сил України та відповідного переліку завдань за сценаріями. Розробляються від трьох до семи часткових сценаріїв виникнення та розвитку ситуації воєнного характеру, що повинні охоплювати усі варіанти застосування перспективного підрозділу. Сценарії мають містити ряд обов’язкових елементів: об’єкт впливу загрози та можливі цілі сторін; опис умов виникнення, можливі суб’єкти, які братимуть участь у досягненні цілей сторін; масштаби реалізації, сили і засоби; задіяні сценарії, часові рамки, інші особливості його реалізації. Визначення переліку необхідних спроможностей та переліку підрозділів, які здатні реалізувати зазначені спроможності.

Відпрацьовується кілька варіантів штатів, які формуються на підставі переліку мінімально-необхідних спроможностей, в яких визначається структура і склад, формуються цілі та критерії досягнення спроможностей, а також здійснюється розподіл спроможностей між підрозділами. Проводиться аналіз визначених завдань за сценаріями, та оцінка імовірності виникнення та розвитку ситуації воєнного характеру. Визначення перспективного переліку носіїв спроможностей виходячи з накладених ресурсних обмежень та з урахуванням можливості додаткового ресурсного забезпечення.Проводиться розіграш всіх сценаріїв застосовуючи діючий та розроблені варіанти перспективного штату, здійснюється аналіз носіїв спроможностей, оцінка відповідності органів управління, органів та установ всебічного забезпечення життєдіяльності військ, перспективної інфраструктури для утримання та підготовки перспективного складу. При отриманні більше одного варіанту, що відповідає вимогам щодо необхідних спроможностей, кожний з них оцінюється з точки зору його ефективності щодо виконання визначених завдань, а також вартості трансформації існуючого складу у перспективний. Вартість визначається необхідними обсягами витрат на персонал, озброєння та військову техніку, запаси матеріально-технічних засобів, військову інфраструктуру, експлуатаційні витрати. Ефективність виконання визначених завдань і вартість досягнення необхідних спроможностей є критерієм вибору оптимального варіанту перспективного штату.**Висновок.** Дана методика визначає процедуру та процеси, які необхідно виконати особовим складом РГ при формуванні оптимального варіанту перспективного штату підрозділу видів (родів) військ (сил) ЗС України на основі критеріїв “результат/вартість” та може бути застосована органами військового управління в ході відпрацювання пропозицій щодо організаційно-штатної структури підрозділів видів (родів) військ (сил) ЗС України.

V.Sidorenko (VITI named after Heroes of Kruty)

EVALUATION OF GLOBAL POSITIONING SERVICES TO PROVIDE THE NEEDS OF SPECIAL USERS

Topicality. This topic is that for many years, everything that was associated with the high-precision location of moving objects, was available only to the military and other security forces. These methods were used exclusively in navigation, aviation and mapping. The creation of such navigation systems as GPS and GLONASS has radically changed the situation. Today, navigation receivers are firmly entrenched in our lives, and location has become a service possible for everyone.

Global positioning systems are widely used by both civilian and special users, such as the Armed Forces of different countries. The analysis of the use of SmGP showed that they are used to control the transportation of dangerous important goods, in artillery navigation systems, to build communication networks, namely for the correct placement of mobile and trunking base stations. Evaluation of SmGP services is an important scientific and applied task.

Formulation of the problem. Evaluate the services of the global positioning system to meet the needs of special users.

Substantive provisions. GNSS (GNSS) is a global satellite navigation system that can be used to obtain the coordinates of the location of an object at any point on the earth's surface by processing satellite signals.

Any GNSS consists of three segments: space, ground and user. The space segment is represented by the constellation of satellites that transmit information about their position in orbit; the ground segment consists of stationary stations that provide monitoring and control of the position of satellites, as well as their technical condition; the user segment covers activities related to the development of military and civilian user equipment (ie receivers).

There are currently four SRSs operating or under development:

• Global Positioning System (GPS) operated by the US government; Global Navigation Satellite System (GLONASS) operated by the Russian government;

• Galileo Satellite Positioning System operated by the European Union;

• Compass Satellite Positioning System (Compass) operated by the Chinese government.

Any GNSS consists of three segments: space, ground and user. The space segment is represented by the constellation of satellites that transmit information about their position in orbit; the ground segment consists of stationary stations that provide monitoring and control of the position of satellites, as well as their technical condition; the user segment covers activities related to the development of military and civilian user equipment (ie receivers).

Each satellite continuously sends a message containing time information, the orbit point of the satellite from which the message was sent, and the general state of the system and approximate orbit data of all other system satellites. These signals propagate at the speed of light in space (and at a slightly lower speed - in the atmosphere).

The receiver determines the delay time in the signal and calculates the distance to the satellites, based on which, determines its location. The resulting coordinates are converted into a visual form (latitude and longitude or position on the map) and displayed to the user.

Theoretically, to determine its own coordinates, it is sufficient to determine the distance to three satellites. However, to calculate the position you need to know the time with high accuracy. To eliminate the need for a high-precision watch, information is usually obtained from 4 or more satellites.

At the moment, the current providers of SmGP are GLONASS and GPS.

According to its structure, GLONASS, like GPS, is considered a dual-action system, ie it can be used for both military and civilian purposes.

The GNSS space segment consists of the constellation of satellites and the spaceport from which they are launched. The satellite itself is a container, inside which is placed all sorts of equipment. All systems are powered by solar panels.

The main functions of satellites are as follows:

- reception and storage of data transmitted by the control segment;
- maintenance of exact time by means of several onboard atomic standards of frequency;
- transmission of information and signals to the user

The ground segment is designed to control the correct operation, continuous refinement of orbit parameters, control and information support of all spacecraft of the system and consists of the following interconnected stationary elements: system control center; central synchronizer; network of control stations; phase control system; quantum optical stations; navigation field control equipment.

The user segment forms a set of receiving and computing equipment - designed for the user of navigation receivers capable of performing measurements on navigation signals satellites. All the variety of navigation receivers can be classified on several grounds: military and civilian;

- navigation and geodetic;
- code or phase;
- single-system multi-system;
- single-channel and multi-channel;
- universal and specialized.

Navigation systems also have their drawbacks.

A common disadvantage of using any radio navigation system is that under certain conditions the signal may not reach the receiver, or arrive with significant distortions or delays. For example, it is almost impossible to determine its exact location in the depth of the apartment inside a concrete building, in the basement or in a tunnel.

Because the operating frequency of the GPS is in the decimeter range of radio waves, the level of signal reception from the satellites can deteriorate significantly under dense leaves of trees or due to very high clouds. Interference from many terrestrial radio sources, as well as from magnetic storms, can interfere with the normal reception of GPS signals. Active interference with signal receivers has been used effectively to combat cruise missile guidance during US and British operations in Iraq, as well as NATO's "Decisive Force" in Yugoslavia. This led to the self-destruction of cruise missiles and their abnormal flights on unauthorized trajectories.

To reduce the uncertainty of navigation measurements, many receivers use mathematical methods of navigation data processing, which allows to smooth the difference between range measurements based on counting the number of wavelengths of the navigation signal since the last measurement and the speed of the subscriber.

There are appropriate methods for solving navigation problems, we will consider in more detail the radial-velocity method, which in my opinion is the most effective and has the least number of disadvantages. The radial velocity method is based on the measurement of three radial velocities of the consumer relative to the three NCA.

The physical basis of the method is the dependence of the radial velocity of the point relative to the satellite, the coordinates and the velocity of the satellite in orbit.

Thus, to determine the components of the consumer velocity vector, you need to know: the vector of coordinates and velocities of the three NCAs, as well as the coordinates of the consumer. The disadvantage of this method is the inability to measure coordinates on a real time scale. In addition, in medium-altitude SRNs, slow changes in radial velocity lead to small values of differences in navigation calculation algorithms and, as a consequence, to a decrease in calculation accuracy, an additional disadvantage of the method is the need for a highly stable frequency standard. frequency, and, consequently, to additional errors in measuring the components of consumer speed. Therefore, nowadays the use of modern navigational aids is necessary in the process of solving the problems of radiation, chemical and biological reconnaissance, as well as engineering reconnaissance of areas and objects, as human losses are not allowed. This also applies

to the conduct of basic reconnaissance activities carried out by modern mobile technical means. Among them, as a rule, there is a navigation tool that uses information from space navigation systems.

Thus, navigation support occupies an important place in the system of combat support of the Armed Forces, which is determined by modern requirements for providing military management with operational navigation information, which characterizes the spatial - temporal position of troops in real time; development of high - precision means of destruction, changes in their tactical and technical characteristics and strengthening of combat capabilities, development and adoption of new strike systems and systems, introduction of automated control systems for troops and weapons.But the use of CPHC in the interests of location and navigation of moving objects, as well as in solving special problems makes higher demands on the accuracy of characteristics, so the main requirement for CPHC is high accuracy of measurement of these parameters, and for this it is necessary to increase receiver accuracy.

Conclusion. The evaluation of global positioning system services to meet the needs of special users was considered. To date, CPHc GPS and GLONASS are fully deployed and operational.Thus, global navigation systems solve very important tasks in the field of navigation to meet the needs of both military and civilian users, there are several positioning systems in the world, but truly global can be considered GPS GLONASS.

The positioning system consists of a space segment, a ground segment and a user segment, each of which plays an important role in determining the coordinates of users. The benchmark and to some extent the standard for all design positioning systems is GPS, as a navigation system, which was the first to fully deploy a satellite system and implement the location of terrestrial consumers.

Симоненков В.М., ВА (м. Одеса)
Лукаш Р.В., ВА (м. Одеса)
Дідик В.О., ВА (м. Одеса)
Симоненкова І.В., ВА (м. Одеса)

ПИТАННЯ ПОБУДОВИ КАНАЛІВ ПЕРЕДАЧІ ТЕЛЕМЕТРИЧНОЇ ІНФОРМАЦІЇ ТА КАНАЛІВ УПРАВЛІННЯ ТИЛОВИХ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ В УМОВАХ ГРУПОВОГО ЗАСТОСУВАННЯ

Логістичне забезпечення військ, яке пов'язане з доставкою боєприпасів та іншого військового майна безпосередньо у зону ведення бойових дій є, на наш погляд, найбільше складним й надзвичайно небезпечним для особового складу.

Чинною Концепція застосування наземних роботизованих комплексів (НРК) для виконання завдань Збройних Сил України на період до 2020 року та подальшу перспективу, яка затверджена наказом НГШ ЗС України від 03.05.2016 №177дск, передбачено створення тилових НРК для виконання заходів транспортного забезпечення військ, що перебувають у зоні вогневої дії противника.

Вважається за доцільне, що найближчим часом масове застосування бойових роботів на полі бою буде здійснюватися шляхом впровадження саме транспортних роботизованих засобів з метою виконання завдань логістичного забезпечення в умовах ведення бойових дій, коли потрібно постійне поповнення матеріально-технічних запасів, а також евакуації поранених та загиблих.

На даний час, у світі розробляється та прийнято на озброєння низку бойових роботів, які відрізняються за конструкцією, тактико-технічними характеристиками й бойовими можливостями, наприклад, в рамках програми «Модернізація бойових бригадних груп» (англ. Army Brigade Combat Team Modernization) до 2034 року для армії США передбачається створення й впровадження у війська понад 170 типів наземних роботів [1, 2].

Тенденції розвитку наземних роботизованих засобів у розвинених країнах світу показує, що основна увага, на сьогодні, приділяється створенню дистанційно-керованих бойових роботів з метою впровадження їх у повсякденну діяльність військ та масового застосування на полі бою. При цьому особливо складним є застосування НРК в умовах міської забудови й складної місцевості та відсутності надійного зв'язку з пунктом управління (людиною-оператором) або масового застосування засобів РЕБ противника.

У доповіді запропоновано методи вирішення питань, які пов'язані з необхідністю використання «додаткових» пристроїв зв'язку для передачі телеметричної інформації та автоматизації управління у складі підсистеми зв'язку та автоматизації перспективних тилових НРК для потреб Сухопутних військ ЗС України під час застосування за призначенням у складі функціонально-орієнтовних груп.

Для ефективного вирішення бойових завдань під час логістичного забезпечення військ, вважаємо за доцільне використання низки уніфікованих багатоцільових роботизованих платформ (БРП) з підвищеним рівнем автономності, зокрема, з властивостями, що придатні для їх групового застосування за призначенням [3].

Слід зазначити, що технології сумісного доступу в мобільних радіомережах подібних груп, на даний час, активно розвиваються та застосовуються під час створення мереж професійного зв'язку, сенсорних мереж та різноманітних тактичних мереж військового призначення. При цьому, використаються розподілені алгоритми управління мережею, а основним завданням стає вирішення питань самоорганізації вузлів мережі, тобто їх автоматична адаптація під поточну топологію, що склалася на певний момент часу, з метою забезпечення потрібної якості обслуговування.

Отже, в складних умовах інформаційної невизначеності сучасного поля бою, способи самоорганізації вузлів радіомережі (членів групи) повинні враховувати специфіку

застосування роботизованих засобів на полі бою, тобто в умовах швидкозмінного середовища з перешкодами, зокрема, досить низьку надійність «з'єднань» між окремими «елементами» НРК та ймовірної відсутності (знешкодження або знищення) «єдиного» координатора мережі зв'язку та управління (пункту управління).

Вирішення цього завдання передбачає застосування новітніх інтелектуальних підходів й технологій радіозв'язку, які спрямовані на вирішення безпосередньо проблем групового управління та підтримки оперативного обміну потрібних даних (телеметричної інформації). При цьому, на загальному рівні алгоритми групового управління функціонують, як правило, на основі інформації про заздалегідь виявлені перешкоди й умови руху в межах зони застосування та загальні координати групи БРП у складі тилового НРК в цілому. На нижчих рівнях, алгоритми групового управління передбачають оперативний обмін телеметричною інформацією між окремими БРП тільки про взаємні «дії» та відстані між «членами» групи, але не вимагають загального картографування (позиціонування).

Головний напрямок в цій області полягає у використанні новітніх комунікаційних й сенсорних технологій групового безпровідного радіодоступу у складі інтегрованих підсистем зв'язку та автоматизації, так званих «самоорганізуючих однорангових мережах», в яких окремі «вузли» радіомережі можуть зв'язуватися між собою безпосередньо.

Тому, сумісне застосування наземних роботизованих засобів вимагає використання у складі відповідних підсистем зв'язку та автоматизації БРП «додаткових» пристроїв зв'язку, так званої «близької дії», для вирішення безпосередньо групових завдань, які виникають в процесі застосування тилового НРК за призначенням.

На сьогодні, практично усі пристрої зв'язку у складі відповідних транспортних радіомереж (VANET, Vehicular Adhoc Networks, Автомобільні спеціальні мережі) будуються за допомогою протоколів зв'язку стандарту 802.11p (DSRC, Dedicated Short Range Communication, Виділена комунікація короткого радіусу дії) – технології зв'язку короткого радіусу дії, яка тісно пов'язана з поняттям «підключених транспортних засобів» [4].

Саме вона, на наш погляд, є найдоцільнішим типом комунікації мобільних роботизованих засобів під час логістичного забезпечення у складі перспективних тилових НРК в умовах групового застосування.

В ході досліджень розглянуто варіант побудови підсистеми зв'язку та автоматизації перспективного тилового НРК в умовах групового застосування, який призначений для транспортного забезпечення військ, зокрема, під час доставки боєприпасів та військово-технічного майна до пункту боєпостачання батальйону району оборони механізованого батальйону під час ведення оборонного бою або опорних пунктів рот першого ешелону та передових позицій (позиції підрозділу бойової охорони).

Запропонований варіант побудови каналів передачі телеметричної інформації та каналів управління у складі підсистеми зв'язку та автоматизації перспективного тилового НРК дозволить отримати сучасну повнозв'язну інформаційно-телекомунікаційну мережу, яка легко зможе інтегруватися до будь-якої системи управління тактичної ланки (або вищого рівня) та, у подальшому, забезпечити підтримку ведення мережецентричних сценаріїв бойових дій.

Список використаних джерел

1. Армія США: менші бригади, сильніші дивізії і багато роботів. URL: https://www.ukrmilitary.com/2020/11/war-men-and-robots.html. (дата звернення: 20.10.2021).

2. Unmanned Systems Integrated Roadmap. FY2013-2038 URL: https://www.hsdl.org/?abstract&did=747559. (дата звернення: 20.10.2021).

3. Симоненков В. М., Симоненкова І. В., Ковалішин С. С., Лукаш Р. В. Шляхи розширення інформаційних можливостей наземних роботизованих комплексів на підтримку мережецентричних сценаріїв бойових дій // Збірник наукових праць Військової академії (м Одеса).– 2018.– Вип. № 2 (10).– С. 118-123

4. Gozalvez J., Sepulcre M., Bauza R. 802.11p Vehicle to Infrastructure Communications in Urban Environments// IEEE Communications Magazine.– 50 (5), 2012.– 176-183 p.

д.т.н. Сівак В.А. (НАДПСУ)
к.т.н. Яценко К.Г. (ХНУПС)

ПЕРСПЕКТИВИ ІЗ ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ДІАГНОСТУВАННЯ ТЕХНІЧНОГО СТАНУ ТРАНСПОРТНИХ ЗАСОБІВ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Для забезпечення відсічі та стримування збройної агресії з боку Російської Федерації, спостерігається нарощення технічної складової частин і з'єднань сил безпеки та оборони нашої держави. Тільки підрозділи та органи Державної прикордонної служби України за останні 2-3 роки на 25–30 % оновили парк військової техніки, який на сучасному етапі складається із переважної більшості (до 93%) нових сучасних автомобілів та бойових броньованих машин різної модифікації.

Відповідно досить актуальним залишається питання інформатизації процесу еволюції їх експлуатації у різних умовах оперативно-службової діяльності прикордонних підрозділів та органів охорони державного кордону (ООДК).

Результати наукових досліджень за останні 3-5 років, у галузі технічної діагностики дають підстави, як варіант, розглядатиперспективи упровадження діагностики технічного стану військової техніки на основі нечітких нейронних мереж та подальше автоматизоване спостереження за еволюцією її експлуатації, що пропонується здійснювати шляхом ознайомлення з існуючими елементами нових інформаційних технологій та синтезу оптимального комплексу параметрів та структур нейромережевого компоненту.

Одним з найбільш важливих питань при розробці методів і засобів технічного діагностування є визначення їх інформаційних властивостей і можливостей. Особливо це актуально в умовах відсутності стаціонарних авторемонтних підприємств (баз), при постійному виконання оперативно-службових, а нерідко і службово-бойових завдань з охорони державного кордону автономно, що є досить екстремальними за своєю суттю та змістом.

Як свідчать результати наукових досліджень у даній галузі, використання малоінформативних приладів на практиці виявляється малоефективним, у той же час зайва інформативність створює інформаційний шум, перешкоди, завантажує непотрібною інформацією водія та викликає збільшення вартості обладнання. Розв'язання даного питання можливе з використанням математичного апарату прикладної теорії інформації, який довів свою практичну цінність при розв'язанні аналогічних завдань в авіації, на морському й річковому транспорті, у будівельних та дорожніх машинах, тощо.

Залучення методів теорії інформації при розв'язанні завдань діагностування, а особливо завдань керування режимами руху (зокрема, вибором безпечної швидкості) транспортних засобів (ТЗ) військового призначення викликане об'єктивними вимогами до надійності, ефективності й безпеки транспортного процесу, що відбувається в рамках системи «Водій-Дорога-Середовище». Використовуючи елементарні поняття теорії множин у структурі системи «Автомобіль-Водій-Дорога» можна виділити механічну підсистему «Автомобіль-Дорога», біомеханічні підсистеми «Водій-Автомобіль» і «Водій-Дорога». Сам водій, безумовно є складною біологічною й соціально-психологічною системою.

Цінність інформаційних проявів полягає в тому, що завдяки їхній спільності та відносній абстрактності суттєво різнорідні фізичні й технічні компоненти, а також характеристики системи, виявляється можливим виразити через деякі універсальні поняття такі, як ентропія, кількість інформації, пропускна здатність, тощо, а також виразити їх незалежно від фізичної сутності конкретних компонентів системи, причому не тільки виразити, але й зіставити, і не тільки якісно, але й кількісно.

Слід зазначити, що система «Автомобіль-Водій-Дорога» (АВД) ставиться до класу просторово-розподільних систем, характеристики яких (ефективність, продуктивність, безпека) перебувають у функціональній залежності від кількісних характеристик

інформаційного обміну між її структурними складовими. При цьому кількісною характеристикою інформаційного блоку є величина інформаційного (ентропійного) потоку.

При розв'язанні класу завдань, які пов'язані з керування об'єктом у складній системі, теорія інформації значною мірою опирається на закон необхідного різноманіття, який був уперше сформульований У.Р.Ешбі.

У відповідності із цим законом різноманіття можливих збурень у системі повинне компенсуватися таким же різноманіттям керуючого впливу.

Відповідно, кількісна оцінка необхідної інформативності бортових засобів діагностування ТЗ, особливо в умовах відсутності стаціонарних діагностичних пунктів, дозволить також вибрати необхідну точність і вірогідність датчиків систем та механізмів ТЗ, а також дискретність шкал контрольно-вимірювальних приладів, що в цілому буде сприяти створенню більш ефективного діагностичного устаткування для забезпечення достатнього рівня експлуатаційної безпеки ТЗ підрозділів та ООДК.

У свою чергу, специфіка розробки методу синтезу оптимального комплексу параметрів, на основі нейронної мережі полягає в тому, що структура нейронної мережі й кількість параметрів, по яких буде здійснюватися прогнозування факту відмови систем і механізмів ТЗ нерозривно пов'язані. Справа в тому, що кількість нейронів у вхідному шарі мережі повинна дорівнювати кількості параметрів. Тому пропонується комплексний алгоритм методики визначення як оптимальної структури тришарової нейронної мережі прямого поширення, так і оптимального комплексу (за кількістю й номенклатурою) прогностичних (вхідних) параметрів.

Алгоритм має наступний принцип роботи. Уся безліч наявних векторів даних, випадковим чином розбивається на дві частини (вибірки): навчальну і тестову. У процесі навчання на вхід нейронної мережі пред'являються приклади з навчальної вибірки. Тестова вибірка використовується для контролю узагальнюючої здатності мережі (якості класифікації, що виконується мережею, на даних, які не відносяться до навчальної вибірки).

На першому етапі будується мережа із числом нейронів у другому (схованому) шарі «оптимальним» для повного набору вхідних параметрів, шляхом визначення верхньої межі числа нейронів з наступним спрощенням (контрастуванням) мережі на основі показника значимості нейронів прихованого шару. На другому етапі проводиться видалення надлишкових вхідних параметрів шляхом контрастування на основі показника значимості вхідних параметрів з можливим збільшенням складності мережі шляхом додавання нейронів у другий (прихований) шар.

Показники значимості обчислюються у два етапи: спочатку вони обчислюються для одного вектору даних (навчального прикладу), а потім - за всією вибіркою.

Даний алгоритм дозволяє побудувати тришарову нейронну мережу із близьким до мінімального набором вхідних параметрів та кількістю нейронів у другому (прихованому) шарі.

Відповідно, впровадження нових інформаційних технологій та синтезу оптимального комплексу параметрів та структур нейромережевого компоненту дозволить підвищити інформативність отриманні інформації про точний діагноз технічного стану зразків ТЗ військового призначення в процесі еволюції їх експлуатації.

Таким чином, можливості застосування нових інформаційних технологій (зокрема, нейронних мереж та нечіткої логіки) для вирішення завдань інформатизації процесу еволюції експлуатації ТЗ військового призначення у різних умовах оперативно-службової діяльності в ДПСУ мають досить привабливі перспективи.

Проте, необхідно мати значений обсяг статистичних даних для створення вхідного інформаційного потоку для роботи нейронних мереж, що безумовно можливе з часом.

Скиба О.В. (ДНДІ ВС ОВТ)
Руденко О.В. (ДНДІ ВС ОВТ)
Панасенко С.В. (ДНДІ ВС ОВТ)

ІНФОРМАЦІЙНО-ДОВІДКОВА СИСТЕМА ЗАБЕЗПЕЧЕННЯ ТА ПІДТРИМКИ ПРОЦЕСІВ ПІДГОТОВКИ ДО ПРОВЕДЕННЯ ВИПРОБУВАНЬ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ (СПЕЦІАЛЬНОЇ) ТЕХНІКИ

Актуальність. Процес підготовки до випробування озброєння та військової (спеціальної) техніки (ОВСТ) потребує пошуку та оброблення чималого обсягу даних, на підставі яких формується комплект організаційно-методичних документів для проведення випробувань. Враховуючи, що останнім часом до оборонного відомства України від виробників регулярно надходять пропозиції щодо можливості виготовлення та постачання для потреб оборони тих чи інших зразків ОВСТ, система випробувальної діяльності поступово навантажується [1].Це потребує перерозподілу зусиль фахівців Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки (ДНДІ ВС ОВТ), оптимізації діяльності установи та окремих підрозділів, удосконалення підходів до підготовки і проведення випробувальних заходів.Як засвідчує досвід, підготовка до випробування кожного разу передбачає виконання тотожних (але не абсолютно однакових) процедур, пов’язаних з вивченням складу, призначення, можливостей та показників функціонування зразка, віднесення його до певної кліматичної групи, визначення обсягу і методів перевірки, опрацювання стандартів, оперативно-тактичних та загальних вимог тощо. Кінцевим результатом є розроблення проєкту програми та методик (ПМ) випробувань [2], [3].

Комплекс перелічених заходів є достатньо рутинним і, на нашу думку, може бути оптимізований та автоматизований.

Постановка задачі. Провести аналіз діяльності, яка виконується фахівцями ДНДІ ВС ОВТ на етапі підготовки до випробування. Розробити пропозиції з підвищення оперативності проведення підготовчих заходів для розроблення ПМ шляхом автоматизації окремих процесів.

Мета. Викладення поглядів щодо підвищення продуктивності та якості підготовки до проведення випробувальної діяльності шляхом впровадження інформаційно-довідкової системи (ІДС).

Основні положення. Для підвищення якості підготовки до випробування ОВСТ і збільшення продуктивності випробувальної діяльності в цілому нами пропонується розробити та втілити спеціальну ІДС, розгорнуту в інституті на базі локальної обчислювальної мережі.

У складі зазначеної ІС передбачається мати:

– файл-сервер – для розміщення нормативно-правових актів (НПА), нормативно-технічних документів (НТД), типових методик випробувань, інформацію щодо залучення фахівців інституту до раніше проведених випробувань тощо;

– автоматизоване робоче місце (АРМ) адміністратора (АРМ чергової зміни інформаційно-телекомунікаційного вузла) – для адміністрування ІДС;

– АРМ працівників науково-технічної бібліотеки (НТБ) – для наповнення, редагування, вилучення з файл-сервера НПА, НТД, типових методик тощо;

– АРМ науковців ДНДІ ВС ОВТ (рекомендовано не менше одного АРМ на відділ) – для пошуку необхідних документів, їх перегляд, завантаження, друк, а також для автоматизованого визначення обсягу випробувань, методології проведення перевірок зразків на основі початкових вхідних даних та для обрання складу випробувальної бригади на основі даних про залучення фахівців інституту до раніше проведених перевірок.

Використання ІДС усіма переліченими типами користувачів здійснюється через спеціальне програмне забезпечення (СПЗ), яке одночасно й частково реалізує функції

розмежування прав доступу.

Передбачається, що науковцю достатньо вказати тип випробувального зразка ОВСТ, його кліматичну групу, а СПЗ, з урахуванням НТД, зокрема [4], [5] та інших, сформує перелік обов'язкових перевірок та "підтягне" відповідні типові методики. Наприклад, випробуванню підлягатиме засіб цифрового зв'язку, яким передбачено укомплектувати бойову машину піхоти. Тоді відповідно до [4] користувачу відобразяться обов'язкові перевірки, а також буде запропоновано визначитися з потребою проведення тих випробувань, необхідність яких залежить від характеристик конкретного зразка ОВСТ.

Крім того, користувач може додатково опціонально обрати, чи передбачено десантування бойової машини піхоти, – у такому разі СПЗ автоматично це врахує при видачі ("підтягуванні") рекомендацій для методики з перевірки на міцність. Те саме стосується інших чинників, які впливають на обсяг та умови перевірки: користувач обирає певні заздалегідь передбачені опції, а програмна компонента допомагає формувати підходи до випробування. При цьому, користувач також може обрати інші види випробувань, які раніше застосовувалися фахівцями ДНДІ ВС ОВТ, та отримати для них типові методики перевірки (як основу для розроблення методик випробувань іншого зразка ОВСТ).

Іншим завданням, яке реалізовується в ІДС, є формування пропозиції з комплектування випробувальної бригади. Це здійснюється з урахуванням попередніх залучень фахівців інституту у випробуваннях подібних зразків або ідентичних питань в інших типів зразків. За допомогою ІДС можливо здійснювати планування залучення особового складу ДНДІ ВС ОВТ до підготовки випробувань в залежності від їх зайнятості в інших перевірках.Напрямком подальшого розвитку ІДС (за вирішення питань кібербезпеки) є організація віддаленого доступу до системи. Це надасть змогу фахівцям ДНДІ ВС ОВТ, які проводять випробування, отримати доступ до положень НПА, НТД, типових методик, потреба у яких виникла вже безпосередньо у ході перевірки.

