

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

**СУЧАСНІ ПРОБЛЕМИ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
НА ТРАНСПОРТІ**

СПІБТ–2024

МАТЕРІАЛИ

**ХІІ Всеукраїнської науково-технічної конференції
з міжнародною участю**

12–13 грудня 2024 року

*Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв*



МИКОЛАЇВ • НУК • 2024

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

**Матеріали публікуються за оригіналами, наданими авторами.
Претензії до організаторів не приймаються.**

Відповідальна за випуск В. В. Трибулькевич

У–45

Сучасні проблеми інформаційної безпеки на транспорті: матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю [Електронний ресурс]. – Миколаїв : НУК, 2024. – 234 с.

У збірнику подано матеріали XII Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

© Національний університет кораблебудування
імені адмірала Макарова, 2024

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТРАНСПОРТНИХ ЗАСОБІВ І СИСТЕМ

ЗАГРОЗИ ОБ'ЄКТАМ МОРСЬКОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ТА НАПРЯМКИ ДОСЛІДЖЕНЬ ЩОДО ЇХ НЕЙТРАЛІЗАЦІЇ

Автори: Блінцов В.С., д.т.н., професор; Буруніна Ж.Ю., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Україна є морською державою, у територіальних водах якої до повномасштабного вторгнення РФ велась активна морегосподарська діяльність, пов'язана з вантажними та пасажирськими перевезеннями, видобуванням енергетичних ресурсів та продуктів харчування, проведенням наукових досліджень. Вказані види діяльності проводились на відкритих морських акваторіях та у прилеглий зоні України, де розташовані об'єкти морської критичної інфраструктури (МКІ) – об'єкти водного транспорту та рекомендовані водні транспортні шляхи, порти та військово-морські бази, морські стаціонарні платформи та підводні трубопроводи, суднобудівні та судноремонтні заводи, інші стратегічно важливі для економіки і національної безпеки об'єкти.

Зазначені об'єкти мають стратегічне значення для функціонування економіки та національної безпеки. В сучасних умовах бойових дій на морі та зростаючій кількості гібридних загроз, МКІ стає вразливою до диверсій, атак безпечіпажних систем, кіберзагроз та природних катастроф [1, 2].

Виходячи з принципів системного підходу [3] розглянемо основні види загроз МКІ України. До таких загроз, у першу чергу, слід відносити наступні три види:

військово-технічні загрози – атаки морських дронів (надводних та підводних), диверсійні підводні операції, ракетні та артилерійські удари по портовій інфраструктурі, використання морських мін;

кіберфізичні загрози – втручання в автоматизовані системи керування портовими операціями, атаки на навігаційні системи (AIS, GPS spoofing), виведення з ладу енергетичних об'єктів через SCADA-системи;

екологічні та техногенні ризики – пошкодження трубопроводів і морських кабелів, аварії на нафтогазових платформах, зміна кліматичних умов і екстремальні погодні явища.

Попередній аналіз показує, що на цей час актуальними є наступні основні напрямки наукових досліджень щодо нейтралізації загроз об'єктам МКІ України [4]:

- розробка інтелектуальних системи моніторингу морської обстановки у територіальних водах України;

- використання автономних, прив'язаних та буксированих підводних апаратів-роботів для приладової інспекції морського дна;

- створення підводних сенсорних мереж (Underwater Sensor Networks, USN);

- супутниковий моніторинг та системи розпізнавання аномалій на основі спеціально розроблених систем штучного інтелекту;

- розробка антидронових технологій захисту акваторій – виявлення та перехоплення надводних та підводних безекіпажних систем, використання гідроакустичних пасток, активні перешкоди й дезорієнтація систем керування мілоських дронів противника;

- розробка та впровадження новітніх систем кібербезпеки МКІ – впровадження систем активного захисту SCADA, багаторівневе шифрування каналів передачі даних, моделювання атак у цифрових двійниках об'єктів МКІ.

Очевидно, що останній напрямок нейтралізації загроз об'єктам МКІ України вимагає розробки потужного прикладного математичного інструментарію для моделювання та прогнозування процесів протистояння сучасним загрозам [5]. До першочергових робіт у цьому напрямку віднесемо:

- розробку ефективних технологій математичного моделювання для оцінки вразливості об'єктів МКІ до різних типів загроз;

- розробку ефективних технологій мультиагентного моделювання атак на об'єкти МКІ та моделювання заходів щодо протидії цим атакам;

- розробку ефективних технологій геоінформаційного моделювання сценаріїв виникнення ризиків об'єктам МКІ та моделювання сценаріїв організаційно-технічної протидії загрозам, що можуть виникнути на захищених акваторіях України.

Таким чином, сучасні загрози об'єктам МКІ України мають комплексний характер і потребують міждисциплінарного підходу до їх

вивчення. Подальші дослідження мають бути спрямовані на розробку автономних систем моніторингу, підвищення кіберстійкості, та впровадження цифрових двійників для прогнозування та оцінки ризиків.

Створення адаптивної системи захисту морської інфраструктури є ключем до забезпечення національної безпеки України на морі.

Список літератури:

1. План заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року. Затверджено розпорядженням Кабінету Міністрів України від 10 листопада 2023 р. № 1025-р.

2. Морська безпека в умовах великої війни: як Україна, ЄС та НАТО повинні захищати себе від агресії росії. <https://www.youtube.com/watch?v=ojQPhGuPfw>

3. Pahl G., Beitz W., Feldhusen J., Grote K.H. Engineering Design: A Systematic Approach. Third Edition. Springer, 2006. <https://www.amazon.co.uk/Engineering-Design-Systematic-Approach-Pahl/dp/1846283183>

4. Велично Л. Ю., Білоконь М.В. Гібридні загрози транспортній інфраструктурі: виклики для державного регулювання та національної безпеки. Теорія та практика державного управління. 2024. Вип. 2 (79). С. 442–464. <http://doi.org/10.26565/1727-6667-2024-2-23>

5. Блінцов В. С., Майданюк П. В. Модель інформаційної платформи управління проектами захисту об'єкта морської критичної інфраструктури. Shipbuilding & marine infrastructure, 2019. №2(12). С. 4-17.

УДК 004.4

АНАЛІЗ ЗАГРОЗ СИСТЕМІ ІНФОРМАЦІЙНОГО ОБМІНУ МІЖ ПОСТОМ КЕРУВАННЯ ТА ДРОНОМ

***Автор:** Гололобов О.В., студент, Національний університет кораблебудування імені адмірала Макарова, Миколаїв, Україна*

***Науковий керівник:** Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. Використання дронів та інших форм безпілотних апаратів (БПА) з часом зростає від військових операцій, таких як спостереження, розвідка, до комерційних операцій, таких як транспорт, сільське господарство. Однак, оскільки ці БПА стають все більш поширеними, вони

створюють низку вразливостей кібербезпеки, які можуть мати значні наслідки, якщо їх не усунути належним чином. Розуміння цих вразливостей і вивчення стратегій їх пом'якшення є важливими для забезпечення безпечного та надійного розгортання мереж дронів.

Мета роботи провести аналіз вразливостей при інформаційному обміні між постом керування та дроном.

Основна частина.

Типова робота БПА передбачає зв'язок у реальному часі між дроном і наземною станцією керування, що часто покладаються на загальнодоступні мережі для передачі даних. Це налаштування вразливе до різноманітних кіберзагроз, таких як глушіння сигналу, перехоплення даних і навіть прямі атаки на керуюче програмне забезпечення.

До атак, що впливають на конфіденційність БПА можна віднести:

- аналіз трафіку: аналіз трафіку виконується для вивчення трафіку БПА, щоб отримати корисну інформацію від пристроїв і мереж БПА. Трафік містить пакети, які спільно використовуються між БПА і наземними системами керування. Криміналістика пакетів у трафіку виявляє конфіденційну інформацію. Пакети містять інформацію про місцезнаходження, підключення БПА із датчиками та отримані дані з датчиків;

- перехоплення: у перехопленні зловмисник бере участь хтось, хто регулярно відстежує мережевий трафік. Знайти такого зловмисника, який пасивно стежить за мережею, дуже складно. У критичних місіях БПА містить конфіденційну інформацію; отже, відстеження та моніторинг БПА може бути небезпечним для агенцій, які відповідають за такі місії;

- збір даних і криміналістика: за допомогою аналізу трафіку з БПА можна зібрати величезну кількість даних. Навіть якщо зашифровані дані не розкривають жодної корисної інформації, експертиза даних допомагає отримати конфіденційну інформацію із зібраних даних, наприклад місце виробництва, конфігурацію тощо.

На цілісність даних БПА впливають такі атаки:

- підміна або зміна інформації: зміна – це концепція додавання неправдивої або неправильної інформації в повідомлення та зміни початкового значення даних. Різноманітні форми змін включають

модифікацію, виготовлення, заміни та ін'єкції даних, які змінюють дані, що використовуються для передачі БПА. Зміна даних вводить користувачів в оману сфабрикованою інформацією.

- модифікація керування доступом: засоби керування доступом – це правила та політики, які керують тим, як інші пристрої в БПА спілкуються та як користувач отримує доступ до даних. Якщо зломисник отримує контроль доступу, він може змінити всі дозволи, привілеї та повноваження, що може призвести до величезних втрат.

- атаки людина по середині: атаки людина по середині дозволяють зломисникам отримувати дані про зв'язок між БПА і датчиками. Rogue Access Point використовується для володіння бездротовою точкою доступу та спонукання пристроїв поблизу приєднатися до її домену в комунікації БПА. Через ці точки доступу зломисник може маніпулювати мережевим трафіком;

- підробка повідомлень: під час атаки підробки повідомлень в БПА повідомлення запиту на вхід попередніх сеансів через загальнодоступний/відкритий канал підробляються під час виконання протоколу автентифікації. Після цього зломисник може змінити та повторно передати повідомлення користувачеві.

На доступність БПА можуть вплинути такі атаки:

- DoS і DDoS: DoS визначається як заборона доступу до ресурсів або перешкоджання законним користувачам отримати доступ до каналу зв'язку для надсилання та отримання. Якщо зломисник виконує запити флуду на цих каналах, мережа переривається, що призводить до недоступності ресурсу.

- підробка GPS: GPS використовується для визначення положення транспортного засобу та надання маршрутних точок для польоту до визначеної цілі. Зломисник може змінювати вміст отриманих сигналів GPS або генерувати сигнали підробки за допомогою генераторів сигналів GPS. Затримки сигналів GPS також спричинять значні втрати в БПА, оскільки це може порушити координацію, що призведе до зіткнень у повітрі.

- перешкоди каналу зв'язку: Попередньою метою перешкод є навмисне порушення каналу зв'язку БПА [4]. Уразливості в каналі зв'язку можуть вплинути на БПА. Перешкоди можуть викликати колізію БПА або недоступність сервісів [26].

– маршрутизаційні атаки: маршрутизаційні атаки включають флуд, ізоляцію вузла, атаки розкриття розташування тощо.

Висновки

Кібербезпека безпілотних апаратів – це складна галузь, що швидко розвивається, яка потребує мультидисциплінарного підходу для вирішення різноманітних викликів і загроз, які представляють безпілотні апарати.

Ключ до захисту безпілотних літальних апаратів полягає в розумінні їх вразливості, загроз і потенційного впливу, а також у впровадженні ефективних контрзаходів і найкращих практик, які збалансують переваги та ризики.

Список літератури:

1. K. Hartmann and C. Steup. The vulnerability of uavs to cyber attacks-an approach to the risk assessment. In Proc. of the 5th IEEE International Conference Cyber Conflict (CyCon'13), Tallinn, Estonia, pages 1–23. IEEE, June 2013.
2. Shafique Arslan, Mehmood Abid, Elhadeif Mourad, Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. 2021 Access. PP. 1-1. 10.1109/ACCESS.2021.3066778.
3. Potential vulnerabilities of drone networks to cyberattacks and how they can be mitigated URL: <https://www.linkedin.com/pulse/drones-security-vulnerability-exploitation-awareness-dror-amrami>

УДК 004.056.5:656.025.2

ОЦІНКА БЕЗПЕКИ БАЗ ДАНИХ NOSQL У СИСТЕМАХ ВІДСТЕЖЕННЯ ТА МОНІТОРИНГУ ТРАНСПОРТУ

***Автор:** Євдокимов С.О., аспірант, Херсонський державний університет, м. Івано-Франківськ, Україна*

Зростаюча кількість даних, що генеруються системами відстеження та моніторингу, вимагає впровадження потужних і гнучких рішень для їх обробки та зберігання [1-2].

NoSQL — це тип баз даних, який не використовує традиційну реляційну модель для зберігання та організації даних. На відміну від

реляційних баз даних (далі – БД), де дані зберігаються у вигляді таблиць, NoSQL використовують більш гнучкі структури, що дозволяє їм краще масштабуватись і справлятися з великими обсягами даних, що надходять у реальному часі, що робить їх ефективними для використання в сучасних розподілених системах, таких як системи моніторингу та відстеження транспорту. Однак, разом із перевагами, виникають серйозні виклики в сфері безпеки, оскільки недостатній захист даних може призвести до несанкціонованого доступу та витоку інформації, в результаті чого фінансових втрат та дестабілізації внутрішніх процесів підприємства [1, 4].

Метою даного дослідження є оцінка безпеки БД NoSQL у системах відстеження та моніторингу транспорту, а також розробка рекомендацій для підвищення їх захищеності. Основні завдання дослідження включають:

1. Виявлення і класифікація вразливостей, що характерні для NoSQL баз даних у контексті систем моніторингу (Рис. 1).
2. Оцінка ефективності існуючих заходів безпеки та розробка рекомендацій щодо їх поліпшення (Табл. 1).
3. Формулювання конкретних стратегій та заходів, які можуть бути впроваджені для підвищення рівня безпеки NoSQL баз даних у транспортних системах.

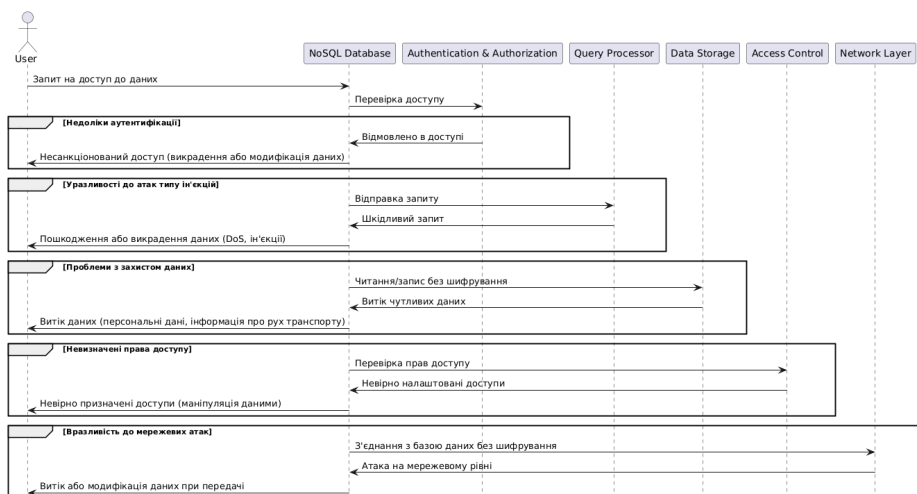


Рис. 1. Вразливості систем моніторингу та відстеження транспорту

Таблиця 1. Результати дослідження виявлення та класифікації вразливостей NoSQL у контексті систем моніторингу транспорту

Тип вразливості	Приклад БД	Рекомендації щодо захисту	Оцінка ризику (1-5)	Пріоритет виправлення (1-5)
Недоліки в механізмах аутентифікації та авторизації	MongoDB, Cassandra, Redis	Використання складних паролів, двофакторна аутентифікація, OAuth 2.0, обмежені API-ключі	4	5
Вразливості до атак типу ін'єкцій	MongoDB, Redis	Параметризовані запити, валідація вхідних даних, моніторинг запитів	5	5
Проблеми із захистом даних при їх зберіганні та передачі	MongoDB, Cassandra	Шифрування AES-256 на зберіганні та TLS 1.2/1.3 при передачі, захист SSL/TLS-сертифікатами	3	4
Невизначені права доступу	MongoDB, Cassandra	Налаштування політик доступу, RBAC, аудит доступів	4	4
Вразливість до мережових атак	MongoDB, Redis	Зашифровані з'єднання через TLS/SSL, VPN, брандмауер для обмеження доступу	3	3

Діаграма на рис. 1 показує взаємозв'язок між користувачем, NoSQL базою даних та різними етапами перевірки доступу, що демонструє, як вразливості в системі можуть впливати на безпеку даних. Дана

інформація була встановлена автором, шляхом детального аналізу вразливостей NoSQL, зокрема через огляд літератури, яка включала наукові статті, технічні звіти та дослідження в галузі безпеки інформаційних систем. Наприклад, «Evaluating the Security of NoSQL Databases in IoT Environments» аналізує вплив IoT на безпеку NoSQL баз даних, виявляючи специфічні вразливості в контексті транспортних систем. В рамках дослідження також було проведено тестування на вразливості в спеціально створених середовищах таких як VirtualBox, Docker-контейнери та Metasploit (Kali Linux), які імітували реальні умови експлуатації транспортних систем.

Автор проводив симуляції атак, таких як SQL-ін'єкції, спроби несанкціонованого доступу, а також тестував конфігурацію шифрування даних для оцінки рівня безпеки. Крім того, автор досліджував існуючі механізми захисту, такі як реалізація багаторівневої аутентифікації, використання API-ключів і впровадження шифрування TLS/SSL, оцінюючи їхню ефективність у запобіганні вразливостям, виявленим під час тестування. Це дозволило виявити основні проблеми безпеки та визначити їхній вплив на системи моніторингу та відстеження транспорту, а також розробити рекомендації щодо поліпшення заходів захисту (Табл. 1).

Для підвищення безпеки доступу до даних у NoSQL базах даних транспортних систем необхідно впровадити багаторівневі механізми аутентифікації та авторизації. Один із найефективніших способів захисту – це використання OAuth 2.0 для забезпечення авторизації через сторонні сервіси (наприклад, за допомогою корпоративних облікових записів), а також API-ключів для автентифікації автоматизованих систем, що взаємодіють із базою даних. Для додаткової безпеки також доцільно застосовувати двофакторну аутентифікацію (2FA), що вимагає підтвердження особи через додаткові канали (наприклад, через смс-коди або мобільні додатки). Це забезпечить більш надійний доступ до критичних даних і зменшить ймовірність несанкціонованого доступу. Регулярне тестування на вразливості та проведення пентестінгу є важливою частиною стратегії безпеки для будь-якої системи, що використовує NoSQL бази даних. Спеціалізовані інструменти, такі як Nessus, Burp Suite або OWASP ZAP, можуть бути використані для виявлення вразливостей у системах, що використовують MongoDB, Cassandra або Redis.

Висновок. Аналіз вразливостей та загроз безпеці NoSQL баз даних, що використовуються в транспортних системах, дозволив виокремити ключові проблеми, які можуть серйозно вплинути на функціонування таких систем. Для ефективного захисту даних та забезпечення надійної роботи транспортних систем необхідно застосовувати комплексний підхід, а також важливо враховувати постійну еволюцію загроз у світі кібербезпеки, що вимагає адаптації до нових технічних умов і появи нових методів атаки [4-7]. Перспективи розвитку безпеки NoSQL баз даних у транспортних системах безпосередньо пов'язані з використанням передових технологій, таких як нейронні мережі та штучний інтелект для забезпечення кібербезпеки, особливо у сфері виявлення аномалій та прогнозування атак.

Список літератури:

1. Євдокимов, С., & Таранущенко, В. (2024). Розробка сучасної моделі запобігання дорожньо-транспортним пригодам за допомогою згорткової нейронної мережі. Інформаційні технології і засоби навчання, (5), 45–52. DOI: 10.14308/ite000769.
2. Zeldovich, M. L., Kaminsky, M., & Kaushik, M. (2020). Machine Learning Approaches to Detect Security Vulnerabilities in NoSQL Databases. Proceedings of the IEEE Security and Privacy Conference.
3. Miller, D. D. L., & Bruen, D. K. (2019). Data Privacy and Encryption Techniques for NoSQL Databases. Cybersecurity and Privacy Journal, 5(3).
4. Євдокимов, С. О. (2023). Сучасні системи захисту інформації: [перше видання]. Київ: ФОП Гуляєва В. М. 380 с. ISBN 978-617-7901-89-0.
5. R. Patel, A. Singh, and L. Nair. "Security Enhancement Techniques for NoSQL Databases in Smart Transportation Systems," Journal of Transportation Cybersecurity, vol. 10, no. 1, 2024, pp. 35–48.
6. T. Williams, D. Smith, and A. Taylor. "NoSQL Database Vulnerability Assessments for Real-Time Transport Monitoring," Cybersecurity Advances in Transport Infrastructure, vol. 6, no. 1, 2024, pp. 15–29.
7. B. McCarthy, C. Evans, and P. Johnson. "Artificial Intelligence-Based Vulnerability Detection in NoSQL Databases," International Journal of Data Science and Cybersecurity, vol. 18, no. 2, 2024, pp. 78–92.

УДК 004.932

ПЕРСПЕКТИВИ КОМП'ЮТЕРНОГО ЗОРУ В ЗАДАЧАХ ПІДВОДНОГО МОНІТОРИНГУ

Автор: Іванов В.А., студент, Національний університет кораблебудування імені адмірала Макарова, Миколаїв, Україна

Науковий керівник: Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Вступ.

Розвиток комп'ютерного зору (КЗ) та технологій штучного інтелекту створює нові можливості в автоматизованому аналізі підводних даних, забезпечуючи можливість оперативного реагування на зміни стану об'єктів і навколишнього середовища. Інтеграція комп'ютерного зору з підводними апаратами (ПА) сприяє моніторингу важкодоступних ділянок морських та океанічних просторів.

Невелика частина акваторій України має достатньо велику прозорість. Каламутності в воді зазвичай накладають велике навантаження на роботу оператора, виділення основних компонентів та підказки які можуть надавати системи КЗ можуть значно спростити та підвищити ефективність роботи оператора.

Мета роботи: є аналіз задач, що можуть бути вирішенні впровадженням технології комп'ютерного зору для систем підводного моніторингу.

Основна частина

Комп'ютерний зір дозволяє автоматизувати задачі, що раніше потребували значних ресурсів і людської участі. Система КЗ може бути застосована, як до систем відеофіксації так і до гідроакустичних засобів, що представляють вихідні дані в графічному вигляді.

Серед таких задач, що можуть бути вдосконалені можна виділити наступні:

– моніторинг та діагностика підводних інфраструктурних об'єктів. Комп'ютерний зір дає можливість безперервного нагляду за станом підводних комунікаційних кабелів, трубопроводів, транспортних тунелів тощо. Системи КЗ надають можливість виявлення пошкоджень (наприклад, тріщин чи корозії) по засобами відеофіксації або магнітометричного обстеження та виявлення артефактів в структурі;

– охорона портів та стратегічної інфраструктури. Автоматизовані системи з комп'ютерним зором підвищують рівень безпеки в прибережних зонах, здійснюючи контроль підозрілої активності біля стратегічних об'єктів (портів, нафтоналивних терміналів тощо). Завдяки алгоритмам розпізнавання об'єктів та аналізу поведінки можливе своєчасне виявлення потенційних загроз.

– моніторинг підводного середовища. Використання ПА для екологічного моніторингу дозволяє відстежувати рівень забруднення, зміни у фауні й флорі, а також інші екологічні параметри. Це сприяє кращому розумінню впливу людської діяльності на екосистему і запобіганню екологічним катастрофам.

– вивчення затонулих об'єктів і археологічних артефактів. Завдяки 3D-модельованню та аналізу зображень комп'ютерний зір значно полегшує дослідження затонулих кораблів та історичних об'єктів під водою. Цифрове відтворення дозволяє археологам проводити детальний аналіз без ризику пошкодити ці об'єкти;

– аналіз поведінки морських видів для збереження біорізноманіття. Комп'ютерний зір дає змогу спостерігати за морською фауною, виявляти рідкісні або під загрозою зникнення види та аналізувати їхню поведінку. Це сприяє збереженню видового різноманіття та покращує ефективність природоохоронних програм.

Для підвищення ефективності даних задач КЗ може використовувати наступні інструменти:

– постобробка зображень та підвищення їх якості корегуванням контрастності, яскравості, насиченості кольорів тощо;

– розпізнавання образів – виявлення та ідентифікація об'єктів та аналомалій;

– виділення артефактів – визначення контурів об'єктів для поліпшення виявлення аномалій оператором ПА;

– надання автоматичних підказок для користувача.

Висновок

Використання комп'ютерного зору в підводному моніторингу є ключовим інструментом у забезпеченні точного та своєчасного моніторингу важливих підводних об'єктів, що знижує витрати на

обслуговування та мінімізує ризики, пов'язані з людським фактором. Подальший розвиток технологій комп'ютерного зору та ШІ дозволить вдосконалити методи моніторингу, забезпечуючи підвищену безпеку та надійність глобальної інфраструктури.

Список літератури:

1. Han, J., et al. "Anomaly Detection in Underwater Environments Using Deep Learning Approaches." IEEE Journal of Oceanic Engineering, 2020.
2. Torres, J., et al. "Real-Time Event Processing Architecture for Underwater Networks." Oceanography Systems Journal, 2021.
3. Parker, D., et al. "DLP and Cryptographic Solutions for Underwater Data Transmission." Information Security in Maritime Engineering, 2019.
4. Kim, H., et al. "Deep Learning-Based IDS and IPS for Underwater Networks." Journal of Marine Technology, 2020.
5. Smith, M. A., and Johnson, K. "Advances in Autonomous Underwater Surveillance Systems." Journal of Autonomous Systems in Marine Science, 2019.
6. Yamamoto, N., et al. "Environmental Monitoring with Autonomous Underwater Vehicles." Sensors and Actuators in Marine Science, 2018.
7. Williams, T., and Brown, A. "Network Traffic Analysis in Underwater Wireless Sensor Networks." IEEE Transactions on Wireless Communications, 2019.

УДК 004.056.5

**КРИТЕРІЇ ВИБОРУ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ
ДЛЯ ВОДНОГО ТРАНСПОРТУ**

***Автор:** Тотх М., магістрантка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Зростаюча інтеграція комп'ютерних систем та автоматизації в морському транспорті, хоча й підвищує ефективність та маневреність суден, не навмисно створила складне середовище, чутливе до кібератак. Поширення взаємопов'язаних систем на судах та в портах сильно збільшило площу

атаки, зробивши ці об'єкти першочерговими цілями для зловмисників, і змусило приділяти їм особливу увагу. Зокрема за даними [1]:

– 2022 рік: внаслідок кібератаки програм-вимагачів під назвою LockBit на web-сайт порту web-сайт порту був закритий на кілька днів, викрадені фінансові звіти, контракти, судові журнали та іншу інформація. Атака на дві німецькі нафтові компанії з метою викрадання інтелектуальної власності призвела до значних проблем у галузі доставки та розподілу нафти, компанія Shell змушена була змінити маршрут поставок нафти, що вплинуло на системи завантаження та розвантаження компаній. Міністр внутрішньої безпеки США Александро Майоркас заявив, що кібератаки є найбільшою загрозою для портів США;

– 2023 рік: внаслідок атаки програм-вимагачів на програмну компанію, яка постачає кораблі, її сервери для власної системи ShipManager були вимушено вимкнені, що мало негативний вплив на більше ніж 1000 суден;

– 2024 рік: адміністрація Байдена видала розпорядження про внесення змін, спрямованих на посилення безпеки, зокрема кібербезпеки, у портах США.

Сучасні системи навігації сильно залежать від супутникових технологій, які можуть бути скомпрометовані, що призводить до неточностей навігації та загрожує безпеці мореплавства. Крім того, широке впровадження електронних систем для управління вантажами, контролю руху суден та інших портових операцій піддає ці критично важливі інфраструктури кіберзагрозам, що може призвести до порушення роботи та компрометації безпеки.

Системи виявлення вторгнень (СВВ) є одним із сучасних засобів забезпечення кібербезпеки сучасних інформаційно-комунікаційних систем і можуть застосовуватися в різних галузях діяльності, зокрема у сфері водного транспорту. Дослідженню специфіки і перспектив їх застосування на водному транспорті присвячено роботи багатьох фахівців [2-6], однак, на даний час методики вибору СВВ для критичної морської інформаційної інфраструктури відсутні.

Метою даної роботи є визначення критеріїв вибору систем виявлення вторгнень для водного транспорту.

Для досягнення даної мети необхідно вирішити наступні задачі:

- провести комплексний аналіз сучасних проблем застосування СВВ у морському середовищі;
- визначити унікальні компоненти СВВ, адаптовані для морського транспорту;
- визначити критерії і оцінити за ними продуктивність та придатність сучасних СВВ для морських застосувань.

При виборі СВВ для застосування у галузі водного транспорту необхідно враховувати їх здатність виявляти кібератаки на морі, здійснювані найчастіше застосовуваними зловмисниками способами, такими як [1]:

- фішинг, що спрямовується на велику кількість людей з метою отримання хоча б однієї відповіді, яка дозволить отримати доступ до атакваної системи або інформаційних ресурсів;
- шкідливе програмне забезпечення, яке часто надсилається через посилення в електронних листах і застосовується зловмисниками для порушення функціонування системи, що є об'єктом атаки, до того, як власники чи оператори ідентифікують загрозу, або для отримання інформації про об'єкт атаки, яка може бути використана для атак в майбутньому чи сама по собі становить цінність для зловмисників;
- маніпуляція паролем, що здійснюється зловмисником за допомогою програмного забезпечення для систематичного вгадування паролів, щоб отримати несанкціонований доступ;
- соціальна інженерія, яка не є високотехнологічним способом організації кібератак і передбачає проведення прямих чи віртуальних розмов з особами, що володіють необхідною зловмиснику інформацією, при чому зловмисник може видавати себе за іншу особу або хибно посилятися на відому об'єкту атаки особу для отримання інформації.

При виборі СВВ витрати на їх придбання чи розробку, встановлення і експлуатацію не повинні перевищувати очікувані потенційні втрати внаслідок відсутності СВВ. Як наслідки кібератак у морській галузі можуть розглядатися збитки в короткостроковій і довгостроковій перспективі внаслідок збоїв у роботі суднового і портового обладнання:

- порушення судноплавства та роботи портів;
- порушення логістичних ланцюгів, пов'язаних із пасажирськими і грузовими перевезеннями, портами, річковим і морським транспортом;

- порушення інтересів стейкхолдерів;
- порушення безпеки судноплавства;
- порушення екологічної безпеки;
- порушення функціонування систем зв'язку та навігації на судах;
- викрадання і втрати вантажу;
- ускладнення геополітичних відносин;
- репутаційні збитки тощо.

Ці атаки можуть завдати шкоди окремим працівникам на судах і в портах, які можуть втратити дохід та роботу, тобто кібератаки здійснюватимуть негативний вплив на соціум. Збої в роботі систем безпеки, навігації та зв'язку можуть призвести до аварій на судах і в портах, які можуть спричинити травмування чи загибель персоналу та пасажирів.

Захист морської інформаційної інфраструктури, що включає бази даних, системи відстеження вантажів та електронні системи безпеки, є надзвичайно важливим. Охорона баз даних, які містять критично важливі дані про судна, вантажі, екіпаж та операції, є необхідною. Впровадження надійних заходів автентифікації, авторизації та шифрування є вирішальним. Системи відстеження вантажів повинні бути захищені від несанкціонованого доступу та маніпуляцій, щоб забезпечити цілісність та точність даних. Крім того, системи безпеки, такі як контроль доступу та відеоспостереження, повинні бути захищені від кібератак.

Морські СВВ значно відрізняються від тих, що використовуються в традиційних офісних середовищах. Морська СВВ є складною системою, розробленою для виявлення та моніторингу потенційних вторгнень або загроз морській безпеці. Ці системи можуть застосовуватися на судах та в портах [7-10] і включати:

- радары та системи відеоспостереження для моніторингу оточення судна в реальному часі;
- автоматизовані системи ідентифікації для відстеження руху суден та їх ідентичності;
- біометричні системи ідентифікації для систем контролю доступу на основі розпізнавання облич та інших біометричних даних для підвищення безпеки за рахунок використання багатофакторної ідентифікації;

- системи виявлення аномалій для ідентифікації відхилень від шаблонів нормальної поведінки мереж, суден, суднового та портового обладнання і виявлення потенційних загроз.

- системи глобального позиціонування для відстеження суден та вантажів в реальному часі і перевірки їх місцезнаходження.

- системи виявлення надзвичайних ситуацій та реагування для оперативного реагування на інциденти різного типу, в тому числі – на інциденти інформаційної безпеки.

Інтегровані морські СВВ поєднують різні технічні та програмні рішення для забезпечення комплексної безпеки суден, вантажів, екіпажів та пасажирів. Ці системи дозволяють обробляти ризики, асоційовані із широким спектром загроз, включаючи вторгнення, тероризм, піратство, аварії та інші небезпеки.

Вибір СВВ можна здійснити за множиною критеріїв, які для різних середовищ функціонування СВВ можуть мати різну вагу і поділяються за сутністю на функціональні, експлуатаційні, ресурсні та якісні критерії. До функціональних критеріїв, наприклад, можна віднести:

- здатність СВВ розпізнавати певні класи кібератак, зокрема атаки «0-day», і кількість цих класів;

- доступні методи виявлення атак;

- наявність шаблонів «нормальної» поведінки системи;

- здатність СВВ реагувати на кібератаку певним чином;

- здатність СВВ працювати в режимі реального часу (і параметри, що характеризують цю здатність) та у багатопоточному режимі;

- рівні застосовуваності СВВ (і їх кількість) за моделлю OSI та за мережевою архітектурою, область захисту;

- підтримувані СВВ операційні системи та протоколи (типи і кількість);

- здатність СВВ взаємодіяти з іншим програмним забезпеченням (типи і кількість);

- тип управління СВВ;

- відкритість коду.

Експлуатаційні критерії вибору СВВ характеризують її захищеність, масштабованість, адаптовність, здатність обробляти певний обсяг інформації.

До підмножини ресурсних критеріїв вибору СВВ відносяться:

- умови розповсюдження СВВ і її вартість;
- наявність документації і підтримки розробника при налаштуванні та експлуатації СВВ;
- наявність персоналу з достатнім рівнем кваліфікації;
- витрати часу і коштів на навчання персоналу;
- витрати часу і коштів на встановлення, налаштування та експлуатацію СВВ;
- необхідний обсяг пам'яті і вимоги до середовища функціонування СВВ.

Якісні критерії вибору СВВ включають кількість використовуваних сигнатур і шаблонів; показники ефективності виявлення атак та ефективності протидії атакам певного типу; оцінки зручності оновлення сигнатур і шаблонів нормального стану, зручності інтерфейсу і використання СВВ; здатність адаптувати налаштування під вимоги користувача.

За наведеними вище критеріями можна оцінювати продуктивність та придатність сучасних СВВ для морських застосувань. Загалом, СВВ для водного транспорту суттєво відрізняються від аналогічних систем, застосовуваних в офісних умовах. Оскільки водний транспорт має специфічні загрози, такі як піратство, тероризм, аварії та природні лиха, системи безпеки тут повинні бути адаптовані до відповідних ризиків. Відповідні ключові компоненти морської інформаційної інфраструктури мають захищатися СВВ. Наприклад, проведений в [6] аналіз показав, що система Naval Dome [11], пропонує цілісний підхід до кібербезпеки у сфері морського транспорту, захищаючи окремі компоненти та створюючи кібербезпечне середовище. Ця багаторівнева стратегія захисту ускладнює зловмисникам компрометацію системи, оскільки їм потрібно проникнути через кілька рівнів захисту. Основні компоненти, які Naval Dome може контролювати та захищати, включають системи управління судном, системи зв'язку, захист від піратства, системи управління кризовими ситуаціями та багато інших.

За критеріями адаптовності, швидкості реагування, здатністю виявляти атаки невідомих типів слід визнати перспективними інтелектуальні СВВ, що використовують машинне навчання [12, 13].

Висновки. В даній роботі на основі інформації з відкритих джерел проведено комплексний аналіз сучасних проблем застосування СВВ у морському середовищі; визначені унікальні компоненти СВВ, адаптовані для морського транспорту, критерії оцінювання СВВ та оцінки сучасних СВВ за критеріями продуктивності та придатності для застосування в морській галузі.

Список літератури:

1. Maritime Cybersecurity. URL: <https://www.maritimeinjurycenter.com/accidents-and-injuries/cybersecurity/>
2. Ibokette A. I., Ogundare T. O., Anyebe A. P., Odeh I. I., Okafor, F. C. Mitigating Maritime Cybersecurity Risks Using AI-Based Intrusion Detection Systems and Network Automation During Extreme Environmental Conditions. International Journal of Scientific Research and Modern Technology, 3(10). URL: <https://doi.org/10.38124/ijsrmt.v3i10.73>
3. Farah M.-A.-B., Ukwandu E., Hindy H., Brosset D., Bures M., Andonovic I., Bellekens X. Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. Information. 2022. No.13(1). URL: <https://doi.org/10.3390/info13010022>. URL: https://www.researchgate.net/publication/357654089_Cyber_Security_in_the_Maritime_Industry_A_Systematic_Survey_of_Recent_Advances_and_Future_Trends
4. Li M., Zhou J., Chattopadhyay S., Goh M. Maritime Cybersecurity: A Comprehensive Review. IEEE Transactions on intelligent transportation systems. 2024 URL: <https://arxiv.org/pdf/2409.11417>
5. Smith, J. Cybersecurity in Maritime Transportation: Challenges and Solutions. Journal of Maritime Security. 2018. №10(2). P.145-162. URL: <https://www.mdpi.com/2673-8732/2/1/9>
6. Тотх М. Системи виявлення вторгнень для водного транспорту як основний метод захисту. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК. 2023. С.43-46. URL: <https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf>
7. IACS UR E22 Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e22_rev.3_june_2023_ul.pdf
8. IACS UR E26 Cyber resilience of ships URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf

9. IACS UR E27 Cyber resilience of on-board systems and equipment. URL: <https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103854/UR-E27-Rev.1-Sep-2023-UL.pdf>

10. IAPH Cybersecurity Guidelines for Ports and Port Facilities. URL: https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf

11. Naval Dome. URL: <https://navaldome.com/index.html>

12. Anomaly-Based Intrusion Detection Systems Using Machine Learning. Journal of Cybersecurity and Information Management. 2024. Vol. 14. No. 01. PP. 20-33. URL: <https://americaspg.com/article/pdf/2836>

13. Стефанюк Ю.В. Інтелектуальні засоби в системах виявлення та запобігання вторгнень. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК. 2023. С.129-133. URL: <https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf>

УДК 004.056.5

ЗВАЖЕНЕ ОЦІНЮВАННЯ КРИТИЧНОСТІ ОБ'ЄКТІВ МОРСЬКОГО ТА РІЧКОВОГО ТРАНСПОРТУ

***Автор:** Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Морський та річковий транспорт є підсектором сектору «Транспорт і пошта», критичної інфраструктури (КІ) України, що підпорядковується Мінінфраструктури. Кібербезпеці об'єктів КІ (ОКІ) і об'єктів критичної інформаційної інфраструктури (ОКІІ) приділяється особлива увага як на міжнародному, так і на національному рівнях, оскільки ці об'єкти надають послуги, що є життєво важливими для населення та держави, а часто – і для інших держав.

Наприклад, у червні 2024 року Норвегія, Фінляндія та Швеція прийняли рішення про створення військово-транспортного коридору крізь північні території цих країн, який сприятиме швидкому переміщенню персоналу та матеріалів із портів Норвегії через Швецію до Фінляндії [1].

Зерновим коридором, який був запущений у липні 2022 року, з України експортували щонайменше 33 мільйонів тонн зерна, а після того як Росія вийшла з угоди у 2023 році, Україна у серпні 2023 року оголосила створення "гуманітарного коридору", щоб продовжувати постачання продовольства до африканських та азійських ринків [2]. Перша заступниця голови транспортного комітету ВРУ про Чорне море Юлія Клименко в своєму інтерв'ю [3] зазначила, що «Морська економіка і морська безпека мають розвиватися паралельно», оскільки блокада українських портів Росією є економічною блокадою, що має на меті подолання України як конкурента на міжнародних ринках і «не має нічого спільного з військовими діями». Однак, саме витискання російського флоту з Чорного моря дозволило Україні у 2024 році відправити морським коридором 66 мільйонів тонн вантажів і вийти на довоєнний рівень експорту 2021 року [2]. На даний час «свобода навігації ... досягається виключно озброєнням нашого військово-морського флоту, коли ми можемо захистити наші порти, пробити собі морські коридори, ні у кого не питаючи дозволу, а виключно на основі міжнародного права» [3].

Таким чином, безпека річкового і морського транспорту є складовою національної економічної безпеки, а Стратегія розвитку водного транспорту має передбачати різні типи заходів, які дозволять відстояти інтереси України. Передумовою впровадження різних заходів і засобів захисту на ОКІ є визначення їх категорії критичності. Категоризація ОКІ проводиться згідно Закону України «Про критичну інфраструктуру» [4] і «Загальних вимоги до кіберзахисту об'єктів КІ» [5] за затвердженою методикою [6, 7]. Розв'язку комплексної проблеми захисту КІ проблеми присвячені роботи багатьох науковців та практиків, документи міжнародних організацій [8-13] тощо, однак на даний час методика визначення категорії [7] ОКІ базується на чітких бальних оцінках, що може привести до похибок категоризації.

Метою даної роботи є розробка пропозицій до удосконалення процедур категоризації об'єктів критичної інфраструктури.

Для досягнення поставленої мети необхідно провести аналіз нормативно-правової бази категоризації, визначити наявні недоліки методики категоризації і розробити пропозиції до її удосконалення.

При оцінюванні критичності ОКІ за методикою, затвердженою постановою Кабінету міністрів України [6], і методичними вказівками,

затвердженими Наказом Адміністрації ДССЗЗІ [7], віднесення ОКІ до певної категорії критичності здійснюється на підставі належності показника нормованої оцінки рівня критичності ОКІ PK_{OKI} до певного інтервалу значень. Показник PK_{OKI} визначається як доля максимально можливого значення $\Sigma PK_{\max}$ для конкретного ОКІ і обчислюється як відношення суми оцінок ОКІ за секторальними і між секторальними критеріями ΣPK_i до $\Sigma PK_{\max}$.

Оцінка за кожним критерієм PK_i згідно [7] визначається експертом як чітке число, хоча для окремих критеріїв підставою для визначення оцінок є належність певного кількісного показника до певного числового діапазону, що за змістом відповідає носію нечіткої множини. Крім того, експерт може не бути впевнений на 100% у належності кількісного показника певного між секторального критерію до конкретного інтервалу. Наприклад, експерт з $\mu_1=0,8$ може відносити значення певного показника до інтервалу 1, а з мірою впевненості $\mu_2=0,2$ – до інтервалу 2. Тоді зважена оцінка за цим показником дорівнюватиме: $\mu_1 \cdot 1 + \mu_2 \cdot 2 = 0,8 \cdot 1 + 0,2 \cdot 2 = 1,2$. Відповідно, різниця зваженої оцінки і чіткої оцінки становитиме 0,2, якщо експерт вибрав інтервал 1, і 0,8, якщо експерт вибрав інтервал 2. Такі похибки накопичуватимуться від одного показника до іншого. Оскільки максимально можливого значення є константою для певного ОКІ, то накопичені похибки безпосередньо вплинуть на значення, і відповідно на присвоюваний ОКІ рівень критичності.

Оцінка критичності ОКІ за секторальними критеріями визначається для кожного підсектору залежно від наслідків порушення надання послуг цим підсектором і отримується за 1 або 2 показниками, визначеними [7] окремо для кожного підсектору.

Наприклад, для підсектору річкового та морського транспорту знищення, пошкодження або порушення функціонування ОКІ може привести до катастрофічних наслідків (припинення надання морських послуг у морських портах більш як на 72 години, оцінка 4 бали), критичних наслідків (припинення надання морських послуг у морських портах від 24 до 72 годин, оцінка 3 бали), значних наслідків (припинення надання морських послуг у морських портах до 24 годин, 2 бали). Незначні

наслідки в цьому підсекторі не оцінюються. Таким чином, оцінка у підсекторі морського та річного транспорту здійснюється за одним секторальним критерієм з показником «тривалість припинення надання морських послуг у морських портах», визначеним на вісі часу.

Для інформаційного сектору наслідки порушення надання основних послуг ОКІ в разі його знищення, пошкодження або порушення функціонування оцінюються за двома секторальними критеріями, з показниками «час відновлення функціонування у штатному режимі» і «кількість жителів». Оцінки надаються катастрофічним (4 бали), критичним (3 бали), значним (2 бали) і незначним (1 бал) наслідкам.

Таким чином, зважена оцінка за секторальними критеріями може розраховуватися як $\sum_{j=1}^2 \sum_{i=1}^4 i \mu_{ij}$, де $\sum_{i=1}^4 \mu_{ij} = 1$; $i = \overline{1, 4}$ – номер оцінки, що відповідає кількості балів; $j = \overline{1, 2}$ – номер показника. За методикою [7]

оцінка за секторальними критеріями дорівнюватиме $\sum_{j=1}^2 PK_j$, де $PK_j \in \{1, 2, 3, 4\}$. Різниця між чіткими і нечіткими оцінками ОКІ певного підсектору в загальному випадку становитиме

$$\Delta = \sum_{j=1}^2 \sum_{i=1}^4 i \mu_{ij} - \sum_{j=1}^2 PK_j = \sum_{j=1}^2 \left(\sum_{i=1}^4 i \mu_{ij} - PK_j \right).$$
 Якщо критичність підсектору оцінюється тільки за одним показником, то $\mu_{i2}=0, PK_2=0$.

Прийmemo, що конкуруючими є тільки сусідні терми оцінок [14]. Тоді

- для незначних наслідків

$$\Delta = \sum_{j=1}^2 (\mu_{1j} + 2\mu_{2j} - 1) = \sum_{j=1}^2 (\mu_{1j} + 2(1 - \mu_{1j}) - 1) = \sum_{j=1}^2 (1 - \mu_{1j});$$

- для катастрофічних наслідків

$$\Delta = \sum_{j=1}^2 (4\mu_{4j} + 3\mu_{3j} - 4) = \sum_{j=1}^2 (4\mu_{4j} + 3(1 - \mu_{4j}) - 4) = \sum_{j=1}^2 (\mu_{4j} - 1);$$

- для критичних наслідків

$$\Delta = \sum_{j=1}^2 \left((4\mu_{4j} + 3\mu_{3j} + 2\mu_{2j}) - 3 \right) = \sum_{j=1}^2 \left((4\mu_{4j} + 3(1 - \mu_{4j}) + 2\mu_{2j}) - 3 \right) = \\ = \sum_{j=1}^2 (\mu_{4j} + 2\mu_{2j});$$

– для значних наслідків

$$\Delta = \sum_{j=1}^2 \left((3\mu_{3j} + 2\mu_{2j} + \mu_{1j}) - 2 \right) = \sum_{j=1}^2 \left((3\mu_{3j} + 2(1 - \mu_{3j}) + \mu_{1j}) - 2 \right) = \\ = \sum_{j=1}^2 (\mu_{3j} + \mu_{1j}).$$

Аналогічно можна визначити різниці між чіткими і нечіткими оцінками ОКІ за міжсекторальними критеріями, для яких оцінки отримуються за 16-ма показниками. Якщо міра впевненості експерта в оцінці кожного показника є досить високою, припустимо 90%, а на інші оцінки припадає лише 10%, то накопичена похибка за секторальними і міжсекторальними критеріями для водного транспорту становитиме 1,7 бали, а нормована оцінка рівня критичності ОКІ буде відрізнятися на 2,5%, що може вплинути на рішення щодо категорії критичності ОКІ. Якщо середня міра впевненості експерта в оцінках буде гранично низькою – 60%, то накопичена похибка становитиме 6,8 балів, що змінить оцінку рівня критичності ОКІ на 10%.

Таким чином, недоліком наявної методики є потенційна наявність похибок внаслідок недостатньої впевненості експертів при оцінюванні критичності наслідків порушення надання ОКІ основних функцій. Для усунення цього недоліку рекомендується модифікувати методику [7], додавши до експертних оцінок міру впевненості експертів у цих оцінках. Необхідність застосування модифікованої методики можна визначити шляхом оцінки впливу граничних величин накопиченої похибки на рішення щодо категоризації ОКІ.

Крім того, для морського і річкового транспорту в секторальних критеріях враховується тільки припинення надання морських послуг у морських портах, хоча порушення надання послуг річковими портами

також може мати масштабні наслідки. Внаслідок того, що склад стейкхолдерів в портах постійно змінюється, доцільно переглядати рівень критичності портів кожного разу при плануванні через них масштабних поставок і перевезень небезпечних чи цінних (з точки зору договірних зобов'язань) вантажів.

Висновки

В даній роботі проведено аналіз нормативно-правової бази категоризації, визначені недоліки методики категоризації і розробити пропозиції щодо її удосконалення.

Список літератури:

1. Норвегія, Фінляндія та Швеція створять транскордонний військово-транспортний коридор. URL: <https://suspilne.media/773079-norvegia-finlandia-ta-svecia-stvorat-transkordonnij-vijskovo-transportnij-koridor/>

2. Шмигаль: у 2024 році морським коридором Україна експортувала 66 мільйонів тонн вантажів. URL: <https://suspilne.media/833077-smigal-u-2024-roci-morskim-koridorom-ukraina-eksportovala-66-miljoniv-tonn-vantaziv/>

3. Морська економіка і морська безпека мають розвиватися паралельно – інтерв'ю з Юлією Клименко. URL: https://cfts.org.ua/articles/morska_ekonomika_i_morska_bezpeka_mayut_rozvivatisya_paralelno_intervyu_z_yulieyu_klimenko_1990/137899

4. Закон України "Про критичну інфраструктуру". URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

5. Загальні вимоги до кіберзахисту об'єктів КІ, затверджені постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8>

6. Методика категоризації об'єктів КІ, затверджена Постановою Кабінету міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури» від 9 жовтня 2020 р. №1109. URL: <https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#Text>

7. Наказ № 23 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів КІ». URL: <https://zakon.rada.gov.ua/rada/show/v0023519-21#Text>

8. Cybersecurity in Maritime Critical Infrastructure. Reflection on African Ports. Critical Maritime Routes Programme Monitoring, Support and Evaluation Mechanism (CRIMSON III). (2023) URL: <https://rusieurope.eu/wp-content/uploads/2024/02/cybersecurity-in-maritime-critical-infrastructure-crimson-report-english.pdf>

9. Osei-Kyei R. et al. Critical review of the threats affecting the building of critical infrastructure resilience. International Journal of Disaster Risk Reduction. 60 (2021): 102316.

10. Tadas L. et al. Cyber security management model for critical infrastructure. International Journal Entrepreneurship and Sustainability. Issues ISSN 2345-0282 (online). URL: <http://jssidoi.org/jesi/> 2017 Volume 4 Number 4 (June) [http://doi.org/10.9770/jesi.2017.4.4\(12\)](http://doi.org/10.9770/jesi.2017.4.4(12))

11. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. К.ДУТ, 2015. 288 с. URL: http://www.dut.edu.ua/uploads/p_303_79299367.pdf

12. Рогов П.Д., Ворович Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері. Зб. наук. праць Центру воєнно-стратегічних досліджень Нац-го ун-ту оборони України ім. Івана Черняховського. 2017. № 1. С. 64-72. URL: <http://znpcvsd.nuou.org.ua/article/view/125525>

13. Салієва О.В., Яремчук Ю.Є. Визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури ранжуванням загроз. Реєстрація, зберігання і обробка даних. 2020. Т. 22. № 2. С.63-76. URL: <http://drsp.ipri.kiev.ua/article/view/211279>

14. Турти М.В. Теорія однозначних нечітких систем і нейронні мережі. Монографія. В 2-х част. – М.: Миколаївська філія Європейського університету, 2007. – Ч.1. – 140 с.

УДК 004.056.5

КРИТЕРІЇ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ В МОРСЬКІЙ ГАЛУЗІ

***Автор:** Турти М.Ю., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

У сучасному цифровому світі розвиток морської галузі тісно пов'язаний із впровадженням новітніх цифрових технологій, і, відповідно, успішність функціонування водного транспорту суттєво залежить від здатності критичної морської інформаційної інфраструктури протистояти кіберзагрозам.

Дослідженням практичних і теоретичних аспектів кібербезпеки на морі присвячені праці багатьох українських [1-4] та іноземних [5-11] фахівців, зокрема фахівців Національного університету кораблебудування [1, 3]. Однак, на даний час відсутні затверджені методики управління кіберризиками для критичної морської інформаційної інфраструктури (КМІІ) України.

Метою даної роботи є визначення критеріїв прийняття рішень щодо забезпечення кіберстійкості в морській галузі.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- визначити особливості забезпечення кіберстійкості в морській галузі;
- визначити особливості прийняття рішень в морській галузі;
- сформулювати перелік критеріїв прийняття рішень щодо забезпечення кіберстійкості в морській галузі і визначити принципи їх вибору для вирішення конкретних прикладних задач.

Визначення загального поняття «кіберстійкість» (англ. *Cyber resilience*) наводиться в Стратегії кібербезпеки України [12], згідно з якою кіберстійкість характеризується як здатність:

- до швидкої адаптації до внутрішніх і зовнішніх кіберзагроз;
- до підтримки сталого функціонування національної інформаційної інфраструктури;

– до відновлення сталого функціонування національної інформаційної інфраструктури після кіберінцидентів.

Стратегія кібербезпеки України першочерговою задачею називає забезпечення кіберстійкості об'єктів критичної інформаційної інфраструктури (ОКІ), до якої відносяться і об'єкти КМІ. Кіберстійкість має забезпечуватися на всіх рівнях при взаємодії всіх суб'єктів забезпечення кібербезпеки.

Кожна галузь критичної інфраструктури (КІ) і кожен об'єкт КІ (ОКІ) характеризуються виконанням специфічних функцій, наслідки неналежного виконання котрих визначають категорію критичності ОКІ. Тому для кожної галузі КІ поняття кіберстійкості пов'язане із такими функціями. Наприклад, кіберстійкість інформаційної інфраструктури банку – із бізнес-процесами, продуктом яких є банківські та фінансові послуги [13], а кіберстійкість в морській галузі – з операційними технологіями, які використовуються для безпечної експлуатації суден, порушення котрих може призвести до порушення безпеки людей, судна та/або навколишнього середовища [6].

За ступенем впливу на безпеку людини, безпеку судна та навколишнього середовища в Рекомендаціях щодо кіберстійкості [6], розроблених Міжнародною асоціацією класифікаційних товариств у 2020 році (остання редакція – 2022 рік, очікується редакція 2024 року) виділяють (із посиланням на UR E22 IACS, які були розроблені у 2006 році, остання редакція – 2023 рік [7]) системи трьох категорій:

- категорія I – системи, вихід з ладу яких не призведе до небезпечних ситуацій;
- категорія II – системи, вихід з ладу яких міг би призвести до небезпечних ситуацій;
- категорія III – системи, вихід з ладу яких може негайно призвести до небезпечних ситуацій.

Згідно Закону України «Про критичну інфраструктуру» [14] встановлюються 4 категорії критичності ОКІ, які визначаються за ступенем тяжкості наслідків порушення функціонування ОКІ:

- I категорія критичності – виникає кризова ситуація державного значення;

- II категорія критичності – виникає кризова ситуація регіонального значення;
- III категорія критичності – виникає кризова ситуація місцевого значення;
- IV категорія критичності – виникає кризова ситуація локального значення.