Висновок. Розгортання вищеописаної ІДС з відповідним СПЗ не є легко і швидко виконуваним завданням та потребує врахування технічних, програмних аспектів, а також вимог захищеності. Проте реалізація такого підходу дозволить більш продуктивно здійснювати підготовки фахівців ДНДІ ВС ОВТ до підготовки і проведення випробувань.

Список використаних джерел

1. Корнієнко І.В. Визначення параметрів якості оцінок стохастичних характеристик випробуваного зразка озброєння та військової техніки / І.В. Корнієнко, С.П. Корнієнко, В.А. Дмитрієв, А.Г. Павленко, Д.О. Камак // Система обробки інформації: збірник наукових праць. – Харків: ХНУПС – 2020.– Вип. № 4 (163). – С. 56-65. – ISSN 1681-7710.

2. Порядок супроводження дослідно-конструкторських робіт та організації проведення випробувань озброєння і військової техніки у ЗС України: наказ Головнокомандувача Збройних Сил України від 31.05.2021 № 143. (Накази Головнокомандувача ЗС України).

3. Система разработки и постановки на производство военной техники. Порядок разработки программ и методик испытаний опытных образцов изделий. Основные положения: ГОСТ В 15.211-78. – Дата введения 1979-07-01. – М.: Издательство стандартов, 2001. – 21 с. (Государственный стандарт СССР).

4. Комплексная система контроля качества. Аппаратура, приборы, устройства и оборудование военного назначения. Общие технические требования, методы контроля и испытаний. Состав и общие требования к проведению испытаний: ГОСТ 20.57.303-76. – [Переиздание 1986 г. с Изменениями № 1, 2, 3, 4, утвержденными в декабре 1980 г., ноябре 1982 г., феврале 1986, июне 1986 г.]. – 20 с. (Государственный стандарт Союза ССР).

5. Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Общие технические требования, методы контроля и испытаний. Требования по стойкости, прочности и устойчивости к воздействию механических… (СТ В СЭВ 067-81): ГОСТ 20.39.304-76. – [Переиздание 1986 г. с Изменениями № 1, 2, 3, утвержденными в декабре 1980 г., ноябре 1982 г., июне 1986 г.]. – 82 с. (Государственный стандарт Союза ССР).

Солодовник В.І. (ВІТІ)
Іманов А.В. (ВІТІ)

ЗАСТОСУВАННЯ ПРОСТОРОВО-ЧАСТОТНОЇ ВЕРСІЇ КОДУ GOLDEN У НЕСТАЦІОНАРНИХ КАНАЛАХ СИСТЕМ ВІЙСЬКОВОГО РАДІОЗВ'ЯЗКУ

Актуальність теми. В умовах динамічної зміни форм та способів збройної боротьби комплекси та засоби зв'язку, що прийняті на озброєння Збройних Сил (ЗС) України, за своїми можливостями й технічним рівнем не відповідають сучасним вимогам системи управління. Збільшення обсягів інформації, що передається в інтересах управління військами та зброєю, вимагає удосконалення системи зв'язку. Оскільки інформаційна перевага на полі бою еквівалентна збільшенню бойової потужності та найчастіше є визначальною, особлива увага приділяється розвитку саме польової компоненти системи зв'язку. Для якісної реалізації об'ємних мультимедійних додатків та забезпечення виконання завдань за призначенням необхідно підвищити ефективність використання засобів радіозв'язку, що забезпечують до 70% інформаційних зв'язків під час проведення Операції Об'єднаних Сил та у мирний час.

За твердженням фахівця в галузі цифрових телекомунікацій Р. Кальдербанка, додаткове використання просторового ресурсу на базі сучасних гнучких та універсальних методів просторово-часового кодування сигналів (Space-TimeCoding, STC) у багатоантенних системах MIMO (MultipleInput – MultipleOutput) дозволяє істотно покращити спектральну (СЕ) та енергетичну ефективність (ЕЕ) системи радіозв'язку (СРЗ), а також можливості та умови обміну ЕЕ на СЕ. Технологія MIMO стала невід'ємною частиною практично всіх сучасних стандартів безпроводового зв'язку: Long-TermEvolution (LTE) і LTE-Advanced (LTE-A), IEEE 802.16 WiMAX та IEEE 802.11 Wi-Fi та базою для СРЗ наступних поколінь.

У ЗС провідних країн світу активно використовуються радіостанції з підтримкою технології MIMO (Falcon III RF-7800W (корпорація L3Harris), Aselsan GRC-5220 (корпорація Aselsan), Streamcaster 4200 LITE, 4200 Enhanced Plus та 4400 Enhanced, Hydra (компанія Silvus Technologies)). Більш того, наміри щодо продовження удосконалення систем військового радіозв'язку (СВРЗ) на базі технологій за стандартом 5 G задекларовано під час зустрічі голів держав та урядів країн-членів НАТО, тому тема дослідження є актуальною.

Метадослідження– підвищення спектральної та енергетичної ефективності систем військового радіозв'язку у нестаціонарному каналі.

Виклад основного матеріалу. Відомі ортогональні та неортогональні методи STC. Ортогональні просторово-часові блочні коди (Orthogonal Space-TimeBlockCoding, OSTBC) забезпечують повне рознесення сигналів з низькою обчислювальною складністю оптимального декодера. Підвищуючи завадостійкість передачі інформації (ЕЕ), такі коди характеризуються низькою кодовою швидкістю, що не перевищує одиниці ($R \le 1$). Забезпечити високі показники СЕ (а відповідно, і швидкості передачі інформації) дозволяють неортогональні просторово-часові блочні коди (Non-Orthogonal, NOSTBC), що дають виграш мультиплексування, проте потребують високоенергетичних каналів через недостатній об'єм рознесення сигналів. Верхньою межею ефективності всіх методів STC є неортогональні Perfect-коди (PSTBC), що забезпечують повне рознесення та мультиплексування сигналів. Слід зауважити, що практична реалізація PSTBC у MIMO великих розмірностей є проблемною через експоненційну обчислювальну складність декодера. Незважаючи на "досконалість" PSTBC, їх завадостійкість, так само як і OSTBC, є критичною до нестаціонарної поведінки каналу, коли неможливо гарантувати незмінність параметрів каналу на довжині слова просторового коду. В умовах динамічного переміщення абонентів забезпечити зазначене складно навіть для OSTBC Аламоуті та PSTBC типу Golden протягом мінімальної довжини просторово-часового кодового слова, що складається з двох сигнальних елементів. Слід зауважити, що обидва згаданих методи STC є невід'ємною частиною стандарту IEEE 802.16eWiMAX та відомі під назвами "код А" та "код С"

відповідно. Разом із тим, для підвищення стійкості СРЗ до часової селективності каналу у системі з стандартом LTE використовується рознесена передача на основі частотної версії коду Аламоуті, що відрізняється від класичної (часової) схеми OSTBC реалізацією передачі пар символів ансамблів сигналів і їх комплексно спряжених копій не на сусідніх тактових інтервалах, а на суміжних піднесучих частотах. Такий ортогональний просторово-частотний блочний код (OrthogonalSpace-FrequencyBlockCoding, OSFBC) дозволяє досягти високої завадостійкості у нестаціонарних каналах та використовується переважно для збільшення дальності зв'язку або підвищення СЕ системи радіозв'язку завдяки обміну отриманого енергетичного виграшу (ЕВ) на збільшення розміру ансамблю сигналів.

Разом із тим, недоліком OSFBC є низька СЕ через кодову швидкість $R=1$. Реалізація передачі лінійних комбінацій із пар комплексних інформаційних символів на суміжних піднесучих за принципом породжувальної матриці Golden дозволяє істотно підвищити ЕЕ системи радіозв'язку у часово-селективному каналі.

Проведені дослідження показують, що при забезпеченні зв'язку між абонентами, що рухаються зі швидкістю до 150 км/год, у MIMO мінімальної розмірності 2×2 просторово-частотний код Golden забезпечує ЕВ до 7 дБ при ймовірності бітової помилки $P_{\text{пом}}=10^{-5}$ порівняно із класичним методом повного мультиплексування V-BLAST (Vertical-BellLaboratoriesLayeredSpace-Time). Такий результат свідчить про те, що у нестаціонарному каналі частотна версія коду Golden зберігає властивості класичної версії в частині повного рознесення та мультиплексування сигналів, а також переваги над неортогональним просторовим кодом V-BLAST ("код B" у WiMAX), який забезпечує рознесення сигналів лише на приймальній стороні.

Висновки. Ключовими вимогами до перспективної СВРЗ є висока достовірність передачі інформації із інтеграцією усіх видів трафіку, можливість адаптації до складної завадової обстановки та конвергенція із цивільними технологіями та протоколами. В умовах постійного динамічного переміщення органів та пунктів військового управління безпроводові канали характеризуються високим рівнем нестаціонарності, а також низькою енергетикою. Внаслідок швидких завмирань та значної фазової нестаціонарності сигналів високоефективне використання реальних каналів зв'язку суттєво ускладнюється.

Базуючись на методах ортогонального та неортогонального просторово-часового кодування сигналів, технологія MIMO дозволяє істотно підвищити спектральну та енергетичну ефективність СВРЗ. Досконалі Perfect-коди є верхньою межею ефективності методів STC у квазістаціонарному релеївському каналі. На сучасному етапі розвитку схемотехніки їх реалізація можлива для систем MIMO невеликої розмірності. В умовах нестаціонарної поведінки каналу доцільно застосовувати частотні версії методів STC, що є потенційно інваріантними до часової селективності каналу.

Проведені дослідження показали, що при організації зв'язку між високомобільними абонентами у MIMO 2×2 частотна версія коду Golden забезпечує ЕВ до 7 дБ при високій достовірності передачі інформації ($P_{\text{пом}}=10^{-5}$). Отриманий ЕВ, залежно від призначення СВРЗ та завадової обстановки, можливо обміняти на підвищення СЕ на 1 … 2 біт/с/Гц (за технологією АМС (AdaptiveModulationandCoding)), що, у свою чергу, при передачі оперативних повідомлень дає можливість зменшити час активного перебування в ефірі у 2 … 3 рази. Останнє дозволяє підвищити якість радіомаскування, зменшити ризик враження живої сили та техніки як стрілецькою, так і високоточною зброєю. Крім цього, отриманий ЕВ можна використати не тільки для збільшення швидкості, але й для підвищення достовірності прийому важливих даних, наприклад, артрозвідки, в умовах низькоенергетичного каналу через частковий вплив засобів постановки навмисних завад. До того ж, зазначений ЕВ можна також використати для збільшення дальності зв'язку або в інтересах зменшення потужності передавача, що також сприяє радіомаскуванню.

Таким чином, частотну версію коду Golden доцільно застосовувати у нестаціонарних каналах систем військового радіозв'язку для підвищення ефективності їх функціонування.

Солодовник В.І. (ВІТІ)
Манухін В.О. (ВІТІ)

МОДИФІКОВАНИЙ ПРОСТОРОВО-ЧАСОВИЙ КОД GOLDENДЛЯ СИСТЕМ ВІЙСЬКОВОГО РАДІОЗВ'ЯЗКУ З ПІДТРИМКОЮ MASSIVEMIMO

Актуальність. Реалізація бойових можливостей Збройних Сил України (ЗСУ) істотно залежить від якісних показників системи управління та її матеріальної основи – системи зв'язку. Досвід проведення Операції Об'єднаних Сил на Сході України показав, що ЗСУ в цілому та війська зв'язку зокрема виявилися неготовими до ефективного ведення бойових дій, не задовольняли вимогам системи управління військами, а тому потребували термінової модернізації. Інформаційна обізнаність забезпечує домінування на полі бою та дає можливість перемогти противника, який має перевагу в чисельності та вогневих засобах. Необхідність високошвидкісної передачі великих обсягів інформації гарантованої якості у режимі реального часу вимагає інтенсивного розвитку системи військового радіозв'язку (СВРЗ), що забезпечує надання послуг зв'язку не тільки на пунктах управління, але й у відриві від них. Технологія багатоантенних систем MIMO (MultipleInput – MultipleOutput) сприяє істотному покращенню показників спектральної та енергетичної ефективності системи радіозв'язку (СРЗ), що визначають її технічний ефект – інформаційну ефективність (ІЕ). Для подальшого удосконалення СРЗ на шляху до 5 і 6 Gоднією з ключових визначено технологію Massive (LargeScale) MIMO на базі цифрових антенних решіток із кількістю антенних елементів 128, 256 і більше. У 2019 році наміри продовження удосконалення СВРЗ на базі технологій за стандартом 5 G задекларовано під час зустрічі голів держав та урядів країн-членів НАТО, тому тема дослідження є вкрай актуальною.

Метадослідження– підвищення інформаційної ефективності систем військового радіозв'язку із підтримкою технології MassiveMIMO.

Виклад основного матеріалу. Технологія багатоелементних антен нерозривно пов'язана із методами просторово-часового кодування сигналів (Space-TimeCoding, STC). У сучасних стандартах LTE-Advanced, Wi-Fi та WiMAX використовуються ортогональні та неортогональні типи кодів. Результатом наукових досліджень останнього десятиліття є створення класу Perfect-кодів (PerfectSpace-TimeBlockCodes, PSTBC), що є верхньою межею ефективності методів STC у частині одночасної реалізації максимальних можливостей щодо рознесення та мультиплексування сигналів. Найвідомішим із PSTBC для MIMO 2×2 є код Golden, що забезпечує максимальні кодову швидкість (дорівнює двом) та об'єм рознесення (чотири). Ключовою перевагою коду Golden є значний енергетичний виграш (ЕВ) – до 2 дБ – порівняно із методом повного мультиплексування типу V-BLAST.

Для систем MIMOіз більшою кількістю антен (від 128), актуальним є питання розробки просторово-часового коду великої розмірності з властивостями породжувальної матриці Golden. У статті Крейнделіна В.Б. запропоновано рекурентний метод формування Єдиної Еквівалентної Віртуальної Матриці Каналу (Equivalent Virtual Channel Matrix, EVCM), що дозволяє перетворити будь-яку породжувальну матрицю STCдо вигляду, аналогічному моделі каналу зв'язку типу V-BLAST. На базі коду Golden розроблено матрицю EVCM для MIMO довільної розмірності з кількістю передавальних та приймальних антен, що є степінню двійки та складається із окремих віртуальних матриць 2×2.

Проведено аналітичне та статистичне моделювання характеристик завадостійкості системи MIMO 8×8 із використанням модифікованої просторово-часової матриці типу Golden. Виявлено, що такий удосконалений код дозволяє отримати ЕВ від 1,2 до 2 дБ порівняно із відомим класичним методом просторового мультиплексування типу V-BLAST. Одержаний ЕВ реалізується в залежності від умов функціонування СВРЗ.

Висновок. Модифікований просторово-часовий код типу Golden зберігає властивості класичного коду PSTBC для MIMO 2×2 та може бути використаний для підвищення інформаційної ефективності СВРЗ з підтримкою MassiveMIMO.

Стемпковська Я.А. (ВІТІім. Героїв Крут)
Власюк І.О. (ВІТІім. Героїв Крут)

ПРОГРАМНИЙ МОДУЛЬ ПОБУДОВИ ОПТИМАЛЬНОГО МАРШРУТУ НА БАЗІ ГЕНЕТИЧНИХ АЛГОРИТМІВ

Актуальність теми.Планування перевозок між виробником і споживачами продукції (військова частина, вищий військовий навчальний заклад, зона Сил Спеціальних Операцій тощо) здійснюється за допомогою задач транспортної маршрутизації, які здійснюється для масових перевозок вантажу. В даний час структура вантажообігу на 80% складає вантажі малих розмірів, які перевозяться за допомогою маятникового або шляхом перевезення (збірним, збірно-перевізним) маршрутом. Задачі маршрутизації особливо важливе для перевезення в міських районах.

Задача програми на маршрутизацію, призначена для виявлення необхідного маршруту і складання графіку перевезень, надавати можливість користувачам зменшити транспортні витрати на 10-15%.

Ряд переваг, які отримують підприємства, коли використовується автоматизована система:

підвищення ефективності роботи;зниження штату логістів;економія палива;зниження навантажень на особовий склад;зменшення рівня не конденсації товару (прострочені харчові товари, псування матеріалів і деталей тощо);зменшення трудового навантаження;збільшення рівня обслуговування на 5-10%;зменшення кількості помилок спричинені людським фактором;можливість працювати в єдиному інформаційному просторі з одними і тими ж даними;контроль за транспортом під час руху.

Метою роботи є побудувати програмний модуль для вивчення генетичних алгоритмів, як спосіб оптимізації їх ефективності і працездатності. В якості рішення задачі була вибрана задача комівояжера, оскільки вона дуже добре вивчена, має різні способи рішення, для того, щоб порівняти з отриманими результатами. Також одна з цілей даної роботи є вивчення розповсюдження генетичних алгоритмів на модель з декількома взаємодіючими популяціями.

Виклад основного матеріалу. В даній роботі проводиться розробка програмного модулю для побудови маршруту за генетичним алгоритмом, яка може отримати своє подальше використання не тільки в зоні проведення Операції Об'єднаних Сил, але й як в цивільному житті, так і в Збройних Силах в цілому. Даний програмний модуль буде розроблено на основі природньої еволюції методом пошуку.

Для розробки буде використано генетичний алгоритм, для пошуку оптимального маршруту, і сіткове планування, для проведення підрахунків, що буде визначати відстані, час та об'єм затрат на перевезення вантажу орієнтуючись на дані, які будуть визначені користувачем.

Висновок. Для роботи з маршрутами буде використано сіткове планування для оптимізації планування і управління складних задач, які вимагають участі невеликої кількості виконавців, в даному випадку ними будуть виступати водії, відправники і отримувачі. Також для вибору маршруту руху буде використано генетичний алгоритм, будучи процедурою пошуку, заснований на механізмі природнього відбору і успадкування, який будуватиме шлях згідно встановлених формул і задач.

Результатом роботи вийшов програмний модуль задача якого показати принцип побудови оптимального шляху за допомогою генетичних алгоритмів, які будують маршрут відштовхуючись від відстані, часу, виведеного на подолання відстані, кількості пального, якості доріг і першочерговості доставки посилки. Побудована програма за допомогою мови програмування *Java*.Легкість, зручність та надійність при використанні є провідними характеристиками для використання даного програмного продукту в ЗСУ.

Стемпковська Я.А (ВІТІ ім. Героїв Крут)
Занін О.Ю. (ВІТІ ім. Героїв Крут)

ПРОГРАМНИЙ МОДУЛЬ РОЗРАХУНКУ ТРАНСПОРТНОЇ МЕРЕЖІ З УРАХУВАННЯМ ОСОБЛИВОСТЕЙ КЛЮЧОВИХ ПУНКТІВ РУХУ

Актуальність. На даний час, розв'язання проблем економічного розвитку України є одними з перших завдань нашої держави. Велику увагу привертає транспортна інфраструктура, яка є однією з ланок забезпечення і є показником як економічного розвитку національної економіки країни життя населення в цілому. Зараз збереження обороноздатності та можливість досягнення високоефективних зовнішньоекономічних відносин країни займає перше місце , отже і ця проблема потребує максимально вдалого рішення. Для створення ефективної системи управління транспортними мережами, пошуку оптимальних рішень з проєктування транспортної мережі та організації структури дорожнього руху необхідно враховувати широкий перелік характеристик, вплив зовнішнього середовища та внутрішніх факторів, котрі впливають на динаміку транспортного потоку. Це завдання потребує компетентності в різних галузях знань та поєднує в собі такі науки, як математику, фізику, економіку, менеджмент та ін.

Було зібрано велику базу знань та досліджень по цьому питанню, але цього буде недостатньо для реалізації проєкт через деякі фактори:

- Рух транспорту є нестабільним та важко піддається прогнозуванню, а отриманні данні не є об'єктивними та в силу малої ресурсомісткості.
- Умови в яких відбувається дорожній рух, як і сам рух в цілому, є хаотичними та непередбачуваними.
- Ухвалення та виконання рішення, навіть з урахуванням всіх факторів можуть призводити до непередбачуваних ефектів.

Мета роботи полягає в створенні програмного додатка, з урахуванням точок руху та їх особливостей, актуальність розробки якого полягає у його використанні для покращення планування маршрутів, швидкої та оптимальної зміни ключових точок маршруту з можливістю подальшого удосконалення функціоналу. Робота додатку полягає в пошукі оптимального рішення, в яке б забезпечувало економію витрат на організацію дорожнього руху, часу всіх залучених в цьому осіб, та ефективних результатів. Також слід не забувати про експериментальну частину роботи, у зв'язку з динамічним збором та обробкою отриманих даних. Додаток повинен мати максимальну ефективність, спираючись на грубій експертній оцінці.

Висновок. Отже, поглянувши на цю проблему більш детально можна зробити висновки, що дана сфера діяльності потребує програмного рішення для успішного та оптимального планування маршруту.

У зв'язку з цим, головним питанням буде урахування особливостей кожного ключового пункту руху та сумісності їх в нашому маршруті. Пошук оптимальних критеріїв оцінки та впровадження їх в основу роботи програмного додатка. Розробка та впровадження моделі для обчислення динаміки руху з урахування більшості факторів, які ми можемо зустріти.

Стемпковська Я.А. (ВІТІ ім. Героїв Крут)
Зборщенко В.С. (ВІТІ ім. Героїв Крут)

ПРОГРАМНИЙ МОДУЛЬ ОБЛІКУ ТА КОНТРОЛЮ РЕЗУЛЬТАТІВ УСПІШНОСТІ КУРСАНТІВ

Актуальність. Автоматизація системи обліку та контролю результатів успішності курсантів надає можливість просто та швидко отримувати необхідну інформацію в зручному форматі, оперувати нею віддалено, виконувати всі потрібні завдання в будь-який момент - це надає перевагу в оперативності. Також, надає можливість систематизувати наявну інформацію про успішність курсантів. В службовому процесі виникають труднощі із упорядкуванням інформації про результати в навчанні, оскільки більшість матеріалів зберігається у паперовому вигляді. Впровадження нових технологій незмінно призводить до суттєвого прискорення процесів обробки інформації, зменшення кількості помилок, можливості швидше обробляти та контролювати результати успішності курсантів, підвищення оперативності та обґрунтованості прийняття рішень.

Введення автоматизованої системи знімає велику кількість ризиків і пришвидшує роботу обліку та контролю результатів успішності, зокрема, в військових навчальних закладах. Крім цього, збільшується додаткові можливості моніторингу, збільшується управлінська здатність і скорочується час який витрачається для заповнення документів, а також система стає більш зрозумілою для керівництва.

Постановка задачі. Провести аналіз сучасних методів обробки та аналізу даних про успішність курсантів у військових навчальних закладах та вдосконалити їх шляхом розробки програмного модуля для обробки та контролю результатів успішності курсантів на основі програмних рішень.

Основні положення. Облік — належним чином організована система збору, нагромадження, обробки, групування, узагальнення і реєстрації (фіксації) необхідної інформації або її сукупних даних, що відображають кількісну чи якісну характеристику подій, явищ, фактів, процесів, об'єктів тощо.

Керівництво військових навчальних закладів, зокрема, навчальні відділи, має потребу в автоматизації обліку та аналізу даних щодо контролю результатів успішності курсантів.

Проаналізувавши особливості організації роботи навчальних відділів у військових навчальних закладах та відповідні керівні документи, можна стверджувати, існує нагальна потреба у автоматизації окремих аспектів організації процесів, особливо тих, що стосуються отримання інформації, що стосується результатів успішності курсантів. Дані аспекти є початковими поняттями, які висувають певні вимоги до проектування та розробки програмного додатку.

Висновок. Причини, які спонукають керівників організацій та установ до цифрової трансформації, з одного боку обумовлені прагненням підвищити продуктивність виконуваних робіт чи усунути їх повторне проведення, а з іншого боку – бажанням підвищити ефективність управління діяльністю організації за рахунок прийняття оптимальних та раціональних управлінських рішень. Очікується, що розроблений модуль зменшить навантаження на особовий склад, що займається обробкою результатів успішності курсантів, а також підвищить ефективність їх діяльності.

Цей програмний продукт є ефективним способом систематизувати процес обліку та контролю результатів успішності курсантів у лавах військових навчальних закладах, адже при теперішній кількості документообігу є великий ризик помилок.

Стемпковська Я.А. (ВІТІім. Героїв Крут)
Салюков І.І. (ВІТІім. Героїв Крут)

ПІДСИСТЕМА РОЗРАЗУНКУ ПОЗИЦІЙ СПОСТЕРЕЖЕННЯ ДЛЯ ТОЧНОГО МОДЕЛЮВАННЯ ТРАНСПОРОТНОЇ МЕРЕЖІ

Актуальність теми. Для пошуку ефективних стратегій управління транспортними мережами на місцевості, оптимальних рішень з проектування транспортної мережі і організації дорожнього руху необхідно враховувати широкий спектр характеристик транспортного потоку, закономірності впливу зовнішніх і внутрішніх факторів на динамічні характеристики змішаного транспортного потоку. Теорія транспортних потоків розвивалася дослідниками різних галузей знань - фізиків, математиків, фахівців з дослідження операцій, транспортників, економістів.

Мета дослідження полягає у покращенні процесів планування маршрутів, організації й управління комплексом спостереження із метою скорочення витрат ресурсів і підвищення ефективності результатів при заданих обмеженнях.

Не можна обійтися одними лише інженерними розрахунками, не провівши математичний експеримент. Тому, моделювання необхідно в силу наступних властивостей транспортної системи:

– компенсація збільшення пропускної здатності при розвитку мережі збільшенням попиту і перерозподілом його в нових умовах;

– непередбачуваність поведінки кожного водія - вибір маршруту, манера водіння тощо;

– вплив випадкових факторів (ДТП, погода тощо)

Виклад основного матеріалу. Враховуючи аналіз існуючих засобів та методів розрахунку ключових та додаткових точок спостереження, в своїй роботі формую вимоги та архітектуру до математичного апарату додаткових точок.

Для задач розрахунку додаткових точок актуальною є проблема планування в умовах обмежених ресурсів, виділених для здійснення завдань, таким чином, щоб задовольнити усі обмеження, що накладаються на завдання в тому чи іншому випадку. В ході планування необхідно організувати роботи так, щоб вони були виконані в стислі терміни з найменшими витратами і найкращим розподілом виділених ресурсів. При цьому для процесу управління складними проектами при всьому їх різноманітті характерні деякі види неточності інформації. Вона, як правило, пов'язана з оцінкою деяких параметрів розрахунку додаткових точок. У зв'язку з тим, що виникають на практиці завдання розрахунку точок мають багатокритеріїв, в роботі пропонується розглянути задачу розрахунку додаткових точок, яка часто виникає на практиці і розробити спосіб її вирішення.

Розрахунки основних параметрів додаткових точок спостереження повинні бути використані при аналізі й оптимізації стратегічних планів. Оптимізація розрахунку додаткових точок полягає у обрахуванні представленної нам інформації для ефективності побудови сприятливого маршруту із метою скорочення витрат економічних ресурсів і підвищення фінансових результатів при заданих обмеженнях.

Висновок. Отже, проаналізувавши дану тематику можемо зробити висновки, що методи розрахунку додаткових точок можуть широко і успішно застосовуються для оптимізації планування маршруту і управління складними розгалуженими комплексами робіт, які вимагають участі невеликої кількості виконавців і витрат.

У зв’язку з цим особливо актуальним є питання розрахунку додаткових точок спостереження для досягнення чітко поставленої мети; головною метою розрахунку додаткових точок спостереження є скорочення до мінімуму витрат та тривалості проекту.

Стемпковська Я.А. (ВІТІ ім. Героїв Крут)
Сичова М.А. (ВІТІ ім. Героїв Крут)

ПРОГРАМНО-АПАРАТНА ПЛАТФОРМА СИСТЕМИ МЕДИЧНОЇ ПАСПОРТИЗАЦІЇ ЗС УКРАЇНИ

Актуальність. Автоматизація системи медичної паспортизації військовослужбовців Збройних Сил України надає можливість просто та швидко отримувати необхідну інформацію в зручному форматі, оперувати нею віддалено, виконувати всі потрібні завдання в будь-який момент - це надає перевагу в оперативності. Також, надає можливість систематизувати наявну інформацію про всіх військовослужбовців і їх стан здоров'я.

В процесі несення військової служби виникають труднощі із упорядкуванням медичної інформації, оскільки більшість матеріалів зберігається у паперовому вигляді. Впровадження нових технологій незмінно призводить до суттєвого прискорення процесів обробки інформації, зменшення кількості помилок, можливості швидше обслуговувати більшу кількість військовослужбовців, підвищення оперативності та обґрунтованості прийняття рішень.