Таким чином, поняття «категорія системи» за UR E22 IACS «Computer-based systems» і поняття «категорія критичності» [7] ОКІ і, відповідно, ОКП за Законом України «Про критичну інфраструктуру» [14] та Методикою категоризації об'єктів критичної інфраструктури [15] не є ідентичними.

Особливості прийняття рішень в морській галузі зумовлені необхідністю узгоджувати інтереси багатьох стейкхолдерів (вантажодержавців і вантажовідправників, страхувальників суден і морських агентів, судновласників і екіпажів, портів і постачальників послуг, берегової охорони і лоцманів, докерів і логістичних компаній тощо), пов'язаних із багатьма бізнес-процесами, наслідки порушення котрих асоціюються із різними ризиками. Крім того, вибір процедур обробки цих ризиків має здійснюватися з врахуванням не тільки вітчизняного законодавства, а й з врахуванням міжнародних нормативних актів, вимог наявних договорів і законодавчих вимог інших країн (найчастіше для морських перевезень).

Крім того, кіберстійкість має визначатися на різних рівнях за різними документами:

- для портів і портових споруд – згідно IAPH Cybersecurity Guidelines for Ports and Port Facilities [10];
- для суден – згідно IACS UR E26 Cyber resilience of ships [8];
- для бортових систем – згідно IACS UR E27 Cyber resilience of on-board systems and equipment [9].

Перелічені вище документи мають рекомендаційний характер (однак з липня 2024 року їм мають відповідати всі нові судна) і не застосовуються до комп'ютерних систем, вимоги до яких визначені на законодавчому рівні. Наприклад, Частина X «Комп'ютерні системи» з «Rules for the survey and construction of steel ships» визначає вимоги до проектування, конструювання, тестування та технічного обслуговування комп'ютерних систем, які підпадають під класифікаційні вимоги,

включаючи апаратне та програмне забезпечення, яке становить такі системи, однак не поширюється на навігаційне обладнання, зазначене в Правилах техніки безпеки, радіоустановки, зазначені в Правилах радіоустановок тощо [11]. Крім того, для вирішення проблем, пов'язаних із забезпеченням відповідності новим вимогам з кібербезпеки невеликих і нетрадиційних суден, сфера застосування UR E27 та UR E26 може бути класифікована як обов'язкова та необов'язкова відповідність залежно від типів і розмірів суден.

Слід враховувати також, що на даний час у міжнародному морському праві існують певні прогалини стосовно регулювання питань кібербезпеки, і на думку багатьох дослідників [2] актуальним є прийняття універсального міжнародного договору з кібербезпеки у морській галузі.

Таким чином, прийняття рішень стосовно кіберстійкості морської інфраструктури має здійснюватися поетапно – починаючи з ознайомлення всіх зацікавлених сторін із наявними нормативними вимогами і рекомендаціями та узгодження складу базової документації до визначення кількісних значень і обробки ризиків, асоційованих із різними стейкхолдерами, країнами, інформаційними ресурсами, загрозами, порушеннями властивостей захищеної інформації, критичними інфраструктурами, ОКІ та ОКП різних категорій критичності (як за законодавством України так і за рекомендаціями Міжнародної асоціації класифікаційних товариств). При цьому мають розглядатися ризики для портів і портівих споруд, бортових систем і судна в цілому та інтегральні ризики для морської інфраструктури з врахуванням міжнародних зв'язків.

В якості критеріїв оцінювання кіберстійкості можуть бути використані:

- для оцінювання швидкості адаптації до внутрішніх і зовнішніх кіберзагроз – час між виявленням нового типу загроз чи сценаріїв атак і впровадженням засобів протидії;
- для оцінювання сталості функціонування ОКІ, ОКП та морської інформаційної інфраструктури в цілому – співвідношення успішних/неуспішних атак до загальної кількості виявлених атак і тренди у цих співвідношеннях, рівні і тренди у ризиках, рівні і тренди у втратах внаслідок кіберінцидентів;

– для оцінювання здатності відновлення сталого функціонування після кіберінцидентів – час відновлення, витрати на відновлення, співвідношення показників якості функціонування та ризиків до кіберінцидентів і після відновлення, ймовірність успішного відновлення.

Вибір критеріїв оцінювання кіберстійкості для вирішення конкретних прикладних задач має здійснюватися за зваженою експертною оцінкою. При цьому вважається доцільним формувати декілька груп експертів, які оцінюватимуть кіберстійкість на різних рівнях (бортові системи, судно, порт, морська критична інформаційна інфраструктура, галузь в цілому). Вагові коефіцієнти експертів при цьому мають залежати від їх кваліфікації в конкретній галузі діяльності і можуть визначатися взаємною оцінкою.

Висновки. В даній роботі на основі аналізу відкритих інформаційних джерел визначені особливості забезпечення кіберстійкості та прийняття рішень в морській галузі, сформовано перелік критеріїв прийняття рішень щодо забезпечення кіберстійкості в морській галузі і визначити принципи їх вибору для вирішення конкретних прикладних задач.

Список літератури:

1. Баронова О., Турти М., Ганчо С. Визначення рівня впливу кіберзагроз на розвиток морської галузі // Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ICT-2020». – Харків: ХНУРЕ, 2020. – С.275-278.

2. Веремчук В.С. Міжнародно-правове регулювання кібербезпеки у морській галузі: сучасний стан та перспективи розвитку // Вісник Одеського Національного ун-ту. Серія: Правознавство. – 2024. – Т.26. – Випуск 1(38). – С.112-117. <https://journals.visnyk-onu.od.ua/index.php/law/article/view/472/462>

3. Зубков А.П. Критерії прийняття рішень щодо обробки ризиків об'єктів морської інфраструктури // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2023. – С.175-181. URL: <https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf>

4. Трофименко А.О., Майданевич С.Б., Войченко Т.О., Дорофєєва З.Я. Деякі проблемні питання впровадження стандартів кібербезпеки на морському транспорті. Водний транспорт. No.1 (37). 2023. С. 179–188. URL: <https://vt.duit.in.ua/index.php/home/article/view/267/224>

5. Juan Ignacio Alcaide, Ruth Garcia Llave. Critical infrastructures cybersecurity and the maritime sector. Trans- portation Research Procedia. 2020. Volume 45. Pages 547–554. URL: <https://www.sciencedirect.com/science/article/pii/S2352146520302209>

6. Recommendation on Cyber Resilience No. 166. URL: <https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/24150438/rec-166-corr2-apr-2022-ul.pdf>

7. IACS E22. Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e22_rev.3_june_2023_ul.pdf

8. IACS UR E26 Cyber resilience of ships. URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf

9. IACS UR E27 Cyber resilience of on-board systems and equipment. URL: <https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103854/UR-E27-Rev.1-Sep-2023-UL.pdf>

10. IAPH Cybersecurity Guidelines for Ports and Port Facilities. URL: https://sustainable worldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf

11. Rules for the survey and construction of steel ships. Part X. Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/rules/465_part_x_e_202406.pdf

12. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука безпечного розвитку країни. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n7>.

13. Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг Постанова № 4 Правління Національного банку України від 16.01.2021 URL: <https://zakon.rada.gov.ua/laws/show/v0004500-21#Text>

14. Закон України "Про критичну інфраструктуру". URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

15. Наказ № 23 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів КІ». URL: <https://zakon.rada.gov.ua/rada/show/v0023519-21#Text>

**СЕКЦІЯ 2. ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ
ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА В ІНФОРМАЦІЙНО-
ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ**

УДК 004.4

**СИСТЕМА АНАЛІЗУ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У
БЕЗДРОТОВИХ МЕРЕЖАХ**

Автор: Бердніков В.В., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Козирев С.С., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Вступ. У сучасному цифровому світі бездротові мережі стали невід'ємною частиною повсякденного життя, особливо в домашньому та малому бізнес-середовищах. Проте розвиток технологій супроводжується зростанням кількості кібератак, які стають дедалі складнішими. Недостатній рівень безпеки може призводити до втрати конфіденційних даних, перехоплення трафіку або несанкціонованого доступу до ресурсів мережі. Це особливо критично для домашніх користувачів, які рідко налаштовують мережі правильно. У цій роботі було проаналізовано сучасні методи забезпечення безпеки бездротових мереж, їх уразливості та розроблено інструмент для оцінки рівня безпеки таких мереж.

Мета роботи. Аналіз сучасних методів забезпечення безпеки у бездротових мережах, виявлення їх вразливостей та розробка програми, яка допоможе користувачам оцінити рівень захисту своєї мережі.

Основна частина.

Безпека бездротових мереж базується на використанні сучасних протоколів, методів шифрування та автентифікації. У цій роботі розглянуто найбільш поширені загрози, проаналізовано їхній вплив на домашні та невеликі мережі, а також досліджено ефективність існуючих методів захисту.

Аналіз типових загроз

Робота приділяє увагу найбільш поширеним атакам:

- KRACK (Key Reinstallation Attacks): ця атака використовує уразливості протоколу WPA2, дозволяючи зловмиснику перехоплювати та

повторно використовувати ключі шифрування. Це може призводити до дешифрування трафіку, зміни даних або навіть викрадення сесій.

- Evil Twin (Злий двійник): зловмисники створюють фальшиву точку доступу, яка імітує легітимну мережу. Користувач підключається до цієї точки, і його дані перехоплюються. Особливо небезпечна ця атака для відкритих Wi-Fi мереж.

- Man-in-the-Middle (MiTM): ця атака передбачає перехоплення трафіку між користувачем і точкою доступу. Зловмисник може змінювати дані, перехоплювати паролі або навіть вводити шкідливі пакети у з'єднання.

- атаки на IoT-пристрої: розумні пристрої (камери, датчики, смарт-розетки) часто мають слабкі паролі за замовчуванням та застаріле програмне забезпечення, що відкриває шлях для атак.

Методи забезпечення безпеки

У роботі проведено аналіз сучасних методів захисту:

- протоколи WPA2 та WPA3: WPA2 залишається популярним, але його уразливість до атак, таких як KRACK, викликає занепокоєння. WPA3 впроваджує більш сучасний механізм аутентифікації – Simultaneous Authentication of Equals (SAE), який забезпечує стійкість до атак словниковим методом.

- методи шифрування: найбільш поширеним методом є AES (Advanced Encryption Standard). У WPA3 реалізовано 192-бітне шифрування, яке відповідає сучасним вимогам безпеки. У старих мережах досі використовується TKIP, який є застарілим і небезпечним.

- хеш-функції: використання хеш-функцій у WPA3 для перевірки автентичності та захисту паролів значно знижує ризик компрометації даних.

- опортуністичне шифрування (OWE): це новий стандарт для відкритих мереж, який впроваджує шифрування навіть у тих випадках, коли пароля немає. Це особливо корисно для гостьових мереж.

Розробка програми для аналізу

На основі проведеного аналізу було розроблено інструмент для автоматизованої перевірки безпеки бездротової мережі. Програма виконує такі функції:

- сканування параметрів мережі: програма перевіряє тип протоколу (WPA2 або WPA3), шифрування (AES чи TKIP) та метод автентифікації (PSK, SAE).

- оцінка складності пароля: аналізує довжину пароля та його стійкість до атак словником.

- перевірка відкритих портів: сканує локальну мережу на наявність небезпечних відкритих портів.

- тестування оновлень прошивки: аналізує, чи використовує маршрутизатор останню версію програмного забезпечення.

Програма надає користувачу звіт, який складається з кольорових індикаторів рівня безпеки (зелений – безпечно, жовтий – є недоліки, червоний – критично) та рекомендацій щодо покращення.

Висновки

У результаті роботи було розглянуто ключові загрози та слабкі місця бездротових мереж, проаналізовано ефективність сучасних методів захисту та створено інструмент для оцінки рівня безпеки. Програма дозволяє користувачам легко перевірити захищеність своєї мережі та отримати рекомендації щодо її покращення. Впровадження таких рішень сприятиме підвищенню рівня кібербезпеки, особливо в домашніх умовах.

Список літератури:

1. Wi-Fi Alliance. (n.d.). Wi-Fi Protected Access (WPA2/WPA3). Retrieved from <https://www.wi-fi.org>
2. Vanhoef, M., & Piessens, F. (2017). KRACK атака на WPA2: технічний опис. Retrieved from <https://www.krackattacks.com>
3. IEEE Standards Association. (n.d.). Opportunistic Wireless Encryption (OWE): документація IEEE 802.11. Retrieved from <https://standards.ieee.org>

АВТОМАТИЗОВАНА СИСТЕМА РЕЄСТРАЦІЇ ВІДВІДУВАЧІВ НА ОСНОВІ WI-FI ПІДКЛЮЧЕННЯ

***Автор:** Білець О.О., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Божаткін С.М., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

В умовах стрімкого технологічного розвитку важливо адаптувати організацію навчальної діяльності під ці зміни. Автоматизація дозволяє значно спростити і оптимізувати чимало задач, роблячи їх більш точними, надійними та ефективними.

Метою даної роботи є розробка системи автоматизованого моніторингу присутності на основі Wi-Fi підключення, яка замінить традиційні методи обліку.

Актуальність роботи зумовлена в першу чергу зручністю системи завдяки своєму віддаленому доступу, можливістю фільтрації даних та проведення статистики відвідування. Крім цього дана система підвищує рівень контролю безпеки. У випадку підозрілої активності можна швидко визначити власника пристрою та прийняти відповідні міри.

Для досягнення поставленої мети необхідно виконати низку завдань:

1. обґрунтувати вибір технологій та архітектуру системи;
2. визначити оптимальні методи збору та обробки даних про підключення пристроїв до Wi-Fi мережі;
3. реалізувати базу даних для зберігання ідентифікаційної інформації про студентів і відвідувачів;
4. розробити інтерфейс для публічного відображення даних про присутніх у навчальному корпусі.

Об'єктом дослідження в даній роботі є процес автоматизованого обліку присутності на основі технології Wi-Fi. Предмет дослідження — алгоритми та методи обробки даних, які дозволяють ідентифікувати підключених до Wi-Fi користувачів та фіксувати їхнє перебування в навчальному корпусі.

Першорядною задачею в проектуванні системи реєстрації відвідувачів є розробка оптимальної клієнт-серверної архітектури, такої, щоб дотримувались наступні вимоги:

- система має бути доступною 24/7, без простоїв;
- система має бути масштабованою, тобто бути легко розширеною та бути здатною збільшувати свою продуктивність у разі збільшення навантаження;
- система має бути надійною, тобто бути здатною реагувати на непередбачувані ситуації;
- дані відвідувачів мають бути захищеними від несанкціонованого доступу.

Розглянемо детально розроблене нами рішення. Серверна логіка реалізована на базі Node.js із використанням фреймворку Express для організації маршрутизації та обробки статичних ресурсів. Дані з точок доступу надходять безпосередньо на сервер через HTTP-запити у форматі JSON. Кожне повідомлення містить ім'я пристрою, MAC-адресу, час підключення або відключення та мережевий статус (підключився/відключився).

Після надходження повідомлення на сервер дані не обробляються одразу, а додаються в чергу обробки. Кожні 100 мс запускається фоновий процес, який перевіряє чергу та групує отримані записи. Якщо у черзі були виявлені повідомлення, відбувається наступний порядок дій:

1. Повідомлення переміщуються в тимчасову змінну та видаляються з масиву черг.

2. Щоб ідентифікувати особистість або класифікувати її як "Гостя" у базі даних перевіряються MAC-адреси.

3. Повідомлення розділяються на дві групи: пристрої зі статусом "connected" (для них створюємо нові записи) та пристрої зі статусом "disconnected" (для них оновлюємо час відключення).

4. Одним SQL-запитом для всіх пристроїв, що відключилися, оновлюється час відключення.

5. Одним SQL-запитом для всіх пристроїв, що підключилися, додаються нові записи.

6. Оброблені дані передаються на фронтенд через WebSocket.

Клієнтський інтерфейс реалізований із застосуванням веб-технологій (HTML, CSS, JavaScript) та функціонує у стандартному браузерному середовищі. З'єднання клієнтів із сервером підтримується двома

каналами: HTTP для початкового завантаження інтерфейсу та WebSocket для оперативної синхронізації даних у реальному часі. Дані відображаються у вигляді таблиці. Кожний рядок містить інформацію про відвідувача: ПІБ, час підключення, відключення та час перебування в корпусі, який щохвилини перераховується для активних клієнтів.

В базі даних реалізовано зв'язок між таблицями, що дозволяє ідентифікувати відвідувачів за їхніми MAC-адресами.

Основна таблиця `wifi_connections` містить дані про кожне підключення: MAC-адресу пристрою, ім'я пристрою, час підключення та відключення, загальний час підключення.

Для визначення особи відвідувача використовується таблиця `student_devices`, яка містить відомості про відповідність MAC-адреси конкретному студенту. Кожен студент має свій унікальний `student_id`, а всі відомі пристрої, що належать йому, прив'язані до цього ідентифікатора через відповідні MAC-адреси.

Інформацію про самих студентів зберігає таблиця `students`. Вона зв'язана з `student_devices` за `student_id`. Таким чином, якщо у `wifi_connections` з'являється запис про MAC-адресу, яка відома в системі (тобто є у `student_devices`), сервер може одразу визначити, який саме студент підключився. Це дозволяє на рівні веб-інтерфейсу замість абстрактної MAC-адреси відображати реальне ПІБ відвідувача, персоналізуючи інформацію та підвищуючи її зручність для адміністративного використання.

Підсумовуючи реалізоване рішення, можна стверджувати, що нам вдалося створити технологічний продукт, який має потенціал замінити застарілі методи обліку. Розроблена система автоматизованої реєстрації відвідувачів інтегрує апаратні та програмні компоненти для безперервного збору та обробки даних про присутність користувачів.

Wi-Fi роутер на базі MikroTik виступає первинною ланкою збору інформації. Це обладнання має власну операційну систему RouterOS, яка надає гнучкі можливості автоматизації та розширення функціоналу за допомогою вбудованих скриптів. В скриптах періодично виконуються наступні дії:

1. Формується поточний список підключених пристроїв. Для цього з таблиці реєстрації Wi-Fi повертається перелік усіх активних клієнтів, де з основних даних вилучаються лише MAC-адреси.

2. Отриманий список MAC-адрес порівнюється з попереднім реєстром підключених пристроїв (збереженим у глобальній змінній). Якщо в поточному списку з'являється MAC-адреса, якої не було в реєстрі, це однозначно свідчить про нове підключення. Аналогічно, якщо MAC-адреса, що раніше була зафіксована, відсутня у поточному списку, вона інтерпретується як відключення.

3. Після виявлення зміни виконується запит для збору розширених даних. Для нового підключення визначається ім'я пристрою (якщо воно доступне, інакше використовується значення «Unknown»), а також збирається поточний час. У випадку відключення збирається час, коли клієнт зник із таблиці.

4. На основі отриманих даних формується структурований JSON-пакет, що містить MAC-адресу, ім'я пристрою (для підключення), час події (підключення або відключення), статус події («connected» для нового підключення або «disconnected» для відключення). Сформований JSON-пакет відправляється на сервер за допомогою HTTP POST-запиту через команду /tool fetch.

5. Після обробки подій глобальний реєстр підключених клієнтів оновлюється поточним списком MAC-адрес.

Слід відмітити, що можливість написання і виконання скриптів у роутерах залежить від прошивки і призначення пристрою. Для реалізації описаної вище автоматизації збору даних, доцільно використовувати обладнання, яке надає підтримку скриптування. Зокрема, закупівля роутерів MikroTik hAP liteTC (RB941-2nD-TC), які ми використовували в проекті, є оптимальним рішенням для даної задачі. Ці пристрої вирізняються доступною ціною та мають достатні апаратні характеристики для невеликих мереж і задач моніторингу.

У випадку стандартних споживчих роутерів (наприклад, деякі моделі від TP-Link, D-Link або Netgear), в офіційних прошивках яких відсутня можливість написання власних скриптів, можливі такі рішення реалізації подібної автоматизації:

- встановлення альтернативної прошивки (наприклад, OpenWrt, DD-WRT або Tomato), яка розширює можливості налаштування та автоматизації;
- інтеграція роутера з зовнішніми системами моніторингу, які отримують дані через SNMP, syslog або інші протоколи.

УДК 004.056.5

МОДЕЛЬ ПРОГНОЗУВАННЯ КІБЕРАТАК НА ОСНОВІ АНАЛІЗУ ПОВЕДІНКИ

Автори: Божаткін С.М., ст. викладач; Гусева-Божаткіна В.А., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна; Пасюк Б.Б., ст. викладач, Національний університет Києво-Могилянська академія, м. Київ, Україна

Фінансово-технічний сектор в останні роки належить до найбільш привабливих цілей кібератак зловмисників та АРТ (Advanced Persistent Threat) угруповань різних країн. Традиційні засоби кібербезпеки (мережеві екрани, системи виявлення вторгнень на основі відомих сигнатур та поведінкового аналізу тощо) не можуть забезпечити повного захисту від сучасних кіберзагроз [1]. Особливо, враховуючи evasion-техніки (наприклад, XOR-ування та обфускація коду), які використовують зловмисниками з метою приховання своїх дій від програмного забезпечення, яке створене для детектування таких дій. Зважаючи на це, у фінтех-компаніях набуває критичного значення поведінковий аналіз мережевого трафіку та дій користувачів для виявлення найменших аномалій, що можуть сигналізувати про приховану атаку. Сучасні підходи із застосуванням штучного інтелекту дозволяють аналізувати великі масиви неструктурованих даних у реальному часі, виявляючи підозрілі шаблони та відхилення у поведінці трафіку, які можуть вказувати на потенційну кібератаку або її підготовку [2]. Таким чином, поєднання методів машинного навчання з безперервним моніторингом аномалій забезпечує проактивне виявлення загроз ще на ранніх стадіях розвитку атак [3].

Метою дослідження є розробка удосконаленої гібридної моделі прогнозування кібератак на основі аналізу поведінки.

Основна частина. Сучасні моделі детектування зловмисних дій в мережі можна умовно поділити на два підходи: сигнатурний (за чіткими паттернами) та аномалійні (поведінкові). Сигнатурні системи виявлення вторгнень (IDS, Intrusion Detection System) спираються на базу

відомих шаблонів атак, що дозволяє з високою точністю розпізнавати відомі загрози при низькому рівні хибних спрацювань. Однак, недоліком IDS рішень є нездатність виявляти нові, невідомі атаки або модифіковані чи обфусковані експлойти, яких немає в базі даних сигнатур [4]. Натомість аномалійні системи (Anomaly-based IDS) визначають та будують профілі нормальної поведінки користувачів і станів мережі, а також виявляють відхилення від цієї норми. Anomaly-based IDS здатні детектувати раніше невідомі загрози й так званих insider-threat атак, але страждають на значну кількість хибнопозитивних (false positives) сповіщень при неправильно визначених порогах та профілях. Від налаштування порогів чутливості залежить баланс між пропущеними атаками та зайвими спрацюваннями, що потребує ретельного калібрування моделі або достатньо довгого часу для самокалібрування. Так само, якщо дана система почне «калібруватись» (навчатись) на вже скомпрометованій мережі – для неї наявна поведінка досить довгий час не буде аномальною, що призводить до відсутності спрацювань.

З метою об'єднання переваг обох підходів пропонуються гібридні системи виявлення загроз. Гібридна IDS інтегрує сигнатурний та поведінковий аналіз на основі штучного інтелекту, щоб одночасно виявляти як відомі, так і невідомі атаки. Комбінування двох методів дозволяє підвищити повноту виявлення загроз: відомі атаки фіксуються сигнатурним компонентом, а невідомі – поведінковим, з використанням ШІ. Слід зазначити, що недоліком багатьох ранніх реалізацій було і є просте паралельне об'єднання результатів без належної оптимізації, що не повністю розв'язувало проблему балансу між точністю і кількістю помилоків спрацювань.

Для фінансово-технічного сектору актуальні підходи *аналізу поведінки користувачів і об'єктів* (UEBA – User and Entity Behavior Analytics). UEBA-системи за допомогою алгоритмів машинного навчання моделюють нормальну поведінку користувачів, пристроїв та сервісів і можуть виявляти аномальні відхилення, пов'язані з компрометацією облікових записів чи зловживанням привілеями (правами) користувача. На відміну від традиційних IDS-рішень з фіксованими правилами, UEBA здатні розпізнати інсайдерські загрози або повільні “low-and-slow” атаки без заздалегідь визначених шаблонів, спираючись лише на статистичні відхилення поведінки. Проте впровадження UEBA у фінансових установах

стикається з проблемами масштабованості (великі обсяги різнорідних даних логів), необхідністю тонкого налаштування під нормальну поведінку специфічної організації та пояснюваністю результатів (чому система вважає ту чи іншу активність підозрілою).

Запропонована модель має *інтегративний характер*, поєднуючи декілька рівнів аналізу для досягнення більшої ефективності. Удосконалена гібридна модель відрізняється від відомих рішень гнучкістю, адаптивністю та широким охопленням різних типів атак. Вона спеціально пристосована до умов фінтех-сектору (висока динаміка операцій, строгі вимоги безперервності сервісів і відповідності регуляторним нормам), що забезпечує її практичну цінність для галузі.

Вхідними даними слугують потоки мережевого трафіку фінтех-компанії (лог-файли брандмауерів, NetFlow, syslog) та журнали подій користувачів/систем (автентифікація, доступи до критичних ресурсів, фінансові транзакції і т.д.). Після попереднього «очищення» та агрегування даних (нормалізація показників, усунення дубльованих записів, формування векторів ознак) інформація надходить до основних компонентів моделі:

1. Модуль виявлення відомих атак (класифікатор) – реалізує сигнатурний підхід із використанням алгоритмів машинного навчання з учителем.

2. Модуль поведінкового аналізу аномалій (детектор аномалій) на основі моделей штучного інтелекту – реалізує аномалійну модель, що профілює нормальну поведінку системи.

3. Інтегрований модуль прийняття рішення – відповідає за об'єднання результатів від двох попередніх модулів і винесення фінального вердикту про кібератаку.

Гібридна модель функціонує у двох режимах: офлайн-навчання і онлайн-виявлення. Запропонована архітектура відповідає специфічним вимогам кібербезпеки фінтех-компаній:

- Покриття широкого спектру атак: від класичних мережевих (DDoS, мережеве сканування, експлойти відомих вразливостей) до складних багатоетапних (наприклад, компрометація облікового запису співробітника з подальшим *privilege escalation*).

– Адаптивність до користувацької поведінки. У мережевій інфраструктурі фінансово-технічних компаній поведінкові патерни можуть змінюватися (нові користувачі, сезонні піки транзакцій, запуск нових функцій). Модуль визначення аномалій здатен коригувати поточну результуючу модель нормальної поведінки відповідно до таких змін, зменшуючи кількість неправдивих (false positive) спрацювань.

– Відповідність вимогам регуляторів. Модель сприяє виконанню принципів безперервного моніторингу й швидкого реагування на інциденти, що є частиною стандартів безпеки (наприклад, вимог PCI DSS та GDPR щодо відстеження аномальної активності в мережі). Впровадження постійного моніторингу мережевого трафіку на предмет аномалій є однією з ключових рекомендацій кібербезпеки для фінансових установ.

– Масштабованість і продуктивність. Модель може бути реалізована із використанням сучасних технологій обробки потоків даних (наприклад, платформи Kafka для збору логів, фреймворки TensorFlow/PyTorch для швидкого ML-інференсу). Це дозволить обробляти великі обсяги подій, характерних для фінтех-компаній (тисячі транзакцій за секунду) з мінімальною затримкою. Компонентна структура (два окремі модулі) полегшує горизонтальне масштабування – за потреби можна виділити окремі сервери для класифікатора та детектора або розподілити навантаження між кількома екземплярами.