Введення автоматизованої системи знімає велику кількість ризиків і пришвидшує роботу медичної допомоги в Збройних Силах України (ЗСУ). Крім цього, збільшується додаткові можливості моніторингу, збільшується управлінська здатність і скорочується час який витрачається для заповнення документів, а також система стає більш зрозумілою для керівництва.

Постановка задачі. Провести аналіз сучасних методів паспортизації, обробки та аналізу даних у військово-медичному закладі Збройних Сил України та вдосконалити їх шляхом розробки інформаційну підсистему медичної паспортизації даних у військових медичних закладах на основі програмних рішень.

Основні положення. Облік — належним чином організована система збору, нагромадження, обробки, групування, узагальнення і реєстрації (фіксації) необхідної інформації або її сукупних даних, що відображають кількісну чи якісну характеристику подій, явищ, фактів, процесів, об'єктів тощо.

Керівництво військових медичних закладів Міністерства Оборони України має потребу в автоматизації обліку та аналізу службових та медичних даних.

Ці дані використовуються для автоматизації процесів повсякденної діяльності медичних установ.

Проаналізувавши особливості організації медичного процесу у ЗСУ та відповідні керівні документи, можна стверджувати, існує нагальна потреба у автоматизації окремих аспектів організації процесів, особливо тих, що стосуються отримання необхідної медичної інформації. Дані аспекти є початковими поняттями, які висувають певні вимоги до проектування та розробки програмного додатку.

Висновок. Причини, які спонукають керівників організацій та установ до цифрової трансформації, з одного боку обумовлені прагненням підвищити продуктивність виконуваних робіт чи усунути їх повторне проведення, а з іншого боку – бажанням підвищити ефективність управління діяльністю організації за рахунок прийняття оптимальних та раціональних управлінських рішень. Очікується, що розроблений модуль зменшить навантаження намедичний персонал військової частини та шпиталів, а також підвищить ефективність їх діяльності.

Цей програмний продукт є ефективним способом систематизувати процес медичної допомоги в лавах ЗСУ, адже при теперішній кількості документообігу є великий ризик помилок.

Стоцький І.В. (ВІТІ ім. Героїв Крут)
Жирук А.О. (ВІТІ ім. Героїв Крут)

ПРОГРАМНИЙ МОДУЛЬ АВТОМАТИЗОВАНОГО ЗБОРУ ДАНИХ З ПЕОМ

Добування інформації є невід'ємною і обов'язковою складовою системи аналізу інформації підрозділів Міністерства оборони України. Для досягнення основних завдань розвідки[1,2] існують різноманітні засоби, які використовуються для автоматизації процесу. Через стрімкий розвиток технологій та систем захисту, більшість з них втрачають свою ефективність, таким чином постає питання на оптимізацію даної задачі дослідження та знаходження альтернативних способів для збору інформації, що визначає **актуальність теми.**

Метою роботи є автоматизація збору даних з ПЕОМ, що вирішує питання забезпеченя корисною інформації, з пристрою цілі, для подальшого аналізу та обробки. Модуль представляє собою систему прихованого збору і обробки даних. Найбільш ефективною та безпечною реалізацією розподіленої системи збору та обробки даних є багаторівнева система безпеки, архітектура якої базується на використанні низькорівневих технологій рівня системи, сервісів управління та шифрування даних на рівні управління даними, серверів (сервісів) збору і обробки даних.

Засновуючись на архітектурі системи безпеки, пропонується використовувати трирівневу архітектуру (рис. 1). На першому рівні знаходиться модуль, який виконує функції джерела даних. На другому рівні знаходиться проміжний сервер, який перенаправляє дані між модулем і сервером збору та обробки даних, також надає команди на виконання ПЕОМ цілі.

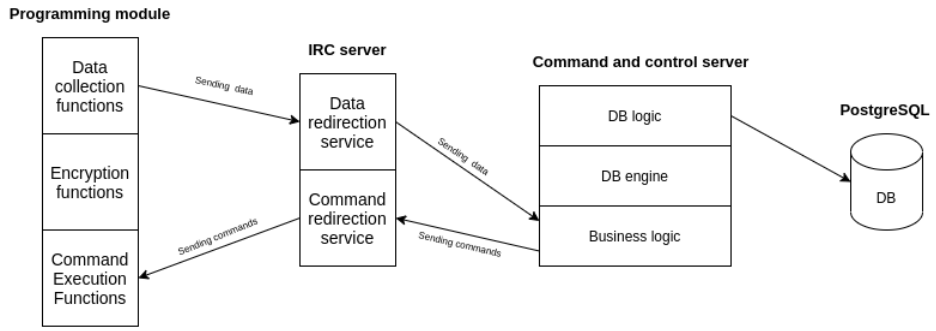


Рисунок 1 — Трирівнева архітектура модуля

Висновки. Використання запропонованого способу пришвидшує та робить безпечнішим процес збору даних. Реалізація модуля з використанням алгоритмів шифрування, прихованої взаємодії з системою, проміжних серверів для унеможливлення відстеження самого процесу передачі даних дозволяє оптимізувати та підвищити безпеку роботи модулю. Програмний модуль можна використовувати в будь-якому підрозділі, як самостійну систему, для збору інформації з метою виконання поставлених завдань.

ЛІТЕРАТУРА

1. Закон України про розвідку [Електронний ресурс].– Режим доступу URL: https://zakon.rada.gov.ua/laws/show/912-20

2. Бойовий статут Збройних Сил України [Електронний ресурс].– Режим доступу URL: https://zakon.rada.gov.ua/laws/show/548-14

д. т. н. Стрельбіцький М. А. НАДПСУ
д. військ. н.Мазур В. Ю. НАДПСУ

КРИТЕРІЙ ЯКОСТІ СИСТЕМИ РОЗМЕЖУВАННЯ ДОСТУПУ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІНОЇ СИСТЕМИ ДЕРЖПРИКОРДОНСЛУЖБИ НА СТАДІЇ МОДЕРНІЗАЦІЇ

Проблеми забезпечення безпеки інформаційних систем (ІС) держави є постійним та актуальним предметом обговорення в наукових колах. Дана проблема також є об'єктом уваги міжнародних організацій. Сучасний стан розвитку суспільства характеризується великою роллю електронних ресурсів, які становлять інформаційну інфраструктуру держави та системи регулювання відносин, що виникають при цьому, зокрема політики безпеки.

Політика безпеки є базовою категорією у галузі захисту інформації інформаційних систем. Під нею розуміють сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Під час розробки інформаційних систем та визначення ступеня їх рівня захищеності суттєву роль відіграють моделі безпеки. Їх застосування забезпечує системний та науково обґрунтований підхід до: вибору й обґрунтування основних підходів до структури інформаційних систем, що визначає способи реалізації методик, методів та засобів забезпечення властивостей інформаційного ресурсу; формального підтвердження стану захищеності інформаційної системи шляхом доказу теорем безпеки використаних моделей політик безпеки; розробка формального опису політики безпеки.

Розробкою та дослідженням моделей інформаційної безпеки присвячена значна кількість робіт дослідників. Водночас розроблена та впроваджена в дію велика сукупність міжнародних і вітчизняних стандартів та нормативних документів у галузі інформаційної безпеки. Моделі інформаційної безпеки не передбачають спільного функціонування з іншими аналогічними моделями на загальному полі даних, як це можливо під час модернізації інформаційних системи у складі ІС. У всіх моделях передбачено функціонування єдиної системи (монітору безпеки, ядра безпеки тощо), яка забезпечує дотримання політики безпеки.

Формування політики безпеки ІС, під час дотримання якої забезпечується дотримання властивостей інформаційного ресурсу, неможливе без моделей інформаційної безпеки, як формалізованого опису її базових засад. Тільки за допомогою формальних моделей можна довести безпеку системи, спираючись при цьому на постулати математичної теорії. Моделі безпеки визначають базові принципи функціонування політики безпеки та використовуються під час її побудови, формування технологічних рішень та обґрунтовують здатність системи забезпечувати дотримання властивостей інформаційного ресурсу. Аналіз структури зазначених моделей дозволяють визначити переваги та недоліки порівняно з іншими моделями, що зі свого боку сприяє опису виду критерію якості систем розмежування доступу, які побудовані на базі цих моделей.

На теперішній час запропоновано достатньо багато стратегій моделювання поведінки системи розмежування доступу. Частина з них, не дозволяючи узагальнено описати деталі, змушені спрощувати або ігнорувати найчастіше важливі деталі системи. У зв'язку з цим доцільно застосувати схему моделювання, що використовує абстрагування для спрощення аналізу захисту, і, разом з тим, ураховує всі деталі поведінки системи, необхідні для повного захисту. Кожна із відомих моделей оперує трійкою: суб’єкт, об’єкт, операція, тобто яку операцію може здійснити суб’єкт над об’єктом (читання, запис, видалення тощо).

Для подання системи розмежування доступу (СРД) визначимо ряд множин: об'єктів – термінали, вузли мережі, канали зв'язку, зовнішні пристрої, програми, томи, каталоги, файли, записи, поля запису; суб'єктів – користувачі або процеси, що виконуються від їх імені (користувачі, адміністратори, програми, процеси, термінали); операцій – послідовності дій суб'єкта по відношенню до об’єкта.

На основі введених вище понять СРД становить об'єкт теоретико-множинного обчислення. Правила розмежування доступу тоді будуть описуватися моделлю інформаційної безпеки, результати якої характеризують дозвіл або заборону операції з боку суб'єкта по відношенню до об'єкта. Якщо перетин множин складових старої та нової версій СРД є пустою множиною, то колізії між новою і старою версіями системи розмежування доступу в ІС відсутні. Дана вироджена ситуація не входить в область дослідження.

Досліджувані суперечності існують, якщо результат взяття декартової різниці між старою та новою версіями буде відмінний від пустої множини. Фізично елементи цієї множини утворюють спільне поле, через яке здійснюється взаємодія різнорідних компонентів ІС. Проаналізуємо, якими властивостями повинна володіти і яким вимогам задовольняти структура СРД, з метою усунення невідповідностей, що призводять до можливості порушення політики безпеки.

Організація доступу до інформаційних ресурсів ІС користувачів або процесів від їх імені відповідно до їх повноважень є призначенням будь-якої СРД. Завдання такого розмежування полягає у дотриманні вимог політики безпеки яка запроваджена в ІС, а саме властивостей інформації. Порушення властивостей інформації трактується керівними документами та науковцями як будь-які небажані дії, що призводять до порушення хоча б однієї із властивостей інформації. Отже, для порушення властивостей інформації необхідна дія (вплив) користувача на об'єкт системи, який містить дану інформацію.

Розглянемо кожну із властивостей інформації на предмет спільних ознак, які призводять до порушення заданої властивості. Відповідно до термінології в галузі захисту інформації, конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом. Тобто наявність недозволеного інформаційного потоку між об'єктом-носієм інформації та користувачем призводить до порушення конфіденційності. Наступна властивість інформації – цілісність, суть якої полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом. Аналогічно попередній властивості, наявність недозволеного інформаційного потоку призводить до порушення цілісності. Ще одна властивість інформації – доступність, як властивість ресурсу системи, яка полягає в тому, що користувач або процес від його імені, що має відповідні політикою безпеки повноваження, має право використовувати ресурс, не очікуючи довше заданого проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, у місці, необхідному користувачеві, і в той час, коли він йому необхідний. У даному випадку відсутність інформаційного потоку, який передбачено політикою безпеки як дозволений, призводить до порушення доступності.

Аналогічно іншим, спостереженість – властивість, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії. Дане визначення передбачає наявність дозволеного інформаційного потоку до журналів обліку діяльності користувачів та процесів, а також фіксації інших дій.

Загальною ознакою порушення кожної із властивостей інформації є наявність недозволеного або відсутність дозволеного інформаційного потоку. Як правило, такого виду потоки виникають в обхід політики безпеки та є прихованими. Під прихованим інформаційним потоком будемо розуміти механізм, за допомогою якого в ІС може здійснюватися інформаційний потік (передача інформації) між сутностями в обхід політики (правил) розмежування доступу.

Водночас сам факт порушення правил виникнення інформаційних потоків (наявність прихованих інформаційних потоків) має імовірнісний характер. Отже, імовірність виникнення прихованих інформаційних потоків адекватно характеризує якість структури системи розмежування доступу.

д.т.н. Субач І.Ю. (ВІТІ ім. Героїв Крут)
Власенко О.В. (ВІТІ ім. Героїв Крут)

СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ КІБЕРЗАХИСТУ СИСТЕМ КЕРУВАННЯ БАЗАМИ ДАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

В Україні продовжує активно розвиватись цифрова галузь. Кожного дня процес діджиталізації суспільних інститутів набирає обертів і це не оминає військову галузь. Автоматизація військових процесів управління є важливим аспектом для процесу інтеграції України в НАТО. У рамках автоматизації військ створюються нові інформаційні системи (ІС), які стрімко впроваджуються та функціонують у повсякденній діяльності посадових осіб органів військового управління. Актуальною проблему для безперебійного функціонування ІС стає забезпечення їхнього кіберзахисту.

Головним елементом структури кожної ІС являються бази даних (БД), в яких зберігаються дані, що є важливим активом кожної системи.Тому безпеку БД не можливо ігнорувати. Завдяки надзвичайній важливості даних захист БД від кібератак є важливим елементом у кіберзахисті системи в цілому. Зазвичай, завдання захисту БД розглядається в контексті трьох основних аспектів: конфіденційність, цілісність та доступність.

Ураховуючи це та на підставі аналізу сучасних наукових публікаційможна визначити основні загрози безпеки БД (рис. 1).

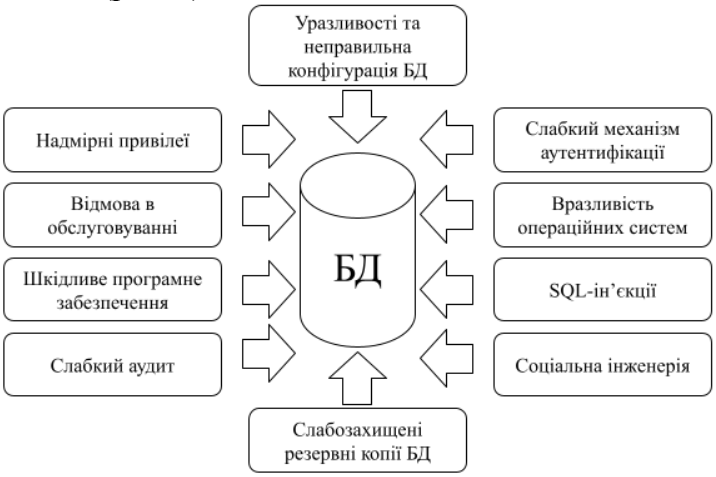


Рис.1. Основні загрози баз даних

Виходячи з цього, атаки на БД можна розділити на такі категорії:

1. Прямі атаки: коли атака здійснюється безпосередньо на цільові дані. Ця атака успішна, якщо БД не містить жорсткого механізму захисту.

2. Непрямі атаки, коли зловмисники не атакують безпосередньо ціль, але інформацію про дані можна зібрати за допомогою інших об'єктів інформаційної системи. Використовуються комбінації різних типів запитів, які важко відстежити.

Додатково атаки класифікуються: на активні, у яких змінюються фактичні значення даних та пасивні, у яких зловмисник спостерігає лише за даними, наявними в БД, не вносячи жодних змін до них.Слід зауважити, що для захисту БД від наведених загроз і кібератак не існує єдиного стандарту моделі безпеки. Більшістю науковців пропонуються вузьконаправлені рішення. Вони, переважно вирішують завдання захисту БД частково. Тому дослідження в даному напрямі є актуальними.

Таким чином, безпека БД є важливим аспектом у забезпеченні функціонування ІС військового призначення. Проведений аналіз дозволив визначити основні загрози і категорії кібератак на БД та показав недостатність сучасних методів та засобів їх кіберзахисту. Тому, наукова задача щодо розробки науково-методичного апарату для захисту БД від кібератак, є актуальною та потребує вирішення.Textovod = 98%

д.т.н. Субач І.Ю. (ВІТІ ім. Героїв Крут)
д.ф. Фесьоха В.В. (ВІТІ ім. Героїв Крут)
Чуджановська Д.С. (ВІТІ ім. Героїв Крут)

МЕТОДИКА ВИЯВЛЕННЯ АНОМАЛІЙ ТРАФІКУ ІНФОРМАЦІЙНОЇ МЕРЕЖІ НА ОСНОВІ ЛОГНОРМАЛЬНОГО РОЗПОДІЛУ

На сьогоднішній день з-поміж існуючих підходів виявлення кібератак на інформаційні мережі (ІМ) найперспективнішим залишається напрямок виявлення аномалій, оскільки дозволяє у своїй більшості з прийнятними показниками точності і повноти виявляти некласифіковані інформаційно-руйнівні (деструктивні) впливи. До того ж, реалізація даного підходу на практиці не вимагає значних зусиль, на відміну від опису сигнатур усіх відомих кібератак, часто достатньо лише опису моделі поведінки ІМ. Так, вихід за межі порогових значень множини досліджуваних параметрів, наприклад, телеметрії мережевого трафіку свідчить про аномальну (відмінну від нормальної, типової) поведінку, що у свою чергу свідчить про факт потенційного здійснення невідомого методу (способу) кібервпливу.

Поряд з цим, не кожна аномалія є кібератакою, оскільки природа їх походження не виключає наслідків як програмних помилок (збоїв), так і апаратних несправностей вузлів ІМ, що у свою чергу характеризує даний процес як імовірнісний.

У зв'язку з цим, виникає актуальне наукове завдання удосконалення існуючих систем кіберзахисту ІМ у руслі ефективнішого виявлення аномалій, природа походження яких є потенційним наслідком кібервпливу.

Аналіз публікацій за даною тематикою показав доцільність застосування до вирішення такого класу завдань методів, побудованих на основі стохастичного аналізу, оскільки процеси цілеспрямованого кібервпливу не піддаються моделям відомих законів розподілу, за винятком, розподілених на великому проміжку часу.

У контексті зазначеного, пропонується удосконалення існуючих систем виявлення аномалій шляхом покладення у їх функціонал двофакторного аналізу телеметрії мережевого трафіка: в першу чергу описується нормальна поведінка ІМ на основі статистичних діапазонів значень телеметрії мережевого трафіку, вихід за межі яких буде сприйматися системою як аномалія; наступним етапом є стохастичний аналіз значень зафіксованої аномалії на предмет її відповідності логнормальному закону розподілу випадкової величини; у випадку відповідності аналізованого вектору значень аномалії даному розподілу аномалія класифікується як ненавмисна (програмний збій, апаратна несправність, некомпетентність користувача), у противному випадку – кібаратака (чіткий сценарій).

Вибір логнормального закону розподілу у якості науково-методичного удосконалення існуючих систем кіберзахисту обумовлено точками перетину його властивостей, трафіку ІМ та природою походження аномалій: значення телеметрії мережевого трафіка і кількості аномалій не може бути від'ємною завдяки асиметрії розподілу, а також дозволяє ефективно описувати процеси, у яких досліджуване значення становить випадкову частку попереднього значення. У графічній інтерпретації застосування такого підходу у кінцевому результаті, на відміну від нормального закону розподілу на системі координат виглядає як згладжування викидів, де явними залишаються навмисні, цілеспрямовані (штучні).

Таким чином, запропонований підхід до виявлення аномалій трафіку ІМ значно підвищить ефективність існуючих систем кіберзахисту за показником точності та дозволить виявляти сценарні кібератаки нульового дня шляхом контролю допустимого відхилення значень телеметрії мережевого трафіка від нормального, опираючись на неможливість реалізації на практиці інформаційно-руйнівного впливу на ІМ, сценарій якого розподілений на короткому проміжку часу. З метою отримання найбільшої вигоди від застосування даного підходу доцільно його використовувати у якості другого ешелону аналізу мережевого трафіку.

Табенський С.М. (НАДПСУ)
к.т.н. Хоптинський Р.П. (НАДПСУ)

КІБЕРФІЗИЧНІ СИСТЕМИ, АНАЛІЗ ТА ПЕРЕДУМОВИ ВИНИКНЕННЯ ВРАЗЛИВОСТЕЙ

Актуальність. Кіберфізичні системи (Cyber-physical systems, CPS) – це системи, які поєднують в собі можливість аналізу фізичного простору (на основі даних з різноманітних датчиків), системи прийняття рішень (програмний модуль), а також кінцевих пристроїв (виконавчі елементи), що дають змогу моніторити зміни в навколишньому середовищі, та реагувати на них в режимі реального часу. На сьогоднішній день сфери використання таких систем постійно зростають: транспорт (автопілоти), медицина (роботизована хірургія та біонічні кінцівки), сектор безпеки (безпілотні літальні апарати, роботизовані системи розмінування, система «Інтелектуальний кордон» ДПСУ) та ін.

Оскільки такі системи складаються з великої кількості різних елементів (як фізичних так і програмних) виникають загрози пов’язані з забезпеченням надійності та достовірності їх функціонування, особливо для критичних галузях, де відмови, обумовлені атаками на вразливості, фізичними і проектними дефектами, можуть призвести до значних матеріальних втрат, аварій, загрози життю людей. Тому протидія таким загрозам є дуже важливим критерієм при прийняті рішення на використання кіберфізичних систем.

Постановка задачі. Для ефективної боротьби з можливими несанкціонованим втручанням в роботу кіберфізичних систем, необхідно провести аналіз вразливостей таких систем, які можуть виникати, як в фізичному так і кіберпросторі в процесі їх експлуатації.

Основні положення. Щоб забезпечити широке впровадження та розгортання систем CPS та використовувати їх переваги, важливо захистити ці системи від будь-яких можливих атак, внутрішніх чи/або зовнішніх, пасивних чи активних.

Фактично, вразливості CPS можна поділити на три основні категорії:

- Вразливості мережі: включають слабкі місця захисних заходів, використання не достатньо захищеного дротового/бездротового зв'язку та з'єднань, атаки "людина посередині, MITM-атаки", підслуховування, сніфінг, спуфінг та атаки на стек зв'язку (мережа/транспорт/прикладний рівень), бекдори, атаки DoS/DDoS та маніпуляції пакетами.
- Вразливості платформи: включають вразливості обладнання, програмного забезпечення, конфігурації та бази даних.
- Вразливості управління: включають відсутність правил, процедур і політик безпеки.

Вразливості виникають з багатьох причин. Серед яких можна виділити:

- Припущення про ізоляцію: при розробці систем працівники керуються припущенням, щодо її ізольованості від зовнішнього світу.
- Масштабованість: при збільшенні площі покриття системи та підключення до неї нових пристроїв збільшується площа можливих атак.
- Неоднорідність складових систем: системи CPS включають різнорідні компоненти сторонніх розробників, які інтегровані в неї, де кожен продукт від різних виробників схильний до різних проблем безпеки.
- Використання USB: це одна з основних причин вразливості CPS, оскільки зловмисне програмне забезпечення знаходиться всередині USB.
- Шпигунство. Системи CPS також схильні до атак шпигунства/спостереження, в основному, використовуючи типи шпигунських програм (зловмисних програм), які отримують прихований доступ і залишаються непоміченими роками.
- Однорідність систем: подібні типи кіберфізичних систем страждають від тих самих вразливостей, які після використання можуть вплинути на всі пристрої.

Висновки. Таким чином представлений аналіз дозволяє більш глибоко розуміти можливі вразливості до яких схильні кіберфізичні системи, та причини їх виникнення, в процесі їх експлуатації та в подальших дослідженнях розробити ефективні методи боротьби з ними.

Ткаченко І. М. (ДУТ)
Мягких Г.Г.

ВИКОРИСТАННЯ ТЕОРІЇ КАТАСТРОФ ДЛЯ ОЦІНКИ СТАНУ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Сучасний кіберзахист об'єктів критичної інформаційної інфраструктури представляє собою сукупність складних систем, раптові зміни функціонування яких потребують поєднання різних способів аналізу їх стану, а також передбачення(прогнозування) їх ефективності.У будь-якій системі, на яку діють різноманітні фактори, відбуваються не тільки плавні, але ірізкі, стрибкоподібні зміни. Різні науки (від фізики до економіки та соціології) ще накопичують достатню кількість аналітичних даних, які дозволили б їм у розрізі часу відслідковувати тренди для прогнозування стрибкоподібних поведінкових змін, та передбачати необхідні реакції у відповідь на них. Про те моделювання поведінки різноманітних систем таких як: механічних, термодинамічних, екологічних, в яких плавна зміна внутрішніх параметрів може спричинити собою стрибкоподібні зміні стану системи дозволяє здійснити опис властивостей цих систем за допомогою деякої функції (f). Порушення ж нормального виконання функції і може бути визначеним як стан катасторофи

Теоретичні аспекти теорії катастроф.

Перші відомості про теорію катастроф з'явилися в західній пресі близько 1970 р. Стверджувалося, що нова наука – теорія катастроф для людства набагато цінніша, ніж математичний аналіз: тоді як ньютонівська теорія дозволяє досліджувати лише плавні, безперервні процеси, теорія катастроф дає універсальний метод дослідження всіх стрибкоподібних переходів, розривів, раптових якісних змін (Арнольд, 1990). Основоположником сучасної теорії катастроф є Рене Том, який у 1972 р. запропонував використовувати топологічну теорію динамічних систем, що веде початок від робіт А. Пуанкаре та А.А. Андронова для моделювання розривних змін у явищах природи. Особливості, біфуркації та катастрофи – терміни, що описують виникнення дискретних структур із гладких, безперервних (Арнольд, 1990). Математична теорія катастроф спрямована на розробку математичних моделей катастроф найрізноманітніших явищ стрибкоподібної зміни функціонування системи у відповідь на плавну зміну зовнішніх умов, що мають деякі спільні риси (Острейковський, 2005). Об'єктом теорії катастроф є стрибкоподібні переходи систем з одного стану до іншого, розриви у плавних, безперервних процесах, раптові якісні зміни поведінки систем. Джерелами теорії катастроф є: теорія гладких відображень Уітні та теорія біфуркацій динамічних систем Пуанкаре та Андронова (Арнольд, 1990).

Біфуркація визначається, як роздвоєння і вживається в широкому значенні для позначення всіляких якісних перебудов або метаморфоз різних об'єктів при зміні параметрів, яких вони залежать.

Біфуркаційною множиною називається кордон, що розділяє області простору керуючих параметрів з якісно різною поведінкою системи, що вивчається (Алексєєв, Сухоруков, 2000).

Однією з головних задач теорії катастроф є отримання так званої нормальної форми досліджуваного об'єкта (диференціального рівняння або відображення) в околиці "точки катастрофи" і побудована на цій основі класифікація об'єктів.

Суттєві ознаки теорії катастроф та біфуркаційної множини в об'єктах критичної інформаційної інфраструктури.

Об'єкт критичної інформаційної інфраструктури – це фізичні та віртуальні системи, об'єкти і ресурси - руйнування, знищення або зниження дієздатності яких призведе до суттєвих загрозам країні (регіону або міста), її національної безпеки, безпеки і здоров'ю населення.

Система кіберзахисту в об'єктах критичної інформаційної інфраструктури, як правило ступінчаста, багаторівнева система, в якій будь-яка невизначеність, випадковість у вхідних

параметрах у нижніх рівнях призводить до невизначеностей та випадковостей у вихідних параметрах підсистем вищого порядку та системи загалом. У такій системі за характерними ознаками можлива катастрофа. Тому для терміну "Катастрофа " в контексті кіберзахисту визначаємо, різку та якісно - негативну зміну(порушення) стану кіберзахисту на об’єктах критичної інформаційної інфраструктури при плавних(поступових у часі) кількісних змінах їх параметрів, від яких він залежить життєдіяльності всього об’єкту чи його окремих складових.

Також слід врахувати, що параметри оцінки ознак рівня катастрофи кіберзахисту мають різну природу та характеризують вплив кризової ситуації на об’єкті критичної інформаційної інфраструктури з різних сторін.

Вони можуть бути представлені(вирахувані) в якісному або кількісному вигляд, у відповідності до методів які будуть застосовуватись для визначення таких ознак.

Загалом же для будь яких систем Ю.К. Алексєєв та А.П. Сухоруков (2000) розглядають такі основні ознаки катастроф:

1) модальність - це властивість об'єкта системи, що полягає в тому, що при деякому значеннікеруючих параметрів можливі кілька положень рівноваги системи (кілька мод);

2) недосяжність - у системі одне з положень рівноваги не досягається і не спостерігається;

3) катастрофічні стрибки - стрибкоподібний перехід системи з одного положення рівноваги до іншого;

4) гістерезис – перехід системи з одного стану в інший і назад за різних значень керуючих

параметрів;

5) розбіжність - мала зміна шляху в просторі параметрів призводить до якісно відмінного кінцевого стану системи

Теорія особливостей Уітні – узагальнення дослідження функцій на максимум та мінімум.

Завдання будь-якої економічної системи – оптимізація. Метою моделі оптимізації в основномує максимізація прибутку чи мінімізація витрат.

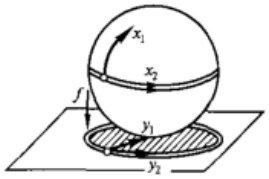


Рис. 1 Складка Уітні

Теорія особливостей Уітні найбільш застосовна до систем, у яких будь-якої миті часу натлі ситуації, що змінюється, мінімізується або максимізується деяка функція (Острейковський, 2005).

Теоретично Уітні розглядаються відображення, тобто. набори функцій кількох змінних.Виникають спеціальні геометричні перетворення Р. Том назвав елементарними катастрофами.До таких геометричних перетворень відноситься відображення поверхні на площину, тобтозіставлення кожній точці поверхні точки площини. Відображеннягладке, якщо функції, що задають відображення, гладкі (диференційованідостатня кількість разів – наприклад, багаточлени) (Арнольд, 1990).

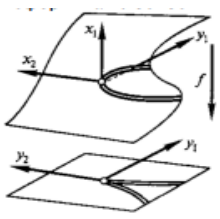


Рис.2Складання Уітні

Якщо точка поверхні задана координатами (x1; x2)поверхні, а точка площини - координатами (y1; y2) на площині, товідображення задається парою функцій y1 = f1(x1; x2), y2 = f2(x1; x2).

Особливості зустрічаються лише двох видів.

1) Складка Уітні - виникає при проектуванні сфери на площину точках екватора (рис. 1) і задається формулами:

$$y1 = x12,$$
$$y2 = x2.$$

2) Складання Уітні - виходить при проектуванні на площину поверхні (рис. 2) і задається формулами:

$$y1 = x13 + x1x2,$$
$$y2 = x2.$$

Уітні довів, що будь-яка особливість гладкого відображення поверхні на площину після відповідного малого ворушіння розсипається на складання та складки. Особливості цих двох видів стійкі та зберігаються при малих деформаціях відображення (Арнольд, 1990). Один з найбільш важливих висновків теорії особливостей полягає в універсальності декількох простих образів: складки, збирання та точки повернення. Ці образи мають зустрічатися повсюдно (Острейковський, 2005).

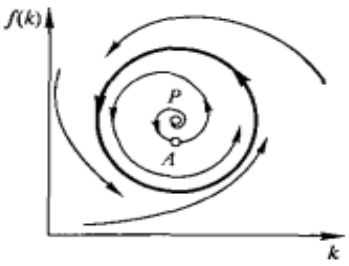


Рис. 3Фазоваплощина системи

Рівновага та втрата стійкості у фазовому просторі.

Еволюційний процес будь-якої системи, зокремкіберзахисту математично описується векторним полем у фазовому просторі. Точка фазового простору визначає стан системи. Доданий у цій точці вектор вказує швидкість зміни стану системи. У деяких точках вектор може дорівнювати нулю. Такі точки називаються положеннями рівноваги, у яких стан системи у часі не змінюється.

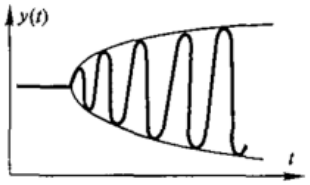


Рис.5 М'якавтратість стійкості

Будь-яка системи кіберзахистунеспроможна перебувати тривалий час у рівновазі. Вона схильна вплив різних чинників, тому можуть виникнути нерівноважністани (коливання), тобто. система може стати нестійкою. Коливання, що встановилися, зображуються замкненою кривою - граничним циклом на фазовій площині (Арнольд, 1990). Приклад фазової площини системи показано на Рис. 3.

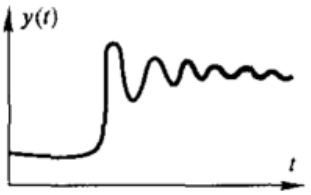


Рис. 6 Жорсткавтратість стійкості

Якщо положення рівноваги – режим, що встановився в реальній системі, то при зміні параметра спостерігаються наступні явища, що спостерігаються і в поведінці системи кіберзахисту:

1) Після втрати стійкої рівноваги режимом, що встановився, виявляється коливальний періодичний режим.

Цей вид втрати стійкості називається м'якою втратою стійкості (Рис. 5).

2) Перед тим як режим, що встановився, втрачає стійкість, область тяжіння цього режиму стає дуже малою, і завжди присутні випадкові обурення викидають систему з цієї області ще до того, як область тяжіння повністю зникає. Цей вид втрати стійкості називається жорсткою втратою стійкості. У цьому система йде зі стаціонарного режиму стрибком і перескакує інший режим руху (Рис. 6) (Арнольд, 1990).

Режим, що встановився, може бути іншим стійким стаціонарним режимом, або стійкими коливаннями, або більш складним рухом. Такі режими руху отримали назву «Атракторів», оскільки вони "притягують" сусідні режими (перехідні процеси) (Арнольд, 1990). Атрактор (від англ. toAttract - притягувати) приваблює безліч динамічної системи. Компактне інваріантне підмножина фазового простору, що асимптотично стійке, тобто. воно стійке по Ляпунову, і всі траєкторії з його околиці прагнуть до нього при $t \to \infty$ (Острейковський, 2005).

Втрата стійкості стану рівноваги не обов'язково пов'язана з біфуркацією, система може втрачати рівновагу внаслідок наростання коливань, що самопідтримуються.

Визначення основних видів критичних точок в об'єктах критичної інформаційної інфраструктури.Основним методом дослідження стрибкоподібних переходів від плавної зміни будь-яких параметрівв об'єктах критичної інформаційної інфраструктури, в тому числі системи кіберзахисту є наявність у гладкої речової функції критичних точок, в яких похідна звертається в нуль. Дослідження критичних точок гладких функцій важливе у зв'язку з наступним твердженням: якщо деякі властивості системи описуються функцією f, що має сенс потенційної енергії, то з усіх можливих переміщень дійсними будуть ті, при яких f має мінімум (фундаментальна теорема Лагранжа про те, що мінімум повної потенційної енергії енергії системи є достатньою для стійкості). Під впливом чинників стан кіберзахисту об'єктів критичної інформаційної інфраструктури у стійкому рівновазі, якщо функція потенціалу має суворий локальний мінімум. При перевищенні певних значень цих факторів система плавно змінюватиме свій стан, якщо критична точка невироджена. При деякому збільшенні навантаження критична точка вироджується, вироджена критична точка як структурнонестійка розпадається на невироджену або зникає. Стан системи кіберзахистуїх у своїй стрибкоподібно перетворюється на новий стан (втрата стійкості, руйнація, пластичні деформації тощо.). Численні особливості, біфуркації та катастрофи (стрибки) виникають у всіх завданнях про знаходження екстремумів, завдання оптимізації, управління та прийняття рішень. У загальному випадку в теорії катастроф розроблений наступний підхід для дослідження властивостей системи: функція f розкладається в ряд Тейлора, і потрібно знайти відрізок цього ряду, який адекватно описує властивості системи поблизу критичної точки для даної кількості керуючих параметрів (Пітухін, 1998). Обчислення при цьому проводяться за рахунок правильного відкидання одних членів ряду Тейлора та залишення інших – "найважливіших" (Острейковський, 2005). Найбільш поширені типи критичних точок для гладкої функції – це локальні максимуми, мінімуми та точки перегину. Для двох та більше змінних завдання ускладняється завдяки широкому діапазону геометричних можливостей. Класифікація типів критичних точок – це одне з головних математичних джерел теорії катастроф (Острейковський, 2005).

Структурна стійкість.

Поняття " структурна стійкість " було вперше запроваджено теорії диференціальних рівнянь А.А. Андроновим та Л.С. Понтрягіним в 1937 р. під назвою "грубість системи" (Алексєєв, Сухоруков, 2000). Рене Том вказав на важливість вимог структурної стійкості чи нечутливості до малих збурень (Острейковський, 2005).

Функція f структурно стійка, якщо всім досить малих гладких функцій p критичні точки f і (f + p) мають і той ж тип. Наприклад візьмемо функцію f(x) = x 2 і p = 2εx, де ε – мала константа. Обурена функція набуде вигляду: f(x) = x 2 + 2εx = (x + ε) 2 – ε 2 . Таким чином, критична точка зрушила (причому величина усунення гладко залежить від ε), але не змінила свого типу. Чим вище ступінь n, тим гірше поводиться x n : обурення f(x) = x 5 може призвести до чотирьох критичниxx точок (двох максимумів і двох ммінімумів). Структурна стійкість може застосовуватись до поточних інцидентів та незначних кіберзагроз (інформаційних впливів), що суттєво не порушують стану кібербезпеки в об'єктах критичної інформаційної інфраструктури.

Таким чином, можна зробити висновок:

1) оскільки достану кіберзахисту об'єктів критичної інформаційної інфраструктури ставляться завдання оптимізації (максимізація функції виконання всіх поточних завдань об'єктом критичної інформаційної інфраструктури або мінімізація функції втрати його дієздатності), то тут найбільш застосовною може виявитися доцільною для використання теорія особливостей Уітні;

2) теорію катастроф можна застосувати як метод дослідження стрибкоподібних переходів, розривів, раптових якісних змін стану кіберзахисту об'єктів критичної інформаційної інфраструктури ;3) важливим є поняття структурної стійкості функції чи нечутливості до малихобурення системи, що актуальне в сьогоденні при постійному зміні стану кіберзахисту з урахування появи нових індикаторів кіберзагроз.

к.т.н. ТрушО.В. (КНУ ім. Т. Шевченка)
к.е.н. Труш М.С. (КНУ ім. Т. Шевченка)
Деркач Т.М. (ВІТІ)

ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ЯК ФРАГМЕНТУ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Залежно від принципів керування, розрізняють такі різновиди безпілотних літальних систем:

безпілотні некеровані;

безпілотні автоматичні;

безпілотні дистанційно-пілотовані літальні апарати (ДПЛА).

Вступ

Розвиток безпілотних літальних апаратів та інфраструктури розумних міст ставить безліч нових теоретичних і практичних завдань. Одне з них побудова сенсорної мережі, як мережі толерантної до затримок, із застосуванням безпілотних літальних апаратів в якості засобу доставки даних. Ця задача передбачає організацію взаємодії вузлів БСМ із засобами зв'язку РЛА з урахуванням особливостей їх руху.

Літаюча сенсорна мережа як система масового обслуговування

Вузли БСМ деяким чином в загальному випадку випадково, розподілені по території, що обслуговується.

Припустимо, що кластеризація наземної мережі відсутня, а РЛА рухається по деякій заданій траєкторії.Тоді основний показник якості функціонування такої мережі — це час збору і доставки даних буде залежати від швидкості руху літального апарата. Вибір швидкості руху обмежений як технічними характеристиками самого літального апарату, так і ймовірно-часовими характеристиками процесу обміну даними між засобами зв'язку РЛА і вузлами БСМ.

Модель фрагмента літаючої сенсорної мережі для передачі даних на великі відстані

З урахуванням аналізу типових структур побудови ЛСМ була розроблена архітектура мережі передачі даних на великі відстані, що складається:

1) З наземного сегмента ЛСМ, що складається з безлічі сенсорних вузлів, об'єднаних в бездротову сенсорну мережу.

2) Літаючого сегмента ЛСМ, що включає в себе:

- безпілотний літальний апарат.
- групи безпілотних літальних апаратів

3) Базової станції мережі LPWAN – Інтернет

У даній архітектурі безпілотний літальний апарат, з встановленим на ньому пристроєм, який виконує роль шлюзу, є вузлом, що збирає дані з наземного сегмента мережі. У зв'язку з невеликою тривалістю польоту РЛА загального користування і великою відстанню до LoRa – IPбазова станція потрібно організувати канал передачі даних в реальному часі. Для організації такого каналу використовують проміжні РЛА.

Завдання обслуговування безлічі вузлів доцільно розглянути для двох типових випадків: у першому випадку — координати вузлів відомі, у другому — ні.

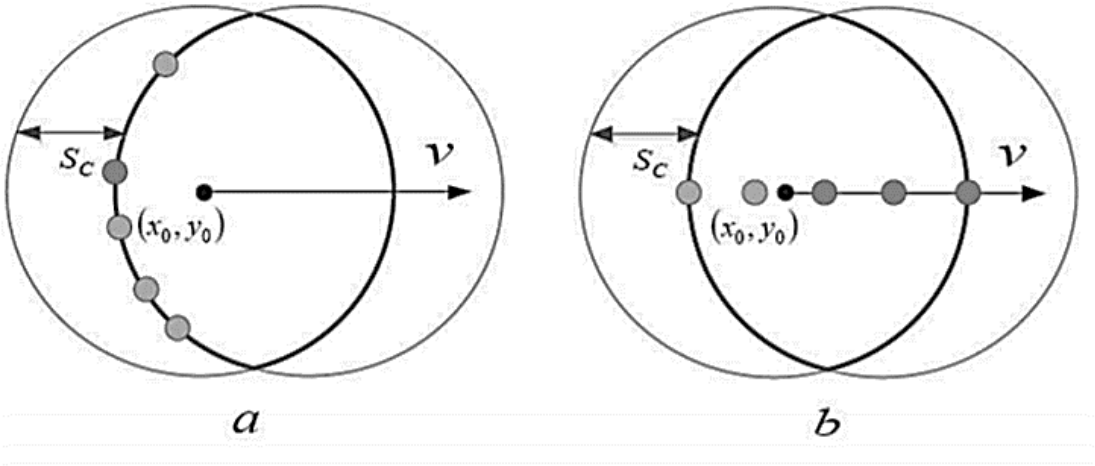


Рис 1 . Різне розміщення вузлів в зоні обслуговування.

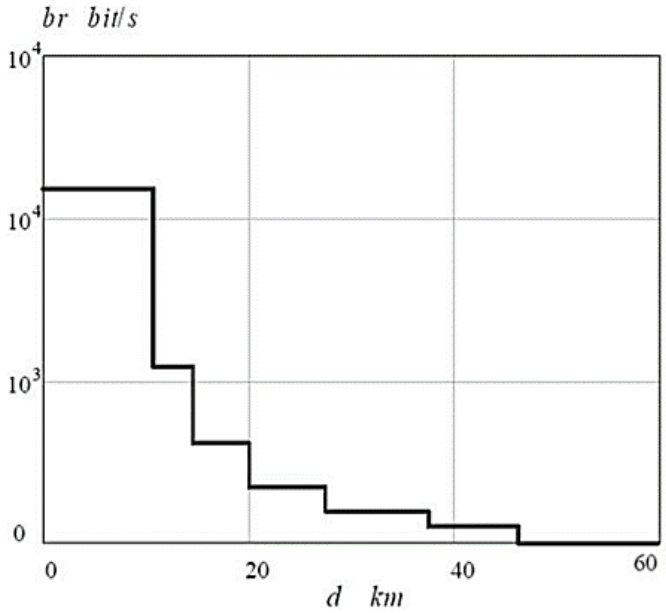


Рис. 2. Залежність швидкості передачі від відстані між приймачем і передавачем

Таким чином, запропонована модель дозволяє встановити залежність часу обслуговування пакета у вузлах зв'язку, затримки на очікування та ймовірності втрат пакетів від параметрів маршруту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аль-Наггар Я. М. Алгоритм выбора головного узла кластера для всепроникающих сенсорных сетей с использованием нечеткой логики и диаграмм Вороного / Я. М. Аль-Наггар // Электросвязь. 2014. — No 9. — С. 14-18.

2. Andriy Dudnik; Lyudmyla Kuzmych; Olexander Trush; Tetyana Domkiv; Olga Leshchenko; Viktor Vyshnivskyi. Smart Home Technology Network Construction Method and Device Interaction organization Concept. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), 25-27 листопада 2020 р.

к.т.н. Труш О.В. (КНУ ім. Т. Шевченка)
к.т.н.Радзівілов Г.Д. (ВІТІ)

СИСТЕМААНАЛІЗУ ТА ПРОГНОЗУВАННЯ ІНТЕРНЕТ-ТРАФІКУ ТА ЇЇ ВПРОВАДЖЕННЯ В МЕРЕЖЕВІ ТЕХНОЛОГІЇ

Зі стрімким зростанням мережевого трафіку (рис 1) та все більшим числом методів мережевих атак, традиційна система моніторингу мережевого трафіку не може задовольнити вимоги щодо зберігання даних та запитів у режимі реального часу. Тому, як ефективно контролювати масштабний мережевий трафік, стало важливою проблемою для управління безпекою мережі[1]. Для цього я розробила систему, що зможе коректно прогнозувати стан трафіку в мережі за допомогою методу аналізу наявних варіантів створення та прототипів, розробка алгоритмів роботи підсистеми, збору даних, системи зв’язку.

Розроблена система є актуальною, оскільки дозволяє кожному українському провайдеру в будинках, приватних закладах не відставати від сучасних технологій, які можуть використовувати свої функції за допомогою нейронної мережі:

1) прогнозування;
2) аналіз;
3) кластеризація

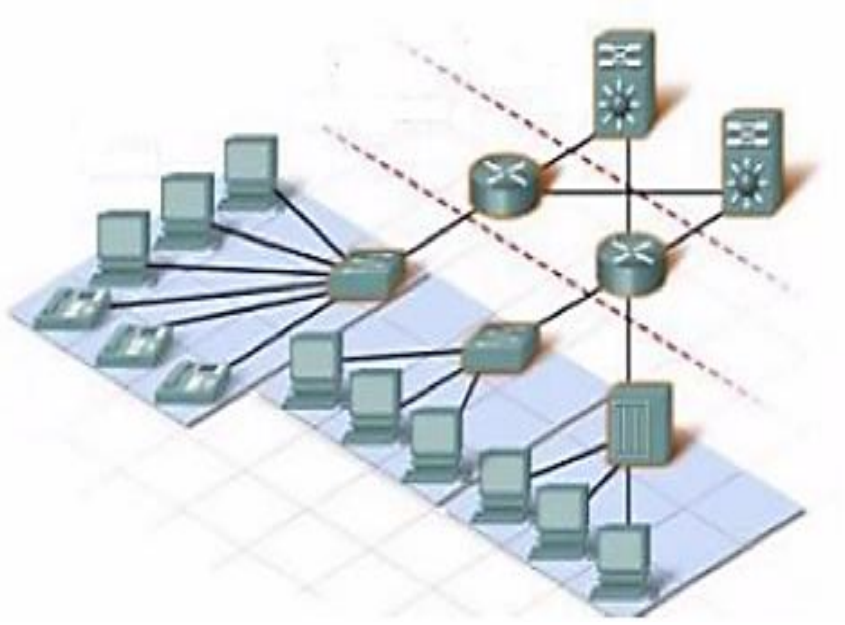


Рис 1. Мережевий трафік

Інтернет реалізований за допомогою програмного пакета, модулів та системних структур. В інтересах розробленого проекту було проведено дослідження стандартів архітектурної розробки. Модельовані алгоритми: робота мережі, збір даних, системи зв'язку на випадок прямої необхідності вдосконалення наявних розробок.

Інтернет-трафік – обсяг інформації, що передається через комп'ютерну мережу за певний проміжок часу. Кількість трафіку вимірюється як в пакетах, так і в бітах, байтах і їх похідних: кілобайт (КБ), мегабайт (МБ).

Програми, які здійснюють підрахунок мережевого трафіку: TMeter, BWMeter, NetWorx, DU Meter, NetTraffic, NetBalancer.

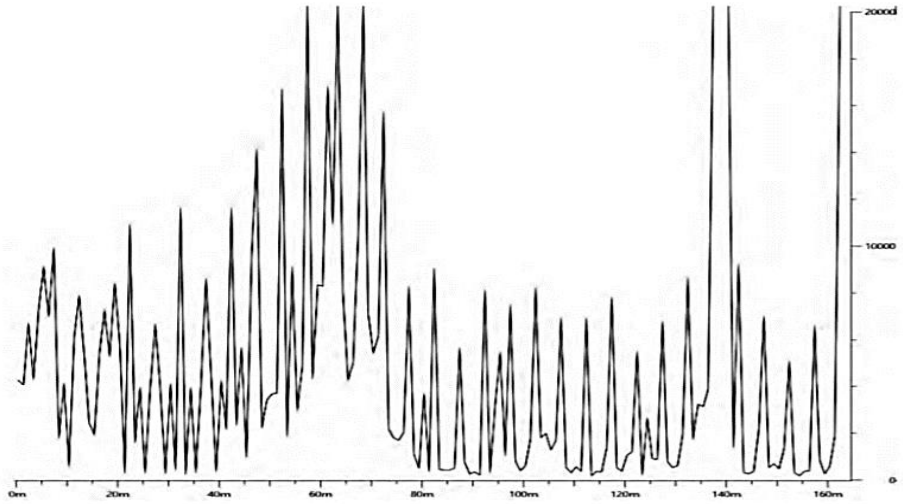


Рис. 2 - Приклад прогнозування мережевого трафіку

Ви можете аналізувати трафік за допомогою таких методів:

- аналізуючи фонове електромагнітне випромінювання і таким чином відновлюючи трафік, який фактично «прослуховується»;
- через гілку (апаратне чи програмне забезпечення) трафіку, а також надсилаючи її копію снайферу;
- "прослуховування" мережевого інтерфейсу (цей метод ефективний при використанні в сегменті концентраторів ("концентраторів") замість перемикачів ("комутаторів"), інакше метод дуже неефективний, оскільки аналізатор мережевих протоколів отримує лише окремі кадри);
- підключення аналізатора мережевих протоколів до розриву каналу;
-через атаку на рівні мережі (IP-спуфінг) або каналу (MAC-спуфінг), що призводить до перенаправлення даних про трафік "жертви" або всього трафіку.

Розроблену систему пропонується розробити за допомогою Python. Цей продукт дозволяє поєднувати різні програмні технології: C ++, PHP, SQL, HTML. Практичне значення результатів дає змогу користувачам розробленої підсистеми регулювати трафік залежно від прогнозів, які зробила нейронна мережа.

Аналіз результатів роботи системи моніторингу Інтернет-трафіку на основі методу аналізу наявних варіантів і прототипів, розробка алгоритмів для підсистеми, збору даних, системи зв'язку дозволяє досягти економічного ефекту та економії часу провайдерів завдяки:

1) спрощенню процесу прогнозування помилок;
2) скороченні часу на аналіз стану дорожнього руху;
3) можливості безпосереднього спілкування з системою, додатковою платформою для майбутньої оптимізації системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Анатомия беспроводных сетей» / Сергей Пахомов. – Компьютер- Пресс, №7,2017

2. Yurii Kravchenko, Oleksandr Trush; Olena Starkova. Model of Information Protection System Database of the Mobile Terminals Information System on the Territory of Ukraine (ISPMTU). IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T) Date of Conference: 6-9 Oct. 2020

Фесенко О.Д.(ВІТІ)
Бєляков Р.О. (ВІТІ)
Радзівілов Г.Д. (ВІТІ)

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ БЕЗПЛАТФОРМНОЇ ІНЕРЦІАЛЬНОЇ НАВІГАЦІЙНОЇ СИСТЕМИ БПЛА НА ОСНОВІ НЕЙРОМЕРЕЖЕВИХ АЛГОРИТМІВ

У зв'язку із тим, що у військовій сфері перевага надається мініатюрному класу безпілотних літальних апаратів (БПЛА) через: високу мобільність, дешевизну, легкість маскування, високу маневреність, зростає необхідність розробок алгоритмів інтелектуальних систем управління БПЛА в автономному режимі польоту незалежно від наявності сигналів глобальних систем позиціювання.

В загальному вигляді,модель траєкторії БПЛА будується на основі данихнавігаційної системи від глобальної системи позиціювання GPS та процесів роботи МЕМС інерціальної системи навігації на основі вдосконаленого фільтру Маджвіка, яка в сутності представляє собою 18-мірний вектор стану, що показано в рівнянні:

$$P = \left[\phi_{E,N,U}\ \Delta V_{E,N,U}\ \Delta P_{l,\lambda,h}\ \Delta g_{x,y,z}\ \Delta a_{x,y,z}\ \Delta m_{x,y,z}\right]^T,$$

де $\phi_{E,N,U}$ −вектор похибки орієнтації відносно платформи БПЛА, який представляє собою проекцію обертання Землі на осі (east-north-up), $\Delta V_{E,N,U}$ − похибки даних швидкості БПЛА відносно локальної системи координат БПЛА, $\delta_{l,\lambda,h}$ − похибка довготи, широти та висоти, $\Delta g_{x,y,z}$ −похибки постійного відхилення гіроскопа в системі координат відносно МЕМС датчиків, $\Delta a_{x,y,z}$ – похибки постійного зміщення акселерометра, $\Delta m^{\mathrm{E}}{}_{x,y,z}$ −похибки магнітометра (феромагнітний вплив) відносно визначення магнітної півночі, індекс Е – еталонна модель магнітного поля.

В момент раптового зникнення сигналу глобальної системи позиціювання для визначення оцінки позиціювання безпілотного літального апарату, тобто (швидкість і положення БПЛА), застосовується алгоритм нейронної мережі для заміни сигналу GPS для прогнозування позиції БПЛА в просторі.

Експериментальне дослідження процесів керування траєкторією БПЛА під час зникнення сигналів GPS здійснювалось в програмному середовищі Simulink Matlab (версія 2020.b) та мови програмування Python з використанням бібліотек Google Tensor Flow (версія 2.1.0) з відкритим кодом, для глибокого навчання використовуючи реальний набір даних датчиків БІНС. Експериментальна платформа зібрана на основі макетної плати ProsKitBx-4123 із використанням розробленої імітаційної моделі (рис. 1).

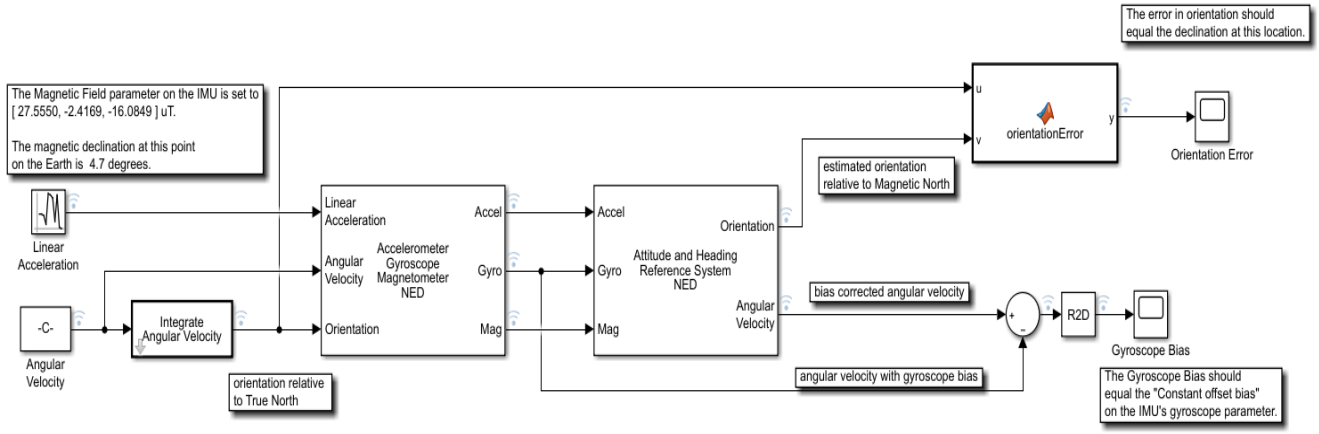


Рис. 1.Імітаційна модель обробки навігаційних параметрів Simulink Matlab

Враховуючи вихідні дані, обмеження та допущення здійснюється оцінка позиціювання безпілотного літального апарату (швидкість і положення БПЛА) з використанням алгоритму ELM – Kalman та WANN –RNN Madgwick.

Вхідні дані:

Q={ $q1(\phi_{E,N,U}), q2(\varepsilon V_{E,N,U}), q3(\varepsilon P_{l,\lambda,h})$ } – вектор еталонних параметрів позиціювання БПЛА.

Вихідні дані:

T={ $q1(\phi_{E,N,U}+\Delta_{t+1}), q2(V_{E,N,U}+\Delta_{t+1}), q3(P_{l,\lambda,h}+\Delta_{t+1})$ } – цільові вихідні параметри прогнозування траєкторіїБПЛА в автономному режимі польтупід час зникнення сигналу GPS.

Обмеження:

$\mathrm{T}(\Delta_{\omega\text{БПЛА}}) \le \{0.012 \dots 0.18\}^{\circ}\frac{1}{\mathrm{c}}$ –відхилення від цільової траєкторії БПЛА в автономному режимі польоту [4-6];

період навчання нейромережі - $t_{lerningrate} \le \{10 \dots 100\}$с ;

швидкість адаптивного навчання нейромережі $-t_{\text{adaptive learning}\,rate} \le \{0.034 \dots 0.05\}$с.

Цільова функція: $F(\mathrm{T}(\Delta_{\omega\text{БПЛА}})) \rightarrow min \Rightarrow \min_{\beta}\left\|H\beta - T`\right\| \Rightarrow optimum(NNA)$.

Допущення: Швидкість польоту БПЛА є сталою.