Висновки: Проведений аналіз показав необхідність поєднання різних підходів (сигнатурного та поведінкового за допомогою ШІ) з метою подолання обмежень кожного з них окремо. Запропонована гібридна модель поєднує аналіз мережевого трафіку та поведінкових аномалій із застосуванням алгоритмів машинного навчання, щоб забезпечити своєчасне виявлення як відомих типів атак, так і нових, раніше невідомих загроз. Основними перевагами даної моделі є висока повнота і точність виявлення атак (в тому числі нових складних атак), знижений рівень хибних тривог завдяки гібридизації методів, а також адаптивність. Отже, запропонована гібридна модель демонструє значний потенціал у підвищенні рівня кібербезпеки фінтех-сектору. Реалізація такої моделі сприятиме захисту фінансових даних і сервісів, зменшуючи ризики фінансових та репутаційних втрат від кіберінцидентів, і стане кроком до створення більш стійких та інтелектуальних систем кібероборони у критично важливій фінансовій сфері.

Список літератури:

1. Fortinet. What Is User Entity and Behavior Analytics (UEBA) Fortinet Cyber Glossary. 2025. URL: <https://www.fortinet.com/resources/cyberglossary/what-is-ueba>
2. DR Bank. Cybersecurity in Fintech: Protecting Your Financial Data. DR Bank. 2025. URL: <https://drbank.com/whats-new/cybersecurity-in-fintech-protecting-your-financial-data>
3. Uma Maheswari S., Gargi Chaudhary, Francis Manna, Vivek Pandurang Khalane, E. Muthukumar. Cybersecurity Challenges In Fintech: Assessing Threats And Mitigation Strategies For Financial Institutions; Educational Administration: Theory and Practice, 2024, 30(5): 1063–1071. DOI: 10.53555/kuey.v30i5.3010.
4. Imperva. User and Entity Behavior Analytics (UEBA): How UEBA Works and Best Practices. Imperva Learn. URL: <https://www.imperva.com/learn/data-security/ueba-user-and-entity-behavior-analytics>
5. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J., Alazab A. Hybrid Intrusion Detection System Based on the Stacking Ensemble of C5 Decision Tree Classifier and One Class Support Vector Machine. Electronics, 2020, 9(1): 173. URL: <https://doi.org/10.3390/electronics9010173>

**ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ПРИХОВАНИХ КАНАЛІВ
СУЧАСНИХ МЕСЕНДЖЕРІВ**

Автор: Восков К.П., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Козирев С.С., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Актуальність дослідження. Сучасні інформаційні технології глибоко інтегруються в суспільне життя, трансформуючи засоби комунікації. Месенджери стали основним інструментом зв'язку, що об'єднує мільярди користувачів, забезпечуючи зручний, швидкий і надійний обмін інформацією. Водночас постає питання конфіденційності та безпеки комунікацій, особливо в умовах зростання інтересу до персональних даних з боку держав, бізнесу та кіберзлочинців.

web-site: conference.nuos.edu.ua | email: conference@nuos.edu.ua; tel (+380512) 709444; 709105|

Одним із напрямів досліджень у цій галузі є приховані канали зв'язку в месенджерах – засоби передачі інформації, що можуть використовуватися як для захисту даних, так і для приховування інформації.

Мета дослідження: дослідити сучасні методи прихованої передачі даних у месенджерах та розробити фреймворк для аналізу прихованих каналів сучасних месенджерів.

Методи дослідження: моделювання, розробка, тестування.

Результат дослідження: У рамках проведеного дослідження нами було спроектовано та розроблено фреймворк мовою програмування php для реалізації та аналізу прихованих каналів на основі нейронних мереж.

Фрагмент коду запиту кодування:

```
Request URL: http://127.0.0.1:8000/api/encode/deepstego
Request Method: POST
Status Code: 200
Remote Address: 127.0.0.1:8000
Referrer Policy: strict-origin-when-cross-origin
Payload: data: { filename: 'image.png' }
```

Код відповіді:

```
{
  "status": "success",
  "task_id": "49cab987-4da9-47c6-a747-2f40e92a8b61" ,
  "hidden_message": "TmFzdHlhIGtpc2EgbnVtYmVyIDE=",
  "message": "Message processed successfully."
}
```

Використання стеганографії є важливим інструментом для приховування інформації у цифрових носіях, таких як зображення, аудіо або відео. У даному дослідженні ми здійснили експеримент із застосування стеганографічного методу за допомогою API, розміщеного за адресою <http://127.0.0.1:8000/api/encode/deepstego>. Для цього був сформований HTTP-запит методом POST, у якому передали зображення з назвою image.png. Результатом виконання запиту стала відповідь із кодом успішності та закодованим повідомленням у форматі Base64:

TmFzdHlhIGtpc2EgbnVtYmVyIDE=. Успішність процесу підтверджується статусом "success" та отриманим ідентифікатором завдання.

Основною метою цього експерименту було приховування текстового повідомлення у зображенні, що може бути застосовано для забезпечення конфіденційності передачі даних, захисту авторських прав або прихованого обміну інформацією. Стеганографічний підхід забезпечує ефективний спосіб передавання даних, мінімізуючи ризик виявлення, що особливо важливо у сфері цифрової безпеки. Закодоване повідомлення, отримане у відповідь, може бути розшифроване шляхом декодування Base64, що дає змогу отримати текстовий вміст, впроваджений у зображення. Цей експеримент демонструє можливості стеганографії як методу інтеграції даних у цифрові носії для досягнення високого рівня захисту інформації.

Висновок: У результаті проведеного дослідження було розглянуто сучасні методи прихованої передачі даних у месенджерах, зокрема через стеганографію, яка дозволяє ефективно інтегрувати інформацію в цифрові носії, такі як зображення. Розроблений фреймворк на основі нейронних мереж став важливим інструментом для реалізації та аналізу прихованих каналів зв'язку, що демонструє великий потенціал цих технологій для забезпечення конфіденційності даних. Виявлені можливості та обмеження прихованих каналів відкривають нові перспективи для їх застосування в різних сферах, зокрема в забезпеченні безпеки інформації та захисті даних.

Список літератури:

1. Kessler, G. C. (2014). Steganography: Hiding Data in Plain Sight. <http://www.garykessler.net/library/steganography.html>
2. Memon, N., & Hussain, F. (2017). Security and Privacy Issues in Mobile and Web Communication. Springer International Publishing.
3. Wilson, C., & Moffat, A. (2017). The use of metadata and its role in data protection. Communications of the ACM, 60(8), 40-47.

УДК 004.4

АНАЛІЗ ТА ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК ГРУБОЇ СИЛИ НА ІНТЕРНЕТ-СЕРВІСИ

***Автор:** Десятов А.М., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Козирев С.С., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ

В умовах зростаючої кількості кіберзагроз особливу увагу привертають атаки грубої сили (brute force), спрямовані на отримання несанкціонованого доступу до інтернет-сервісів. Такі атаки часто стають першою фазою більш масштабних зловмисних кампаній. Їх виявлення та запобігання є критично важливим завданням для забезпечення кібербезпеки.

Метою роботи є аналіз методів виявлення атак грубої сили на інтернет-сервіси, а також оцінка ефективності застосування сучасних інструментів моніторингу та аналізу трафіку.

Основна частина

Характеристика атак грубої сили

Атака грубої сили полягає у переборі можливих комбінацій логінів і паролів для отримання доступу до системи. Найбільш вразливими є сервіси з відсутністю обмежень на кількість невдалих спроб автентифікації.

Основні характеристики атак:

- Автоматизація: Використання спеціалізованого програмного забезпечення, такого як Hydra або Medusa, для швидкого перебору облікових даних.
- Цільові сервіси: FTP, SSH, RDP, HTTP(S)-авторизація тощо.
- Поведінкові ознаки: Велика кількість запитів на автентифікацію за короткий проміжок часу.

Методи виявлення

Аналіз логів:

- Використання інструментів, таких як Fail2Ban або Logwatch, для автоматичного аналізу логів і блокування підозрілих IP-адрес.
- Виявлення повторюваних невдалих спроб входу за короткий період.

Мережевий моніторинг:

- Інтеграція систем виявлення та запобігання вторгнень (IDS/IPS), таких як Snort або Suricata.

- Аналіз трафіку на предмет аномальних шаблонів запитів.

Машинне навчання:

- Використання кластеризації та класифікації для виявлення підозрілих активностей у мережевому трафіку.

- Застосування алгоритмів аналізу поведінкових аномалій, таких як Isolation Forest чи DBSCAN.

Запобігання атакам

- Обмеження спроб автентифікації: Встановлення лімітів на кількість невдалих спроб входу.

- Двофакторна автентифікація (2FA): Додавання додаткового рівня захисту.

- Використання CAPTCHA: Ускладнення автоматизованих атак.

- Чорні списки: Блокування IP-адрес із відомою зловмисною активністю.

Інструменти для аналізу

- Fail2Ban: Автоматичне блокування IP-адрес на основі аналізу логів.

- Snort/Suricata: Мережеві IDS для аналізу і класифікації трафіку.

- Wireshark: Детальний аналіз мережевих пакетів для виявлення аномалій.

Висновки

Ефективне виявлення та запобігання атакам грубої сили вимагає комплексного підходу, що включає моніторинг логів, мережевого трафіку та використання інструментів з елементами штучного інтелекту. Впровадження таких рішень дозволяє значно підвищити рівень захищеності інтернет-сервісів.

Застосування сучасних інструментів для виявлення аномалій та автоматизація процесів захисту є перспективним напрямком розвитку кібербезпеки в умовах зростаючої кількості загроз.

Список літератури:

1. Скрипник, В. І., & Галушко, С. І. (2020). Сучасні підходи до виявлення кіберзагроз у мережах підприємств. *Вісник НТУУ «КПІ» Інформатика, управління та обчислювальна техніка*, №4(98), с. 23-30. URL: <http://bulletin.kpi.ua>
2. Закон України «Про основні засади забезпечення кібербезпеки України». (2017). URL: <https://zakon.rada.gov.ua>
3. Ковальчук, О. В., & Ткаченко, В. А. (2019). Методологія аналізу логів для виявлення атак грубої сили в інформаційних системах. *Науковий вісник Черкаського державного технологічного університету*, №1, с. 48-54. URL: <http://journals.cdu.edu.ua>
4. Мельник, А. В. (2020). Інструменти захисту веб-додатків від атак грубої сили. *Інформаційна безпека та кіберзахист: Праці науково-практичної конференції*, с. 123-130. URL: <https://cybersecurityconf.org.ua>
5. Snort – Відкрите ПЗ для виявлення вторгнень. URL: <https://snort.org> (українська документація доступна через локалізовані форуми).
6. Статті з ресурсу DOU.ua (професійна IT-спільнота): URL: <https://dou.ua>
7. Репозитарій українських наукових публікацій з кібербезпеки: URL: <https://elibrary.kpi.ua>

**ДОСЛІДЖЕННЯ ФУНКЦІОНУВАННЯ СИСТЕМИ
ЗАХИЩЕНОГО ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В
ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ**

Автор: Дзюбас Д.С., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Анотація. Люди – це основний ресурс людства. Однією з основних функцій людини є створення мови, створення інформації і сприйняття її від інших людей, створення і вживання. З одного боку, у нас є той що творить інформацію або володіє нею, а з іншого – особа або група осіб, які бажають завладіти даною інформацією. Виходячи з цього, один з перших пунктів при будівництві системи захисту інформації,

необхідно вивчити склад співробітників, тому що вони є вірогідним джерелом витоку.

Актуальність роботи визначається функціонуванням систем захищеного електронного документообігу в підрозділах Національної поліції України

Ключові слова: Комплексна система захисту інформації, канали витоку інформації, структури системи захищеного документообігу, аналіз систем захищеного електронного документообігу, носії інформації, аналіз організації інших країн, СЗЕД.

Вступ

У сучасному світі органи внутрішніх справ виконують важливі функції з забезпечення безпеки громадян та суспільства. Проте, з постійно зростаючим обсягом інформації та розвитком інформаційних технологій, стало зрозуміло, що безпека інформації відіграє ключову роль ефективності роботи правоохоронних органів. Зміна геополітичної ситуації в країні стимулює органи влади до реформ та перебудови нинішньої системи захисту, оскільки нинішня система вже не може гарантувати громадянам навіть часткової анонімності з низки причин. Будь то різного роду зливи особистих даних, злами інформаційних мереж, людський фактор, нестабільність роботи ПЗ та інше. У країнах центральної Європи це питання викликає жаркі обговорення, бо останніми роками було безліч прецедентів з втратою величезної кількості даних користувачів, у різних областях.

Кількість інцидентів втрати інформації в органах внутрішніх справ невідносно зростає, навіть з урахуванням усієї роботи, що ведеться постійно. Очевидно, що Україна відстала від партнерів щодо захисту інформації в органах внутрішніх справ. Певна частина законів та нормативних актів – застаріли і повинні бути замінені. Процес навчання персоналу необхідно перебудовувати та вдосконалювати, для цього необхідно включати в навчання сучасні курси з навчання співробітників із країн, які стоять вище за Україну в цьому питанні: США, ЕС, Велика Британія.

Метою роботи є дослідження існуючих систем захисту інформації в органах внутрішніх справ та розробка комплексного підходу до їхнього розвитку. У процесі дослідження було проведено аналіз існуючих загроз

та вразливостей, з якими стикаються правоохоронні органи, а також вивчено передові методи та технології у сфері інформаційної безпеки.

Для досягнення поставленої мети вирішувалися такі наукові завдання:

Проведено огляд нормативно-правове забезпечення захищеного документообігу у Україні та світова практика їх використання в органах правопорядку;

Проаналізовано принципи побудови систем безпеки та доступу до інформації в системах захищеного електронного документообігу;

Проведено аналіз критичних вразливостей системи захищеного електронного документообігу та методів їх запобігання;

Розроблено та узагальнено рекомендації що до запобігання виникнення інцидентів в СЗЕД, що використовуються в підрозділах Національної поліції України;

Нормативно-правове забезпечення захищеного документообігу в Україні.

Ключовою задачею будування складної системи захисту інформації, як і в цілому захисту інформації в органах внутрішніх справ, є попередження втрати, збитків, незаконного використання інформації, пов'язаної з їхньою діяльністю. Збитки внутрішнім органам в наслідок зливу/розголошення конфіденційної інформації можуть бути колосальними. Також однією з основних цілей є попередження крадіжки як матеріальних накопичувачів інформації, так і електронних.

Виходячи з досвіду нашої держави, для боротьби, супротив з цією сукупністю протизаконних дій вимагається організація процесів протидії.

Маються визначені рекомендації про будову системи безпеки інформаційних об'єктів органів внутрішніх справ (далі ОВС) [4]:

- в першу чергу забезпечення безпеки не може бути одноденним, одномісячним та ін.. Це постійний безперервний процес, який полягає в постійній реалізації раціональних способів, методів, форм, поліпшення та ускладнення системи безпеки. Необхідність в постійному, безперервному управлінні, знаходження слабких місць в системі і їх найскоріше закриття.

- повноцінний захист можливо отримати тільки при використанні всіх доступних засобів захисту та протидії крадіжки інформації. У найбільш вдалому варіанті необхідно створити єдиний механізм, який називається – система безпеки ОВС.

– навіть найкраща система безпеки не зможе захистити інформацію в усіх її видах при некваліфікованому персоналі. Підготовка співробітників і нагляд за тим, аби вони безперечно наслідували правилам зробити систему ще більш захищеною.

Система безпеки також є складною системою, яка являє собою певну сукупність спеціальних служб, засобів, методів і заходів, які повинні забезпечити захист ОВС від зовнішніх та внутрішніх загроз.

Базуючись на досвіді інших держав, із нашого досвіду, ми прийшли до того, що забезпечити виконання стількох функцій і вимог до безпеки системи захисту в ОВС повинна дотримуватись певних умов, охоплювати всю область інформаційної діяльності і характеризуватися певними пунктами:

- різновид використаних засобів і багаторівневої системи з ієрархічною послідовністю доступу;
- доступність і відкритість для змінення і поліпшення мір безпеки співробітникам охорони;
- унікальність в плані вибору захисту (Не треба вірити в успіх в питаннях захисту!);
- простота технічного обслуговування, надійність і зручність;
- комплексність. Це означає, що жодна частина системи не може бути вилучена, відключена, знищена без шкоди для всієї іншої системи.

При організації системи захисту в ОВС також важлива правова основа питання. Її формують як документи державного рівня, так і відомчі, які формують вимоги і рекомендації по розробці на об'єктах захисту (див. рис. 1).

Базисними документами в галузі забезпечення безпеки є: Конституція України та інші закони України, міжнародні договори і зобов'язання, згода на які була дана Верховною Радою України, а також видані нею же інші нормативно-правові акти.

Методи виявлення вразливостей

1. Статичний аналіз коду

- Опис методу: статичний аналіз полягає у вивченні вихідного коду програмного забезпечення без його виконання. Він дає можливість виявити вразливості в логіці коду або його архітектурі.

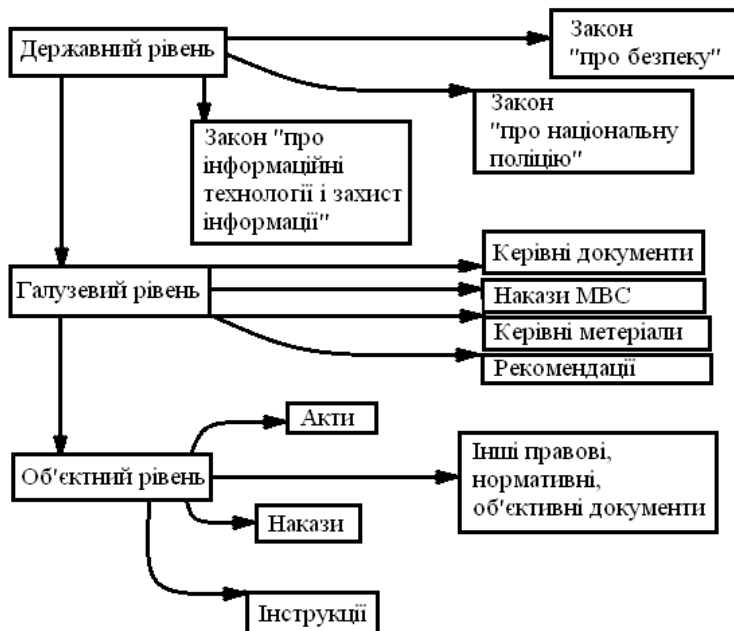


Рисунок 1 – Схема класифікації нормативно-правових документів в галузі захисту інформації

– Інструменти: використання спеціалізованих інструментів, таких як SonarQube, Checkmarx, для сканування коду на предмет потенційних вразливостей, зокрема некоректної обробки даних, неправильного використання криптографічних алгоритмів тощо.

2. Динамічний аналіз безпеки

– Опис методу: цей метод дослідження включає аналіз безпеки системи під час її виконання. Він дозволяє виявляти проблеми, пов'язані з взаємодією компонентів, неправильною обробкою запитів та експлуатацією мережових вразливостей.

– Інструменти: OWASP ZAP, Burp Suite, які дозволяють симулювати атаки на систему, виявляючи потенційні уразливості, зокрема у веб-інтерфейсі системи ЗЕДО.

3. Метод "Penetration Testing" (тестування на проникнення)

– Опис методу: метод полягає у симуляції кібератак з метою виявлення можливих шляхів проникнення та експлуатації вразливостей.

– Алгоритм виконання:

- a) Збір інформації про систему (reconnaissance);
- b) Сканування відкритих портів та аналіз конфігурацій;
- c) Використання експлойтів для тестування захищеності;
- d) Оцінка наслідків.

– Інструменти: Metasploit, Nmap, Kali Linux.

4. Фаззинг (Fuzz testing)

– Опис методу: фаззинг передбачає автоматичну генерацію випадкових або непередбачуваних вхідних даних для тестування програмного забезпечення. Цей метод дозволяє виявити слабкі місця у валідації вхідних даних, що може бути використано для атак на систему.

– Інструменти: AFL (American Fuzzy Lop), Peach Fuzzer.

Рекомендації що до запобігання виникнення інцидентів в СЗЕД, що використовуються в підрозділах Національної поліції України

1. Посилення автентифікації та управління доступом

- Впровадження багатофакторної автентифікації (MFA):
- Посилення політики паролів:
- Регулярний аудит прав доступу:
- Управління обліковими записами:

2. Покращення моніторингу та логування

- Впровадження SIEM-систем:
- Збільшення терміну зберігання логів:
- Регулярний аналіз логів:

3. Оновлення та патч-менеджмент

- Регулярне оновлення системи:
- Вразливість сканування:

4. Захист від шкідливого ПЗ та кібератак

- Інтеграція з антивірусними рішеннями:
- Захист веб-додатків:

- Сегментація мережі:
- Розділити мережу на ізольовані сегменти для критичних сервісів.
- Обмежити доступ до серверів з системою "Документ" ззовні.
- 5. Підвищення обізнаності персоналу
 - Регулярні тренінги з кібербезпеки:
 - Симуляція фішингових атак:
 - Комунікація про важливість безпеки:
- 6. Впровадження політик та процедур безпеки
 - Оновлення політик безпеки:
 - План реагування на інциденти:
 - Відповідність нормативним вимогам:
- 7. Технічні заходи безпеки
 - Шифрування даних:
 - Брандмауери та IDS/IPS:
 - Резервне копіювання та відновлення даних:

Дії по виявленню вразливостей та аналізу інцидентів

1. Виявлення вразливостей
 - Проведення аудиту безпеки:
 - Тестування на проникнення:
 - Використання інструментів виявлення вразливостей:
2. Аналіз інцидентів
 - Створення команди реагування на інциденти (CSIRT):
 - Розробка та впровадження процедур реагування:
 - Використання SIEM та інших інструментів:
 - Документування та післяінцидентний аналіз:

Висновки

В роботі виконано дослідження існуючих систем захисту інформації в системах захищеного електронного документообігу в підрозділах Національної поліції України. Проаналізовано основні загрози та вразливості, з якими стикаються у сфері інформаційної безпеки. Розглянуто методи, способи та технології захисту інформації.

За результатами аналізу організації, структури та особливості функціонування документообігу в інших країнах, було виділено їх особливості та функції, що дало змогу сформулювати перелік можливих загроз в залежності від каналу витоку інформації.

Проведено дослідження вразливостей та інцидентів в системах захищеного електронного документообігу в підрозділах національної поліції України, що дозволило сформулювати рекомендації по вдосконаленню системи безпеки та доступу до інформації в системах захищеного електронного документообігу.

Список літератури:

1. Про державну таємницю // сайт Верхов. Ради України (ВВР). URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text> (10.10.2024).
2. Захист конфіденційної інформації – персональних даних. Засоби захисту від несанкціонованого доступу. // ООО НИИ «Автопром». URL: <http://avtoprom.kiev.ua/avtoprom /ru/content/защита-конфиденциальной-информации-персональных-данных> (10.10.2024).
3. Федеральне бюро розслідувань. Федеральне бюро розслідувань ФБР. // FBI.gov. URL: <https://www.fbi.gov> (10.10.2024).
4. MI5 // Вікіпедія. URL: [https://uk.wikipedia.org/wiki/MI5#:~:text=Служба%20Обезпеки%2C%20також%20відома%20як,i%20оборонної%20розвідки%20\(DI\)](https://uk.wikipedia.org/wiki/MI5#:~:text=Служба%20Обезпеки%2C%20також%20відома%20як,i%20оборонної%20розвідки%20(DI)). (14.10.2024).
5. Australian Security Intelligence Organisation // Вікіпедія. URL: [https://ru.wikipedia.org/wiki/Австралийская_служба_безопасности_и_разведки#:~:text=Australian%20Security%20Intelligence%20Organisation\)%20—%20часть,на%20австралийскую%20систему%20обороны%2C%20и](https://ru.wikipedia.org/wiki/Австралийская_служба_безопасности_и_разведки#:~:text=Australian%20Security%20Intelligence%20Organisation)%20—%20часть,на%20австралийскую%20систему%20обороны%2C%20и) (11.10.2024).
6. Про основи національної безпеки України: Закон України від 18.06.2003 р. № № 964-IV. // ФДМУ. URL: <https://www.spfu.gov.ua/ua/documents/1819.html#:~:text=> (10.10.2024).
7. Open AI. ChatGPT. URL: <https://chat.openai.com> (10.10.2024).
8. Rework A.I. AgentGPT. URL: <https://agentgpt.reworkd.ai/ru> (10.10.2024).
9. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № № 2136-XII. // ВРУ. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text> (11.10.2024).
10. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція від 28.01.1981 р.: станом на 6 лип. 2010 р // ВРУ. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (11.10.2024).

11. Про захист персональних даних: Закон від 23.02.2012 р. № № 4452-VI: станом на 29 лип. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (15.10.2024).

12. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон від 20.11.1989 р. № № 51: станом на 20 листоп. 2012 р. URL: <https://zakon.rada.gov.ua/laws/show/383-18#Text> (17.10.2024).

13. CISA // America Cyber Defence Legacy. URL: <https://www.cisa.gov> (16.10.2024)

14. NIST // National Institute of Standards and Technology. URL: <https://www.nist.gov> (16.10.2024).

15. DarkReading // Dark Reading. URL: <https://www.darkreading.com> (16.10.2024).

16. KoS // Krebs on Security. URL: <https://krebsonsecurity.com> (дата звертання: 16.10.2024).

17. SANS // Cyber Security Practitioners & Teams. URL: <https://www.sans.org/emea/> (дата звертання: 16.10.2024).

18. THN // The Hacker News. URL: <https://thehackernews.com> (дата звертання: 16.10.2024).

19. CSO // CSO Online. URL: <https://www.csoonline.com> (16.10.2024).

20. TP // Threatpost. URL: <https://threatpost.com> (16.10.2024).

УДК 004.056.52.:53:004.942

**РОЗРОБКА ПАКЕТУ ДОКУМЕНТІВ ДЛЯ АТЕСТАЦІЇ АС-1
«ГЕРМЕС-2» НА IV КАТЕГОРІЮ ОБМЕЖЕННЯ ДОСТУПУ
КАФЕДРИ КТІБ**

***Автор:** Дибченко М.Є., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Анотація. Інформація, що є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю.

Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством України та нормативними документами системи технічного захисту інформації (ТЗІ).

Ключові слова: Захист інформації, комплексна система захисту інформації, атестація АС, експертиза АС

Вступ. Атестація АС– це спільний шлях організації, яка виконує роботи з атестації АС, та заявника (власника системи), який вони мають пройти разом від першого до останнього кроку.

Результатом цієї роботи стає отримання заявником Атестату відповідності вимогам безпеки інформації.

Атестація АС є завершальним етапом цілого комплексу робіт із захисту інформації, який включає наступні основні складові:

- визначення вимог безпеки інформації, яким має відповідати АС/ІВ.
- створення системи захисту інформації відповідно до вимог безпеки інформації.
- після створення системи захисту інформації можливе проведення атестаційних випробувань.

Класифікація АС :

1. АС опрацьовує інформацію, що становить державну таємницю
2. АС використовується при організації захисту інформації, що міститься в державних інформаційних ресурсах
3. АС використовується при виконанні вимог щодо ліцензування по ТЗКІ та СКЗД
4. АС використовується при виконанні вимог щодо ліцензування СКЗІ
5. АС використовується при обробці інформації в державних та муніципальних інформаційних системах
6. АС є об'єктом критичної інформаційної інфраструктури
7. АС є системою обробки персональних даних

Метою роботи є аналіз вимог до комплексу документації на системи комплексного захисту інформації в відповідності до оновлених нормативних вимог та особливостей проходження їх експертизи.

Для досягнення поставленої мети вирішувалися такі наукові **завдання** дослідження:

1. Провести аналіз документів зі створення КСЗІ в АС;
2. Провести аналіз попередньо проведених робіт зі створення КСЗІ в АС;
3. Провести аналіз організаційно-розпорядчих та програмно-експлуатаційних документів.

Аналіз документів зі створення КСЗІ в АС

Розробка КСЗІ для об'єктів критичної інфраструктури (ОКІ) є однією з пріоритетних задач в інформаційно-правовому полі України. Це набуло особливо вагомого значення в умовах збройного нападу Росії на Україну. Захист та відновлення інформаційних ресурсів, протидія кібератакам та деструктивним діям російських диверсійно-розвідувальних груп та їх поплічників можливий тільки при комплексному підході до побудови системи захисту. При цьому об'єкти критичної інфраструктури України після 24 лютого стали основними об'єктами нападу як в фізичному відношенні, так і в кібернетичному.