Під час експерименту для забезпечення коректного зняття вимірів гіроскопа (прискорення, кутової швидкості) використовується датчик інерціальної навігаційної системи MEMS MPU-9250. Далі, сигнал отриманий на вході датчика демодулюється та проходить через 16-бітний АЦП. Швидкість АЦП (Sample Rate) може програмно варіюватися від 3.9 до 8000 вибірок в секунду (Samples per second, SPS).

Результат експериментів показав, що застосування алгоритму на основі ELM – Kalman точність навчання нейромережі безплатформної інерціальної навігаційної системи (ІНС) була кращою в порівнянні з алгоритмом MELM – Madgwick на 13.94%, та WANN – RNN – Madgwick на 29.82 % [10]. Однак, необхідно зазначити, що точність навчання покращувалась із зростанням кількості нейронів в структурі прихованого рівня < 500, що підвищує обчислювальну складність та відповідно збільшує час процесу навчання.

Застосування розробленої методики керування траєкторією БПЛА в автономному режимі польоту на основі нейромережевого алгоритму MELM – Madgwick [10] дозволило здійснити адаптацію структури прихованого рівня, яка становить 100 нейронів прихованого рівня, що дозволяє його використання у якості компромісного варіанту, що підтверджено імітаційним моделюванням.

Таким чином, розроблена нова методикакерування траєкторією БПЛА в автономному режимі польоту на основі нейромережевого алгоритму MELM – Madgwick, дозволяє:

по-перше, інтегрувати розроблений алгоритм в системи управління БПЛА на базі МЕМС технології мікрокомп’ютерівArduino Nano, під час зникнення GPS сигналу, на часовому інтервалі t = (10...300 с), що являється критичним для класу мікро – та малих безпілотників;

по-друге, розроблений алгоритм MELM – Madgwick дозволяє апроксимувати, та екстраполювати вхідні сигнали навігаційних параметрів в динамічному середовищі, за рахунок процесу адаптивного навчання в реальному часі (оптимізації нейромережевої структури);

по-третє, вперше було запропоновано застосувати блок перетворювача навігаційних даних в кватерніону форму для зменшення розмірності вхідних даних, без застосування процесу квантування;

по-четверте, вперше був застосований нейромережевий алгоритм MELM для вирішення задач автономної навігації для зменшення відхилення БПЛА від цільової траєкторії під час зникнення GPS сигналів;

в результаті застосування методики керування траєкторією БПЛА в автономному режимі польоту на основі нейромережевого алгоритму MELM – Madgwick під час зникнення сигналів глобальних супутникових систем позиціювання, похибка прогнозування

навігаційних параметрів траєкторії найменша і склала ≈30–33 м, що додатково підтверджує доцільність його використання для мікро - БПЛА.

Напрямком подальших досліджень є розробка методики управління міні – БПЛА в мережах FANETs (Flying Ad-hoc Networks) з урахуванням особливостей організації каналів управління і зв'язку.

ЛІТЕРАТУРА

1. Fendy Santoso, Matt Garratt, Anavatti, S.G. (2018). State-of-the-art intelligent flight control systems in unmanned aerial vehicles. IEEE Transactions on Automation Science and Engineering, Volume: 15, Issue: 2, April 2018, 613-627. https://doi.org/10.1109/TASE.2017.2651109

2. Ding, S., Ma, G., Shi, Z. (2014). A rough RBF neural network based on weighted regularized extreme learning machine. Neural processing letters, vol. 40, no. 3, 245–260.View at: https://link.springer.com/article/10.1007/s11063-013-9326-5

3. Xiaoji Niu, Sameh Nassar, Naser El-Sheimy. (2007). An accurate land-vehicle MEMS IMU/GPS navigation system using 3D auxiliary velocity updates. Navigation, 54(3): September 2007, 177-188. https://doi.org/10.1002/j.2161-4296.2007.tb00403.x

4. Fesenko, O. D., Bieliakov, R. O., Radzivilov, H. D., Hulii, V. S. (2020). Eksperymentalnyi analiz zastosuvannia neironnykh merezh dlia keruvannia traektoriieiu polotu BPLA. Zbirnyk naukovykh prats VITI № 1 – 2020. Data dostupu 02.02.2021. http://www.viti.edu.ua/files/zbk/2020/11_1_2020.pdf

5. Fesenko O., Bieliakov R., Radzivilov H. and oth. (2020) Trajectory Control Method Of UAV In Autonomous Flight Mode Using Neural Network MELM Algorithm. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). 25-27 Nov. 2020. https://doi.org/10.1109/ATIT50783.2020.9349317.

6. Elsken Thomas, Metzen Jan Hendrik, Hutter Frank (2019). Neural architecture search: A Survey. Journal of Machine Learning Research. 20 (55), 1–21. View at: https://www.jmlr.org/papers/volume20/18-598/18-598.pdf.

7. Adam Gaier, David Ha. (2019). Weight agnostic neural networks.Submitted on 11 Jun 2019 (v1), last revised 5 Sep 2019 (this version, v2). View at: https://arxiv.org/abs/1906.04358

8. Itay Hubara, Matthieu Courbariaux, Daniel Soudry, Ran El-Yaniv, Yoshua Bengio. (2018). Quantized neural networks: training neural networks with low precision weights and activations. Journal of Machine Learning Research 18, 1-30. View at: https://jmlr.org/papers/v18/16-456.html

9. Lashley, M., Bevly, D. M., Hung, J. Y. (2009). Performance analysis of vector tracking algorithms for weak GPS signals in high dynamics. IEEE Journal of Selected Topics in Signal Processing, vol. 3, no. 4, 661–673, 2009. https://doi.org/10.1109/JSTSP.2009.2023341

10. Bieliakov, R. O., Radzivilov, H. D., Fesenko, O. D. (2019). Method of the intelligent system construction of automatic control of unmanned aircraft apparatus. Radio Electronics, Computer Science, Control. National University "Zaporizhzhia Polytechnic", Vocabulary. Part 28. Artificial intelligence vol. 1, 2019, 218–229. https://doi.org/10.15588/1607-3274-2019-1-20.

д.ф. Фесьоха В.В. (ВІТІ ім. Героїв Крут)
Ванівський Н.І. (ВІТІ ім. Героїв Крут)
Вірста А.В. (ВІТІ ім. Героїв Крут)
Літвін О.В. (ВІТІ ім. Героїв Крут)

АВТОМАТИЗАЦІЯ ПОВСЯКДЕННОЇ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ ВВНЗ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

В умовах зростання темпів автоматизації діяльності оборонного сектору України залишається відкритим питання ефективного й оперативного виконання рутинних повсякденних завдань підрозділами вищих військових навчальних закладів (ВВНЗ). Так, наряду із провадженням базової діяльності у відповідності до функціональних обов'язків науково-педагогічним персоналом та особовим складом навчально-лабораторних комплексів існує потреба у постійному виконанні множини типових (шаблонних) другорядних (меш пріоритетних) завдань (оповіщення особового складу на місцях, ідентифікація прибуваючих осіб, запобігання ситуаціям, що загрожують здоров'ю людей (виникнення пожежі), формування щоденної звітності тощо).

Аналіз публікацій за даною тематикою показав, що актуальним та доцільним шляхом вирішення такого класу питань є впровадження стеку інформаційних технологій штучного інтелекту (машинне навчання (machine learning), машинне мислення (machine reasoning), машинний зір (machine vision) та машинний слух (machine hearing)).

У зв'язку з цим, виникає актуальне науково-прикладне завдання щодо розробки інтелектуальної комп'ютерної системи автоматизації повсякденної діяльності (САПД) підрозділу ВВНЗ на основі технологій штучного інтелекту, впровадження якої дозволить вирішити вищезазначене завдання та надасть можливість військовослужбовцям ефективніше використовувати службовий час.

Суть даного підходу полягає у програмній реалізації наступного функціоналу САПД:

ідентифікація як особового складу підрозділу, так і керівного складу ВВНЗ на основі техніки машинного зору засобами цифрової камери;

аудіальна взаємодія людини з системою через програмний інтерфейс підсистеми машинного слуху з метою оперативного отримання звітної інформації, постановки типових завдань по команді, а також віртуального асистування;

оповіщення особового складу підрозділу на місцях засобами акустичної системи і сервісами електронної пошти та/або миттєвого обміну текстовими (голосовими) повідомленнями віддалено в позаслужбовий час про виникненні події у відповідності до пріоритету;

комп'ютерна підсистема навчання у відповідності до кваліфікації, що здобувається;

побудова профілів користувачів системи з метою адаптивної обробки завдань під особистість засобами машинного навчання;

планувальник шаблонних (типових) завдань загального призначення;

моніторинг стану локальної мережі та електронних сервісів підрозділу;

запобігання ситуаціям, що загрожують здоров'ю людей (виникнення пожежі).

В основу науково-методичного забезпечення запропонованої САПД доцільно покласти комплекс наступних методів інтелектуального аналізу даних: штучних нейронних мереж – для підсистем машинних зору і слуху, когнітивного аналізу – для комп'ютерної системи навчання, колаборативної фільтрації та опорних векторів – для моніторингу локальної мережі, глибокого навчання для побудови профілів користувачів, а також подієво-орієнтований механізм для підсистеми оповіщення особового складу.

Таким чином, впровадження запропонованої системи у діяльність ВВНЗ дозволить військовослужбовцям багато в чому ефективніше виконувати свої функціональні обов'язки, делегуючи виконання другорядних завдань інтелектуальній комп'ютерній системі (перевід задачі у «фоновий» режим).

д.ф. Фесьоха В.В. (ВІТІ ім. Героїв Крут)
Ковальчук А.І. (ВІТІ ім. Героїв Крут)

ВИЗНАЧЕННЯ НЕЧІТКОГО МЕТАМОРФНОГО ЯДРА КІБЕРАТАК НА ОСНОВІ КЛАСТЕРНОГО АНАЛІЗУ

Тенденції розвитку технологій створення і поширення зловмисного програмного забезпечення тісно пов'язані із удосконаленням методів, способів та засобів його виявлення.Так, існуючі засоби виявлення кібератак не завжди підтверджують задекларований рівень ідентифікації кібератак, що проявляється впостійних спалахах зловмисної активності. Збитки, заподіяні шкідливим програмним забезпеченням, сягають трильйонів доларів (6 трильйонів доларів відповідно до звіту компанії Cybersecurity ventures за 2021 рік).

Серед множини методів кібервпливу одне з центральних місць займають метаморфні кібератаки, оскільки складають основну частку вторгнень нульового дня.

Складність виявлення такого типу інформаційно-руйнівних впливів обумовлена використанням технологій модифікації власного програмного коду з кожною новою ініціалізацією. Два екземпляра однієї і тієї ж метаморфної кібератаки будуть синтаксично різними, але матимуть однаковий вектор впливу, що не дозволяє побудувати її сигнатуру, залишаючи питання виявлення метаморфних кібератак відкритим.

Аналіз публікацій за даною тематикою показав доцільність та ефективність застосування для вирішення даного питання методів (моделей), що побудовані на основі апарату теорії нечіткої логіки, оскільки демонструють найвищі показники точності та повноти виявлення поліморфних і метаморфних кібератак, а також прийнятної обчислювальної складності. Застосування зазначених методів передбачає використання експертного досвіду у вигляді баз нечітких продукційних правил. Так, описано модель виявлення метаморфних кібератак, побудова нечіткого класифікатора для якої передбачає експертне визначення найбільш значущих досліджуваних параметрів із множини наявних для кожного класу кібератак (у випадку KDD-99 – 41 параметр мережевого трафіку), формуючи таким чином метаморфне ядро кожного класу відомих кібератак. Застосування такого підходу дозволяє виявляти кібератаки, вектор впливу яких однаковий, обходячи механізми самомодифікації програмного коду. Поряд з цим, визначення найбільш значущих ознак (поведінкових характеристик) кібератак виконується експертом у ручному режимі, що вимагає найвищої кваліфікації фахівця з кібербезпеки, значних часових затрат, а також можливості виявляти неочевидні (скриті) особливості і зв'язки у статистичних наборах даних. У зв'язку з цим, виникає актуальне науково-прикладне завдання підвищення ефективності виявлення метаморфних кібератак шляхом автоматизації процесу визначення метаморфного ядра для класу кібератак із офіційних джерел даних (KDD).

З урахуванням показників максимальної правдоподібності, а також природи походження зазначених кібератак, пропонується підхід до вирішення даного завдання шляхом використання науково-методичного апарату кластерного аналізу (задача розбиття множини досліджуваних об'єктів на підмножини (кластери), так, щоб кожен кластер складався із схожих об'єктів, а об'єкти різних кластерів істотно відрізнялися), зокрема методу ефективної категоризації за ознаками – методу нечіткої кластеризації С-середніх (Fuzzy C-Means Clustering). На відміну від чітких, даний алгоритм не відносить досліджуваний об'єкт (наприклад, фіксований вектор мережевого трафіка) однозначно до певного кластера (класу ознак кібератак), а визначає кожному із них ступінь належності об'єкта, формуючи тим самим матрицю належності для визначення міри подібності на основі відстані між ними у *n*-вимірному просторі ознак.

Таким чином, запропоноване удосконалення науково-методичного апарату існуючих систем виявлення кібератак дозволить вирішити окреслену проблематику, що у свою чергу значно підвищить їх ефективність у руслі виявлення метаморфних кібератак, які складають значну частку інформаційно-руйнівних впливів нульового дня.

д.ф. Фесьоха В.В. (ВІТІ ім.Героїв Крут)
Кондратюк А.Г. (ВІТІ ім.Героїв Крут)
Ковба Р.В. (ВІТІ ім.Героїв Крут)

ПІДСИСТЕМА ВИЯВЛЕННЯ АНОМАЛЬНОГО ФУНКЦІОНУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ МЕТОДУ ОПОРНИХ ВЕКТОРІВ

В умовах прогресивного розвитку технологій та інструментів кібервливу на комп'ютеризовані системи і мережі у вигляді кібератак, несанкціонованого втручання, а також функціонального зловживання програмним забезпеченням (ПЗ) залишається відкритим питання їх ефективного кіберзахисту.

Серед існуючих напрямків кіберзахисту інформаційно навантажених комунікаційних систем та мереж особливої уваги заслуговує контроль функціонування наявного прикладного ПЗ, оскільки досить велика частка деструктивних інформаційно-руйнівних впливів реалізують вектор атаки саме його засобами. Так, наприклад, кібератака Petya.A на Україну здійснювалася через програму для звітності та документообігу M.E.doc.

Факт неможливості виявлення кібератак нульового дня існуючими системами захисту комп'ютеризованих систем і мереж обумовлює актуальність подальших досліджень, які полягають у підвищенні ефективності їх застосування у контексті виявлення аномального функціонування ПЗ на основі аналізу поведінки спостережуваного процесу. Під аномальним функціонуванням ПЗ у даному випадку розуміється поведінка процесів, яка відрізняється від нормальної, типової (штатної) у конкретній ситуації, або яка не представлена достатньою множиною прикладів у навчальній вибірці.

Аналіз публікацій за даною тематикою показав, що з-поміж існуючих науково-методичних апаратів вирішення класифікаційної задачі виявлення аномалій, таких як: графи сценаріїв кібератак, методи, засновані на специфікаціях, методи на сплайнах, мережі Петрі, дерева рішень, імунні системи, одним з найефективніших є метод опорних векторів (support vector machine) – техніка машинного навчання з учителем, оскільки демонструє досить високу точність та прийнятну обчислювальну складність, а також дозволяє виявляти аномальну поведінку у часі, близькому до реального.

Суть даного методу полягає у формуванні фіксованого вектора ознак стану ПЗ, побудові та навчанні бінарного класифікатора, у результаті чого відбувається його віднесення до певного класу функціонування: правомірного (еталонного) чи забороненого (аномального). Так, у процесі експлуатації підсистема виявлення аномального функціонування ПЗ порівнює реальну поведінку процесів із шаблоном їх нормального функціонування і при виявленні значних розбіжностей сигналізує про факт вірогідного порушення (наприклад, позапланове оновлення ПЗ, як у випадку кібератаки Petya.A).

Для формування опорних векторів аномального та нормального класів функціонування ПЗ ознаками поведінки для оптимальної роздільної двомірної гіперплощини (лінійної регресії) обрано:

показники станів взаємодії процесу (процесів) ПЗ з іншими процесами та/або ресурсами;

послідовність переходів процесів ПЗ, що відбуваються закономірним порядком у вигляді правил.

Наступним етапом є визначення межі прийняття рішення із максимальним зазором, який розділяє вектори на два вищевказаних класи, залишаючи місце для неправильної класифікації. Гіперплощину доцільно будувати з жорстким зазором (hard-margin SVM) – вектору не дозволяється потрапляти на неї.

Таким чином, запропонована підсистема дозволить підвищити ефективність існуючих систем кіберзахисту шляхом виявлення аномального функціонування ПЗ, що у свою чергу дозволяє ефективно виявляти кібератаки нульового дня, а також значно ускладнює використання уразливостей ПЗ.

д.ф. Фесьоха В.В. (ВІТІ ім.Героїв Крут)
Лаврик М. А. (ВІТІ ім.Героїв Крут)

ІНТЕЛЕКТУАЛЬНА ПІДСИСТЕМА ПРОГНОЗУВАННЯ НЕСПРАВНОСТЕЙ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ПІДХОДУ КОЛАБОРАТИВНОЇ ФІЛЬТРАЦІЇ

У контексті глибокої автоматизації діяльності усіх без винятку галузей держави пріоритетною задачею є забезпечення надійного функціонування комп'ютерних інформаційних систем.

Одним із актуальних напрямків вирішення даного завдання є забезпечення стабільного і надійного функціонування апаратного забезпечення (АЗ) інформаційних технологій, оскільки навіть незначна несправність АЗ може призвести до відмови роботи усього стеку системного та/або прикладного програмного забезпечення.

Аналіз публікацій за даною тематикою показав доцільність діагностичного підходу та спектрального аналізу АЗ до виявлення несправностей у режимі реального часу. Проте, вказані підходи не дозволяють завчасно відреагувати на поточну несправність АЗ, приходиться розбиратися із нею постфактум, що у свою чергу може призвести до непередбачуваних наслідків, в тому числі порушення цілісності і доступності даних на прикладному рівні.

У контексті зазначеного виникає завдання пошуку та розробки (удосконалення) підходу до попередження несправностей АЗ, здатного завчасно попереджувати користувача (відповідальну особу) про несправність АЗ, яка імовірно може виникнути (факт появи несправності ще не відбувся), адже виникнення несправності АЗ, як правило, не відбувається випадково, а передбачає низку передуючих цьому подій.

Завдання даного класу традиційно покладаються на предиктивні (прогнозуючі) моделі, оскільки їх науково-методичний апарат дозволяє з прийнятною точністю прогнозувати події на основі описаного попереднього досвіду.

У зв'язку з цим, пропонується розробити інтелектуальну підсистему прогнозування несправностей АЗ, яка дозволить вирішити описану проблематику. В основу науково-методичного апарату запропонованої підсистеми, враховуючи однотипність засобів зв'язку та автоматизації у Збройних силах України, доцільно покласти підхід на основі методу колаборативної фільтрації (collaborative filtering), зокрема алгоритм «заснований на сусідстві». Суть даного підходу полягає у реалізації наступної послідовності дій:

хронологічний збір даних про події та показники функціонування АЗ усіх вузлів локальної мережі;

збір даних про виникнення несправності АЗ мережі;

автоматизоване збереження хронологічного настання подій, які слідували появі несправності АЗ комп'ютерної техніки у вигляді сценаріїв;

циклічне порівняння ланцюга подій АЗ вузла мережі із наявними сценаріями у базі даних шляхом застосування вищеописаного науково-методичного апарату.

Так, інтелектуальна підсистема прогнозування несправностей АЗ робить висновки про вірогідний стан АЗ на основі методу колаборативної фільтрації засобами попередньо описаного хронологічного сценарію подій: «ЯКЩО хронологія подій на вузлі мережі з типовим АЗ співпадає із формальним сценарієм подій у базі даних, який призвів до певної несправності АЗ, ТО з певною вірогідністю можна зробити прогноз виникнення даної несправності».

Таким чином, запропонована підсистема здатна зробити висновок про виникнення несправності АЗ до її настання та попередити про даний факт відповідальну особу, що дозволить здійснити необхідні превентивні заходи по збереженню (реплікації) даних на прикладному рівні, що у свою чергу підвищить безвідмовність (стабільність) функціонування інформаційних систем.

Фесьоха Н. О. (ВІТІ ім. Героїв Крут)
Мамчур В. О.(ВІТІ ім. Героїв Крут)

ПРОГРАМНО-АПАРАТНА ПЛАТФОРМА ІДЕНТИФІКАЦІЇ ОСОБОВОГО СКЛАДУ НА БАЗІ МІКРОКОНТРОЛЕРА RASPBERRYPI

Актуальність. Враховуючи активний перехід ЗСУ на стандарти NATO, зокрема FMN(FederatedMissionNetworking), СЗ TaxonomySTANAG, їх використання у процесі обліку особового складу, речового майна, озброєння та організації логістики, на сьогоднішній день актуальним є питання автоматизації пропускного режиму. Головною задачею якого є не допустити проникнення сторонніх людей на територію військової частини. Зараз пропуск відбувається через пропускні квитки чи по військовому квитку який звіряють по списку військовослужбовців частини. Автоматизація цього процесу повинна спростити перевірку особистості та зменшити час на видачу пропусків та занесення в базу особового складу.

Мета. Автоматизація контрольно пропускного режиму на всіх режимних об’єктах .

Виклад основного матеріалу. Дана програмно-апаратна платформадля ідентифікації особового складу міститиме наступні складові:

5. Спосіб ідентифікації посадової особи.
6. Можливість вносити дані про особовий склад в базу.
7. Редагування та перегляд усіх існуючих осіб в базі.
8. Ідентифікація з перевіркою по базі для допуску на режимний об’єкт.

Для виконання поставленого завдання передбачається вирішення серії завдань:

- проаналізувати існуючі підходи по формалізації предметної області дослідження. Визначення обмежень, ускладнень та проблем, що не дозволяють досягнути максимальної ефективності процесу ідентифікації особового складу військовослужбовців;

-визначення технологічних підходів в ідентифікації особового складу військовослужбовців. Обґрунтування архітектури, структури алгоритмів роботи, веб орієнтованого застосування спрямованого на автоматизацію процесу дослідження;

- вибір оптимальної архітектури для інтерактивних систем;

- реалізація вибраного рішення.

Огляд сучасних рішень в реалізації інтерактивності інструментів всієї Web−системи розглянуто в рішеннях таких провідних вчених як Ли Цзена, Назар Подольчака, Світлани Сисоєвої. В роботі Ли Цзена відзначається, що безумовними перевагами інтерактивної системи є:

- одностороння прив'язка даних, що дозволяє з першого погляду визначати причини змін/помилок, що істотно прискорює налагодження;

- ніякої обов'язкової прив'язки до класів, що полегшує код;

- компоненти інтерфейсу можна виразити у вигляді наборів чистих функцій.

Для реалізації поставленої задачі перевага віддана технологічним інтерактивним підходам.

Висновок. ЗС України потребують використання нових технологій, для того щоб покращити не лише умови праці, але й функціонування військових частин.Сучасні технології дозволяють забезпечити більш високий рівень безпеки, автоматизацію робочих процесів по ідентифікації особового складу та допуску до об’єкту. Запропонований програмний модуль дозволить підвищити ефективність процесу ідентифікації особового складу у військових частинах.

д.ф. Фесьоха В.В. (ВІТІ ім. Героїв Крут)
Стемпковська Я.А. (ВІТІ ім. Героїв Крут)
Іваніна А.В. (ВІТІ ім. Героїв Крут)

ПІДСИСТЕМА АДАПТАЦІЇ КОМП'ЮТЕРНОЇ СИСТЕМИ НАВЧАННЯ НА ОСНОВІ КОГНІТИВНОЇ КАРТИ КОМПЕТЕНТНОСТЕЙ

В умовах модернізації державної політики цифрового розвитку та ініціатив Міністерства освіти і науки України, а також Міністерства цифрової трансформації України важливе місце відводиться застосуванню комп'ютерних інформаційних технологій (ІТ) у сфері вищої освіти як одного з найефективніших інструментів пізнання. До того ж, системно збільшується роль дистанційного навчання, як основного способу безпечної інформаційної взаємодії учасників освітнього процесу в умовах пандемії, що у свою чергу негативно впливає на глибину засвоєння навчального матеріалу об'єктом навчання. У зв'язку з цим, виникає актуальне науково-прикладне завдання пошуку (розробки) ефективного підходу до застосування ІТ в освітньому процесі, зокрема для забезпечення засвоєння об'єктом навчання необхідного рівня знань, і як наслідок, оволодіння достатньо повною множиною професійних компетентностей у відповідності до кваліфікації.

Аналіз публікацій за даною тематикою показав наявність підходу, який лише частково вирішує окреслену проблематику – впровадження у освітній процес комп'ютерних систем навчання (КСН). Так, дані системи взаємодіють із здобувачем освітнього рівня в інтерактивному режимі, демонструють необхідний матеріал, здійснюють необхідний зріз знань, аналізують профіль здобувача, таким чином беручи на себе певні функції тьютора. Поряд з цим, функціонал існуючих КСН забезпечує оволодіння фаховими компетентностями традиційно (повторне проходження тесту з метою набору необхідної кількості балів), що не гарантує необхідного рівня кваліфікації. На основі викладеного, пропонується удосконалення існуючих КСН шляхом реінжинірингу їх функціональної архітектури, зокрема додаванням підсистеми адаптації КСН, здатної визначати рівень засвоєння знань на відповідність кваліфікації, що здобувається. Враховуючи стиль та інтенсивність взаємодії учасників освітнього процесу, спосіб досягнення стратегічної мети (суб'єкт – об'єкт навчання), а також високі показники ефективності у процесах командної роботи в основу науково-методичного апарату даної підсистеми доцільно покласти підхід на основі когнітивного аналізу. Даний науково-методичний апарат передбачає послідовну причинно-наслідкову структуризацію інформації про досліджуваний процес:

будь-яка подія, що відбулася у системі, викликається причинами, поява котрих пов'язана із рухом матеріальних та нематеріальних потоків (інформаційна взаємодія);

кожен із виділених потоків описується відповідною сукупністю факторів. Об'єднання усіх сукупностей складає множину факторів, у термінах котрих описуються процеси у системі;

визначаються взаємозв'язки між факторами шляхом розглядання причинно-наслідкових ланцюгів, що описують рух кожного потоку.

Когнітивна карта – сутність когнітивного моделювання, як способу визначення сили і напрямку впливу факторів на переведення об'єкта управління у цільовий стан із урахуванням схожості та відмінності у впливі різних факторів на об'єкт керування (у контексті освітнього процесу: суб'єкт навчання і об'єкт навчання). Іншими словами це зважений орієнтований граф, у якому вершини однозначно відповідають факторам (компетентностям), в термінах яких описується предметна область (професійна кваліфікація), а дуги відображують безпосередні зв'язки (взаємовплив) між ними.

Множину визначених професійних компетентностей зі спеціальності у вищому навчальному закладі можливо представити у вигляді багатошарового графу (рис. 1) (багатовимірної матриці) компетентностей, де окремий шар – множина пов'язаних компетентностей навчальної дисципліни, окрема вершина – компетентність (сукупність

знань, умінь, здібностей і готовності особистості діяти у складній ситуації й вирішувати фахові завдання з високим рівнем невизначеності; здатність до досягнення більш якісного результату праці, ставлення до професії як до цінності). Компетентний спеціаліст відрізняється критичним мисленням, вмінням серед множини рішень обрати оптимальне, аргументовано спростовувати хибні рішення.