Згідно з оновленими вимогами до розробки та впровадженню КСЗІ на об'єктах критичної інфраструктури алгоритм проведення робіт з атестації КСЗІ проходить в три етапи (див. рис.1).

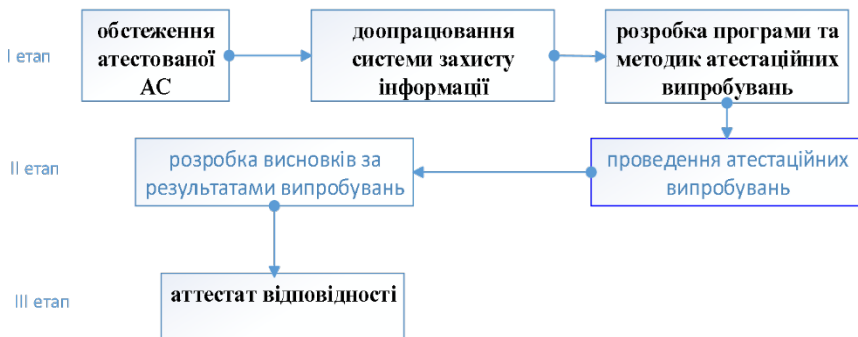


Рисунок 1 – Послідовність робіт з атестації КСЗІ

Під час випробувань проводиться розробка наступних атестаційних документів:

- програми та методики проведення випробувань;

- створення протоколу атестації;
- висновки, які створюються за результатами проходження атестації;
- сам атестат відповідності.

Етапи робіт з атестації АС

Етап I. Підготовчий

А. Доопрацювання системи захисту інформації

Для успішної атестації необхідно провести роботи з доопрацювання системи захисту інформації. Вони можуть включати:

- додаткове налаштування засобів захисту інформації;
- коригування організаційно-розпорядчої та експлуатаційної документації.

В. Розробка програми та методик атестаційних випробувань

Організація, яка проводить атестацію, розробляє програму та методику атестаційних випробувань. У них мають бути визначені:

- вимоги, на відповідність яким проводиться атестація;
- склад атестаційної комісії;
- методи перевірки відповідності вимог інформаційної безпеки АС;
- наявність технічних засобів для перевірки витоку інформації з технічних каналів (за потреби).

Етап II. Атестаційний

Атестаційний етап поділяється на два під етапи:

А. Проведення атестаційних випробувань АС у реальних умовах, у яких перевіряється фактичне виконання вимог щодо захисту інформації на різних етапах технологічного процесу обробки інформації, що захищається.

В. Розробка висновку на підставі протоколу атестаційних випробувань, в якому містяться оцінка відповідності системи захисту інформації АС вимогам безпеки інформації, рекомендації щодо контролю за функціонуванням АС та висновок про можливість видачі атестату відповідності або необхідні рекомендації щодо усунення зауважень, виявлених у результаті атестаційних випробувань.

Етап III. Заключний

Атестат відповідності оформляється та видається організацією, яка проводила атестацію, після затвердження позитивного висновку за результатами атестаційних випробувань АС.

Весь час експлуатації АС або протягом терміну дії атестату відповідності заявник зобов'язаний дотримуватись усіх вимог щодо експлуатації, описаних в організаційно-розпорядчій та експлуатаційній документації.

У разі зміни розміщення технологічних засобів, умов експлуатації або зміни засобів захисту інформації власник атестованих АС зобов'язаний сповістити про це організацію, яка видала атестат відповідності вимогам інформаційної безпеки.

У разі, якщо це необхідно, організацією призначаються додаткові перевірки ефективності системи захисту.

Проведення атестації АС класу 1

АС-1 – однокомп'ютерний розрахований на багато користувачів комплекс, що не має підключення до локальної мережі підприємства і мережі Інтернет. Зазвичай використовується для обробки інформації з грифами «Для службового користування» (4-а категорія секретності) та «Секретно» (3-я категорія секретності).

АС-1 це персональний комп'ютер у захищеному виконанні та комплекс додаткового ПЗ (антивірус, засоби розмежування доступу тощо) розташований у спеціальному, обладнаному для нього приміщенні (кімнаті).

Проведення державної експертизи КСЗІ для отримання «Атестату відповідності» проводить третя сторона, тому вартість проведення експертизи не включена до вартості проекту.

Середній термін виконання робіт із побудови КСЗІ АС-1 становить 2-4 календарні місяці, термін виконання робіт із проведення державної експертизи КСЗІ може становити від 2-х до 3-х календарних місяців.

Основні завдання, що повинні вирішуватись при проведенні атестації АС класу 1

1. Врахування вимоги щодо розміщення поблизу об'єкта іноземних представництв та з'ясувати, що електроживлення об'єкта здійснюється від трансформаторної підстанції, яка розташована в межах контрольованої зони та не має сторонніх споживачів.

2. Перевірка діючих інформаційних та експлуатаційних документів:

- протокол вимірювання опору контуру заземлення;
- специфікації апаратних та апаратно-програмних засобів ОІД;
- опис програмного забезпечення з номерами ліцензій та підтвердженням, що ПЗ придбане без порушення авторських прав, (підтвердити рахунками-фактурами, ліцензіями (паспортами), серійними номерами).

На встановлене антивірусне програмне забезпечення робочих станцій, серверів Замовник повинен надати експертні висновки Адміністрації Держспецзв'язку України та підтвердити, що оновлення баз даних проводиться у відповідності до нормативно-правової бази.

– відповідність комплексу засобів захисту інформації від несанкціонованого доступу (КЗЗ від НСД) з визначеним рівнем гарантії вимогам нормативних документів системи технічного захисту інформації у обсязі функцій, сукупність яких визначається функціональним профілем захищеності та наявність експертного висновку Адміністрації Держспецзв'язку України.

3. Перевірка діючих нормативних та організаційних документів:

– наказ про проведення робіт зі створення КСЗІ на ОІД з висновками щодо обмеження грифу обмеження доступу до інформації, що обробляється в АС та призначення відповідальних осіб;

- наказ щодо створення служби захисту інформації;
- наказ про створення комісії з проведення випробувань КСЗІ в АС;
- наказ про забезпечення захисту інформації в АС;
- наказ про введення АС в дослідну експлуатацію тощо;
- інструкцію про порядок введення в експлуатацію КСЗІ в АС;
- інструкцію про порядок модернізації КСЗІ в АС;
- інструкцію системному адміністратору;
- інструкцію адміністратору безпеки при роботі в АС;
- інструкцію користувачу.

4. Результати роботи Експерта оформлюються у вигляді протоколу виконання експертних робіт за підписом Експертів, які її виконували. Протокол затверджується Організатором.

5. Результати робіт, визначених окремою методикою, узагальнюються Організатором в Експертному висновку. За результатами проведених робіт Організатор складає Експертний висновок відповідного змісту щодо відповідності об'єкта експертизи вимогам нормативних документів з ТЗІ, підписує його і подає до Адміністрації.

На підставі позитивного рішення щодо експертизи КСЗІ Замовнику видається зареєстрований Атестат відповідності за підписом Голови (заступника Голови) Держспецзв'язку.

Атестат відповідності є підставою для Замовника видати наказ про введення КСЗІ в ІТС в постійну експлуатацію та оформити Паспорт-формуляр по захисту секретної інформації на ОІД.

Висновки

В роботі проведено аналіз відкритої нормативно-правової бази та встановлено що пакет документів на експертизу повинен включати наступні документи:

1. Замовник, серед інших документів, повинен надати Експерту Акт обстеження АС.

2. В комплекті документів на КСЗІ повинен бути «Протокол про визначення вищого ступеня обмеження доступу до інформації», зміст якого впливає на обґрунтований вибір необхідного рівня захисту ІзОД від витоку технічними каналами, використання тих або інших норм, положень, методик і рекомендацій, викладених в нормативній базі системи ТЗІ.

3. Документ «Окрема модель загроз для інформації на ОІД, де розміщено АС», що містить питання можливих технічних каналів витоку ІзОД на ОІД для подальшого створення комплексу ТЗІ на об'єкті.

Список літератури:

1. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: загрози конфіденційності (Confidentiality), цілісності (Integrity), доступності (Availability), спостереженості. Модель СІА.»

2. НД ТЗІ 2.3-025-24 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»

3. НД ТЗІ 2.6-004-21 «Порядок авторизації безпеки інформаційних систем»

4. НД ТЗІ 3.6-004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в ІКС, в яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці»

5. НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації»

6. НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»

7. Наказ Адміністрації ДССЗІ №354 від 10.07.2024. «Рекомендації з оцінки достатності заходів захисту інформації КСЗІ в інформаційних, електронних комунікаційних та ІКС, створених з використанням профілів безпеки інформації»

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ПРОТОКОЛУ КЕРУВАННЯ БЕЗПІЛОТНИМ АПАРАТОМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Автор: Душенко О.В., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Анотація. Вже майже три роки народ України веде криваву та виснажливу війну за свободу, незалежність та саме існування української держави та нації. Повітряні Сили формують повітряний щит над нашими містами та бойовими порядками військ, організовують прикриття об'єктів критичної інфраструктури, а роль військової авіації у війні щодаля тільки зростає. Особливо це стосується безпілотної авіації, адже широке застосування безпілотних літальних апаратів (БпЛА) та безпілотних авіаційних комплексів (БпАК) в ході ведення бойових дій стало однією з особливостей сучасного етапу російсько-української війни.

Ключові слова: безпілотний апарат, пульт, радіоканал, протокол, шифрування, DJI, модуляція

Вступ.

Досвід бойових дій на території України свідчить про використання великого різноманіття БпАК, що надаються в рамках допомоги країнами-партнерами та виробляються вітчизняними виробниками. Особливістю перших є обмежений програмно-апаратний функціонал. Це пов'язано з високою комерційністю та скритністю зазначеного

напрямку. В свою чергу, до основних тенденцій розвитку ворога в напрямку БПАК відносяться наступні: використання сучасних інформаційних технологій для удосконалення навігаційних систем (автоматизована корекція маршрутів, ройове використання); використання технологій комп'ютерного зору та глибоко машинного навчання для автоматизованого виявлення та класифікації об'єктів інтересу. Це призводить до зростання деструктивного впливу противника в повітряному просторі України, що вимагає від вітчизняного виробника динамічної адаптації та інтеграції технологій зазначеного напрямку в розвиток БПАК вітчизняного виробництва, оскільки вразливість до кібератак призводить до серйозних наслідків, таких як викрадення даних, втрата контролю над апаратом або його знищення. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством України та нормативними документами системи технічного захисту інформації (ТЗІ).

Метою роботи є аналіз протоколів керування БПЛА для виявлення їх вразливих місць та розробка методів захисту від потенційних загроз.

Для досягнення поставленої мети вирішувалися такі наукові **завдання дослідження**:

1. Провести огляд сучасних стандартів бездротової передачі даних та нормативно-правової бази використання БПЛА.
2. Дослідити технічні характеристики та режими роботи різних моделей безпілотних апаратів.
3. Проаналізувати методи реінжинірингу протоколів дистанційного керування.
4. Розробити методiku дослідження протоколів керування та побудувати лабораторний стенд для проведення експериментів.
5. Провести експериментальне дослідження протоколів, що використовуються у БПЛА, та проаналізувати отримані результати.

Огляд сучасних стандартів бездротової передачі даних та нормативно-правової бази використання БПЛА

Сучасні дрони розрізняються за способом польоту та його дальністю, вагою корисного навантаження та іншими характеристиками. Поєднання практичних властивостей в одному апараті робить його використання ефективним у різних видах діяльності, починаючи від бойових дій та закінчуючи будівництвом.

За експлуатаційними характеристиками дрони класифікуються відповідно кількості та розташуванню гвинтів або крил, мети використання, дальності польоту, масі корисного навантаження, базового механізму та ін.

За технічними характеристиками виділяють дрони трьох видів:

- вертолітного/коптерного (мультироторні – мультикоптерні та спілвісні);
- літакового (з нерухомим крилом);
- гібридного (з гвинтами та крилами) [49].

За типом управління безпілотики поділяються на GPS і FPV дрони. GPS дрони найчастіше використовуються для реалізації стабілізованої аерозйомки. Завдяки автоматичним функціям експлуатація GPS дронів максимально проста і не вимагає від користувача особливих навичок пілотування. Потенціал GPS дронів завжди обмежений електронікою, як у потужності, так і в управлінні, що в цілому визначає їх вузьке призначення (аерозйомка /картографія /моніторинг/ пошук та порятунок). FPV (First Person View) квадрокоптери відрізняються від звичайних квадрокоптерів, мають особливі властивості і ці властивості визначили їх застосування як дронів-камікадзе.

Крім доставки вибухівки БПЛА можуть вирішувати такі військові завдання:

- авіарозвідка (на сьогодні формально це основне їхнє призначення);
- управління вогнем та цілевказівки;
- перехоплення повітряних цілей;
- мінування та розмінування;
- постановка радіоперешкод;
- ретрансляція повідомлень та даних;
- розкриття систем протиповітряної оборони (дрон-приманка);
- доставка вантажів підрозділам [50].

У зв'язку з багатоцільовим призначенням військові дрони діляться ще на кілька видів:

- Літак-носіє, "авіаматка" – БПЛА носії інших безпілотики.
- Літак-мішень можуть використовуватися як літаючі мішені, для випробувань і виявленнь зенітних ракетних комплексів (ЗРК).

– БПЛА РЕБ – ставить радіоперешкоди, блокує GPS або бореться з іншими ворожими дронами, може бути ретранслятором радіосигналів.

Баражуючий боеприпас (дрон-камікадзе) — тип БПЛА з бойовою частиною, які здатні тривалий час у режимі очікування перебувати в повітрі в районі мети та оперативно атакувати її після отримання відповідної команди від оператора, або виконувати завдання, що передбачаються закладеним алгоритмом. Подібний боеприпас, за вартості набагато менше мільйона доларів, може знищити найновіший танк або ракетний комплекс набагато більшої вартості.

В Україні зараз активно використовуються військові тактичні безпілотники "Лелека-100", Spectator-M1, "Фурия", PD-2, "Валькірія", призначені для розвідки. Український ударно-розвідувальний БПЛА Punisher застосовують і в рятувальних операціях, дрон допомагає транспортувати медичні засоби, щоб надавати допомогу пораненим, розвідувальні комплекси "Shark", «Гор», багатоцільові БПЛА «PD-2, "Довбуш", "Інквізитор", "Ельф", "Колдун", "Баба Яга", «Пегас», «Бобер». більшу частину дронів, що виробляються в Україні, становлять 7 і 8 дюймові FPV квадрокоптери «камікадзе», як то –

- FPV дрон VR-7D – розроблений МагураВПК,
- FPV-дрон «Шпак» – розроблений Flykrop.,
- безпілотний авіаційний комплекс із назвою "Чорна вдова", дрон-бомбер, безпілотник тактичного рівня дії, може використовуватися і у якості ударного FPV,
- ударний FPV-дрон KH-S7,
- деякі українські дрони, дрони-дракони тепер мають на озброєнні шрапнельні та термобаричні боеголовки,
- безпілотники-перехоплювачі сіткомети компанія Ptashka Drones,
- безпілотник-перехоплювач Sting української групи «Дикі шершні» здатний перехоплювати російські безпілотники-камікадзе іранської розробки Shahed-136
- зенітні дрони, які перехоплюють російські розвідувальні безпілотники Zala і "Орлан-10" та перехоплювачі типу «крило»,
- фахівці компанії AirUnit працюють над FPV-дронами з самонаведенням.

На часі, крім українських, серед популярних моделей дрони для різних цілей та різного рівня користувачів які випускає китайська Компанія DJI. Найбільш актуальна потреба у квадрокоптерах, тобто дронах з чотирма гвинтами:

- DJI Phantom – найпопулярніша та швидкісна лінійка мультикоптерів. Середня швидкість сягає 36 км/год, польотний час – до 15 хвилин. Максимальна швидкість останньої версії модельного ряду 4 Pro складає 70 км/год, а одного заряду акумулятора вистачає на 28 хвилин польотного часу.

- DJI Inspire – модельний ряд квадрокоптерів для професійної аерозйомки. Вони більше за розмірами та вагою, ніж Phantom, а також мають більш розвинені технічні характеристики. Головна особливість – кут огляду камери в 360 °, що уможливило необмежений огляд.

- DJI Mavic – відрізняються мобільністю та високою якістю зйомки, невеликим розміром та триосьовим стабілізатором, що забезпечує якісне зображення. Завдяки портативності їх легко брати із собою навіть на далекі відстані.

- DJI Spark – як і Mavic, компактні та зручні. Дрон Spark може злітати одразу з руки пілота. Швидкість – до 50 км/год, польотний час – 16 хвилин.

- DJI Mini – один з найменших і найлегших дронів, його вага складає всього 249 г. Однак він оснащений триосьовим механічним стабілізатором і дозволяє знімати відео в 2.7K.

- DJI Air 2S – портативний коптер DJI з 1-дюймовою CMOS-матрицею та великим набором функцій. Важить до 600 г, підходить для аерофотозйомки в будь-якому місці та в будь-який час доби.

- DJI FPV – БПЛА з потужною відеокамерою та унікальним керуванням: у оператора створюється ілюзія знаходження всередині дрону.

Радіопротоколи, що використовуються для БПЛА

Найбільш поширені радіопротоколи та вказано особливості їх застосування наведено в табл. 1

Таблиця 1 – Радіопротоколи, що використовуються для БПЛА

Протокол	Частотний діапазон	Ширина смуги	Шифрування	Основні особливості	Приклади застосування
DJI Lightbridge	2.4 ГГц, 5.8 ГГц	Динамічна	AES-256	Пропріетарний протокол DJI, висока стійкість до перешкод, використовується для передачі відео і команд управління.	DJI Phantom, DJI Inspire
DJI OcuSync	2.4 ГГц, 5.8 ГГц	Динамічна	AES-256	Висока якість передачі відео, низька затримка, автоматичний вибір частоти для зменшення перешкод.	DJI Mavic, DJI Air
Wi-Fi	2.4 ГГц, 5 ГГц	20 МГц, 40 МГц	WPA2, WPA3	Використовується для передачі відео і команд управління, відносно низька дальність та висока затримка в порівнянні з спеціалізованими протоколами.	Бюджетні та саморобні дрони
Bluetooth	2.4 ГГц	1 МГц	AES-128	Низька дальність, низька швидкість передачі, використовується для передачі команд управління та телеметрії на невеликих відстанях.	Іграшкові дрони для навчання
ZigBee	2.4 ГГц	2 МГц	AES-128	Низька швидкість передачі, низька енергоспоживання, використовується для передачі команд управління та телеметрії в мережах з великою кількістю вузлів.	Промислові дрони, сільськогосподарські дрони

Протокол	Час- тотний діапа- зон	Ширина смуги	Шиф- рування	Основні особливості	Приклади застосу- вання
Futaba FHSS	S-2.4 ГГц	0.5 МГц	Про- прістарне	Використовується для пе- редачі команд управ- ління, низька затримка, висока стійкість до пере- шкод, використовується в радіоуправлінні моделей літальних апаратів.	Про- фесійні та спортивні дрони
FrSky ACCST	2.4 ГГц	0.5 МГц	Про- прістарне	Висока надійність, низька затримка, можливість ви- користання кількох при- мачів для підвищення надійності сигналу.	Про- фесійні дрони, радіокеро- вані моделі
LoRa	433 МГц, 868 МГц, 915 МГц	Вузька (до 250 кГц)	AES-128	Низька швидкість пере- дачі, висока дальність, слові висока стійкість до пе- решкод, використо- вується для телеметрії та управління на вели- ких відстанях.	Проми- сло- ва та сільсько- госпо- дарські дрони
Xbee	2.4 ГГц, 900 МГц	1 МГц	AES-128	Використовується для передачі команд управ- ління та телеметрії, се- редня швидкість пере- дачі, висока стійкість до перешкод.	Промисло- ві та сіль- ськогоспо- дарські дрони

Протоколи DJI Lightbridge та DJI OcuSync

Технічні аспекти протидії перехопленню

1. **Шифрування: Lightbridge** використовує шифрування для захисту передаваних даних. Це означає, що навіть якщо сигнал буде перехоплено, розшифрувати його без відповідних ключів буде дуже складно.

2. **Частотне хоппінг:** Протокол може використовувати частотне хоппінг (динамічну зміну частот передачі), що ускладнює перехоплення сигналу, оскільки необхідно синхронізуватися з частотами, на яких передаються дані.

3. **Пропрієтарність протоколу:** Lightbridge є пропрієтарним протоколом DJI, що означає, що його специфікації не є загальнодоступними. Це ускладнює розробку пристроїв та програмного забезпечення для перехоплення та аналізу сигналів.

Засоби протидії БПЛА

1. Радіоелектронні перешкоди:

Jamming: Генерація радіошумів, які заглушують сигнали управління та навігації дронів.

Spoofing: Надсилання підроблених сигналів, які імітують легітимні сигнали навігації (наприклад, GPS), щоб змусити дрон змінити маршрут або приземлитися.

2. Перехоплення сигналів:

Signal Interception: Перехоплення та аналіз сигналів управління дронами для визначення їх протоколів і вразливостей.

3. Лазерні системи:

Laser Systems: Використання лазерів для знищення або пошкодження сенсорів і електроніки дронів.

4. Системи фізичного захоплення:

Net Guns: Використання сіток для фізичного захоплення дронів.

Використання РЕБ проти протоколів DJI

1. Проти Lightbridge та OcuSync

– Jamming: Використання широкодіапазонних заглушок для придушення сигналів на частотах 2.4 GHz та 5.8 GHz

– Spoofing: Імітація легітимних сигналів для взяття під контроль дронів або введення їх в помилку.

2. Проти WiFi протоколів:

– Jamming: Придушення WiFi сигналів для розриву зв'язку між дроном та його контролером.

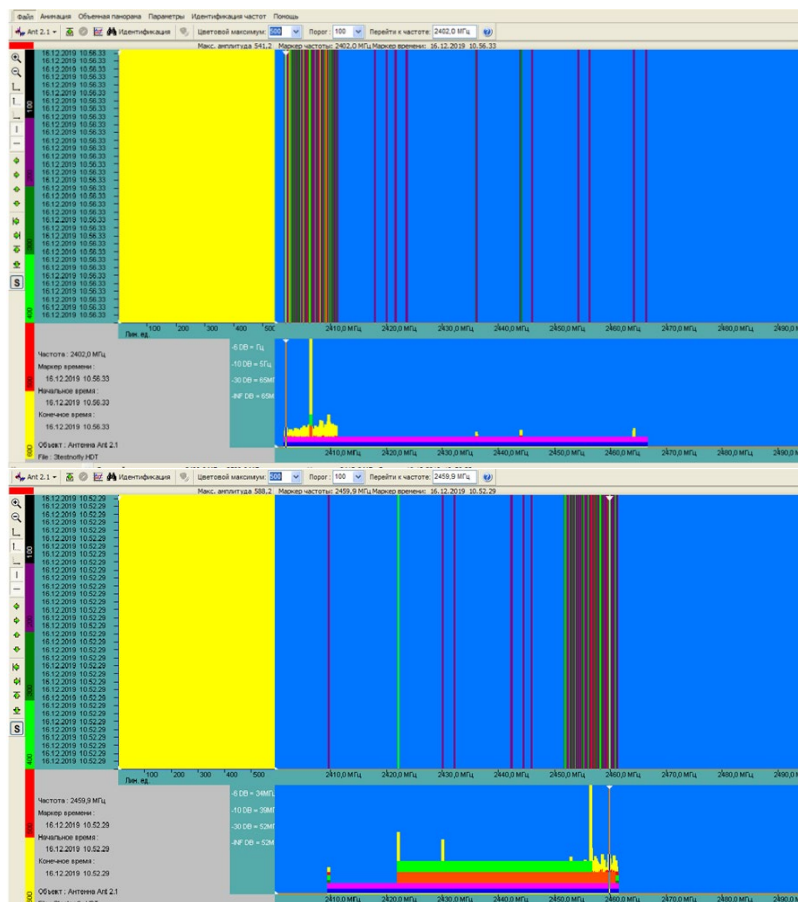
– Signal Interception: Перехоплення і аналіз незашифрованих WiFi сигналів.

3. Проти DroneID:

– Signal Interception: Перехоплення сигналів ідентифікації для збору даних про дрони.

– Spoofing: Імітація DroneID сигналів для введення в оману системи моніторингу.

Результати сканування радіоефіру та дослідження параметрів протоколу обміну виконане на апаратно-програмному комплексі Акор-2 в режимі Hypervisor (див. рис. 1).



**Рисунок 1. – Контроль параметрів протоколу обміну АПК
Акор-2 в режимі Hypervisor**

Висновки

Проведено комплексне дослідження з метою виявлення можливих вразливостей у протоколах, що використовуються для управління безпілотними літальними апаратами (БПЛА).

Ідентифіковано низку потенційних вразливостей в основних протоколах, що використовуються для керування БПЛА, таких як DJI Lightbridge, OcuSync та інші.

Виявлені вразливості включають можливості перехоплення сигналів, здійснення атак типу "відмова у наданні послуг" (DoS) та атаки підміни сигналів (spoofing).

Розроблено рекомендації щодо підвищення безпеки протоколів керування БПЛА, зокрема, впровадження більш стійких методів шифрування та аутентифікації.

Список літератури:

1. Конституція України. – Офіційний вісник України. – 2010, № 72 /1 Спеціальний випуск/, стор. 15, стаття 2598.
2. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року N 514/2009. – Офіційний вісник Президента України. — 2009, № 20, стор. 18, стаття 677.
3. Стратегія кібербезпеки України. Офіційний вісник Президента України від 05.04.2016 – 2016 р., № 10, стор. 39, стаття 198.
4. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року №392/2020. URL – <https://www.president.gov.ua/documents/3922020-35037>
5. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Постанова Кабінету Міністрів України; Порядок від 11.11.2020 №1176. URL – <https://zakon.rada.gov.ua/laws/show/1176-2020-n#Text>.
6. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України. Розпорядження Кабінету Міністрів України; План, Заходи від 19.12.2023 №1163-р. URL – <https://zakon.rada.gov.ua/laws/show/1163-2023-n#Text>.
7. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної

таємниці”, затверджене наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215.

8. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.

9. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.

10. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.

11. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

12. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.

13. Бевз С. І., Стадник В. Я. Посилення адміністративної відповідальності в умовах воєнного стану: окремі аспекти. Юридичний науковий електронний журнал. 2023. №5. С. 193-195. URL – <https://doi.org/10.32782/2524-0374/2023-5/47>

14. Мамка Г. Безпілотники під час війни: законодавче врегулювання та відповідальність за порушення повітряного простору. 25 червня 2023. URL – <https://bdf.gov.ua/bezpilotnyky-pid-chas-viyny-zakonodavche-vrehuliuvannia-ta-vidpovidalnist-za-porushennia-povitriano-ho-prostoru/>

УДК 004.056.5

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ОЦІНЮВАННЯ РИЗИКІВ ГЛОБАЛЬНОЇ МАРШРУТИЗАЦІЇ

***Автор:** Єсипенко А.О., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Актуальність захисту системи глобальної маршрутизації зумовлена зростанням обсягів даних, що передаються через Інтернет, поширенням онлайн-сервісів і практики зберігання інформації в хмарі або банках даних як окремими особами, так і організаціями, державними органами і соціальними групами. Кібербезпека передавання даних через Інтернет забезпечується тільки надійністю системи глобальної маршрутизації, що робить її привабливим об'єктом для зловмисників [1], який має низку переваг у застосуванні:

- дозволяє мати в раз успіху теоретично необмежений вплив на мережу і завдати шкоди у великих масштабах за рахунок ефекту ланцюгової реакції;

- вимагає менших витрат на організацію атаки порівняно з іншими видами розповсюджених кібератак;

- має передумови для успіху організації атак: уразливості у базових протоколах глобальної маршрутизації, високу ймовірність наявності хоча б у одного провайдера недоліків налаштування роутерів, складність узгодження дій всіх провайдерів і операторів для успішної протидії, впровадження підтримуваних Інтернет-спільнотою взаємно узгоджених норм безпеки маршрутизації (англ. Mutually Agreed Norms for Routing Security, MANRS [1]) є добровільним для провайдерів і операторів.

Забезпечення надійності глобальної маршрутизації є особливо актуальним для галузі річкового та морського транспорту, оскільки:

- навігаційні системи, логістичні системи і системи відстеження вантажів передають і приймають дані через незахищене середовище;

- в цій галузі наявна велика кількість стейкхолдерів [2], які обмінюються інформацією через Інтернет, і інтереси яких мають бути враховані при ідентифікації та оцінюванні ризиків;

– водний транспорт відноситься до критичної інфраструктури, і порушення кібербезпеки може спричинити значну шкоду національній безпеці, нормальним умовам життєдіяльності і здоров'ю населення, соціальній сфері, державному суверенітету, економіці та екології [3];

– порушення кібербезпеки водного транспорту може мати негативний вплив на пов'язані з ним інші сектори критичної інфраструктури держави та зарубіжжя.

Розробці методів забезпечення безпеки маршрутизації присвячено роботи багатьох зарубіжних [1, 4, 5] і вітчизняних [6-10] науковців, однак на даний час на ринку відсутні засоби автоматизації, які дозволяли б ефективно впроваджувати MANRS, механізми та засоби протидії найбільш вагомим загрозам маршрутизації.

Метою даної роботи є розробка системи підтримки прийняття рішень (СППР) щодо оцінювання ризиків глобальної маршрутизації.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– провести аналіз відкритих літературних джерел і визначити загрози інформаційній безпеці системи глобальної маршрутизації та особливості методів оцінювання асоційованих з ними ризиків;

– розробити основні алгоритми і структуру СППР щодо оцінювання ризиків глобальної маршрутизації.

Як показав проведений аналіз відкритих літературних джерел, загрозами глобальній маршрутизації є:

- викрадення префіксів або маршрутів;
- виток маршрутів;
- підробка IP адрес.

При цьому в системі глобальної маршрутизації з різною ймовірністю можуть виникати загрози, які за моделлю STRIDE [6] відносяться до наступних типів:

- відмова в обслуговуванні (D) – з дуже високою ймовірністю;
- підміна мережевих об'єктів (S) і розголошування інформації (I) – з високою ймовірністю;
- модифікація даних (T) і відмова від авторства (R) – із середньою ймовірністю;
- підвищення рівня привілеїв (E) – з нульовою ймовірністю.

Наслідки реалізації загроз глобальній маршрутизації можуть бути визначені і оцінені шляхом аналізу накопичених статистичних даних за методикою DREAD згідно з прийнятою бальною шкалою і в узагальненому вигляді на підставі визначеної долі ризиків різних категорій у сумарному ризику. За даними [6, 7]:

- потенційний збиток (D), відтворюваність (R) і область ураження (A) наслідки реалізації загроз глобальній маршрутизації оцінюються як високі;

- легкість організації атаки (E) – як середня;

- складність виявлення (D) може мати оцінки в діапазоні значень Висока-Середня-Низька.

Наслідки реалізації загроз глобальній маршрутизації можуть бути представлені у вигляді ієрархії:

- рівень 1 – хибна інтерпретація або внесені випадково чи цілеспрямовано зміни в таблицю маршрутизації;

- рівень 2 – несанкціонована модифікація напрямку трафіка;

- рівень 3 – дії зловмисника, який отримав несанкціонований доступ до трафіка, із даними (наприклад, накопичення, аналіз, модифікація) і з самим трафіком (наприклад, блокування трафіку чи його частини);

- рівень 4 – результати дій зловмисника на рівні 3 (наприклад, реалізація ddos-атаки, розсилка спаму, переадресація на фальсифікований сайт);

- рівень 5 – наслідки реалізації загроз глобальній маршрутизації для автономних систем;

- рівень 6 – наслідки для бізнес-процесів.

Отримані оцінки ризиків по категоріях моделі DREAD дозволяють обчислити інтегральний ризик, асоційований із загрозами моделі STRIDE. Проведений аналіз показав, що впорядковані за спаданням інтегрального ризику загрози моделі STRIDE можуть бути представлені у вигляді наступного списку:

- 1) підміна мережевих об'єктів (S);

- 2) відмова в обслуговуванні (D);

- 3) розголошення інформації (I);

- 4) модифікація даних (T) і відмова від авторства (R);

- 5) підвищення рівня привілеїв (E).

При оцінюванні ризиків глобальної маршрутизації слід враховувати їх особливості, визначені в [9]:

– джерелом загроз, з якими асоціюються ризики, зазвичай є суб'єкти глобальної маршрутизації (загрози типів А – цілеспрямована діяльність суб'єктів і D – випадкові помилки суб'єктів за ДСТУ ISO/IEC 27005:2023 [11]);

– загрози реалізуються через вразливості протоколів маршрутизації, налаштувань роутерів і недоліки організаційного забезпечення інформаційної безпеки;

– наслідки реалізації загроз є взаємопов'язаними і утворюють ієрархічну систему як за послідовністю так і за структурними складовими інформаційно-комунікаційних систем, де вони проявляються.

Узагальнений алгоритм оцінювання ризиків у розроблюваній СППР наведено на рис.1.

Алгоритм оцінювання узагальнених показників ризиків за оцінками ризиків R_{ij} , який застосовується на етапі «Кількісна оцінка ризику» рис.1 наведено на рис.2. При цьому оцінки ризиків R_{ij} представлені у вигляді матриці, в якій $i \in \{S, T, R, I, D, E\}, j \in \{Dam, R, E, A, Dis\}$. Узагальненими показниками ризиків є суми ризиків за категоріям моделей DREAD та STRIDE, загальний сумарний ризик, долі ризиків, що відповідають категоріям моделей DREAD та STRIDE, інтегральний інтегральний ризик для кожної і-ої загрози, який розраховується як $0,2 \sum_j R_{ij}$. Оцінювання ризиків здійснюється за обраною шкалою, для

котрої визначені одиниці вимірювання O , кількість діапазонів H , ліва і права границі кожного h -го діапазону ($\{gl_h, gr_h\}$), де $h=1, 2, \dots, H$), множина можливих якісних оцінок ризиків $\{Y_h\}$, в якій Y_h є лінгвістичними термами (наприклад, Нульовий, Дуже низький, Низький, Середній, Високий, Дуже високий). Ризики R_{ij} кількісно оцінюються експертним шляхом, а якісно – за наступними правилами: Y_1 , якщо $R_{ij} < gl_1$; Y_h , якщо $gl_h \leq R_{ij} < gr_h$ і $h \neq 1, h \neq H$; Y_H , якщо $R_{ij} \geq gr_H$. Аналогічно визначаються якісні оцінки узагальнених показників ризиків.

Структура СППР, в якій реалізуються розроблені алгоритми, наведена на рис.3

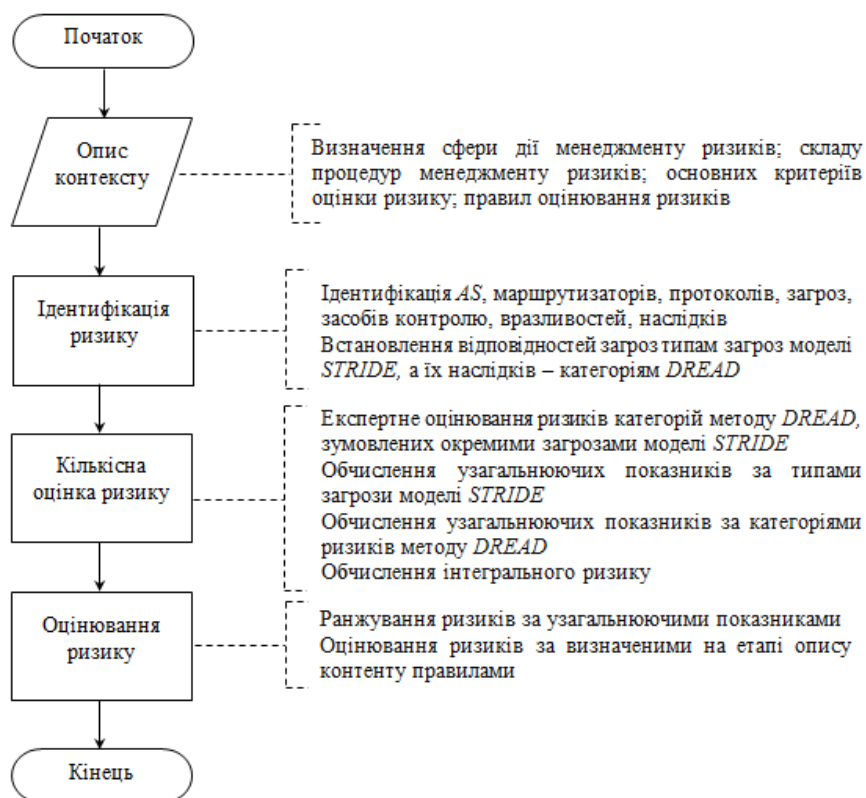


Рисунок 1 – Узагальнений алгоритм оцінювання ризиків

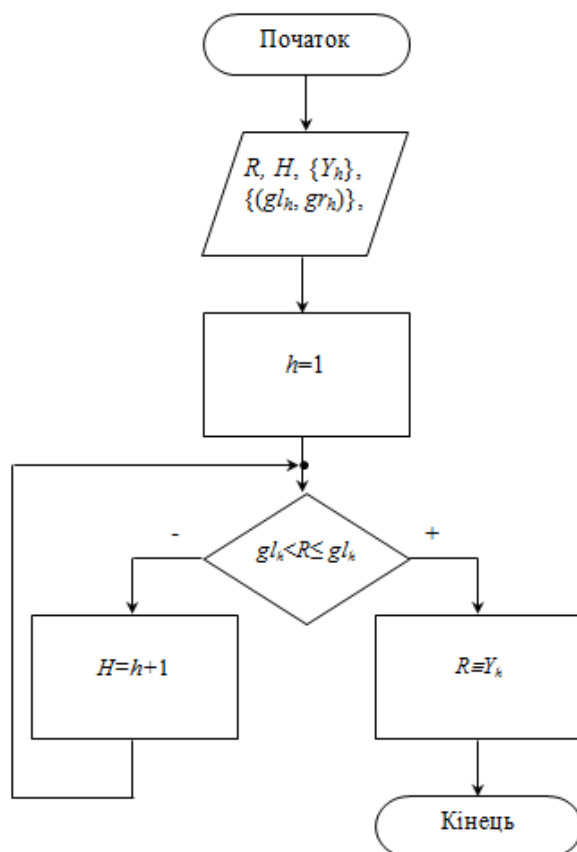


Рисунок 2 – Алгоритм оцінювання узагальнених показників ризиків

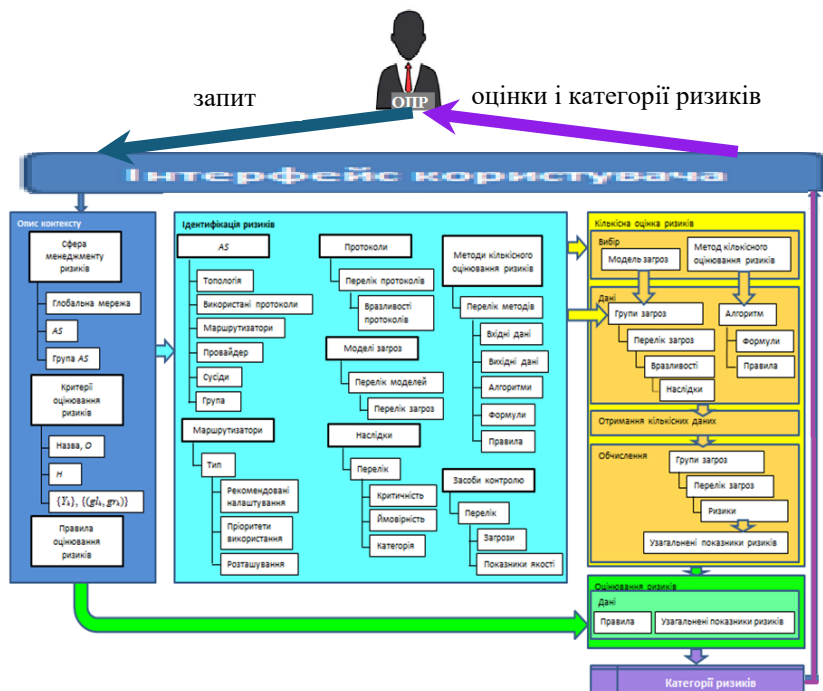


Рисунок 3 – Структура СППР

Висновки

В даній роботі проведено аналіз відкритих літературних джерел і визначені загрози інформаційній безпеці системи глобальної маршрутизації та особливості методів оцінювання асоційованих з ними ризиків, розроблено базові алгоритми і структуру СППР щодо оцінювання ризиків глобальної маршрутизації загрози

Список літератури:

1. MANRS: Protect the Internet URL: <https://www.manrs.org/>
2. IAPH Cybersecurity Guidelines for Ports and Port Facilities. URL: https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf
3. Про критичну інфраструктуру. Закон України URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

4. Jiajia L., Yih-Chun H., Mingwei X., Jianping W. BGP with BGPsec: Attacks and Countermeasures. IEEE Network. 2019. Vol. 33. Issue 4. PP. 194-200. URL: <https://ieeexplore.ieee.org/document/8594708>

5. Lakshmanan R. Researchers Uncover New BGP Flaws in Popular Internet Routing Protocol Software. URL: <https://thehackernews.com/2023/05/researchers-uncover-new-bgp-flaws-in.html>

6. Зубок В.Ю. Оцінювання ризиків глобальної маршрутизації. Електронне моделювання. 2019. Т.41. №2. С.97-109. URL: <https://www.emodel.org.ua/images/em/41-2/Zubok.pdf>

7. Зубок В.Ю. Мохор В. В. Кібербезпека топології INTERNET: монографія. К.: ПІМЕ ім. Г.Є.Пухова, 2022. 191 с. URL: https://ipme.kiev.ua/wp-content/uploads/2022/07/Zubok_Mokhor_Kiberbezpeka_Topologii_Internet.pdf

8. Патент України №107617 Н04L 12/00, МПК (2016.01). Спосіб маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог інформаційної безпеки / Снігуров А.В., Чакрян В.Х.; власник Харківський національний університет радіоелектроніки. – № u201600667; заявл. 27.01.2016; опубл. 10.06.2016, бюл. № 11

9. Турти М.В. Загрози глобальній маршрутизації в сучасному кіберпросторі. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК, 2023. С.83-92. URL: <https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf>

10. Чакрян В.Х. Моделі та методи маршрутизації трафіку в телекомунікаційних мережах з урахуванням вимог інформаційної безпеки. Кваліфікаційна наук. праця на правах рукопису. Дисертація на здобуття наук. ступеня канд. техн. наук (доктора філософії) за спеціальністю 05.12.02 «Телекомунікаційні системи та мережі» (172 – Телекомунікації та радіотехніка). – Харківський нац. ун-т радіоелектроніки, Харків, 2017. URL: https://nure.ua/wp-content/uploads/2018/Dissertation/diss_Chakryan.pdf

11. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. URL: https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400

УДК 004.056.5;057.2

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО КАТЕГОРИЗАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

***Автор:** Злочевська О.В., магістрантка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Критична інфраструктура (КІ) будь-якої країни характеризується покладеними на неї особливими функціями, що є життєво важливими для населення та держави. При цьому порушення у виконанні цих функцій певним об'єктом критичної інфраструктури (ОКІ) з належними показниками якості може мати негативний вплив не тільки в межах однієї країни, а й зачіпати інтереси інших країн, КІ котрих є взаємопов'язаними фізично або за економічними і політичними договорами [1, 2]. Наявні в сучасному світі тенденції до зростання організованої злочинності і до посилення екстремізму та тероризму знаходять своє віддзеркалення в кіберпросторі. При цьому типово злочинні технології, зокрема хакерські атаки, використовуються за підтримки урядів як для проведення інформаційних так і для проведення звичайних військових і терористичних операцій. Тому забезпечення безпеки КІ є складовою задачі забезпечення національної безпеки особливо в Україні, в умовах військового стану.

Розв'язок проблеми захисту КІ вимагає комплексного вирішення питань нормативно-правового, організаційного, технологічного і технічного забезпечення з врахуванням ступеня критичності кожного ОКІ і кожного об'єкта критичної інформаційної інфраструктури (ОКІІ). Цій проблемі присвячені роботи багатьох науковців [3-9], однак забезпечення кіберготовності і кіберстійкості КІ вимагає в умовах динамічного кіберпростору багатократного аналізу стану інформаційної безпеки (ІБ) на ОКІ і швидкого прийняття адекватних рішень, що неможливо без впровадження засобів автоматизації.

Метою даної роботи є розробка структури системи підтримки прийняття рішень щодо категоризації об'єктів критичної інфраструктури.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- провести аналіз відкритих літературних джерел і визначити типові процедури категоризації ОКІ, їх алгоритми, вхідні та вихідні дані системи підтримки прийняття рішень (СППР) щодо категоризації ОКІ;

- розробити структуру СППР щодо категоризації ОКІ.

Нормативно-правову базу категоризації ОКІ в загальному випадку складають:

- Директиви Європейського Союзу [1, 2];
- Закони України: «Про критичну інфраструктуру» [10], «Про основні засади забезпечення кібербезпеки України»;
- Стратегія кібербезпеки України та План реалізації Стратегії кібербезпеки України;
- Постанови Кабінету міністрів України: №518 (2019 рік), № 943 (2020 рік), №1109 (2020 рік), №821 (2022 рік);
- Наказ № 23 Адміністрації ДССЗІ (2021 рік).

При цьому протягом 2020-2024 років ці документи неодноразово коригувалися. Для конкретного сектору і підсектору можуть бути наявні додаткові документи у вигляді нормативних документів (наприклад, «Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг», затверджене Постановою № 4 Правління Національного банку України від 16.01.2021) або рекомендацій (наприклад, Recommendation on Cyber Resilience, розроблені Міжнародною асоціацією класифікаційних товариств для морської галузі).

Методичну основу категоризації ОКІ складають:

- Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави, затверджений Постановою КМУ №1109;
- Порядок віднесення об'єктів до об'єктів критичної інфраструктури затверджений Постановою КМУ №1109;
- Порядок формування переліку об'єктів критичної інфраструктури, затверджений Постановою КМУ № 943;
- Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної

інфраструктури, його формування та забезпечення функціонування, затверджений Постановою КМУ № 943;

- Методика категоризації об'єктів критичної інфраструктури, затверджена Постановою КМУ №1109 [11];
- Методичні рекомендації щодо категоризації об'єктів критичної інфраструктури, затверджені Наказом № 23 Адміністрації ДССЗІ [12];
- Порядок здійснення моніторингу оцінки рівня безпеки об'єктів критичної інфраструктури, затверджена Постановою КМУ №821.

Аналіз нормативних документів дозволив виявити наступні типові процедури категоризації ОКІ:

- створення державою списку основних послуг, надання яких визначає належність досліджуваного об'єкта до ОКІ, із визначеними секторами і під секторами і відповідальними органами;
- створення робочої групи в межах сектору або під сектору;
- ідентифікація ОКІ у відповідному секторі або під секторі КІ;
- проведення категоризації ОКІ;
- проведення категоризації ОКІІ;
- створення секторального переліку ОКІ;
- подання відомостей щодо категорованих ОКІ галузі до Національного переліку ОКІ і формування державного реєстру ОКІ;
- моніторинг оцінки рівня безпеки ОКІ.

Наведені типові процедури представлені у порядку їх виконання, і кожна з них здійснюється за окремим алгоритмом. Зокрема, віднесення ОКІ до певної категорії критичності [11, 12] здійснюється шляхом визначення інтервалу, в який потрапле нормована оцінка критичності PK_{OKI} даного ОКІ, отримана за секторальними і міжсекторальними критеріями оцінювання. Віднесення об'єкта інформаційної інфраструктури до ОКІІ даного ОКІ – на підставі висновку про суттєвий вплив об'єкта інформаційної інфраструктури на процес виконання ОКІ його основних функцій, що отримується шляхом перевірки ряду умов. Узагальнений алгоритм категоризації та відповідна інформаційна модель наведені в [9] і охоплюють процедури оцінювання за секторальними і міжсекторальними критеріями.

Прийняття рішень стосовно категоризації ОКІ здійснюється за ієрархічною схемою. На міжнародному рівні приймаються рішення щодо

визначень критичних інфраструктур, принципів їх захисту і взаємодії держав у цій галузі. На основі міжнародних нормативних документів і міжнародних договорів на рівні держави:

- приймаються рішення щодо основних функцій ОКІ, секторів і підсекторів критичної інфраструктури держави, порядку формування національних реєстрів;

- визначаються відповідальні за процедури категоризації та ведення реєстрів особи і структурні підрозділи на рівні держави та правила формування відповідальних структурних підрозділів і осіб на рівні секторів (робочих груп);

- визначається формат і порядок документообігу з категоризації;
- визначаються критерії оцінювання критичності, рівні критичності і умови віднесення до них ОКІ та ОКІІ;

- розробляються та оприлюднюються методики оцінювання рівнів критичності.

На рівні секторів приймаються рішення щодо:

- створення робочих груп;
- ведення секторальних переліків ОКІ та ОКІІ;
- передавання даних до національних реєстрів;
- порядку моніторингу оцінки рівня безпеки ОКІ;
- розробляються пропозиції щодо змін до доповнень переліків основних функцій ОКІ, секторів і підсекторів критичної інфраструктури держави.

На рівні робочої групи приймаються рішення щодо:

- категоризації ОКІ;
- категоризації ОКІІ;
- оцінювання рівня безпеки ОКІ та його динаміки за результатами моніторингу;

- необхідності удосконалення систем захисту ОКІ.

На рівні ОКІ приймаються рішення щодо:

- застосування певних методів і засобів захисту ОКІ та моніторингу його рівня безпеки;
- визначення можливих наслідків порушень виконання основних функцій ОКІ;

– визначення можливих наслідків порушень функціонування об'єктів інформаційної інфраструктури ОКІ;

– визначення ступеня впливу об'єктів інформаційної інфраструктури ОКІ на виконання ОКІ його основних функцій.

На міжнародному рівні, рівні держави і секторів приймаються організаційні рішення, а на рівні ОКІ – рішення щодо організаційного і технічного захисту ОКІ, рішення щодо взаємного впливу структурних складових ОКІ, рішення щодо наслідків порушення штатного функціонування структурних складових ОКІ та ОКІ в цілому. Рішення, прийняті на цих рівнях є вхідними даними для прийняття рішень на рівні робочої групи. На кожному рівні до СППР повинні мати доступ користувачі із різними правами.

Структура СППР має містити:

1) блок інтерфейсу із розмежуванням прав доступу;

2) блок даних, які поділяються на:

– вбудовані дані, визначені на рівні держави;

– відносно статичні дані, визначені на рівні секторів і підсекторів, які стосуються робочих груп, секторальних переліків ОКІ та ОКІІ, а також містять відомості, які необхідні для заповнення звітної документації на рівні робочої групи, під секторів і секторів;

– динамічні дані, визначені на рівні ОКІ;

3) блок оцінювання критичності;

4) блок формування звітності.

Висновки

В даній роботі проведено аналіз відкритих літературних джерел і визначені типові процедури категоризації ОКІ, їх алгоритми, вхідні та вихідні дані СППР щодо категоризації ОКІ, розроблена структура СППР.

Список літератури:

1. Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 06 липня 2019 року "Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу". URL: https://zakon.rada.gov.ua/rada/show/984_013-16#n3

2. Директива Ради 2008/114/ЄС від 08 грудня 2008 року "Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту". URL: https://zakon.rada.gov.ua/rada/show/984_002-08#n4

3. Limba, Tadas, et al. Cyber security management model for critical infrastructure. (2019). *The International Journal Entrepreneurship and Sustainability*. Issues ISSN 2345-0282 (online) URL: [http://jssidoi.org/jesi/2017/Volume 4 Number 4 \(June\) http://doi.org/10.9770/jesi.2017.4.4\(12\)](http://jssidoi.org/jesi/2017/Volume%204/Number%204/(June)/http://doi.org/10.9770/jesi.2017.4.4(12))

4. Osei-Kyei, Robert, et al. Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reductio*. V.60 (2021): 102316. URL: <https://www.sciencedirect.com/science/article/abs/pii/S221242092100282X>

5. Бірюков Д. С. Захист КІ в Україні: від наукового осмислення до розробки засад політики. *Науково-інформаційний вісник Академії національної безпеки*. 2015. № 3-4. С. 155-170. – URL: http://nbuv.gov.ua/UJRN/nivanb_2015_3-4_14.

6. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. К.: ДУТ, 2015. 288 с. URL: http://www.dut.edu.ua/uploads/p_r_303_79299367.pdf

7. Зелена книга з питань захисту КІ в Україні (друга версія проекту документа). URL: https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf

8. Рогов П.Д., Ворович Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері. *Зб. наук. праць Центру воєнно-стратегічних досліджень Національного університету оборони України ім. Івана Черняховського*. 2017. № 1. С. 64-72. URL: <http://znpcvds.nuou.org.ua/article/view/125525>

9. Турти М.В., Злочевська О.В. Інформаційна модель категоризації об'єктів критичної інфраструктури. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали X Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК, 2022. С.140-147. URL: <https://www.nuos.edu.ua/wp-content/uploads/2023/05/SPIBT-2022-Materiali-s-obkladinkoju.pdf>

10. Закон України "Про критичну інфраструктуру". URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

11. Методика категоризації об'єктів КІ, затверджена Постановою Кабінету міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури» від 9 жовтня 2020 р. №1109. URL: <https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#Text>

12. Наказ № 23 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів КІ». URL: <https://zakon.rada.gov.ua/rada/show/v0023519-21#Text>

УДК 004.056.53

АНАЛІЗ СИСТЕМИ ЗАХИСТУ ПЛАТФОРМИ BLYNK

***Автор:** Зобова Е.В., студентка, Національний університет кораблебудування імені адмірала Макарова, Миколаїв, Україна*

***Науковий керівник:** Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ.

Інтернет речей (IoT) — це інформаційна мережа фізичних об'єктів (датчиків, машин, автомобілів, будівель та інших предметів), яка об'єднує всі ці об'єкти та дозволяє їм взаємодіяти один з одним для досягнення спільних цілей.

У наш час, коли світ стрімко рухається до цифрової трансформації, Інтернет речей стає невід'ємною частиною нашого життя. Мільярди пристроїв, від смартфонів до промислових датчиків, підключені до мережі, створюючи безмежні можливості для автоматизації та аналізу даних. Однак, разом із зростанням кількості підключених пристроїв, зростають і ризики. Киберзагрози, такі як хакерські атаки, віруси та шкідливе програмне забезпечення, стають все більш витонченими та спрямованими на вразливість IoT-систем. Захист цих систем набуває критичного значення, оскільки від цього залежить безпека не тільки окремих користувачів, але й цілих інфраструктур.

Метою роботи є дослідити вбудовані системи захисту для середовища розробки Інтернет речей – Blynk.

Основна частина.

Blynk — це повний набір програмного забезпечення, необхідного для прототипування, розгортання та віддаленого керування підключеними електронними пристроями будь-якого масштабу: від персональних IoT проєктів до мільйонів комерційних підключених продуктів.

Користувачами системи, є як новачки в розробці електронних пристроїв так і професійні розробники. Розробник Blynk — це спеціальний

користувач, який має доступ до всіх функцій, необхідних для налаштування платформи для використання кінцевими користувачами (їх також називають клієнтами або кінцевими клієнтами).

Велика аудиторія користувачів Blynk вимагає спеціалізованого захисту продукції, що випускається. Наразі Blynk має прив'язку кожного пристрою до мережі за допомогою унікальних ідентифікаторів та захист при передачі даних.