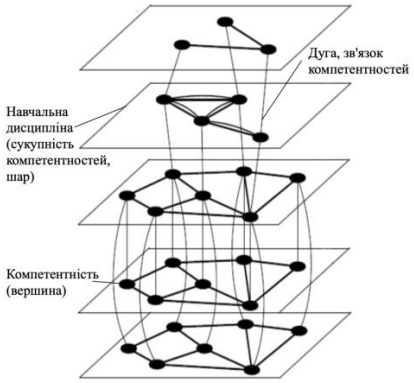


Рис. 1 Багатошаровий граф професійних компетентностей зі спеціальності

Описаний підхід дозволяє формалізувати процес засвоєння знань здобувачем рівня вищої освіти та визначити найбільш ефективні управлінські рішення та/або сценарії розвитку подій у освітньому процесі на основі виділених професійних компетентностей та зав'язків між ними (структурно-логічна схема), які кількісно та якісно характеризують поточну ситуацію виконання навчальної програми, а також оцінки взаємовпливу складових процесу.
На практиці, здобувач рівня вищої освіти, опановуючи матеріал навчальної дисципліни засобами КСН надає підсистемі інформацію для здійснення комплексної оцінки поточної ситуації, визначення причинно-наслідкових зв'язків успішного (неуспішного) засвоєння матеріалу, а також джерел впливу на процес навчання в цілому. Для вирішення завдання ефективного оволодіння професійними компетентностями, на відміну від традиційного підходу (повторне проходження тесту з метою набору необхідної кількості балів) пропонується підхід перезважування дуг графа компетентностей навчальної дисципліни. Так, у випадку виявлення КСН недостатнього рівня оволодіння компетентністю здобувачем освітнього рівня на основі певної множини знань, умінь, здібностей під час тестування, підсистемою адаптації КСН здійснюється перезважування дуг графа з метою позначення відповідальної за компетентність вершини як пріоритетної із визначенням сценарію часткового повторного вивчення матеріалу на основі когнітивної карти. Перехід до освоєння нового матеріалу, взаємопов'язаного із даною компетентністю блокується. До того ж, формалізований сценарій даного процесу представляється на узгодження науково-педагогічному працівнику із зазначенням виявлених причинно-наслідкових подій неуспішного засвоєння матеріалу здобувачем, що у свою чергу дозволяє підібрати необхідний матеріал для найефективнішого закриття прогалин у знаннях, або прийняти рішення про тимчасове зниження рівня складності навчального матеріалу до його засвоєння. Для процедури перезважування дуг графа компетентностей доцільно застосувати метод зворотного розповсюдження помилки, який показав високу ефективність у процесі навчання штучних нейронних мереж для різноманітних задач.Таким чином, запропоноване удосконалення існуючих КСН на основі когнітивної карти компетентностей значно підвищить ефективність освітнього процесу, зокрема у аспекті дистанційного навчання, що у свою чергу відповідає вектору зміни знаннєвої парадигми навчання на компетентнісну. До того ж, описаний у доповіді підхід позитивно вплине на якісну характеристику випускників навчальних закладів в умовах сьогодення, адже отримання диплому у результаті здобуття кваліфікаційного рівня свідчитиме про оволодіння кожною без винятку професійною компетентністю.

Фесьоха Н.О. (ВІТІ ім. Героїв Крут)
Яровий Я.С. (ВІТІ ім. Героїв Крут)

ПРОГРАМНИЙ МОДУЛЬ АВТОМАТИЗАЦІЇ ОПИТУВАННЯ ВІЙСЬКОВОСЛУЖБОВЦІВ ПІДРОЗДІЛУ

Опитування військовослужбовців підрозділу є невід'ємною і обов'язковою складовою службової діяльності в Збройних силах України. Одним з основних завдань опитувань - є автоматизація створення опитувань та швидкий аналіз відповідей військовослужбовців підрозділу і прийняття відповідного рішення. Для організації опитувань у підрозділах використовуються застарілі способи, з використанням паперових носіїв інформації, що затратно як матеріально, так і за часовими показниками. Таким чином, постає питання на знаходження альтернативних методів і способів для автоматизації створення опитувань та оперативне отримання результатів командирами, використовуючи сучасні інформаційні технології.

Пропонується здійснити розробку програмного модулю автоматизації опитування військовослужбовців підрозділу на основі веб платформи. Однією з переваг такого підходу є той факт, що даний модуль не залежатиме від конкретної операційної системи користувача та набагато простіший у використанні в порівнянні з нативними додатками.

Програмний модуль представлятиме собою систему збору і обробки результатів опитування. Найбільш поширеною реалізацією розподіленої системи збору та обробки даних є багаторівнева система безпеки, архітектура якої базується на використанні сенсорів на рівні даних, сервісів управління на рівні управління даними, сервісів на рівні даних на системному рівні, автоматизації робочого місця і контролерів безпеки на рівні користувача.

Опираючись на архітектуру системи безпеки, пропонується використовувати мікросервісну архітектуру (рис. 1). Програмний модуль буде розміщений на сервері, який включає в себе два мікросервіси. Перший мікросервіс відповідає за інтерфейс користувача (UI), другий (API) відповідає на запити з інтерфейсу користувача і працює з базою даних, яка знаходиться на іншому сервері.

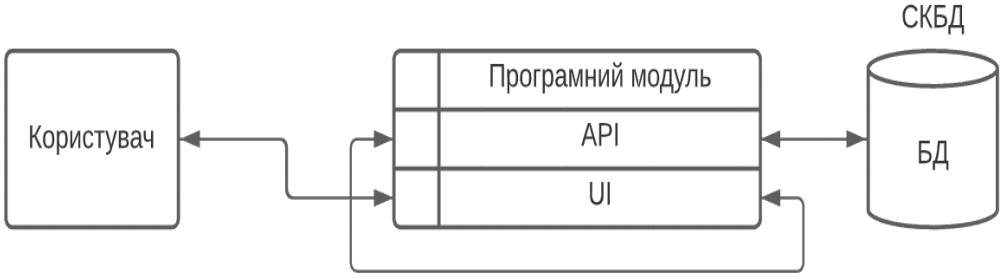


Рисунок 1 - Мікросервісна архітектура

Програмний модуль реалізований на основі мікросервісної архітектури можливо використовувати у підрозділах, як незалежну систему для проведення тестування, збору, аналізу, результатів. Крім того, на основі статистики відповідей, командири мають змогу робити висновки підрозділу

ЛІТЕРАТУРА

1. Чиста архітектура – Роберт Мартін
2. Ідеальний код – Стів Макконнел
3. Netflix і культура інновацій - Рид Хастингс, Ерін Меєр
4. Наказ Генерального Штабу №153 від 29.04 Оцінка Морально Психологічного Стану
5. Збірникметодик для діагностики негативних психічних станів військовослужбовців – науково дослідницький центр гуманітарних проблем ЗСУ.

д.ф. Фесьоха В.В. (ВІТІ ім. Героїв Крут)
Фесьоха Н.О. (ВІТІ ім. Героїв Крут)
Доброштан О.С. (ВІТІ ім. Героїв Крут)

КОНТРОЛЬ ДОСТУПУ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НА ОСНОВІ ПАСИВНОЇ БІОМЕТРІЇ

В умовах постійного удосконалення інструментарію кібершпигунства та інформаційно-руйнівних втручань, питанням забезпечення конфіденційності, доступності та цілісності інформації, а також надійного функціонування інформаційних систем спеціального призначення (ІССП) приділяється особлива увага. Ефективність кібербезпеки ІССП багато в чому залежить від ефективності систем контролю доступу, що обумовлює необхідність розробки нових та/або удосконалення існуючих систем кіберзахисту.

Одним з основних напрямів вирішення даного наукового завдання є удосконалення механізмів автентифікації користувачів ІССП, оскільки саме на цьому етапі контролю доступу встановлюється автентичність пред'явленого користувачем ідентифікатора (пароль, відбиток пальця тощо).

Аналіз досліджень з даної тематики показав доцільність застосування методів автентифікації на основі підходу пасивної (поведінкової) біометрії, зокрема підходу на основі аналізу клавіатурного почерку, оскільки надає винятково дешевий спосіб для аналізу поведінки користувача протягом усієї сесії роботи з ІССП, що у свою чергу дозволяє виявитифакт зміни користувача в умовах відсутності статичних біометричних даних (паролю, фізичного токену), які можливо використати для компрометації. Також описано підхід до побудови профілю користувача на основі його поведінки під час відтворення закономірних та притаманних йому поведінкових характеристик клавіатурного вводу (кількість пальців, задіяних під час набору тексту; швидкість друку – кількість введених символів розділена на час друку; тривалість натискання клавіш; час між натисканнями клавіш; динаміка друку – час між натисканням клавіш і часом їх утримання; сила натискання клавіш; частота виникнення помилок при введенні; частота використання певних комбінацій клавіш; використання основної або додаткової частини клавіатури).

Поряд з цим, реалізація такого підходу на практиці вимагає досить високих показників точності, оскільки аналіз множини досліджуваних ознак поведінки користувача на предмет відповідності його профілю здійснюється з урахуванням динаміки роботи з клавіатурою у режимі реального часу.

У контексті викладеного, пропонується шлях до підвищення показника точності визначення автентичності пред'явленого користувачем ідентифікатора на основі його поведінкової біометрії з урахуванням динаміки роботи з клавіатурою шляхом автоматизованої генерації досліджуваних ознак.

До процесу побудови профілю поведінки користувача на основі множини досліджуваних ознак (характеристик клавіатурного вводу) доцільно додати генерацію множини додаткових досліджуваних ознак на основі техніки машинного навчання Feature engineering. Вибір даної техніки навчання обумовлено збільшенням показників точності встановлення відповідності на аналогічних наборах даних. Так, із значень множини існуючих досліджуваних ознак утворюються нові ознаки, шляхом здійснення над їх комбінаціями математичних операцій (множення, логарифмування, піднесення до степеню, тощо), тим самим будуючи додаткову функціональну залежність (у графічній інтерпретації описаний підхід передбачає генерацію додаткових вимірів).

Таким чином, запропонований підхід до удосконалення процедури визначення автентичності пред'явленого користувачем ідентифікатора значно підвищить ефективність існуючих систем контролю доступу на основі аналізу його поведінки протягом усієї сесії роботи з ІССП.

Фисюк А.О. (ВІТІ ім. Героїв Крут)
Шевченко Д.С. (ВІТІ ім. Героїв Крут)

ПІДСИСТЕМА ІНФОРМАЦІЙНОЇ ПІДТРИМКИ АГІТАЦІЙНОЇ РОБОТИ ПО ВСТУПУ ДО ВВНЗ НА ОСНОВІ 3D-МОДЕЛІ КАФЕДРИ

В Україні продовжує активно розвиватись сфера інформаційний технологій, особливо великих успіхів досягла цифрова галузь. Постійне розширення процесу діджатилізації в повсякденному житті та залучення все більшої кількості нових користувачі в цей процес потребує постійного розвитку суспільних інститутів, що також не може оминути військову діяльність ЗС України. Популяризація військової справи та здобуття військової освіти зазнає регулярних змін, що в свою чергу активно впливає на заохочення цивільних осіб до проходження військової служби та піднятя патріотичних настроїв серед молоді. У рамках популяризації здобуття військової освіти у військових вищих навчальних закладах (ВВНЗ) та проходження військової служби, існує потреба вдосконалення та розвитку інструментів агітаційної роботи для конкуренції з іншими навчальними закладами. Актуальною задачею для конкурентного суперництва з передовими вузами є залучення до навчання мотивованих і розумних абітурієнтів для підтримання лідируючих позицій в освітній та науковій діяльності.Невід'ємним елементом популяризації освітніх послуг є візуальне відображення, яке легко сприймається та є цікавими для людей, що є важливою складовою для розповсюдження та впливу.Тому важливість графічного відображення можливостей військової освіти не можна ігнорувати. Проведення агітаційної роботи для здобуття військової освіти є необхідною складовою для популяризації в цілому. Зазвичай, відображення 3D-моделі об'єктів проходить в контексті трьох основних аспектів: гнучкість, точність та компонування.Ураховуючи це та на підставі аналізу сучасних наукових публікаційможна визначити основне завданнятривимірного моделювання (Рис. 1).

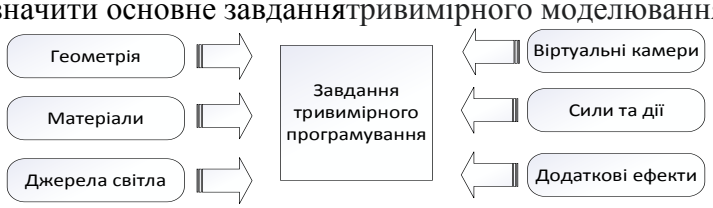


Рис.1. Основні завдання тривимірного моделювання

Так, розробку тривимірного моделювання можна розділити на такі категорії:

1. Геометрія (побудована з використанням різних методів моделі, наприклад, побудови).
2. Матеріали (інформація про візуальні властивості моделі, такі як колір стін і відбивна/заломлююча сила вікон).
3. Джерела світла (регулювання напрямку, потужності, спектру світла)
4. Віртуальні камери (вибір точки та кута проєкції)
5. Сили та дії (налаштування динамічного спотворення об'єктів, використовується переважно в анімації)
6. Додаткові ефекти (об'єкти, що імітують атмосферні явища: світло в тумані, хмари, полум'я тощо)

Слід підкреслити, що не існує конкретного стандарту моделі безпеки для розробки та проектування об'єктної моделі. Більшість вчених пропонують вузько сфокусовані рішення. Вони здебільшого не вирішують задачі формування існуючого уявлення про кафедру. Тому дослідження в цій сфері є актуальними.Таким чином, розробка тривимірної моделі навчального підрозділу є важливим аспектом у розвитку механізмів популяризації освітнього процесу у ВВНЗ. Проведений аналіз дозволяє визначити основні завдання розробки для усунення невизначеностей під час відображання переваг здобуття військової освіти. Тому, наукова задача щодо розробки 3D-моделі кафедри з відображенням складових процесів навчання у ВВНЗ та поширення зацікавленості у військовій справі серед цивільного населення, є актуальною та потребує вирішення.

Фомін М.М. (ВІТІ)
Погребняк Л.М. (ВІТІ)

УДОСКОНАЛЕНИЙ МЕТОД ДВОСТОРОННЬОЇ ОЦІНКИ СТРУКТУРНОЇ НАДІЙНОСТІ СТРУКТУРНО-СКЛАДНИХ СИСТЕМ

Досвід проведення Антитерористичної операції, на теперішній час Операції Об'єднаних Сил та стратегічних командно-штабних навчань показав, що ефективність функціонування системи військового зв'язку суттєво залежить від складових її підсистем і елементів. Зазначені особливості пов'язані зі значним збільшенням обсягів інформації, що передається в інтересах управління військами та зброєю, причому у режимі реального часу. Таким чином, від якісного стану системи зв'язку значною мірою залежить ступінь виконання поставлених бойових завдань.

Мережі військового зв'язку (МВЗ) відносяться до класу систем, надійність телекомунікаційного обладнання яких суттєво впливає на показники якості відповідних послуг. Ефективність функціонування таких мереж залежить від надійності її підсистем та елементів, а також від складності зв'язків між ними. Структурна надійність залежить від обраної структурної схеми мережі, ступеню дублювання обладнання, ймовірності пошкодження окремих ліній зв'язку чи комутаційних центрів та повинна забезпечувати зв'язність користувачів мережі з якістю не гірше чим визначена. Надійність мережі з розгалуженою структурою безпосередньо пов'язана з результуючими показниками якості відповідних послуг.

На сьогоднішній день не одержали достатнього розвитку методи визначення структурної надійності таких мереж, тому питання обґрунтування загального підходу до оцінки структурної надійності мережі військового зв'язку за заданими показниками надійності, яка залежить як від надійності її елементів, так і від способу їх взаємного з'єднання є актуальними. Мережа військового зв'язку функціонує, якщо забезпечується можливість обміну повідомленнями між комутаційними центрами мережі, іншими словами якщо існує, принаймні, один шлях між комутаційними центрами. Структурна надійність мережі в цілому буде визначатись, як ймовірність зв'язності всіх комутаційних центрів мережі, що приймають участь у обміні повідомлень.

При проектуванні реальних мереж військового зв'язку або оцінці діючих мереж зазвичай відсутня необхідність точних розрахунків структурної надійності мережі, тому що вихідні дані по надійності елементів мережі задаються або виводяться експериментальним шляхом, з певною кінцевою точністю. Проектувальникам мереж або організаціям, що здійснюють експлуатацію мереж, необхідно лише переконатися в тому, що структурна надійність мережі, з одного боку, не нижче заданої, а з іншого боку, не має економічно необґрунтованого запасу надійності. Інакше кажучи, на практиці достатньо гарантувати, що дійсне значення структурної надійності W_0перебуває в деяких межах $W_{min} \le W_0 \le W_{max}$.

Таким чином задача побудови структурно надійної мережі зводиться до задачі аналізу різних варіантів її структури за заданими показниками надійності, які залежать, як від надійності її елементів так і способу їх взаємного з'єднання.

Запропоновано загальний підхід, який базується на висновку, що застосування точних методів оцінки структурної надійності мереж військового зв'язку на практиці жорстко обмежено розмірністю аналізуємих мереж. З іншого боку, різні методи наближеної оцінки в залежності від складності алгоритмів і аналітичних виразів, що у них застосовуються, дозволяють отримувати неоднакові за точністю результати.

Пропонується використання удосконаленого методу двосторонньої оцінки структурної надійності, при якому здійснюється комплексне врахування взаємних зв'язків шляхів і перетинів, що дозволяє значно скоротити трудомісткість розрахунків та гарантує заданий рівень точності оцінки структурної надійності мережі військового зв'язку у порівнянні з іншими методами розрахунку та оцінки.

д.т.н. Хлапонін Ю.І. (КНУБА)

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ - ОСНОВА КОНЦЕПЦІЇ «SMART CITY»

Розглядаються питання забезпечення кібербезпекиінформаційних систем Smart City. Стрімкий розвиток “розумних” міст (Smart City) в усьому світі здатний значно поліпшити життя пересічних городян. Але разом з тим дає додаткові можливості кіберзлочинцям і викрадачам інформації.

Останні нововведення в технологічних областях, таких як вбудовані обчислення, зв'язок, датчики та виконавчі елементи концепції Smart City дозволили впровадити складні системи, здатні контролювати та координувати фізичні та організаційні процеси в локальному та глобальному масштабі за допомогою комунікаційних технологій. Однак, це має включати необхідність впровадження кращих практик в галузі кібербезпеки і кіберрішень для всіх технологій, що використовуються в “розумних” містах.

Стрімкий розвиток «розумних міст» (Smart City) в усьому світі здатний значно поліпшити життя пересічних городян. Але разом з тим дає додаткові можливості кіберзлочинцям і викрадачам інформації.

За прогнозами міжнародної мережі компаній в галузі консалтингу та аудиту PwC (PricewaterhouseCoopers) ринок технологій для Smart City до 2025 року сягне позначки в 2,5 трильйони доларів. Але взаємопов'язаність як реальної так і віртуальної інфраструктури через Інтернет створює нові загрози. Аналітики відзначають, що Smart City вразливі до загроз з боку всього арсеналу кіберзлочинців - починаючи від “традиційних” шкідливого програмного забезпечення, malware і DDoS-атак, і закінчуючи несанкціонованим проникненням з метою повністю або частково вивести з ладу Інтернет-ресурс, Web-сайт, ігровий сервер або державний ресурс чи розкрадання даних або втручання в роботу інформаційних систем [3].

Критичними до кіберзагроз в “розумному” місті є:

- системи тепло-, газо-, водо-, енергопостачання, розподіу та обліку;
- транспортні та логістичні системи;
- комунальна система, що включає побутові інтелектуальні лічильники (моніторинг споживання електрики і газу) з бездротовим підключенням;
- система обробки грошових переказів і банківські операції;
- система веб-камер, підключених до мережі Інтернет;
- автоматизована система контролю дорожнього руху;
- медичні системи розподілу та прийому карет “швидкої” допомоги;
- інші підключені до мережі пристрої міських інформаційних систем.

Основними проблемами інформаційних систем «розумних» міст з точки зору кібербезпеки є велика кількість технологій і практичних рішень, які повинні взаємодіяти і зв’язуватися один з одним, нерівна якість різних вбудованих технологій, дистанційна і безпосередня експлуатація інформаційних систем Smart City, величезні обсяги даних для аналізу і зберігання.

В концепції “розумного міста” застосовуються так звані кіберфізичні системи (КФС) - це інтелектуальні системи, що включають інженерно-взаємодіючі мережі фізичних та обчислювальних компонентів [1].

“Розумні” міста допомагають скоротити експлуатаційні витрати та витрати на утримання міської інфраструктури, а також забезпечити авторитетне стратегічне планування, одночасно оптимізувати комфорт та поважати потребу кожного громадянина.

Однак для того, щоб ці можливості мали місце, потрібно вирішити проблеми технічного, правового характеру та захисту від кіберзагроз [1,4]:

Надійність. Складовими інформаційних систем Smart City є кіберфізичні системи, які можна використовувати в таких критично важливих областях, як охорона здоров'я,

інфраструктура, транспорт і багато інших. Основними вимогами є надійність і безпека, оскільки виконавчі елементи впливають на навколишнє середовище та мають вплив на людину. Фактично вплив виконавчих елементів може бути незворотнім, тому ймовірність їх непередбаченої поведінки повинна бути зведена до мінімуму. Виконавець робіт з впровадження КФС, як учасник господарсько-правових відносин повинен нести відповідальність за помилкові результати роботи КФС, які негативно вплинули на людину або обмежили її права. Для цього державними органами мають бути прийняті відповідні управлінські рішення та внесені парламентом відповідні зміни до Кримінального кодексу України та Кодексу про адміністративні правопорушення.

Конфіденційність. Проблема полягає в підтримці балансу між збереженням конфіденційності та захистом персональних даних - і доступністю даних для надання більш якісного обслуговування. Оскільки КФС керують значними обсягами даних, що включають таку конфіденційну інформацію, як здоров'я, стать, віросповідання і багато інших персональних відомостей, виникають серйозні проблеми захисту персональних даних. Для КФС необхідні політики забезпечення конфіденційності, тому потрібен інструмент знеособлення даних, що дозволяє видаляти персональну інформацію перед обробкою даних системою [2]. Водночас, відсутність або недосконаліть законодавства та підзаконних актів у сфері забезпечення КФС значно підвищує ймовірність реалізації різного виду загроз або шахрайства в даній галузі**,** що негативно впливає на загальний рівень кібербезпеки.

Ризики занадто великі і українські міста повинні розглядати кібербезпеку з самої ранньої стадії впровадження концепції Smart City на всіх можливих рівнях. З метою забезпечення кіберстійкості “розумних” міст з’явилася міжнародна ініціатива Securing Smart Cities, активно підтримувана низкою організацій в усьому світі. Заявленою місією ініціативи є визначення викликів кібербезпеки, що стоять перед “розумними” містами, і вироблення ефективних рішень протидії. Це включає просування кращих практик в галузі кібербезпеки для всіх технологій, що використовуються в “розумних” містах. Ініціатива націлена на вирішення кіберпроблем на кожному етапі розвитку Smart City – від планування до фактичної реалізації інтелектуальних міст [2,5].

Таким чином, в зв’язку з бурхливим розвитком концепції Smart City та неминучістю такого розвитку постає необхідність приведення національного законодавства України до міжнародних стандартів, покладення на відповідні державні органи чітких повноважень в сфері Smart City, визначення викликів кібербезпеки, що стоять перед “розумними” містами, і вироблення ефективних рішень протидії.

Література**:**

1. Закон України «Про основні засади забезпечення кібербезпеки України” (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403).

2.FrameworkforCyber-PhysicalSystemsRelease 1.0 May 2016 Cyber Physical Systems Public Working Group, www.nist.gov

3.https://biz.nv.ua/kibervoiny_i_biznes/smart-city-nuzhna-li-umnomu-gorodu-kiberbezopasnost-1593208.html.

4. Кібербезпека в інформаційному суспільстві, Інформаційно-аналітичний дайджест, № 6 (червень), Київ – 2019.

5. Концепція Київ Смарт Сіті 2020. –Режим доступу : http://kscf.in.ua/ Smart_City_UKR_Print_final.pdf

к.т.н. Хусаінов П.В. (ВІТІ)

ЕВРИСТИЧНЕ РОЗШИРЕННЯ АЛГОРИТМІЧНИХ ПРОЦЕДУР РОЗПІЗНАВАННЯ ОБРАЗІВ В ЗАДАЧАХ ІДЕНТИФІКАЦІЇ КІБЕРІНЦИДЕНТА

Суб'єкти забезпечення кібербезпеки у межах своєї компетенції повинні забезпечувати виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків. Виявлення кіберінцидентів можна інтерпретувати у контексті задачі ідентифікації приналежності формалізованого опису стану об'єкта кіберзахисту до того чи іншого класу кіберінцидентів.

Ідентифікація –встановлення на підставі певних ознак тотожностірізноманітних об'єктів. Тотожність – категорія, яка виражає рівність, однаковість предмета, явища з самим собою або рівність кількох предметів. Про предмети А і Б говорять, що вони є тотожними, однаковими, якщо і тільки якщо всі властивості (і відношення) якими характеризують А, характеризують і Б, і навпаки. Тотожність є не абстрактним, а конкретним поняттям. Відомі прикладні задачі розпізнавання образів спрямовані на класифікацію об'єктів. Особливістю таких задач є те, що заздалегідь невідома залежність вимірюваних ознак об'єкта від класу до якого він належить. Разом з тим вважається заданою, так звана, навчальна множина об'єктів, кожний з яких має опис у формі сукупності ознак та категорію приналежності до певного класу. Як правило, рішення конкретної прикладної задачі обумовлює неформалізований вибір ознак об'єкта, алгоритмів навчання та розпізнання з наступною їх реалізацією. Розрізняють алгебраїчний, лінгвістичний, евристичний, та структурний підхід до розроблення прикладних задач розпізнавання образів.

Доповідь присвячена оприлюдненню результатів аналізу методологічних підходів теорії розпізнавання образів для вирішення задачі ідентифікації кіберінцидентів (кібератак) у кіберпросторі об'єкта кіберзахисту, який дозволив прийти до висновку про необхідність їх комбінування та евристичного розширення алгоритмічних процедур. Під поняттям "кіберпростір об'єкта кіберзахисту" будемо розглядати таку частину кіберпростору, яка утворюється межами відповідальності органу кібербезпеки стосовно контрольованого об'єкта кіберзахисту.Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Ключовим питанням автоматизації задачі ідентифікації кіберінцидента є створення математичної моделі об'єктів розпізнавання яка повинна якомога повно описувати предметну область, уособлювати її особливості, що, в свою чергу, обумовлює та визначає:

склад, якісний вміст ознак формалізованого опису стану елементів кіберпростору об'єкта кіберзахисту, класифікацію їх образів, а також інтерпретацію типових варіантів реагування на кіберінциденти (кібератаки);

порядок розроблення алгоритмів навчання, класифікації та ідентифікації опису станів елементів кіберпростору об'єкта кіберзахисту на приналежність до класів кіберінцидентів.

Висновки. Застосування алгебраїчного, лінгвістичного, евристичного або структурного підходу в задачах ідентифікації кіберінцидентів у кіберпросторі зв'язано з низкою труднощів. По-перше, рівень формалізації не може бути основою для синтезу відповідної моделі на засадах класичних математичних канонів з можливістю їх подальшого дослідження аналітичними та чисельними методами. По-друге, обумовлюють значні витрати обчислювальних та часових ресурсів, які суттєво перевищують корисний ефект чи виходять за межі технічних можливостей.

Найбільш плідним напрямом подолання окреслених труднощів на сучасному етапі вважається евристичного розширення алгоритмічних процедур (емпірична аксіоматика), які знайшли застосування у методологічному апарату розпізнавання образів. Останнє полягає у введенні емпіричних аксіом, оцінювання достовірності ланцюгів висновку для уникнути повного перебору можливих варіантів рішень на основі математичної логіки.

Циганок А.С.

ГЕНЕРАЦІЯ ПРОДУКЦІЙНИХ ПРАВИЛ ДЛЯ НЕЧІТКОЇ СИСТЕМИ ЛОГІЧНОГО ВИВОДУ НА ОСНОВІ АНАЛІЗУ ДЖЕРЕЛ ДАНИХ

З розвитком інформаційних технологій збільшується кількість вразливостей та загроз спрямованих на різноманітні системи обробки інформації. За для їхньої безпеки, забезпечення нормального функціювання та попередження вторгнень необхідні спеціалізовані засоби безпеки. В умовах сьогодення перспективним напрямком, що швидко набирає обертів у розвитку стає кібербезпека. Провевши аналіз джерел інформації, можна побачити, що для інформаційних систем та мереж, проблема оперативного реагування на виявленні зловживання та аномалії була та залишається актуальною. Тому удосконалення систем, що являють з себе спеціалізовані програмні засоби, які направлені на виявлення підозрілої активності або втручання в інформаційну систему та здатні приймати адекватні заходи щодо запобігання кіберзагроз, є пріоритетом в розвитку та розробці.

Метою дослідження є розробка програмного модулю генерації продукційних правил нечіткої системи логічного виводу на основі аналізу джерел даних.

Виклад основного матеріалу. Поява нових загроз та аномалій, створених діями атак з невідомими або нечітко визначеними властивостями, здебільшого залишаються непоміченою, що підкреслює неефективність сучасних засобів виявлення аномалій. Це зумовлено відсутністю в системах виявлення вторгнень при генерації правил ідентифікації атак адаптивно та гнучко реагувати на нові вторгнення. Для вирішення даної проблеми ефективно застосовувати апарат нечіткої логіки. На відміну від традиційної математики, що вимагає на кожному кроці моделювання точних і однозначних формулювань закономірностей, нечітка логіка пропонує зовсім інший рівень мислення, завдяки якому творчий процес моделювання відбувається на найвищому рівні абстракції, при якому постулюється лише мінімальний набір закономірностей. Обробка даних в умовах нечіткої визначеності зумовлює потребу впровадження систем аналізу даних, що будуються на основі апарату нечіткої логіки, оскільки такий підхід здатний забезпечити вирішення даної проблеми. Але в сучасному світі з його намаганням до автоматизації всіх процесів, системи аналізу даних передбачають монотонну та рутинну роботу експертів з великими обсягами статистичних даних, визначення діапазонів нечітких термів та побудови нечітких правил для систем нечіткого логічного виводу. Використовуючи апарат нечіткої логіки можна розробити програмний модуль генерації продукційних правил на основі аналізу джерел даних. При подальшому застосуванні даного модуля в системах виявлення вторгнень можна забезпечити ефективну протидію новим чи модифікованим видам загроз, які для більшості систем залишаються невидимими. Бази правил нечіткої логіки ґрунтуються на базах знань, побудованих на основі людського досвіду. Отже, вихідним результатом генерації модулю продукційних правил нечіткої системи логічного виводу має бути файл, що містить в собі етапи фазифікації, дефазифікації та наданні нечіткого логічного висновку, на основі вхідних даних наданих експертами з даної області.

Саме завдяки програмному модулю генерації продукційних правил систему виявлення вторгнень можна постійно досліджувати і удосконалюватися для забезпечення неперервності в ефективності її роботи, за рахунок правильно згенерованих правил досягається ефективна робота системи. Беручи до уваги викладений матеріал виникає завдання розробки програмного модулю автоматизованої побудови продукційних правил для системи нечіткого логічного виводу, що значною мірою невілює головний недолік таких систем, а саме суб'єктивну думку експерта та значного зменшує час на побудову нечітких продукцій. **Висновки.** Підводячи підсумок, бачимо, що актуальним на сьогодні є розробка програмного модуля генерації продукційних правил в основу якого покладено методи та принципи нечіткої логіки. В процесі розробки необхідно провести аналіз існуючих методів генерації продукційних правил, недоліків апарату нечіткої логіки, механізмів побудови експертних систем, що значно спростить опис предметної області.

Цуканов О.Ф.(НТУУ «КПІ»)
Якорнов Є.А. (НТУУ «КПІ»)

ПІДВИЩЕННЯ ТОЧНОСТІ ОЦІНЮВАННЯ ПАРАМЕТРІВ РУХУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ НА ОСНОВІ ВИКОРИСТАННЯ ДРОБНИХ РЯДІВ ТЕЙЛОРУ

При оцінюванні параметрів руху (ПР) безпілотних літальних апаратів (БПЛА) нині застосовуються методи з урахуванням фільтра Калмана [1] чи методу найменших квадратів (МНК). Потенційна точність оцінювання цих методів практично однакова, але фільтр Калмана набув ширшого поширення порівняно з МНК. На наш погляд, оптимальним підходом до оцінювання ПР є використання цих методів одночасно. Причому фільтр Калмана необхідно використовувати при побудові моделі руху БПЛА. При цьому, основна проблема оцінювання ПР полягає в отриманні високоточних оцінок для забезпечення стійкості маневрування БПЛА в бойових умовах. При вирішенні задачі забезпечення стійкості процесу оцінювання може також використовуватися і МНК за наявності гіпотези моделі руху. При цьому питання забезпечення стійкості вирішується шляхом використання «ковзного вікна», а забезпечення необхідної точності підбором відповідного ступеня полінома апроксимації. Тобто, точність та стійкість процесу оцінювання МНК визначається порядком полінома апроксимації. Завдання вибору ступеня полінома апроксимації залежить від маневру БПЛА, наприклад при переході від рівномірного руху до маневру ступінь полінома слід підвищувати. При цьому кількість членів апроксимуючого полінома також збільшується і змінюється не тільки його ступінь, а й значення кожного коефіцієнта полінома. Залежно від помилки оцінювання ПР ступінь полінома змінюється дискретно.

Тому виникає таке завдання: при оцінці ПР БПЛА за допомогою рядів Тейлора, що сходяться, не збільшуючи ступеня апроксимуючого полінома зменшити значення його дискретності. Для цього скористаємося відомим рядом Тейлора в цілих похідних

$$f(x) = f(x_0) + f(x_0)'(x-x_0) + f(x_0)''\frac{(x-x_0)^2}{2!} + .. f(x_0)^n\frac{(x-x_0)^n}{n!} \quad (1)$$

і запишемо його у вигляді

$$f(x) = \sum_{k=0}^{n} f(x_0)^k \frac{(x-x_0)^k}{k!}, \quad k=0,1,2,3,\ldots.. \quad (1.a)$$

На основі роботи [2] представимо вираз (1.а) наступним чином

$$f(x) = \sum_{k=0}^{n} f(x_0)^k \frac{(x-x_0)^k}{\Gamma(k+1)}, \quad k=0,\ 0.5,\ 1,\ 1.5,\ 2,\ 2.5\ldots \quad (2)$$

где $\Gamma(k+1)$ – гамма функцыя.

Назвемо додаткові члени ряду дрібними. Це має на увазі існування дробових похідних у ряді (2). При цьому цілу похідну можна записати як

$$\frac{d^n}{dx^n}x^k = \frac{k!}{(k-n)!}x^{k-n}, \quad (3)$$

а дробову похідну статечної функції подати у вигляді

$$\frac{d^n}{dx^n}x^k = \frac{\Gamma(k+1)}{\Gamma(k-n+1)}x^{k-n}. \quad (4)$$

Пояснимо з математичної точки зору сутність введеної похідної дробової. Зокрема, для похідної дробової дорівнює 0.5 її величина займає середнє значення між першоподібною і першою похідною. Відповідно похідна 1.5 - середнє значення між першою та другою похідною і т.д. При цьому можна стверджувати, що якщо, наприклад, n-я похідна дорівнює 0, а n-1 відмінна від нуля, то похідна яка займатиме проміжне положення не завжди буде нульовою.

Проведений авторами попередній аналіз фізичного сенсу коефіцієнта апроксимації при ступені 1.5 показує, що його не потрібно враховувати якщо значення цього параметра не використовується в наступних розрахунках у цьому і є деяке обмеження використання дробових рядів Тейлора. Оцінювання ПР БПЛА з точки зору підвищення точності оцінювання за рахунок зменшення дискретності похідних у ряді Тейлора.

Зокрема, рис 1 показано результат апроксимації поліному 4 ступеня з шумом

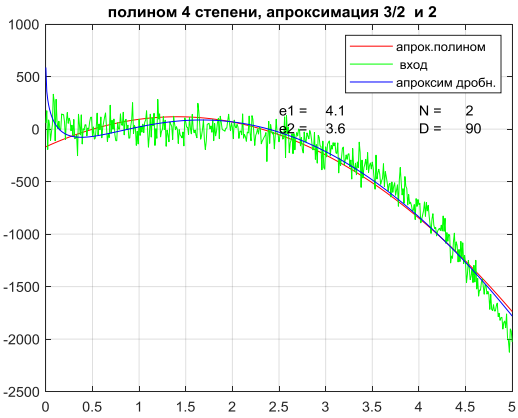


Рис. 1

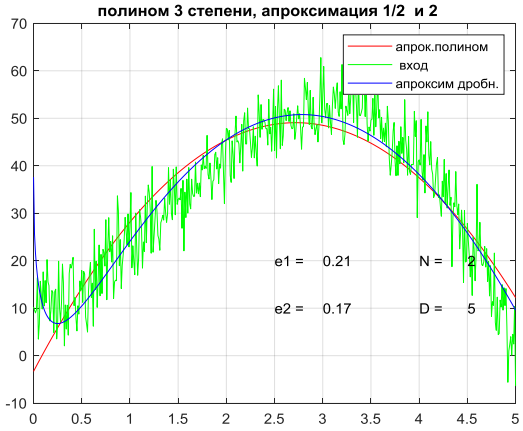


Рис. 2

розподіленим за нормальним законом методом найменших квадратів поліномом другого ступеня Y = $a_0 + a_1x^1 + a_2x^2$ і МНК поліномом ступеня 3/2 через дробові ступеня ½ Y = $a_0 + a_1^*x^{0.5} + a_2x^1 + a_3^*x^{\frac{3}{2}}$, де a_1^* , a_3^* - коефіцієнти має сенс дробових похідних. З графіків видно, що помилка оцінювання МНК поліномом з дробовими ступенями 1/2 підвищується на 10-12%.

У таблиці наведено деякі порівняльні результати моделювання

№	Ступінь апроксимації цілим поліномом	Ступінь апроксимації дробовим поліномом	Помилка апроксимації цілим поліномом	Помилка апроксимації дробовим поліномом	Підвищення точності %
1	2	3/2	2.1	1.7	10%
2	2	2	3.3	2.6	22%
3	3	2.5	2.1	0.02	90%

Попередні результати роботи показують, що застосування рядів Тейлора з дробовими похідними дозволяє суттєво розширити клас завдань для використання МНК у задачах оцінювання ПД БПЛА. Використання дробових поліномів у задачі апроксимації МНК при оцінюванні ПР маневрують БПЛА військового призначення дозволяє не застосовувати складні алгоритми на основі зміни ступеня полінома. Результати моделювання показують, що для БПЛА, що здійснюють бойові маневри, найбільш прийнятним методом оцінювання є МНК з дробовими ступенями 2.5.

ЛІТЕРАТУРА

1. YevgeniiYakornov, OlegTsukanov. Sustainable Algorithm for Estimating the Motion Parameters of Unmanned Aerial Vehicles. International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 2019, pp. 1-5.

2. A. Kilbas, H. Srivastava and J. Trujillo, Theory and Applications of Fractional Differential Equations. Amsterdam: Elsevier, 2006.

д.т.н. Чевардін В.Є.(ВІТІ ім.Героїв Крут)
Лаврик І.В.(ВІТІ ім.Героїв Крут)

НЕБЕЗПЕКА АЛГОРИТМУ ШОРА ДЛЯ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Відомо, що сучасні стандарти асиметричного шифрування, основані на складності факторизації чисел та дискретного логарифмування. Для обчислення приватних ключів за допомогою методів перебору комп'ютерам потрібно 300 трильйонів років для обчислень [1]. Це пов'язано з назькою обчислювальною потужністю. Кожен біт у класичній комп'ютерній системі обмежений значеннями 1 або 0, а квантового комп'ютер замість цього використовує кубіти в суперпозиції [2]. Суперпозиції дозволяють квантовим комп'ютерам виконувати обчислення для багатьох станів одночасно, це означає, що теоретично часові показники ефективності квантових алгоритмів зростають експоненціально в порівнянні з класичними методами.

У 1994 році Пітер Шор, професор прикладної математики, розробив алгоритм, відомий як «алгоритм Шора», для обчислення простих множників чисел. Алгоритм Шора починається з визначення деякого числа g, яке, ймовірно, може бути простим множником числа N. Число g не обов'язково має бути чистим множником N, воно також може бути будь-яким числом, яке має спільні множники з N, наприклад, 2 є коефіцієнтом як 4, так і 6, хоча 4 не є коефіцієнтом 6. Алгоритм Евкліда [3] можна використовувати для ефективного пошуку спільних множників між числами, що дозволяє обчислювати чисті коефіцієнти. Якщо алгоритм Евкліда знайде спільний коефіцієнт – процес завершено, і N можна розділити на спільний коефіцієнт, щоб отримати інший множник. Складність факторизації великих числел полягає в тому, що сучасні комп'ютери не можуть розкладати їх на множники. Однак для дуже великих чисел, які використовуються в сучасних алгоритмах асиметричного шифрування, ця ймовірність є нескінченно малою при випадкових припущеннях, де й застосовується алгоритм Шора.

Для будь-яких двох цілих чисел A і B, які не мають спільного множника, множення самого A в кінцевому підсумку призведе до числа, кратного B, плюс 1. Тобто $A^P = mB + 1$, або для нашого великого числа N і деякого g, $g^P = mN + 1$ [4]. Це еквівалентно $g^P - 1 = mN$, або $(g^{P/2} + 1)(g^{P/2} - 1) = mN$, і $(g^{P/2} + 1)$ і $(g^{P/2} - 1)$ є новими, більш точними припущеннями, щодо прямих множників або чисел, які мають спільні множники з N [5].

Існують три обмеження щодо використання цієї формули для обчислення простих множників. По-перше, жодне число не може бути кратним N. По-друге, ступінь P не може бути непарною, тому, що $P/2$ призведе до десяткового числа, тобто $g^{P/2}$, ймовірно, також не буде цілим числом. Проте, навіть з цими двома обмеженнями, враховуючи будь-яке початкове g, існує шанс 37,5% знайти коефіцієнт N. Це означає, що за 10 спроб ми з ймовірністю 99% знайдемо коефіцієнти N [6]. Однак третє обмеження – це складність знаходження значення P. Щоб перетворити випадкове g у набагато точніше припущення $g^{P/2} \pm 1$, ми повинні підносити g у ступінь P, поки не отримаємо число на одиницю менше, ніж N. Це досить складне обчислення для будь-якого класичного комп'ютера, тому саме тут доцільно застосувати квантові обчислення.

На відміну від класичних обчислень, які дають лише одну відповідь для заданого входу, квантові обчислення використовують суперпозицію кубітів для одночасного обчислення кількох можливих результатів з одного входу. Однак, ви все одно отримуєте лише один із можливих результатів обчислень. З цієї причини існує вимога встановити квантову суперпозицію для обчислення всіх можливих відповідей одночасно, а також зробити так, щоб усі неправильні відповіді деструктивно заважали одна одній. Таким чином, результат ймовірності правильності обчислюваного результату зростає. Алгоритм Шора – це процес, необхідний для створення такої квантової системи, де некоректні результати деструктивно заважають одне одному[7].

Завдяки принципу роботи квантового комп'ютера ми можемо ввести суперпозицію чисел, і одночасно отримаємо суперпозиції всіх можливих значень для P і g^P , а потім на скільки більше кожне з цих gP значень до найближчого кратного N. Математичне спостереження про те, що $g^x = mN + r \equiv g^{x+P} = m_2N + r$ (оскільки $g^P = mN + 1$) означає, що P має властивість повторення. Ми можемо згенерувати квантову суперпозицію і обчислити значення, більше за найближче кратне N +r, щоб випадковим чином отримати одне з можливих значень r. Це число не має сенсу, але гарантує, що ми повинні залишити суперпозицію значень, які могли б привести до залишку r. Через властивість повторюваності P кожен з виходів точно є P.

Після цього можна застосувати квантове перетворення Фур'є [8] до суперпозиції значень P, щоб отримати єдине значення $1/P$, яке можна обчислити. Таким чином, з обчисленим значенням P можливо застосувати формулу $(g^{P/2} + 1)(g^{P/2} - 1) = mN$ і отримати числа, які є дуже ймовірними множниками N.

У випадку створення ідеального 4099-кубітового квантового комп'ютера зі стабільними кубітами шифрування RSA-2048 можна буде зламати всього за 10 секунд, на відміну від 300 трильйонів років класичного комп'ютера [1]. Постійний зріст обчислювальних спроможностей квантових комп'ютерів знижує стійкість асиметричних криптографічних алгорітмів, що використовуються. Саме тому є необхідним здійснити перехід до нових, більш сучасних алгоритмів, стійких до криптоанлізу в постквантовий період.

Список використаної літератури

1. AndreasBaumhof. Breaking rsa encryption - an update on the state-of-theart - quintessencelabs. https://www.quintessencelabs.com/blog/breaking-rsaencryption-update-state-art/, 2019

2. Surya Teja Marella and Hemanth Sai Kumar Parisa. Introduction to quantum computing | intechopen. https://www.intechopen.com/online-first/introductionto-quantum-computing, 2020.

3. N. Sklavos, K. Papadomanolakis, P. Kitsos, and O. Koufopavlou. Euclidean algorithm vlsi implementations. In *9th International Conference on Electronics, Circuits and Systems*, частина 2, с. 557–560 vol.2, 2002. doi:10.1109/ICECS.2002.1046226.

4. Franklin de Lima Marquezino, Renato Portugal, and Carlile Lavor. *Shor's Algorithm for Integer Factorization*, pages 57–77. Springer International Publishing,Cham, 2019. doi:10.1007/978-3-030-19066-8_4.

5. Fang Xi Lin. Shor's algorithm and the quantum fourier transform. *McGill University*, 2014.

6. Franz Kappel and Alexei V Kuntsevich. *An Implementation of Shor's r-Algorithm*. 2000. doi:10.1023/A:1008739111712.

7. V. Bhatia and K. R. Ramkumar. An efficient quantum computing technique for cracking rsa using shor's algorithm. In *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, с. 89–94, 2020. doi: 10.1109/ICCCA49541.2020.9250806.

8. L. Hales and S. Hallgren. An improved quantum fourier transform algorithm and applications. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, с. 515–525, 2000. doi:10.1109/SFCS.2000.892139.

V.Chevardin
O.Marchuk
V.Savchuk
O.Karpyshynets
I.Lavryk

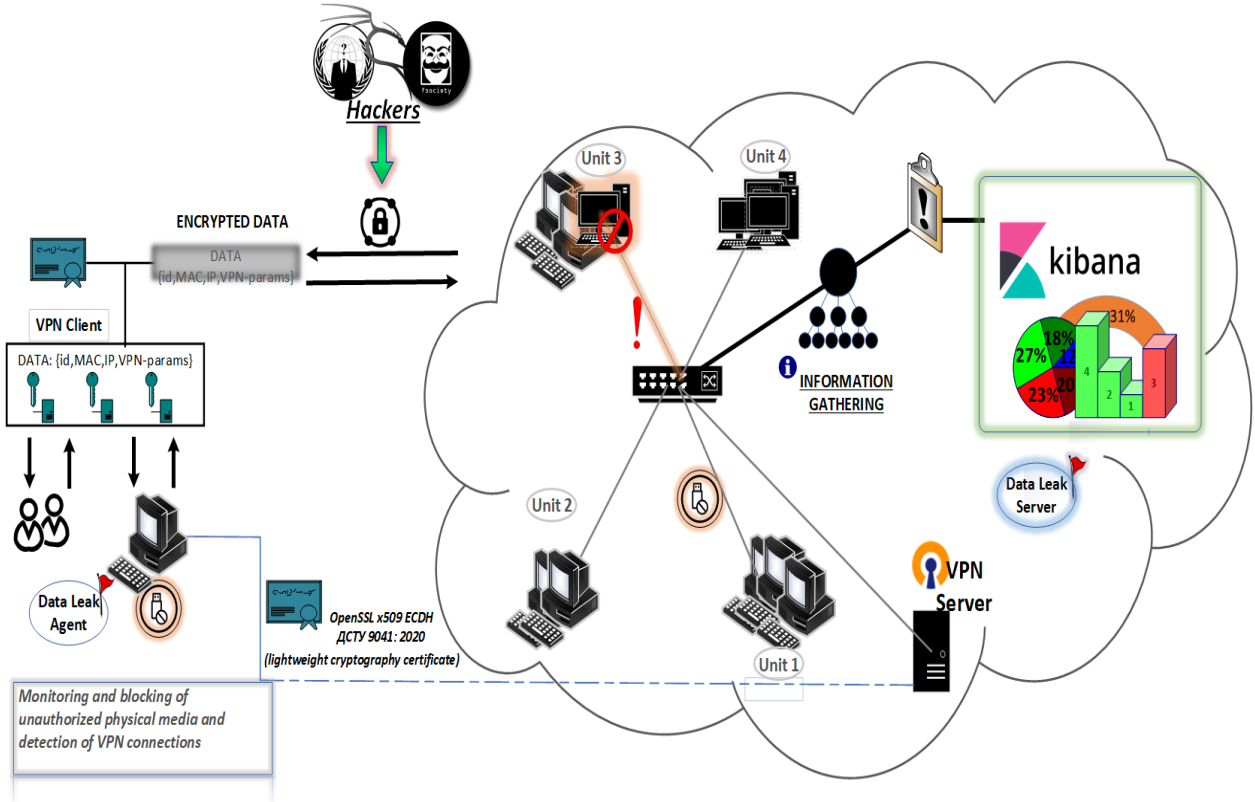
DEVELOPMENT OF SOFTWARE AGENT «DATA LEAKAGE DETECTOR»

In August 2021, the President of Ukraine approved the Cyber Security Strategy of Ukraine for 2021-2025. The document notes that cybersecurity is one of the priorities in Ukraine's national security system. Thus, cyberspace is recognized as one of the possible theaters of war, while the number and complexity of cyber threats will only increase and spread to all spheres of life.

In order to improve the cyber security of critical infrastructurestate, architectural solution for the information security system of the critical infrastructure object was developed.

The project name is“DataLeakDetector”[1].**Main idea of the solution** istouse national standardized cryptosystems for critical infrastructure cybersecurity systems building.**Thegoal is** toincrease the efficiency of the information protection system against data leakage at critical infrastructure objects.

Purposed solution consists of two components (pic. 1). First component is agent “Date Leakage Detector”, which is designed to collect the parameters of the software and hardware environment of the workstation, record of the user of the operating system Windows or Linux,parameters of the VPN connection, which can be created by the user.



Picture 1. “Data Leak Detector” processing scheme.

The agent can be installed both in the local network and in the Internet.The first part is local agent installed on the workstation and working in the background.

After the connection of registered USB-device everything is working in normal mode and nothing changes and the process is adding to the log journal on the server side.Afterthe installing of

unregistered USB-device connection the work station is blocked immediately, and can be unlocked only with administrator password.

This event also is added to the log journal in order to give to the administrator information about the cyber incident.

The second component is the server part which is developed on the basis of the Logstage Kibana software.Appropriate rules for filtering and analysis of “Data leak Agent” agents have been created

On the main page are next components:

– the graph which shows the number of connected USB-devices during the period of time. Time period can be changed;

– the graph wpich shows the percentage of authorized and unauthorized, USB-devices connected to the workstations in the network;

– the log journal which shows the detailed information about USB-connection incidents. Information about workstation IP, USB-device MAC and serial number, workstation hostname, system username and the incident time;

– two panels. First shows total number of USB-device incidents, second shows the number of USB-device connection incidents by users.

Adding of USB-devices serial number and MAC- address is made with the help ofadmin web-panel. An admin panel was developed to manage and create a user base of USB-devices and VPN settings for users.

Communication between agents and the server part is created using VPN protocols, certificates of lightweight cryptosystems (LWC). In addition to detection of unauthorized USB devices, VPN tunnels are also detected.

With future development this software solution will solve the problem number 1 from the purposed list.

Efficiency assessment in comparison with existing solutions:

1. Open source software that allows you to develop your own additional solutions.
2. The openness of the code allows to receive certificates for comprehensive systems of information protection in the future
3. Usage of ELK Stack software components in the Armed Forces of Ukraine and agencies of the sector.

REFERENCES

1. [Electronic resource]https://gitlab.ua30.gov.ua/CSD33/dataleak-detector/

Чередніченко В. В. (НАДПСУ)
к.т.н. Басараб О. К. (НАДПСУ)

БЕЗПЕКА ПЕРЕДАЧІ ПОВІДОМЛЕНЬ МЕСЕНДЖЕРАМИ ПРИВАТНИХ КОМПАНІЙ

Актуальність дослідження. В процесі охорони кордону зв'язок з прикордонними нарядами, як правило, організований з використанням УКХ радіостанцій. Проте, географічні особливості окремих ділянок кордону, не завжди забезпечують суцільне УКХ-покриття, а апаратне забезпечення є занадто громіздким і складнішим у використанні в порівнянні зі звичайним смартфоном. Тому, з метою обміну відкритою інформацією військовослужбовці Державної прикордонної служби України можуть використовувати мобільні програмні додатки для передачі інформації – месенджери, якими користуються і у повсякденному житті. Але разом зі зручністю використання виникає проблема небезпеки передачі повідомлень, адже існує вірогідність витоку інформації, бо приватна компанія може надавати дані третім особам.

Метою дослідження є підвищення рівня захисту інформації під час обміну службовими повідомленнями військовослужбовцями Державної прикордонної служби України за рахунок їх шифрування власним програмним продуктом.

Виклад основного матеріалу. На даний момент найбільш популярні месенджери використовують однакові або дуже подібні методи захисту. До основних методів відносяться: двоетапна перевірка; наскрізне шифрування повідомлень, що засноване на асиметричному алгоритмі, в якому на кожній стороні є два ключі – публічний і приватний; секретні (приховані) чати та видалення повідомлень через заданий час.

Більш детально розглянемо три найбільш популярних месенджери:

Viber. У Viber використовується новітнє наскрізне шифрування та можливість створення прихованих чатів. До мінусів можна віднести відсутність двоетапної перевірки і те, що сервери цієї компанії розташовані в Росії. Хоча в компанії повідомляють, що на російських серверах знаходяться лише дані російських користувачів, проте цю інформацію перевірити неможливо, а у зв'язку із ситуацією на кордоні з цією країною на це варто особливо звернути увагу. Telegram. До переваг з боку захищеності месенджера можна віднести можливість подвійної аутентифікації, через що зловмисникам буде тяжче привласнити собі аккаунт. Є можливість спілкування у «секретних чатах», де під час передачі повідомлення використовується наскрізне шифрування. Головною особливістю телеграму є те, що у ньому дозволяється використовувати псевдонім для ідентифікації в мережі в той час коли у інших месенджерах ця функція непередбачена. Вона дозволяє з'єднатися з іншими користувачами, без потреби вказування власного номеру телефону. До недоліків варто віднести те, що цей месенджер був розроблений російськими програмістами.

WhatsApp. Даний месенджер був розроблений українськими програмістами, у ньому підтримується двоетапна перевірка, наскрізне шифрування та можливість налаштування автоматичного видалення повідомлень в групових чатах. До недоліків варто віднести, що у 2014 році месенджер був викуплений компанією Facebook, яка відома агресивними механізмами отримання інформації про своїх користувачів. Крім цього у компанії Facebook нещодавно відбувся масштабний збій в роботі системи.Наша пропозиція полягає в розробці власного програмного забезпечення, яке зашифровує повідомлення відразу на мобільному пристрої перед відправленням, використовуючи симетричні алгоритми шифрування, тому що вони не потребують попередньої передачі відкритих ключів через канали зв'язку приватних компаній.

Висновок. Не зважаючи на те, що канали передачі інформації месенджерів є доволі надійними, і зловмисникам дуже важко обійти захист та отримати несанкціонований доступ до інформації, проте вони не гарантують безпеки службової інформації, що може передаватись. Тому, пропозиція шифрування повідомлень на мобільних пристроях до їх відправки у месенджері є достатньо надійним методом передачі службової інформації.

Чередниченко О.Ю. (ВІТІ)
Процюк Ю.О. (ВІТІ)
Куклюк М.М. (ВІТІ)

АНАЛІЗ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У ВІЙСЬКОВОМУ КОНФЛІКТІ В НАГІРНОМУ КАРАБАСІ

Війни, що відбуваються у XXI столітті стали революційними у військовій справі завдяки появі та застосуванню безпілотних літальних апаратів (БПЛА). Визначення напрямів застосування БПЛА в сучасних війнах має дуже актуальне значення.Аналіз останніх військових конфліктів і локальних війн в Україні, Сирії, Лівії та інших регіонах планети наочно демонструє, що практично в кожному з них має місце новий формат ведення бойових дій, руйнуються класичні уявлення про форми та методи збройної боротьби на полі бою, вносяться суттєві корективи у стратегію і тактику досягнення переможних для кожної сторони результатів. Проведено аналіз та систематизація нової тактики бойового застосування груп БПЛА для ураження ЗРК і придушення системи ППО. Одним із них став так званий “карабаський конфлікт” між Вірменією та Азербайджаном за контроль над територією Нагірного Карабаху.Сучасні безпілотні літальні апарати здатні не лише ефективно виявляти противника вдень та вночі, наводити на нього власні вогневі засоби, але й самостійно знищувати його на значній відстані від поля бою. Розглянемо застосування БПЛА проти зенітно-ракетних комплексів (ЗРК) протиповітряної оборони (ППО) у військовому конфлікт на території Нагірного Карабаху.Таке застосування БПЛА на засоби ЗРК ППО призвело до швидкого вичерпання їх бойового ресурсу і, як наслідок, подальшої нездатності цих комплексів вирішувати завдання по своєму призначенню. Аналіз результатів бойового застосування засобів ППО проти сучасних БПЛА показав, що дальність виявлення ЗРК апаратурою БПЛА стала порівняно однаковою, а часом і перевищує її. В ході військового конфлікту в Нагірному Карабасі була розроблена нова тактика застосування БПЛА, яка дозволяє забезпечити гарантоване ураження ЗРК і тим самим здійснити функціональне придушення системи ППО і забезпечити завоювання переваги в повітрі.

В ході військових конфліктів останніх років засобів ППО проти сучасних БПЛА вони із засобів захисту поступово стали об’єктами “полювання” для БПЛА противника.

Крім того, досвід застосування БПЛА в ході військового конфлікту в Нагірному Карабасі показав, що БПЛА застосовуються в складі груп, які вирішують як розвідувальні, так і ударні завдання одночасно. Вплив перешкод призводить як до зниження дальності виявлення БПЛА з боку радіолокаційної станції (РЛС) ЗРГК, так і до зниження ймовірності правильного цілевказівки зенітним керованим ракетам (ЗКР). В результаті розмір зони ураження ЗРГК засобами, розміщеними на ударному БПЛА, також можна порівняти з розміром зони ураження БПЛА.