Прив'язка пристрою до системи Blynk може бути реалізована трьома способами:

1. Активація пристроїв за допомогою згенерованих вручну AuthTokens. Цей метод рекомендується для етапів прототипування або коли ви створюєте пристрій для себе та маєте доступ до його вихідного коду.

2. Налаштування Wi-Fi за допомогою Blynk.Inject. Для підтримування пристроїв, які можуть підключатися до Інтернету через Wi-Fi, ви можете використовувати метод надання Wi-Fi, вбудований у Blynk.Apps.

Цей метод особливо корисний для комерційних застосувань, оскільки:

- ви заздалегідь не знаєте, до якої мережі Wi-Fi ваші клієнти підключатимуть ваші пристрої

- це спрощує процес виробництва в масштабі, оскільки ви використовуєте той самий код без необхідності вручну додавати AuthToken до кожного пристрою.

3. Активація статичного токена. Цей метод зазвичай використовується в комерційних програмах, коли потрібно розгорнути велику кількість пристроїв, і їх потрібно буде активувати кінцевим клієнтам.

Захист системи обміну полягає в наступному:

- серверна система спроектована так, що тільки користувачі з наданим вами доступом можуть переглядати пристрої в ієрархії вашої організації. Постійний моніторинг забезпечує швидке реагування на потенційні інциденти.

- повідомлення, надіслані через Blynk, залишаються зашифрованими та захищеними, якщо використовується апаратне забезпечення з підтримкою TLS.

- деталізовані дозволи забезпечують контроль над тим, хто і як може отримувати доступ до ваших пристроїв та їхніх даних.
- кожен пристрій оснащений унікальним маркером OAuth і ідентифікатором продукту, комбінація яких забезпечує доступ до пристрою виключно для вашої організації.

Для захисту обміну між пристроями Blynk здебільшого використовує галузеві стандарти, зокрема протокол безпеки транспортного рівня TLS. За замовчуванням сервер Blynk намагається застосовувати найновішу версію протоколу TLSv1.3, або TLSv1.2, якщо версія TLSv1.3 не підтримується.

База даних, що використовуються в пристроях не мають доступу до Інтернету, а доступ до неї можливий лише з приватної мережі. База даних, за замовчуванням, зберігаються в відкритому, незашифрованому вигляді. Шифрування їх доступне як платне доповнення для рішення white-label.

Висновок. У процесі дослідження вбудованих систем захисту для середовища розробки Інтернету речей (IoT) на платформі Blynk було встановлено, що дане середовище використовує низку потужних механізмів безпеки для забезпечення конфіденційності, цілісності та доступності даних. Важливою особливістю є використання сучасних протоколів шифрування, зокрема TLS, для захисту переданих даних між хмарою та базою даних, що мінімізує ризики несанкціонованого доступу до інформації.

Окрім того, ізоляція бази даних в приватній мережі та обмежений доступ до Інтернету гарантують високий рівень захищеності від зовнішніх загроз.

Хоча шифрування самої бази даних не є обов'язковим за замовчуванням, наявність можливості його підключення як платного доповнення забезпечує гнучкість в адаптації до специфічних вимог безпеки користувача.

Загалом, Blynk представляє надійне середовище для розробки IoT-проектів з високими стандартами безпеки, що дозволяє користувачам зберігати контроль над доступом до своїх даних та пристроїв. Однак для підвищення рівня захисту в критичних застосуваннях рекомендується використовувати додаткові можливості шифрування та налаштування безпеки, запропоновані платформою.

РОЗРОБКА РЕКОМЕНДАЦІЙ З ПОКРАЩЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АС-2 ТА АС-3 КЛАСІВ 4 КАТЕГОРІЇ ДЛЯ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Автор: Мацибура Д.О., магістрант, ВЧ; Мельничук О.Ю., магістрант, відділ ЗІ Південноукраїнська АС; Шевченко В.В., магістрант, відділ ЗІ Південноукраїнська АС, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Морський транспортний комплекс є багатофункціональною структурою, що задовольняє потреби національної економіки у транспортному забезпеченні. Від ефективності функціонування морських портів, рівня їх технологічного та технічного оснащення, відповідності системи управління та розвитку інфраструктури сучасним міжнародним вимогам залежить конкурентоспроможність вітчизняного транспортного комплексу на світовому ринку.

Після вторгнення РФ портова галузь України була паралізована. Чотири морські порти – Херсонський, Скадовський, Бердянський та Маріупольський, частка яких у загальній переробці вантажів усіма морськими портами України у 2021 р. становила 7,2 %, або 11,1 млн т на рік, окуповані. Ще шість портів – Білгород-Дністровський, Одеський, Миколаївський, Чорноморськ, Ольвія та Південний змушені були призупинити роботу на відвантаження через небезпеку морських перевезень та загрозу обстрілів.

Одним з проявлень незаконних дій спецслужб РФ та їх союзників (хакерів з КНДР та Ірану) є масовані кібератаки на інформаційні ресурси України, в тому числі й на об'єкти критичної інфраструктури водно-транспортного комплексу України. За інформацією Голови Держспецзв'язку Юрія Щиголя з початку повномасштабного вторгнення Росія здійснила 796 кібератак проти України. З них майже 18,5 % на сервери уряду України та місцеві органи влади та 13 % на сектор безпеки та оборони [1].

Робота присвячена актуальному питанню – на основі методичних рекомендацій щодо конфігурування параметрів безпеки операційної системи Windows 11 Professional в автоматизованих системах класу 2 та 3 розробка апаратно-програмного засобу автоматичного налаштування (конфігурування) політики безпеки операційної системи Windows 11 Professional для автоматизованої системи 2 та 3 класів 4 категорії. Розроблено програмний варіант автоматичного налаштування конфігурування параметрів безпеки та методика ручної перевірки штатними засобами налаштувань параметрів безпеки операційної системи Windows 11 Professional при створенні комплексної системи захисту інформації на об'єкті критичної інфраструктури.

Для досягнення поставленої мети в роботі вирішувались наступні **задачі**:

1) Проаналізовано законодавчу та нормативно-правову базу України щодо захисту інформації з обмеженим доступом (ІзОД) в інформаційно-комунікаційних системах (ІКС).

2) Розглянуто основні принципи побудови систем захисту інформації в Україні та світі.

3) Проведено аналіз особливостей створення та експлуатації комплексної системи безпеки АС 2 та 3 класів 4 категорії.

4) Проведено аналіз виявлених вразливостей та запропоновано рекомендації по вдосконаленню налаштування політики безпеки операційної системи Windows 11 для автоматизованої системи 2 та 3 класів 4 категорії.

Об'єктом дослідження є системи захисту інформації з обмеженим доступом в інформаційно-комунікаційних системах на основі АС 2 та 3 класів 4 категорії.

Предметом дослідження є апаратно-програмні засоби налаштування політики безпеки операційної системи Windows 11 для автоматизованої системи 2 та 3 класів 4 категорії.

Практичною значимістю результатів кваліфікаційної роботи є запропоновані рекомендації по вдосконаленню налаштування політики безпеки операційної системи Windows 11 для автоматизованої системи 2 та 3 класів 4 категорії.

Для вирішення поставлених завдань було застосовано низку загальнонаукових та **спеціальних методів наукового пізнання**. Метод

узагальнення використовувався для аналізу сучасного стану та проблем у сфері забезпечення інформаційної безпеки; метод порівняння та аналогії – для аналізу досвіду інших країн – країн ЄС, США та інших. Системний метод також використовувався для аналізу нормативно-правової бази.

Методологічною основою дослідження є теоретичний розвиток правової та технічної думки у світі, концептуальні положення щодо сучасного стану захисту інформації та інформаційної безпеки, дослідження вітчизняних і зарубіжних вчених та міжнародних організацій з питань захисту інформації та інформаційної безпеки.

Емпіричною базою дослідження є національне та міжнародне нормативно-правове законодавство, архівні матеріали та офіційні публікації з даної тематики.

Об'єктом ОІД для якої створюється КСЗІ є одним із важливіших підрозділів порту задіяних в організації захисту інформації на об'єкті – РСО.

Комплекс ТЗІ створюється за рішенням (наказом) керівника підприємства морської галузі (порту, судноплавної компанії або ін.) про створення комплексу ТЗІ.

Комплекс ТЗІ створюється за такими етапами:

I етап – попередній етап створення комплексу СЗІ;

II етап – проектування і розробка комплексу СЗІ;

III етап – проведення випробувань і передачі в експлуатацію комплексу СЗІ.

Після упровадження проводиться атестація КСЗІ.

Перед створенням комплексу СЗІ визначаються об'єкт інформаційної діяльності та контрольована зона.

У наказі керівника підприємства про визначення об'єкта інформаційної діяльності встановлюється, яка саме інженерно-технічна споруда (приміщення), зона територія або транспортний засіб (із зазначенням відповідної назви, приналежності, адреси, номера приміщення, позначення тощо) є об'єктом інформаційної діяльності, також надається план споруди (зони, території) із зазначенням контуру ОІД, розмірами ОІД та стислим описом розташування ОІД у споруді (місцевості).

У Наказі про визначення контрольованої зони встановлюється межа контрольованої зони навколо ОІД (споруди, в якій розташована

ОІД), надається її опис, вказуються відстані від межі КЗ з точною межею (периметром або контуром).

Визначення об'єкта інформаційної діяльності та контрольованої зони, а також прийняття рішення щодо створення комплексу ТЗІ можуть вказуватися в одному наказі.

Розроблюється Положення про Службу захисту інформації, яка визначить завдання, функції, штатну структуру СЗІ в ІКС. Метою створення СЗІ є організаційне забезпечення завдань керування КСЗІ в ІКС та здійснення контролю за її функціонуванням. На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в АС, проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в АС.

Правову основу для створення і діяльності СЗІ становлять Закон України “ Про захист інформації в інформаційно-телекомунікаційних системах”, Положення про технічний захист інформації в Україні, Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах.

Розроблюється положення про службу захисту. План захисту є обов'язковим документом в установах, організаціях, в яких здійснюється обробка службової інформації в інформаційно-комунікаційних системах (ІКС).

Актуальність роботи обумовлена тим, що підприємства морської галузі відносяться до об'єктів критичної інфраструктури водно-транспортного комплексу [2], від безпеки інформаційних потоків яких залежить сталий розвиток всіх сфер життєдіяльності держави і суспільства [3].

Метою даної роботи є підвищення захищеності підрозділу режимно-секретного органу морського порту від витоку інформації за рахунок впровадження комплексної системи захисту інформації.

Для реалізації поставленої цілі в даній кваліфікаційній роботі було проведено аналіз нормативно-правових документів у сфері технічного захисту інформації, проаналізовано особливості морського порту як об'єкту інформаційної діяльності та розроблення проекту по впровадженню комплексної системи захисту інформації режимно-секретного відділу морського порту. Результати роботи призначені для використання при побудові комплексної системи захисту інформації на об'єктах морської інфраструктури та можуть бути використані в

навчальному процесі для здобуття студентами практичних навичок у відповідності з напрямками підготовки з кібербезпеки.

Висновки

В роботі було проведено огляд нормативних документів, щодо захисту інформації на об'єктах портової галузі. Виконано аналіз особливостей порту як ОІД основних загроз інформації, було розроблено проект по комплексній системі захисту інформації режимно-секретного відділу морського порту та повний комплект для впровадження.

Було розроблено програмний варіант автоматичного налаштування та методика ручної перевірки штатними засобами налаштувань параметрів безпеки операційної системи Windows 11 Professional при створенні комплексної системи захисту інформації на об'єкті критичної інфраструктури.

Розроблена КСЗІ відповідає вимогам відповідних нормативним правових документів. Показано в результатах, що дана КСЗІ відповідає вимогам і дає можливість продовжити з нею працювати від реєстрації до встановлення на реальному об'єкті інформаційної діяльності пов'язана не лише з морською галуззю, а й із всіма іншими.

Список літератури:

1. Росія – законна ціль. Інтерв'ю Голови Держспецзв'язку України Юрія Щиголя про санкції та невдалі кібератаки РФ. [URL]: <https://glavcom.ua/techno/telecom/golova-derzhspeczvyazku-rozpoviv-pro-kilkist-kiberatak-rf-proti-ukrajini-z-pochatku-vtorgnennya-857009.html>
2. Порядок формування переліку об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943 [URL]: <https://zakon.rada.gov.ua/laws/show/943-2020-p>.
3. Про внесення змін до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інфраструктури [Текст]: Наказ адміністрації державно\ служби спеціального зв'язку та захисту інформації України від 10 липня 2021 р. № 343 [URL]: <https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601>

РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ ТА ІНФОРМУВАННЯ ПРО ВІДМОВИ В РОБОТІ ІНТЕРНЕТ-СЕРВІСІВ

***Автор:** Ніколаєв В.Д., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Козирєв С.С., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Анотація. У статті розглядається задача розробки системи моніторингу інтернет-сервісів, яка автоматично виявляє відмови в роботі інтернет-сервісів та негайно сповіщати адміністраторів про відмови у роботі інтернет-сервісів. Система моніторингу інтернет-сервісів є важливою складовою сучасної інфраструктури бізнесу, так, як допомагає мінімізувати можливі втрати, що виникають через відмови, а також підвищує швидкість реагування на критичні ситуації. Дана система моніторингу інтернет-сервісів поєднує в собі автоматизацію моніторингу та сповіщення про відмови, що дозволяє користувачу мати надійну, сучасну та ефективну систему моніторингу інтернет-сервісів з достатнім рівнем масштабованості, що підходить як для малих компаній, так і для великих підприємств.

Ключові слова: система моніторингу, інтернет-сервіси, відмови, сповіщення, автоматизація, повідомлення, масштабованість.

Вступна частина. Інтернет-сервіси стали критично важливими для функціонування сучасного бізнесу та невід'ємною частиною економіки сучасності. Ефективна робота інтернет-сервісів критично важлива для безперебійної діяльності бізнесу, що передбачає високі вимоги до їх доступності, масштабованості та надійності. Відмови інтернет-сервісів можуть призвести до затримок у виконанні важливих процесів, значних фінансових і репутаційних втрат. Тому ефективний моніторинг таких інтернет-сервісів є необхідним для забезпечення їх безперебійної роботи. Сучасні інструменти моніторингу мають певні обмеження, тому було обрано підхід, що поєднує кращі практики та інструменти для розробки ефективної та масштабованої системи моніторингу, яка здатна автоматично виявляти відмови та сповіщати користувачів. Сучасні інструменти моніторингу інтернет-сервісів, такі як Nagios, Zabbix, та Pingdom, забезпечують контроль за станом інтернет-

сервісів, але часто мають обмежену функціональність або не можуть бути адаптовані під специфічні вимоги та не мають достатню масштабованість і доступність. У зв'язку з цим виникає потреба в розробці більш гнучкої, ефективної та масштабованої системи, що дозволить швидко та надійно виявляти відмови, а також повідомляти про відмови користувача у реальному часі.

Метою роботи є розробка автоматизованої системи моніторингу для інтернет-сервісів, яка здійснює перевірку їх працездатності в режимі реального часу, своєчасно сповіщає про виникнення відмов та має зручний інтерфейс користувача, що забезпечує комфортне управління.

Основна частина. Система складається з моніторингового серверу, який відповідає за регулярну перевірку доступності інтернет-сервісів, а саме здійснює запити до сервісів через API для визначення їх доступності. Бази даних, в якій зберігаються результати перевірок. Інтерфейсу користувача, що дозволяє користувачу зручно переглядати статус інтернет-сервісів, налаштовувати параметри моніторингу.

У роботі був використаний метод API-запитів для перевірки доступності інтернет-сервісів. У разі виявлення відмови або збоїв у відповіді спрацьовує механізм сповіщення. Користувач має можливість вибрати декілька типів сповіщень, а саме надіслати лист на електронну пошту, або увімкнути Push-повідомлення у браузері.

Система реалізує можливість проведення перевірки доступності інтернет-сервісів постійно, у потрібний момент або регулювання перевірки за часом, для того щоб забезпечити швидкоку реакцію на відмови та можливість гнучкого налаштування.

Після завершення розробки системи були проведено тестування для оцінки точності моніторингу, що підтвердило правильність системи моніторингу інтернет-сервісів визначення доступності інтернет-сервісів, швидкості сповіщень та навантаження в умовах великої кількості сервісів для моніторингу. Результати тестувань виявили достатній рівень ефективності та швидкості реагування на відмови, її здатність виявляти проблеми та надсилати сповіщення в реальному часі.

Порівнявши з існуючими рішеннями для моніторингу інтернет-сервісів, такі як Nagios, Zabbix, Pingdom. У результаті чого були виявлені

як переваги, так і недоліки існуючих рішень. Такі системи моніторингу інтернет-сервісів мають потужну функціональність, складне налаштування, та обмежену підтримку масштабованості. Були визначені передумови розробки власної більш гнучкої, масштабованої та доступної системи, що здатна адаптуватися до різних умов і масштабів використання.

Висновки. Результатом роботи є розроблена система моніторингу інтернет-сервісів, яка забезпечує надійний контроль за станом інтернет-сервісів та дозволяє швидко реагувати на виникаючі загрози. Також забезпечує можливість сповіщення користувача про виникнення відмов шляхами надіслання лист на електронну пошту, або Push-повідомленням у браузері. Дана система є ефективним інструментом для підвищення стабільності бізнес-процесів і сприяє зменшенню можливих негативних наслідків через відмови інтернет-сервісів.

Список літератури:

1. Nagios. (n.d.). *Nagios Documentation*. Retrieved October 14, 2024, from <https://www.nagios.org/documentation>.
2. Zabbix. (n.d.). *Zabbix documentation*. Retrieved October 19, 2024, from <https://www.zabbix.com/documentation/current/en>.
3. Pingdom. (n.d.). *How Pingdom Can Work for You*. Retrieved October 27, 2024, from <https://www.pingdom.com>.

УДК 004.056.52.:53:004.942

СИСТЕМ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ ДЛЯ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Автор: Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Анотація. Концепція побудови систем захисту мовної інформації основана на використанні білого шуму як такого, що має максимальну спектральну щільність. Вона дозволила в середині ХХ століття розробити теоретичне обґрунтування для створення систем постановки активної акустичної завади та дослідження рівня захищеності мовної інформації на межі виділених приміщень. Враховувались особливості взаємодії аналогових сигналів, що давало змогу перейти до так званої «енергетичної теорії», та рівень розвитку технічних засобів.

Однак, перехід до цифрових методів та засобів обробки інформації призвів до не спроможності таких систем забезпечити захист мовної інформації на об'єктах інформаційної діяльності (ОІД). Виникло протиріччя між концепцією використання білого шуму та спроможністю цифрових методів та засобів до фільтрації таких завад. Його не вдалося призупинити навіть за рахунок суттєвого підвищення рівню SNR, що вказує на системну кризу в використанні даного методу захисту мовної інформації.

Вирішенням проблеми є осучаснення існуючої концепції за рахунок переходу від енергетичного методу приховування інформації до енерго-інформаційного – спотворення мовної (акустичної) інформації з метою унеможливлення відновлення її семантичної (інформаційної) складової.

В роботі запропоновано уточнення до процесу розробки систем захисту мовної інформації для ОІД та осучаснені вимоги до систем постановки активних завад і їх компонентів.

Ключові слова: захист мовної інформації, системи постановки активної завади, мовоподібний сигнал

Вступ

Аналіз нормативно-правової бази (Закони України, НД ТЗІ, наказів Адміністрації Держспецзв'язку та інше) [1-3, 5-7, 15-18], що до нормування правил побудови систем захисту мовної інформації (СЗМІ) на ОІД, вимог до функціонування таких систем та сучасних досліджень з цифрової обробки (відновлення) сигналів (мовної інформації) показує що:

1) Основними критеріями якості роботи СЗМІ є відповідність їх організаційно-структурної будови та функціонального стану вимогам нормативних документів, що підтверджується при проходженні атестації таких систем, та результатами інструментальних контролів.

2) Прийнятий в Україні, як і в більшості країн світу, принцип побудови СЗМІ з використанням систем постановки активних завад (СПАЗ) на базі генераторів білого шуму або його клонів був запроваджений на основі концепції використання білого шуму як такого, що має максимальну спектральну щільність.

3) Методи інструментального контролю рівня захищеності мовної інформації на ОІД засновані на визначенні різниці рівнів акустичного

фону на межі контрольованої зони з включеним та виключеним джерелом тестового сигналу, що знаходиться в нормованих контрольних точках в межах контрольованої зони. В якості тестового сигналу використовується генератор білого шуму.

4) Сучасні методи цифрової обробки сигналів дозволяють суттєво покращити якість фільтрації шумових завад, виділення мовленнєвого сигналу конкретного диктора та проведення процедур реінжинірингу.

Таким чином виникло суттєве протиріччя між можливостями СЗМІ та засобами несанкціонованого перехоплення мовної інформації.

Мета та задачі дослідження

Метою роботи є осучаснення концепції побудови систем захисту мовної інформації для об'єктів інформаційної діяльності за рахунок переходу від енергетичного методу визначення принципів взаємодії акустичних сигналів до енерго-інформаційного методу – спотворення мовної (акустичної) інформації з метою унеможливлення відновлення її семантичної (інформаційної) складової.

Для досягнення поставленої мети вирішувалися такі наукові завдання дослідження:

1) Провести аналіз вимог нормативно-правової бази до організаційно-структурної будови та функціонального стану СЗМІ.

2) Дослідити особливості застосування енерго-інформаційного методу побудови СЗМІ з використанням СПАЗ на базі генераторів скремблерного типу.

Нормативно-правове забезпечення організаційно-структурної будови та функціонального стану СЗМІ

Правила побудови ЗСІ в Україні засновані на досить ефективному поєднанні прав і можливостей власника об'єкту, який підлягає захисту, що до організаційної структури СЗІ та її технічного забезпечення, [3-7, 10] та, з іншого боку, жорсткості вимог до якості роботи таких систем – відповідності технічних характеристик СЗІ вимогам до рівня захищеності інформації (критеріям захищеності та рівню гарантій) [8, 14, 15] та функціонуванню системи і її складових [12-15].

Необхідно вказати, що нормативно-правове забезпечення СЗІ в Україні є досить збалансованим. Воно поєднує консерватизм в підходах до теоретико-методологічних базисів побудови систем з динамічними

змінами в методиках та технологіях їх реалізації, досить швидко реагує на критичні інциденти та постійно вдосконалюється.

З погляду захисту мовної інформації в Україні, як і в інших країнах Європи, США, Канаді та ін. [19,20], головними є організаційні заходи, що засновані на руйнуванні технічного каналу витоку інформації шляхом впливу на джерело сигналу або/та середовища розповсюдження небезпечного сигналу [12-15,18].

Значні зміни, які пов'язані з врахуванням тенденцій розвитку технічних засобів розвідки, що застосовують порушники, відбулись за останні 15 років в використанні засобів постановки активних завад. Ідеологія їх роботи заснована на так званій «енергетичній теорії» та повинна забезпечувати захист конфіденційної інформації шляхом створення активних завад на межі контрольованої зони [21-24]. В якості сигналу завади використовується «білий» шум або його «кольорові» клони («рожевий», «коричневий», «синій», «фіолетовий» та «сірий» шуми).

Однак, як показує огляд джерел інформації, такий підхід є застарілим і малоефективним. Його головний недолік пов'язано з його інституціональному підході до отримання інформації – інформацію повинен почути та сприйняти професійний слухач. В цьому випадку звичайне зашумлення, зі значним перекриттям по амплітуді сигналом завади небезпечного сигналу (-16...-25 дБА), забезпечує досить ефективний захист мовної інформації при використанні традиційних методів та алгоритмів визначення рівня захищеності інформації. Одночасно з цим, використання сучасних методів цифрової обробки сигналів дає змогу знешкодити такий захист.

Раніше, аналогічна ситуація відбулась з радіочастотним каналом – постановка завад в каналі з аналоговими сигналами дозволяла ефективно придушувати сигнали радіопередавачів з контрольованої зони. Однак перехід до цифрових технологій з імпульсними та шумоподібними сигналами призвів до неспроможності існуючих на той момент систем постановки активних завад забезпечити захист від витоку інформації. Це призвело до необхідності розробляти нові методи, які ґрунтуються не на енергетичному придушенні небезпечного сигналу, а на внесенні деструктивних змін в небезпечні сигнали. Такий підхід дав суттєві результати і зараз активно використовується в РЕБ. Але і вони не дає

повної гарантії захисті інформації – з'являються нові методи кодування і передачі цифрових сигналів в радіоканалі, що вимагає постійного вдосконалення систем захисту.

Особливості застосування енерго-інформаційного методу побудови СЗМІ з використанням СПАЗ на базі генераторів скремблерного типу

Аналіз структури сучасних систем захисту мовної інформації та методів визначення рівня її захищеності показує можливість модернізувати їх шляхом зміни інституційних підходів в формуванні сигналу завади – забезпечити перехід від енергетичного придушення небезпечного сигналу до внесення деструктивних змін в небезпечні сигнали, тобто до енерго-інформаційного методу побудови сигналу завади. Це можливо при створенні спеціальних сигналів, що будуть мати структуру та принцип формування аналогічний до небезпечного мовного сигналу. Одним з таких методів є використання генераторів скремблерного типу [25-27].

Головним інституційним недоліком систем захисту мовної інформації, заснованих на використанні виключно енергетичного методу захисту полягає в нерозривному поєднанні метода захисту (зашумлення) і методу визначення рівня захищеності небезпечних сигналів – використання «білого» шуму як для сигналу завади так і для імітації небезпечного сигналу. Це створює небезпечний стан, при якому сигнал завади неможливо відрізнити від тестового сигналу в системах вимірювання. І, відповідно, отримані результати, що засновані на стандартизованих методах, затверджених нормативними документами, є некоректними.

Для вирішення проблеми запропонована системи визначення рівня захищеності мовної інформації, що озвучується в контрольованій зоні

Висновки

В роботі розглянуто концепції побудови систем захисту мовної інформації для об'єктів інформаційної діяльності нормативно-правову базу, методи та технології захисту мовної інформації на об'єкті інформаційної діяльності критичної інфраструктури, що дозволили запропоновано її вдосконалення.

Осучаснення концепції пропонується за рахунок переходу від енергетичного методу визначення принципів взаємодії акустичних сигналів до енерго-інформаційного методу – спотворення мовної

(акустичної) інформації з метою унеможливлення відновлення її семантичної (інформаційної) складової.

Наведено результати дослідження особливості застосування енерго-інформаційного методу побудови систем захисту мовної інформації з використанням систем постановки активних акустичних завад на базі генераторів скремблерного типу.

Список літератури:

1. Про державну таємницю. Закон України від 21.01.1994 № 3855-ХІІ (зі змінами та доповненнями) [Ел. ресурс] – URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>

2. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР (зі змінами та доповненнями) [Ел. ресурс] – URL: <https://zakon.rada.gov.ua/laws/show/80/94-vr#Text>

3. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI (зі змінами та доповненнями) [Ел. ресурс] – URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

4. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;

5. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

6. НД ТЗІ 1.1-003-99 Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

8. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

9. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

10. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

11. ТЗІ НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

12. НД ТЗІ 3.5-001-2017
13. НД ТЗІ 3.6-003-2016
14. НД ТЗІ 3.7-003-2023 Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі [Ел. ресурс] – URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=60385>
15. Наказ Адміністрації Держспецзв'язку від 19.06.2015 № 023 (зі змінами від 23.01.2023 № 01т)
16. Наказ Адміністрації Держспецзв'язку від 31.05.2023 року № 465 «Про затвердження Критеріїв з визначення підприємств, установ та організацій, які мають важливе значення для національної економіки у сферах організації спеціального зв'язку, захисту інформації, кіберзахисту, захисту критичної інфраструктури, електронних комунікацій та радіочастотного спектра в особливий період» [Ел. ресурс] – URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=54181>
17. Наказ Адміністрації Держспецзв'язку від 30.08.2023 року № 773 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу» [Ел. ресурс] – URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=57930>
18. Наказ Адміністрації Держспецзв'язку від 26.09.2023 № 857 «Про внесення змін до Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури» [Ел. ресурс] – URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=60066>
19. ANSI: ANSI S3.5-1997. American National Standard. Methods for the Calculation of the Speech Intelligibility Index. New York: ANSI, 1997.
20. BS EN 60268-16:2011. Sound system equipment. Part 16: Objective rating of speech intelligibility by speech transmission index (BRITISH STANDARD).
21. Loudness, Its Definition, Measurement and Calculation / Harvey Fletcher and W. A. Munson, J. // Acous. Soc. Am. 5, 82 (1933)
22. Relation Between Loudness and Masking / Harvey Fletcher and W. A. Munson // Bell Telephone Laboratories, New York, N. Y. (Received May 24, 1937)
23. Factors Governing the Intelligibility of Speech Sounds / N.R. French, J.C. Steinberg // The journal of the Acoustical society of America, 1947.