В результаті військового протистояння в Нагірному Карабасі була розроблена нова тактика застосування БПЛА – застосування легких і дешевих БПЛА масовано, групами, під прикриттям більш важких розвідувальних БПЛА, обладнаних засобами радіолокаційної (РЛР), оптико-електронної розвідки (ОЕР) і комплексами радіоелектронного придушення (РЕП), в рамках вирішення завдань ураження ЗРК і ЗРГК систем ППО. Аналіз бойового застосування показав надзвичайно низький рівень бойової живучості ЗРГК, в умовах масованого застосування БПЛА.

Незалежно від того, як буде складатися подальший розвиток подій у військових конфліктах, спостерігається тенденція підвищення ефективності застосування БПЛА для придушення ППО, завоювання переваги в повітрі і поразки основних сухопутних засобів озброєння. Це дозволяє зробити висновок про можливу близьку зміну стратегії ведення воєн в частині застосування БПЛА. У війнах найближчого майбутнього можливе масове багатоетапне застосування груп легких розвідувальних і розвідувально-ударних БПЛА, а також “БПЛА-камікадзе”.

Подальший розвиток тактики групового застосування БПЛА істотно ускладнить умови функціонування ЗРК і ЗРГК, а також потребує кардинального перегляду ідеології створення систем ППО.

З початком бойових дій в Нагірному Карабасі, як показано в роботах, азербайджанські збройні сили, за підтримки турецьких військових фахівців, розгорнули масове групове застосування ударних БПЛА, з урахуванням досвіду застосування БПЛА в Сирії та Лівії. Без застосування БПЛА у війні в Нагірному Карабасі, вірменські системи ППО були б цілком спроможні щодо стримування азербайджанської авіації. Не випадково, навіть отримавши перевагу в повітрі, Азербайджан дуже обмежено використовував свою пілотовану авіацію, так як ЗРК, що залишаються на озброєнні Вірменії продовжували представляти для них серйозну загрозу. Однак Вірменія виявилася абсолютно не готова до війни з масовим використанням БПЛА, тактику якої хусити відпрацювали в Ємені, а турки – в Сирії та Лівії.

Результатом масованого застосування груп БПЛА Bayraktar TB2, спільно з "БПЛА-камікадзе" Sky Striker, Harop і Orbiter стало практично повне знищення вірменських ЗРК "Оса" і "Стріла-10", розміщених в Нагірному Карабасі, в перші дні конфлікту. В перший день війни по позиціях цих ЗРК був нанесений заздалегідь підготовлений удар, який позбавив оборону Нагірного Карабаху, за оцінками фахівців, до 80% комплексів ППО – 6 ЗРК "Оса" і 3 ЗРК "Стріла-10" при втратах в 4 БПЛА. Таким чином, за рахунок масовості і раптовості застосування, забезпечивши обмін 2,25 ЗРК на 1 БПЛА, завоювання переваги в повітрі дало можливість Азербайджану за допомогою БПЛА безперервно, в цілодобовому режимі, і безперешкодно атакувати вірменські мотострілкові і механізовані частини, завдаючи їм істотні втрати ще до того, як вони вступали в бій з силами Азербайджану. Це значно полегшило наступ азербайджанської армії і дозволило добитися істотних тактичних успіхів.

При цьому, комплекси ППО, що залишилися на озброєнні Вірменії, такі як С-300ПС та С-300ПТ не призначені для боротьби з БПЛА, в зв'язку з чим вони не можуть бути ефективно використані для оборони повітряного простору Вірменії і Нагірного Карабаху від цього нового типу загроз. Більш того, в результаті грамотно спланованої операції силами БПЛА були знищені 2 пускові установки і 2 РЛС зі складу ЗРК С-300ПС. За інформацією ЗМІ один із знищених ЗРК С-300ПС входив до складу системи ППО Вірменії і знаходився на відкритій місцевості без будь-якого додаткового прикриття. Причиною тому послужило те, що на першому етапі військового конфлікту Азербайджан використовував літаки Ан-2 в безпілотному виконанні, щоб виявити місце розташування вірменських систем ППО. Літаки були збиті, але це дозволило розкрити місце розташування як ЗРК С-300ПС, так і ЗРК ближнього радіусу дії "Оса" і "Стріла-10М3", які здійснювали його прикриття. Після знищення ЗРК ближнього радіусу дії ЗРК С-300ПС залишився без прикриття і пускова установка 5П85С, а також РЛС типу 36Д6, що входять до складу ЗРК, були вражені за допомогою "БПЛА-камікадзе" ізраїльського виробництва Harop.

Таке масове ефективне застосування БПЛА для виявлення і знищення спочатку системи ППО, а в подальшому – живої сили і озброєння сухопутних військ, яке було використано у війні в Нагірному Карабасі, зустрічається у світовій практиці вперше і отримало в ЗМІ назву "війна дронів". Азербайджанська сторона широко розповсюдила в ЗМІ відеозаписи високоточних ударів БПЛА по вірменським позиціях. Основні цілі ударів – це, перш за все, засоби ППО, потім – бронетанкові колони на марші, танки і артилерія на позиціях, рідше – склади, сховища і казарми.

За результатами аналізу досвіду бойового застосування груп БПЛА у військових конфліктах останніх років, зокрема, в Нагірному Карабасі. Аналіз дозволив розкрити основні недоліки сучасних комплексів ППО, як об'єктів поразки, а також провести детальний аналіз групового застосування БПЛА і їх ефективності при роботі по цілями такого типу.

Чміль В.В. (ПрАТ «НВП «Сатурн»)
к.т.н. Ожинський В.В. (ЦКДЗ НЦУВКЗ)
к.т.н. Поіхало А.В. (НЦУВКЗ)
к.т.н. Сундучков І.К. (ПрАТ «НВП «Сатурн)

«МЕТОДИ, СТРУКТУРА ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ УПРАВЛІННЯ КАНАЛАМИ ПРИЙОМУ ТЕЛЕМЕТРИЧНОЇ ІНФОРМАЦІЇ ВІД ШТУЧНИХ КОСМІЧНИХ АПАРАТІВ ПО ДОСЛІДЖЕННЮ СОНЯЧНОЇ СИСТЕМИ»

На прикладі пункту прийому телеметричної інформації (РТ-32) в Центрі космічних досліджень та зв`язку ДКАУ м. Золочів Львівської області описані принципи побудови системи управління.

Приводиться приклад практичної реалізації такого пристрою.

Система управління пристроєм прийому телеметрії від космічних апаратів повинна вирішити наступні задачі: управління антенним комплексом для виведення його в задані координати та супроводження космічного об`єкту по заданій програмі; управління процесом виходу на режим радіоастрономічного приймального комплексу; управління процесами частотно-часової синхронізації та прив`язки до світової шкали часу; управління процесом обробки телеметричної інформації та процесом передачі інформації зацікавленим сторонам; управління процесами прийняття рішень у випадках відхилення від норми в роботі окремих систем чи підсистем, по результатам контролю технічного стану; можливості управління роботою дистанційно, включаючи видачу план-завдань.

Управління технічним станом РТ-32 та його роботою - це складний процес, що вимагає наявності достовірної інформації про поточний стан складових частин (систем та підсистем) радіотелескопу, ефективних механізмів її обробки для забезпечення їх чіткої взаємодії.

Принципи побудови. Головною задачею при прийнятті телеметричної інформації космічних об`єктів є забезпечення надійності роботи систем, в тому числі системи управління, забезпечення прийняття інформації, навіть при виникненні часткової відмови окремих складових систем.

В умовах високого ступеню невизначеності доцільно використати для прийняття рішень, теорію нечітких множин, ймовірнісні способи визначення стану нечітких параметрів.

Теорія нечітких множин і основана на ній логіка дозволяють описувати неточні категорії, уявлення і знання, оперувати ними і робити відповідні висновки.

Нечіткі системи керування використовують наявну базу знань і елементи штучного інтелекту та можуть бути реалізовані за логічними формулами, що використовують логічні операції « І », « АБО », «ЯКЩО» і т. д.

Процес управління можливо описати як лінгвістичні змінні, згрупувавши їх за напрямками та характерним рисам.

Модель управління технічним станом РТ-32 може бути представлено виразом

$Y = fx(x_1 x_2 \dots x_n)$, де х – чинники, які впливають на роботу системи

серед $(x_1 x_2 \dots x_n)$ є чинники, які мають постійний та більше сталий характер, а є чинники, які залежать, у свою чергу, від чинників наступного рангу.

$x_n = f(c_1 c_2 \dots c_m)$

Модель управління буде представляти собою матрицю управлінських рішень.

$$\begin{aligned} Y_1 &= fx(x_{11} + x_{12} \dots + x_{1n}) \\ Y_2 &= fx(x_{21} + x_{22} \dots + x_{2n}) \\ Y_m &= fx(x_{m1} + x_{m2} \dots + x_{mn}), \end{aligned} \qquad (1)$$

де x_{mn} – чинники, які впливають на роботу системи,

а Y_m – управлінські рішення за результатами логічної обробки даних контролю технічного стану x_{mn}., або вхідних даних для проведення сеансу спостережень (зв’язку).

Практичним результатом даного принципу побудови являється алгоритм управління РТ-32 з більш ніж 95-ма логічними операціями та таблиця 227 ймовірних, в тому числі нештатних, ситуацій на базі яких розроблена матриця управлінських рішень (1).

В цілому алгоритм роботи комплексу та реакція системи управління на нестандартні ситуації потребували розробки 32 програм та підпрограм.

ВИСНОВКИ

Дослідна експлуатація РТ-32 показала дієвість структури побудови управління.

Система управління дає можливість виконання поставлених задач при частковому відхиленні параметрів систем від номіналу (збої в системах охолодження, відхилень по первинному та вторинному енергозабезпеченню та інші).

Передбачена робота комплексу протягом не менше 20 хвилин при повній відсутності первинного енергозабезпечення.

Такі заходи дають можливість підняти вірогідність одержання достовірної інформації, особливо при прийнятті телеметрії від зондів штучного походження, ресурс яких в деяких випадках не дозволяє повторне проведення таких сеансів.

Шарнін С. А. (ВІТІ)
Савицький Н. І. (ВІТІ)

КОМПЛЕКС ЗАСОБІВ АВТОМАТИЗАЦІЇ АДМІНІСТРУВАННЯ ІНФОРМАЦІЙНОЇ МЕРЕЖІ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Актуальність. Надійність є дуже важливою властивістю програмного забезпечення (ПЗ). Помилки ПЗ створюють важливу загрозу суспільству, адже комп'ютерні системи виконують важливі технологічні процеси, оброблюють конфіденційну і секретну інформацію, їм делегують відповідальну роботу, від якості виконання якої багато в чому залежить життя і добробут багатьох людей. Під час експлуатації інформаційних мереж необхідно виявляти і усувати помилки (збої), що вимагають посадові обов'язки штату системних адміністраторів. Даний процес часто неоптимізований, оскільки виявлення помилок відкладається до моменту скарг оператора електронної обчислювальної машини (ЕОМ). В умовах глобальної інформатизації діяльності військ, враховуючи провадження ЕОМ у військах, залучення у процес інформаційної діяльності та взаємодії все більшої кількості особового складу, постає актуальним завдання створення комплексу засобів швидкого виявлення, реєстрації критичних помилок (збоїв) у процесі функціонування інформаційних мереж для сповіщення групи системних адміністраторів із розподілом між ними завдань на оперативне усунення несправностей (помилок).

Метою дослідження єрозробка комплексу засобів автоматизації адміністрування інформаційної мережі військового призначення, який буде включати моніторинг програмної і апаратної складової інформаційної мережі. Для досягнення вказаної мети у роботі сформульовано наступні **завдання**: аналіз сучасних підходів щодо збереження безпеки мережі, виконання діагностики і усунення помилок; формування вимог до комплексу засобів автоматизації адміністрування, визначення пріоритетних напрямків розвитку, враховуючи потреби функціонування інформаційної мережі у військах; розробка комплексу засобів автоматизації адміністрування інформаційної мережі військового призначення; оцінка ефективності розробленого комплексу.

Виклад основного матеріалу. При виникненні у роботі ЕОМ програмних помилок (збоїв) в операційній системі (ОС) ЕОМ у першу чергу аналізують журнал подій, який фіксує порушення нормального режиму функціонування ОС. У сімействі ОС Windows служба, яка управляє протоколюванням подій називається «Журнал подій». Задля організації автоматизації адміністрування ЕОМ об'єднаних у локальну обчислювальну мережу (ЛОМ), забезпечений збір інформації про помилки (збої) кожної ЕОМ на сервері ЛОМ. Системним адміністраторам наданий зручний інтерфейс для роботи щодо реєстрації усунення виявлених проблем. Запропонований комплекс визначає пріоритет помилок (збоїв) і виконує розподілення відповідальності за вирішення окремої проблеми між групою системних адміністраторів на основі статистики їхньої зайнятості. Кожному адміністратору у програмному інструментів головним адміністратором надається роль відповідно до кола його обов'язків, доступу до окремих ЕОМ ЛОМ. Комплекс засобів надає можливість:

автоматизувати регулярне резервне копіювання даних журналу подій ЕОМ ЛОМ, оскільки часто виникає необхідність аналізувати події, які відбулися досить давно;

представити ЛОМ у вигляді дерева із можливістю пошуку за IP-адресою або назвою ЕОМ;

використовувати розвинені засоби пошуку подій журналів, сортування, фільтрації, перегляду подій за категоріями;

експорту журналів подій у різні формати файлів (html, xml, json, формату текстових файлів, файлів електронних таблиць), друку звітів.

Висновки. Реалізація запропонованого комплексу засобів сприяє скороченню рутинних задач, підвищенню ефективності роботи системних адміністраторів, і, як наслідок, збільшенню рівня надійності і безпеки роботи ЕОМ комп'ютерної мережі.

Шемендюк О.В.
Чередниченко О.Ю.
Очіченко Р.А.

МОНІТОРИНГСТАНУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ЯК СКЛАДОВА СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Вступ

З розвитком інформаційних технологій збільшується ризик витоку інформації, зараження вірусами, втручання в роботу інформаційної системи. Важливо усвідомлювати стан захищеності ресурсів в інформаційно-телекомунікаційній системі (ІТС), щоб протистояти різним видам загрози її безпеки. Типова інфраструктура мережі, крім серверів і клієнтів, складається з різних унікальних елементів, і важливо контролювати їх. Моніторинг пристроїв мережі необхідний, оскільки він забезпечує повну картину вашої мережі. Наприклад, якщо через помилку в брандмауері можна отримати незаконний доступ до мережі, ви зможете провести ретельне розслідування, лише якщо маєте інформацію про аудит брандмауера.Реальну допомогу в цьому може зробити моніторинг стану захищеності інформаційно-телекомунікаційної системи.

Метою дослідженняє процес моніторингу стану захищеності інформаційно-телекомунікаційних систем спеціального призначення в складі системи управління інформаційною безпекою установи чи організації.

Виклад основного матеріалу дослідження

Основним етапом моніторингу активності та безпеки мережі є збір та аналіз журналів пристроїв мережі.При проектуванні захищених інформаційно-телекомунікаційних систем важливо чітко уявляти, яким вимогам вони повинні задовольняти, перелік основних показників якості, методику контролю і оцінки їх ефективності.

Щоб досягти необхідного стану захищеності ІТС, що задовольняє потреби, необхідно більше, ніж просто купити антивірусне програмне забезпечення, системи мережного захисту або системи резервування даних. Важливий комплексний підхід, що дозволить реалізовувати політику інформаційної безпеки й, що саме головне, ефективно й оперативно реагувати на нові загрози інформації, що постійно з'являються.

Для моніторингу стану захищеності мережі найкращим варіантом є використання готових варіантів спеціального програмного забезпечення або використання програмного забезпечення з відкритим кодом, для доопрацювання його під визначені завдання моніторингу, які обов’язково включають:

моніторинг роботи маршрутизаторів, комутаторів та брандмауерів ІТС, правильність функціонування та налаштування;

розпізнавання підозрілої діяльності (активності) в мережі;

виявлення небажаних пакетів даних, які намагаються проникнути в мережу;

аудит журналів, створених активними пристроями мережі;

контроль трафіку мережі.

Висновки

Таким чином забезпечення моніторингустану захищеності інформаційно-телекомунікаційних систем спеціального призначення є важливим етапом при створення системи управління інформаційною безпекою організації. Моніторинг стану захищеності ІТС дозволить в режимі реального часу надавати актуальну інформацію про значні події у мережі, а саме інформацію про схеми атак, виявлених на різних пристроях, що є надзвичайно важливим, оскільки це дає змогу візуалізувати безпеку та працездатність вашої мережі та відповідно посилити безпеку, а найголовніше зберегти інформацію від несанкціонованих дій з нею.

V.Shypovskyi, PHD , NDU
D.Ilin, PHD, NDU

ANALYSIS OF MODERN CYBERATACS THAT MAY BE IMPLEMENTED FOR DESTRUCTIVE INFLUENCES ON STATE CRITICAL INFRASTRUCTURE

Introduction. During last years, the number of cyber-attacks on critical infrastructure information infrastructure in Europe has doubled. Cyber protection of critical infrastructure - provides security and improves the quality of life of every country in the world. Continuous operation of power plants, trouble-free operation of railway transport, access to food, ensuring payments to the population, etc. A few years ago, in the winter, residents of western Ukraine spent several hours without electricity due to the world's first attack on the energy system by the Blackenergy virus. We also remember the NotPetya virus, due to which many of the usual services did not work - the post office resumed work for several days, there were problems with air transportation, the work of banking institutions, and so on. The Security Service of Ukraine neutralized more than 300 cyberattacks and cyber incidents on critical infrastructure during the first half of 2020. Almost 20 hacker groups were involved in these cyberattacks, which were also exposed and neutralized by the secret service. A significant number of hackers were directly controlled from the Russian Federation. Their purpose was to harm the Ukrainian state bodies and enterprises of the defense-industrial complex. A total of 219 cases of illegal use of electronic payment systems and payment systems were exposed and terminated during this period. To increase the cyber resilience of the state, the Security Service of Ukraine initiated 295 criminal proceedings, including 82 - for unauthorized interference in the work of information systems of critical infrastructure of the state [1].

Purpose and problem statement. The protection of critical infrastructure with the development of information technology is of particular importance and requires careful scientific study. The purpose of the publication is to consider the most common types of cyber-attacks of today to determine the vector of concentrated attention from military science for comprehensive cyber defense of critical infrastructure and national security and substantiate recommendations for improving cyber resilience of critical infrastructure information systems.

Main material. To analyze the most common types of cyber-attacks today, consider the latest ENISA report “ENISA THREAT LANDSCAPE 2021”. Through continuous analysis, ENISA derived trends and points of interest for each of the major threats presented in the ETL 2021. Cybersecurity attacks have continued to increase through the years 2020 and 2021, not only in terms of vectors and numbers but also in terms of their impact. Spurred by an ever-growing online presence, the transitioning of traditional infrastructures to online and cloud-based solutions, advanced interconnectivity and the exploitation of new features of emerging technologies such as Artificial Intelligence (AI), the cybersecurity landscape has grown in terms of sophistication of attacks, their complexity and their impact. Notably, the threat to supply chains and their significance due to their potentially catastrophic cascading effects has reached the highest position among major threats, so much so that ENISA produced a dedicated threat landscape for this category of threat. A series of cyber threats emerged and materialized in the course of 2020 and 2021. Based on the analysis presented in this report, the ENISA Threat Landscape 2021 identifies and focuses on the following 8 prime threat groups. These 8 threat groups are highlighted because of their prominence during the reporting period, their popularity and the impact that materialization of these threats has had.

Ransomware is a type of malicious attack where attackers encrypt an organization’s data and demand payment to restore access. Ransomware has been the prime threat during the reporting period, with several high profile and highly publicized incidents.

Malware is software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of a system. The threat of malware

has been consistently ranked high for many years, albeit at a decreasing rate during the reporting period of ETL 2021.

Cryptojacking or hidden cryptomining is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency.

E-mail related attacks are a bundle of threats that exploit weaknesses in the human psyche and in everyday habits, rather than technical vulnerabilities in information systems. Interestingly and despite the many awareness and education campaigns against these types of attacks, the threat persists to a notable degree.

Threats against data. This category encompasses data breaches/leaks. A data breach or data leak is the release of sensitive, confidential or protected data to an untrusted environment. Data breaches can occur as a result of a cyber-attack, an insider job, unintentional loss or exposure of data.

Threats against availability and integrity. Availability and integrity are the target of a plethora of threats and attacks, among which the families of Denial of Service (DoS) and Web Attacks stand out. Strictly related to web-based attacks, DDoS is one of the most critical threats to IT systems, targeting their availability by exhausting resources, causing decreases in performance, loss of data, and service outages.

Disinformation – misinformation Disinformation and misinformation campaigns are on the rise, spurred by the increased use of social media platforms and online media, as well as a result of the increase of people's online presence due to the COVID-19 pandemic. This group of threats is making its first appearance in the ETL; however its importance in the cyber world is high.

Non-malicious threats. Threats are commonly considered as voluntary and malicious activities brought by adversaries that have some incentives to attack a specific target. With this category, we cover threats where malicious intent is not apparent. These are mostly based on human errors and system misconfigurations, but they can also refer to physical disasters that target IT infrastructures [2].

Conclusions. Analyzing the types of modern cyberattacks, the basis for the development of a mitigation strategy for the prevention of and response against negative cyberinfluence is:

Implementation of secure and redundant backup strategies;

Implementation and auditing of identity and access management (least-privilege and separation of duties);

Training and raising the awareness of users (including privileged users);

Separation of development and production environments;

Information sharing on incidents with authorities and the industry;

Identities and credentials should be issued, managed, verified, revoked, and audited for authorised devices, users, and processes;

Access permissions and authorisations should be managed, incorporating the principles of least privilege and separation of duties;

Separation of development and production environments.

It is not difficult to conclude that every employee of any critical infrastructure object can become an easy target for cybercriminals to use it as a tool of destructive influence on a certain object. Therefore, the main list of measures to prevent cyber impacts on information systems includes not only cyber hygiene measures, personnel involved in the full range of these facilities must be cyber literate. Man remains the weakest link in cyber resilience, so cybersecurity education is becoming a priority.

Шишкін Д.І. (ВІТІ)
Бойко Є.С. (ВІТІ)
Шелар Р.Р. (ВІТІ)

АНАЛІЗ APACHE CASSANDRA ЯК ВІДМОВОСТІЙКОГО СКБД ДЛЯ ВИКОРИСТАННЯ У ВІЙСЬКОВИХ АСУ

Актуальність. Для ефективного використання та забезпечення відмовостійкості СКБД у військових АСУ.

Мета. Проаналізувати використання СКБД, що не підтримує концепцію master/slave (провідний/відомий) в умовах підвищених вимог до відмовостійкості на прикладі Apache Cassandra.

Основні положення. Apache Cassandra – це децентралізована розподілена система, що складається з кількох вузлів, якими вона розподіляє дані. На відміну від багатьох інших Big Data рішень екосистеми Apache Hadoop (HBase, HDFS), ця СКБД не підтримує концепцію master/slave (провідний/відомий), коли один із серверів є керуючим для інших компонентів кластера. Для розподілу елементів даних за вузлами Кассандра використовує послідовне хешування, застосовуючи хеш-алгоритм для обчислення хеш-значень ключів кожного елемента даних (ім'я стовпця, ID рядка та ін.). Діапазон можливих хеш-значень, тобто простір ключів, розподіляється між вузлами кластера так, що кожному елементу даних призначено свій вузол, який відповідає за зберігання та керування цим елементом даних.

Завдяки такій розподіленій архітектурі, Кассандра надає такі можливості:

розподіл даних між вузлами кластера прозоро для користувачів – кожен сервер може приймати будь-який запит (на читання, запис або видалення даних), пересилаючи його на інший вузол, якщо інформація, що запитується, зберігається не тут;

користувачі можуть самі визначити необхідну кількість реплік, створення та управління якими забезпечує Cassandra;

рівень узгодженості даних щодо кожної операції зберігання та зчитування, що настроюється користувачами;

висока швидкість запису (близько 80-360 МБ/с на вузол) - дані записуються швидше, ніж зчитуються за рахунок того, що їх більша частина зберігається в оперативній пам'яті відповідального вузла, і будь-які оновлення спершу виконуються в пам'яті, а потім – у файловій системі. Щоб уникнути втрати інформації, всі транзакції фіксуються у спеціальному журналі на диску. При цьому, на відміну від оновлення даних, записи до журналів фіксації лише додаються, що виключає затримку при обертанні диска. Крім того, якщо не потрібна повна узгодженість записів, Cassandra записує дані у достатню кількість вузлів без вирішення конфліктів невідповідності, які вирішуються лише при першому зчитуванні;

гнучка масштабованість – можна побудувати кластер навіть на сотню вузлів, здатний обробляти петабайти даних.

Висновок. Отже, відсутність центрального вузла позбавляє Кассандру головного недоліку, властивого системам master/slave, у яких відмовляє весь кластер при відмові головного сервера (Master Node). У кластері Cassandra всі вузли рівноцінні між собою і, якщо один з них відмовив, його функції візьме на себе якийсь із тих, що залишився. Завдяки такій децентралізації Apache Cassandra чудово підходить для географічно розподілених систем із високою доступністю, розташованих у різних датацентрах, а також АСУ які потребують високої відмовостійкості. Однак, при всіх перевагах такої гнучко масштабованої архітектури, вона зумовлює особливості операцій читання та запису, а також накладає низку суттєвих обмежень на використання цієї СКБД у реальних Big Data проектах.

Штонда Р.М. (ВІТІ)
Артемчук М.В. (ВІТІ)
Нечушкін М.П. (ВІТІ)

ПЕРСПЕКТИВИ СТВОРЕННЯ ШТАТНИХ ГРУП ШВИДКОГО РЕАГУВАННЯ ДЛЯ ВЕДЕННЯ КІБЕРОБОРОНИ ДЕРЖАВИ

Актуальність. Триваюче "гібридне протиборство" вимагає негайних адекватних відповідей на виклики та загрози національній безпеці України.

Постановка завдання. Одним із пріоритетів національної безпеки України є забезпечення кібербезпеки, реалізація якої здійснюється шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі [1].

Тому, на нашу думку, виникла необхідність в доповіді обговорити окремі аспекти щодо перспектив створення штатних груп швидкого реагування (далі – ШГШР) в складі кібервійськ.

Мета доповіді. Апробувати ідеї щодо необхідності створення ШГШР в складі кібервійськ в системі Міністерства оборони України.

Результат дослідження. Україна вибудовує свою кібербезпеку за напрямками захисту комп'ютерних мереж та протидії кіберзлочинності, за зразком Європейського Союзу, та зміцнення кібероборони, як в НАТО [2]. В НАТО протидія кіберзагрозам визначена поняттям "кібероборона", яка входить до переліку головних цілей колективної оборони, що підкреслює його безпеково-оборонну спрямованість. Тому НАТО зосереджується на захисті власних мереж і посиленні внутрішньої стійкості країн-членів, що є актуальним і для України.

Основними органами із забезпечення кібероборони країн-членів НАТО є: Північно-Атлантична Рада; Комітет кібероборони; Рада управління з кібероборони; Рада консультацій, контролю й управління; Центр операцій у кіберпросторі; Центр можливостей з реагування на комп'ютерні інциденти; Центр передового досвіду із кібероборони. А також створені групи швидкого реагування у кіберсфері, які перебувають у постійній готовності 24/7, спроможні надати допомогу союзникам щодо ведення кібероборони та протидії кіберзагрозам.

Виходячи із вище зазначеного та враховуючи [3], виникає негайна потреба створення в складі кібервійськ ШГШР з метою відсічі агресії в кіберпросторі та забезпечення проведення кібероперацій.

На ШГШР для досягнення поставленої мети необхідно покласти наступні завдання:

надання допомоги підрозділам/установам щодо ведення кібероборони;

запобігання кіберінцидентам та кібератакам;

виявлення та протидія кіберзагрозам;

ліквідація наслідків кіберінцидентів та кібератак;

проведення оцінювання захищеності мережевого та кінцевого обладнання ІТС шляхом аудиту.

Висновки. Таким чином, в результаті створенням ШГШР у складі кібервійськ в системі Міністерства оборони України суттєво підвищаться пріоритети щодо відсічі агресії в кіберпросторі та забезпечення проведення кібероборони.

Перспективи подальших наукових досліджень. Розробка варіантів застосування ШГШР під час ведення кібероборони.

Список використаних джерел

1. Указ Президента України від 26.08.2021 року №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. https://zakon.rada.gov.ua/laws/show/447/2021#n7

2. Співробітництво Україна–ЄС–НАТО з протидії гібридним загрозам у кіберсфері [Електронний ресурс]. Ресурс доступу – ahttps://www.kas.de/documents.

3. Указ Президента України від 26.08.2021 року №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави". [Електронний ресурс]. https://zakon.rada.gov.ua/laws/show/446/2021.