24. Hanbook of acoustic noise control volume ii. noise and man / Walter A. Rosenblith, Kenneth N. Stevens and the staff of bolt, b3eranek and Newman. // Carpenter Litho & Prtg. Co., Springfield. 0. – 1000 – 28 September 1954

25. Касьянов Ю. І., Нужний С. М. Оцінювання ефективності генератора реальної мовоподібної завади за критерієм розбірливості мови. Вісник національного університету «Львівська політехніка». Автоматика, вимірювання та керування. Львів, 2016. № 852. С.105–110. URL: <https://ena.lpnu.ua:8443/server/api/core/bitstreams/82888e90-c7c7-4af0-b6a5-e2def041dda7/content>

26. Blintsov, V., Nuzhniy, S., Parkhuts, L., Kasianov, Y. (2018). The objectified procedure and a technology for assessing the state of complex noise speech information protection. Eastern-European Journal of Enterprise Technologies, 5 (9 (95)), 26–34. <https://doi.org/10.15587/1729-4061.2018.144146> – URL: <https://journals.uran.ua/eejet/article/view/144146>

27. Blintsov, V., & Nuzhniy, S. (2019). Удосконалення методу оцінювання ступеня захисту мовної інформації. Eastern-European Journal of Enterprise Technologies, 6(9 (102), 28–38. <https://doi.org/10.15587/1729-4061.2019.185585> – URL: <https://journals.uran.ua/eejet/article/view/185585>

УДК 004.738.5.056

ОРГАНІЗАЦІЯ ЗАХИСТУ БАЗИ ЗНАНЬ ПРИ РОБОТІ З ХМАРНИМ СХОВИЩЕМ

***Автори:** Письменюк В.А., студентка; Ферцович М.С., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. Сучасний світ переживає стрімкий перехід до цифрових технологій, і разом з цим зростає потреба у зберіганні великих обсягів даних та забезпеченні їх доступності для користувачів по всьому світу. Хмарні середовища надають можливість зберігати, обробляти й обмінюватися даними через інтернет, забезпечуючи легкий доступ до інформації незалежно від місцезнаходження. Завдяки зручності та гнучкості, хмарні

web-site: conference.nuos.edu.ua | [email: conference@nuos.edu.ua](mailto:conference@nuos.edu.ua); tel (+380512) 709444; 709105|

технології активно популяризуються як серед великих корпорацій, так і серед малих підприємств та приватних користувачів.

Однак зі зростанням популярності хмарних сервісів виникає потреба у вдосконаленні методів захисту інформації, що на них зберігається. Без належного захисту даних користувачів існує ризик витоку конфіденційної інформації, а також зловмисного втручання в їх роботу. Забезпечення конфіденційності, цілісності та доступності даних у хмарному середовищі стає критично важливим завданням для компаній, які прагнуть впроваджувати дані технології.

Метою роботи є організація захищеної системи зберігання та обробки документів з багатокористувацьким доступом.

Предметом дослідження є організація багатoshарового захисту бази знань Obsidian при багатокористувачському доступі через хмарне середовище зберігання даних Google Drive. В якості даних, що захищаються використовується студентська база знань підготовки до Єдиного державного кваліфікаційного іспиту.

Основна частина. Obsidian – це персональна база знань і програма для створення нотаток, яка працює з файлами Markdown. Дозволяє користувачам створювати внутрішні посилання між нотатками, а потім візуалізувати зв'язки у вигляді графа [1]. Особливістю багатокористувацької роботи з Obsidian, без використання корпоративної версії, є те що зміни в файлах в момент введення нових значень зразу зберігаються в відповідних файлах, що забезпечує синхронізацію даних у всіх користувачів.

Для якісної організації захисту та системи доступу до бази знань система повинна мати наступні вимоги:

- розмежування прав доступу до ресурсів;
- забезпечення синхронізації змін;
- шифрування інформації в процесі роботи з хмарию;
- зберігання в хмарі в шифрованому вигляді;
- створення резервної копії.

Аби здобувачі мали можливість ознайомлюватися та доповнювати дані, бачити внесені зміни у реальному часі, базу знань було завантажено до хмарного середовища Google Drive. Використання даного хмарного середовища дозволяє надавати доступ до його вмісту лише авторизованим користувачам, що вирішує задачу обмеження та контролю доступу до ресурсів, захисту даних під час їх передачі між користувачами.

Щоб уникнути пошкодження або втрати важливої інформації, було призначено відповідальну особу – адміністратора (модератора), який буде стежити, щоб інформація була доступна усім здобувачам освіти даної навчальної групи, та не порушувалась її (інформації) конфіденційність та цілісність.

Для забезпечення конфіденційності інформації користувачам, що мають доступ до бази знань, було рекомендовано встановити двофакторну аутентифікацію, завдяки чому кожен раз при вході до акаунта, на будь-який з пристроїв, до якого прив'язана електронна адреса, надходить повідомлення, з інформацією про те, з якого пристрою виконується спроба входу та прохання підтвердити вхід, натиснувши відповідну цифру, що висвічується на пристрої з якого здійснюється вхід.

Аби забезпечити доступність інформації та не порушити її цілісність, адміністратор використовує функцію надання різних рівнів доступу. Було встановлено “Обмежений доступ” до папки де зберігається база знань, тобто взаємодіяти з нею можуть лише користувачі, електронним адресам яких надано доступ. Крім того, Google Drive надає можливість налаштувати три рівні доступу опрацювання інформації для кожного користувача:

- користувач із правами перегляду має доступ до файлу, але не може редагувати його, ділитися ним, додавати коментарі й пропозиції;
- користувач із правами коментування може додавати коментарі й пропозиції до файлу, але не може редагувати його або ділитися ним;
- користувач із правом редагувати може редагувати й коментувати файл, ділитися ним, а також приймати й відхиляти пропозиції [2].

Студентам, які приймають активну участь у навчальному процесі було надано можливість редагування. Аби уникнути випадкового видалення та внесення недостовірної інформації студентам, що нерегулярно відвідують заняття, було надано можливість коментування, щоб мати можливість вносити пропозиції або уточнення, які надалі будуть узгоджені чи відхилені редакторами. Учасникам навчально процесу, які проявляють мінімальну активність, було надано можливість читання. Крім того, з адміністратором попередньо було узгоджено наступне: якщо студент без права на редагування має бажання внести зміни та

доповнити наявну інформацію, а його дії попередньо були узгоджені з редактором, то йому на певний час надаються права редактора.

Синхронізація даних у всіх користувачів забезпечується встановленням на їх комп'ютер додатка Google Drive, що забезпечить синхронізацію комп'ютерної та хмарної версії бази знань. Такий підхід надає змогу працювати з файлами всіх форматів та редагувати їх (а не тільки редакторів, що підтримуються компанією Google) із практично миттєвою синхронізацією з хмарою.

Аби уникнути витоку та порушення цілісності інформації через злом акаунту користувача або отримання зловмисником доступу до пристрою, на якому встановлено Google Drive, де є доступ до бази знань, було використано програму Cryptomator. Cryptomator – це простий та безкоштовний інструмент цифрового самозахисту, що дозволяє самостійно і незалежно захищати хмарні дані [3]. Для шифрування файлів та їх назв програма використовує метод шифрування AES з довжиною ключа 256 біт. Крім того, 19 серпня 2021 р. Державною радою Бельгії було підтверджено, що Cryptomator відповідає стандарту GDPR (Загальний регламент про захист даних), що надає високий кредит довіри даному застосунку [4].

Використовуючи вищезазначену програму адміністратор зашифрував на Google диску папку, де знаходилась база знань. Було встановлено пароль, що складався з 21 випадкового символу і поширено його серед студентів даної групи. Після зашифрування папки, навіть якщо акаунт користувача мав до неї доступ як редактор, при звичайному переході до неї або при її завантаженні з хмарного пристрою на фізичний носій, відкривалися файли з незрозумілими назвами. Для отримання доступу до інформації здобувачі повинні встановити програму Cryptomator та знати спеціальний пароль, який їм було надано адміністратором.

Автоматичне резервне копіювання інформації забезпечується можливостями операційної системи адміністратора та зберігається на закритій частині Google диску в зашифрованому вигляді.

Висновки:

Використання хмарних технологій для зберігання та обробки інформації сьогодні є особливо актуальним, зокрема для компаній, співробітники яких працюють дистанційно. Завдяки хмарному середовищу забезпечується зручний доступ до даних у будь-який час і з будь-якого місця, що значно підвищує продуктивність та ефективність роботи. Для

освітнього процесу це дозволяє студентам та викладачам оперативного обмінюватися інформацією, переглядати оновлення в реальному часі та спільно працювати над навчальними матеріалами, що є важливим компонентом сучасного навчання.

У цьому дослідженні було реалізовано комплексний підхід до захисту бази знань, завантаженої у хмарне середовище Google Drive. Впроваджено заходи кібербезпеки, такі як двофакторна аутентифікація, розмежування прав доступу та шифрування даних за допомогою програми Cryptomator, що гарантує високий рівень конфіденційності та цілісності інформації. Такі рішення забезпечують захист бази знань від несанкціонованого доступу та зловмисних дій, надаючи при цьому можливість гнучкого доступу користувачам із різними рівнями прав.

Отже, впроваджені заходи не лише підвищують якість захисту даних у хмарному середовищі, а й роблять його надійним інструментом для дистанційної роботи та навчання.

Список літератури:

1. Obsidian. Help [Електронний ресурс] URL: <https://publish.obsidian.md/help-ru/Obsidian/Obsidian>
2. Стаття: “Як ділитися файлами з Google Диска” [Електронний ресурс] URL: <https://support.google.com/googleone/answer/2494822?hl=uk&co=GENIE.Platform>
3. Cryptomator [Електронний ресурс] URL: <https://cryptomator.org/>
4. Does Cryptomator allow GDPR-compliant file storage? [Електронний ресурс] URL: <https://cryptomator.org/gdpr/>

УДК 004.056.5

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ВИБОРУ ЗАСОБІВ ЗАХИСТУ ВІД DDOS-АТАК

***Автор:** Садалюк Є.О., магістрантка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Актуальність даної роботи зумовлена тим, що стрімкий розвиток апаратно-програмних засобів в галузі ІТ призводить до появи нових загроз у кіберпросторі, удосконалення кібератак і відповідних засобів протидії. Джерелами суттєвої долі кіберризиків протягом тривалого часу залишаються DoS і DDoS-атаки [1-3]. Розробці засобів виявлення і запобігання цим атакам, присвячено багато наукових робіт [4-8], а на ринку наявний ряд різноманітних засобів протидії [1, 2, 9-11], які суттєво різняться за функціональними та експлуатаційними властивостями. Вибір засобу захисту від DoS і DDoS-атак для конкретного середовища функціонування внаслідок цього є складною задачею, для пришвидшення розв'язку якої і уникання помилок доцільно застосовувати засоби автоматизації.

Метою даної роботи є озробка системи підтримки прийняття рішень щодо вибору засобів захисту від DDoS-атак.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- визначити параметри наявних на ринку засобів захисту від DDoS-атак (3DDoSA);
- визначити критерії прийняття рішень щодо вибору 3DDoSA;
- розробити основні алгоритми і структуру системи прийняття рішень (СППР) щодо вибору 3DDoSA.

Наявні на ринку 3DDoSA можуть бути орієнтовані на захист від атак, здійснюваних по відомим алгоритмам, і від новітніх, невідомих на момент створення 3DDoSA, атак, різне середовище функціонування і можуть розповсюджуватися на різних умовах та протидіяти DDoS різними способами. Тому при виборі 3DDoSA необхідно приймати до уваги типи сучасних DDoS-атак, класифікація яких наведена на рис.1 і їх можливі наслідки для певної галузі застосування, зокрема для водного транспорту [7].

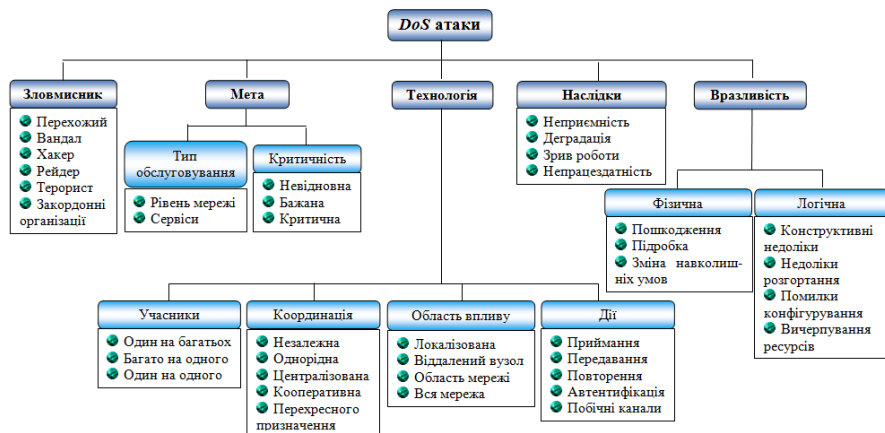


Рисунок 1 – Класифікація DDoS-атак

Вибір 33DDoSA має здійснюватися після ідентифікації, аналізу, оцінювання та обробки ризиків, проведених згідно ISO/IEC 27005:2022 або відповідним Державним стандартом України [12], тобто після того як на етапі обробки ризиків буде прийняте рішення щодо необхідності зниження ризиків, асоційованих із DDoS-атаками, і визначене місце розташування 33DDoSA в інформаційно-комунікаційній системі.

В розроблюваній СППР формування множини альтернативних варіантів 33DDoSA можна здійснити за наступними критеріями, які віддзеркалюють параметри наявних на ринку 33DDoSA:

- критерії придатності, які визначають область захисту, підтримувану операційну систему і протоколи, спосіб маршрутизації, спосіб підключення до мережі провайдера, місце розташування відносно мережевого екрану, рівень виявлення атак, схему підключення, пропускну здатність, можливість додавання сигнатур інших розробників і користувачів;

- ресурсні критерії, які визначають наявність необхідного обсягу пам'яті, документації, персоналу з достатнім рівнем кваліфікації, фінансових ресурсів для придбання, впровадження і підтримки в процесі експлуатації 33DDoSA, можливості співпрацювати із їх виробниками і розповсюджувачами, умови розповсюдження;

– функціональні критерії, які визначають типи DDoS-атак і їх кількість, яка може бути виявлена 3ZDDoSA; рівні моделі OSI і їх кількість, на яких може працювати засіб захисту; метод аналізу трафіку; характер реакції на виявлені атаки і виконувані дії; придатність для роботи у багатопоточному режимі, обміну даними з іншими інформаційно-комунікаційними системами і додатками, визначення прихованих даних і аномальних даних, відновлення TCP потоку і HTTP web-сторінки, декодування протоколу і відображення в додатку шару протоколу, оцінювання критичності трафіку для бізнесу; наявність сповіщення знаходження і мережевої комунікаційної матричної мапи; відкритість коду; Librcap основа, UDP трафік; орієнтований обсяг обробленої інформації;

– якісні критерії, які визначають кількості використовуваних сигнатур і шаблонів нормального стану; ефективність виявлення і протидії DDoS-атакам певного типу; зручність використання, оновлення сигнатур і шаблонів нормального стану; адаптовність налаштувань під вимоги користувача, наявність декількох інтерфейсів, зручність інтерфейсу користувача; підтримку розробником налаштування та експлуатації 3ZDDoSA.

Визначені вище критерії (або вибірка критеріїв) на першому етапі можуть використовуватися для формування множини альтернативних варіантів 3ZDDoSA за умовою наявності у 3ZDDoSA певних властивостей, а на другому – для визначення пріоритетів альтернативних варіантів 3ZDDoSA за методом аналізу ієрархій з врахуванням важливості кожного критерію [13] і формування множини рекомендованих 3ZDDoSA з максимальними пріоритетами, яка надається особі, що приймає остаточне рішення. Узагальнений алгоритм вибору 3ZDDoSA наведений на рис.2, а структура СППР – на рис.3.

Специфіка захисту від DDoS-атак у морській галузі полягає у наявності великої кількості зацікавлених у безпеці об'єктів сторін (у тому числі з різних країн) і залежності життєздатності окремих об'єктів інформаційної діяльності (наприклад, суден) від їх кіберстійкості [14]. За захист морської галузі від кібератак відповідають Уряди та окремі компанії. При цьому уряди часто підтримують порти, а компанії беруть на себе відповідальність за власні судна.

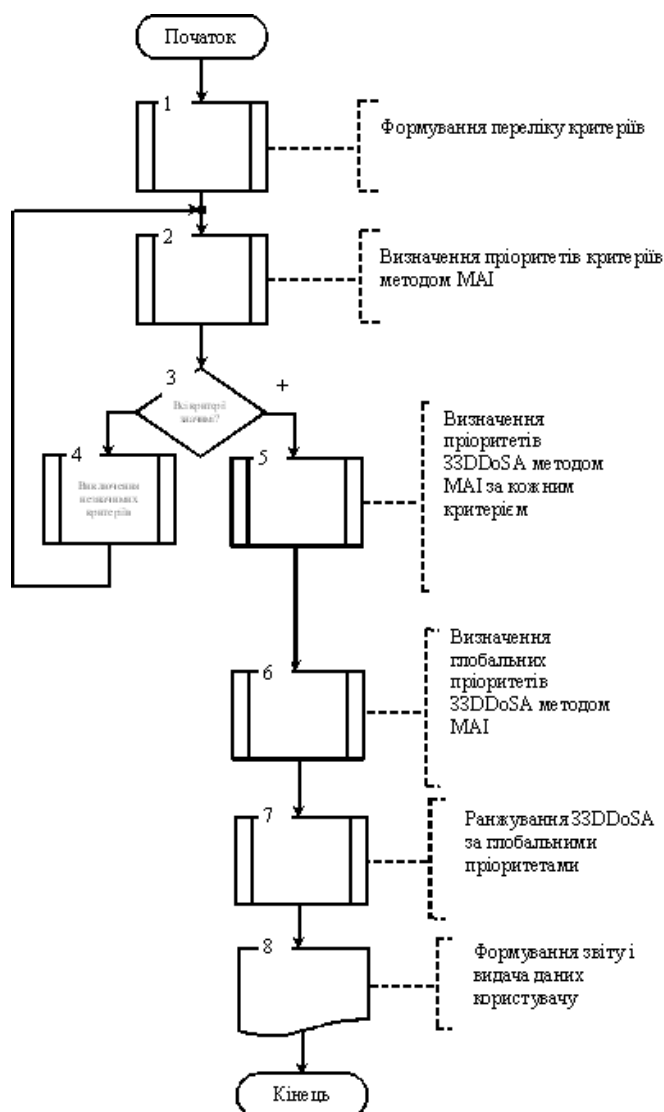


Рисунок 2 – Узагальнений алгоритм вибору 33DDoSA

Секція 2. **Захист інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах**

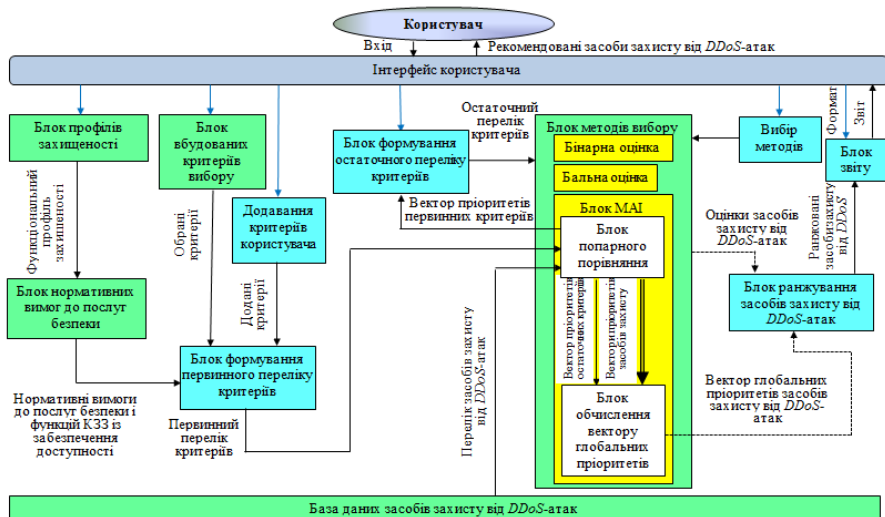


Рисунок 3 – Структура СПДР

Компанії повинні мати можливість визначати вразливі місця системи захисту та усувати їх, щоб запобігти кібератакам. Це означає підтримувати системи в актуальному стані, використовувати найкраще програмне забезпечення для захисту від зловмисних програм, а також створювати та використовувати протоколи безпеки.

Роботодавці також відповідають за навчання працівників і інформування їх про ризики та ознаки кібератак. Працівники повинні знати, як безпечно використовувати технології та як дотримуватися протоколів безпеки. Компанії повинні регулярно оцінювати стан своєї кібербезпеки та за потреби вносити оновлення.

При виборі 33DDoSA слід враховувати, що відшкодувати збитки після кібератаки за судовим рішенням дуже складно, оскільки не завжди зрозуміло, хто ініціював атаку. Реальною підставою для подання позову та відшкодування збитків може бути виявлена недбалість персоналу або недоліки проектування чи експлуатації системи захисту, виявлення зв'язків інцидентів кібербезпеки із порушеннями контрактів або нормативних актів [15].

Висновки.

В даній роботі визначені параметри наявних на ринку засобів захисту від DDoS-атак і критерії прийняття рішень щодо їх вибору, розроблені основні алгоритми і структура СППР щодо вибору засобів захисту від DDoS-атак.

Список літератури:

1. DDoS-атаки – растущая угроза онлайн-сервисам. URL: <https://ictn.e.ws.uz/28/03/2023/ddos/>
2. Обзор первого квартала 2023 года: отчет StormWall о DDoS-атаках. URL: <https://stormwall.pro/otchet-o-ddos-atakah-stormwall-pervyy-kvarta-l-2023>
3. Садалюк Є.О. Актуальні питання захисту інформації в комп'ютерних мережах. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК, 2021. С.184-187. URL: https://nuos.edu.ua/wp-content/uploads/2022/06/SPIBT-2021_materiali.pdf
4. Anthony D. Wood and John A. Stankovic A Taxonomy for Denial-of-Serv ice Attacks in Wireless Sensor Networks. URL: <https://www.cs.virginia.edu/~stankovic/psfiles/computer02-dos.pdf>
5. Jenniefer A., Raybin J. Techniques for Identifying Denial of Service Attack in Wireless Sensor Network. *Survey International Journal of Advanced Research in Computer and Communication Engineering*. Vol.3. Issue 6. 2014. URL: <https://arxiv.org/ftp/arxiv/papers/1011/1011.1529.pdf>
6. Александр М., Корченко О., Карпінський М., Одарченко Р. Дослідження вразливостей сенсорних підмереж архітектури інтернету речей до різних типів атак. *Безпека інформації*. 2016. Том 22. №1. С.12-19. URL: <https://dspace.nau.edu.ua/bitstream/NAU/36403/1/10448-26997-1-SM.pdf>
7. Садалюк Є.О. Наслідки DDoS-атак на водний транспорт. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК, 2023. С.215-217. URL: <https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf>

8. Юрченко Ю.Ю., Куцолабський В.П. Сенсорні мережі загального використання URL: <https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/29183/8940.pdf?sequence=3&isAllowed=y>
9. Smurf attack. URL: https://en.wikipedia.org/wiki/Smurf_attack
10. Спам-атака на телефон. URL: <https://promov.one/spam-ataka-na-telefon/>
11. Управління ключами в інформаційній системі. URL: http://pidruchniki.com/13410927/informatika/upravlinnya_klyuchami_informatsiyniy_sistemi
12. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. URL: https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400
13. Катренко А.В. Системний аналіз об'єктів та процесів комп'ютеризації: Навчальний посібник. – Львів : Новий Світ-2000", 2003. – 424 с.
14. Зубков А.П. Критерії прийняття рішень щодо обробки ризиків об'єктів морської інфраструктури. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК, 2023. С.175-181. URL: <https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf>
15. Веремчук В.С. Міжнародно-правове регулювання кібербезпеки у морській галузі: сучасний стан та перспективи розвитку. *Вісник Одеського Національного ун-ту. Серія: Правознавство*. 2024. Т.26. Випуск 1(38). С.112-117. <https://journals.visnyk-onu.od.ua/index.php/law/article/view/472/462>

УДК 004.056.5; 004.89; 514.743.4

АНАЛІЗ ЗАХИЩЕНОЇ СИСТЕМИ ВІДДАЛЕНОГО КОНТРОЛЮ КЛІМАТИЧНИХ ПАРАМЕТРІВ СЕРВЕРНИХ ПРИМІЩЕНЬ ТА МОЖЛИВІ ШЛЯХИ ЇХ МОДЕРНІЗАЦІЇ

Автор: Стефанюк Ю.О., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Трибулькевич С.Л., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Сучасні серверні приміщення є важливими об'єктами для забезпечення безперебійної роботи інформаційних систем, обчислювальних центрів та комунікаційних мереж. Їх ефективна експлуатація залежить від підтримки стабільного мікроклімату, який мінімізує ризики перегріву обладнання, підвищення вологості чи інших несприятливих умов. Для цього широко застосовуються системи віддаленого контролю кліматичних параметрів, які дозволяють оперативно відстежувати стан середовища та реагувати на критичні зміни. Проте постійний розвиток технологій та підвищення вимог до захисту даних ставлять нові виклики перед такими системами, включаючи їх захищеність від кібератак, підвищення точності вимірювань і зручність у використанні.

Метою даної роботи є аналіз розробленої захищеної системи віддаленого контролю кліматичних параметрів у серверних приміщеннях, виявлення недоліків та визначення можливих шляхів їх модернізації.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- Проаналізувати розроблену захищену систему віддаленого контролю кліматичних параметрів;
- Описати можливі шляхи модернізації розробленої системи.

Захищені системи віддаленого контролю кліматичних параметрів є ключовим елементом управління сучасними серверними приміщеннями. Однак із зростанням частоти кібератак, підвищенням складності ІТ-інфраструктури та потребою в модернізації застарілого обладнання, виникає необхідність перегляду та вдосконалення існуючих систем.

Актуальність дослідження зумовлена необхідністю забезпечення

|web-site: conference.nuos.edu.ua | email: conference@nuos.edu.ua; tel (+380512) 709444; 709105|

Секція 2. Захист інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах

високого рівня захищеності даних, стабільності функціонування серверів та зменшення витрат на енергоспоживання шляхом впровадження сучасних технологій моніторингу й автоматизації.

Розроблена система представляє собою керуючий пристрій у вигляді плати розробника NodeMCU V3 ESP8266 “LoLin” на базі ESP12E, цифрового датчику вологості/температури DHT11 та інфрачервоного світлодіода. Розроблена система була відкритою та не передбачала встановлення в корпус, що значно впливало на фізичну безпеку системи. У ході тестування розробленої системи, було виявлено недоліки стандартних бібліотек та обмеженість у технічних можливостях керуючого пристрою. Зокрема стандартна бібліотека керування інфрачервоним світлодіодом не працює із змінними, що зберігаються у Flash пам'яті. Це призводило до значного зменшення кількості вільної ОЗП (рис. 1), яка є необхідною в умовах, коли й обробка й передача даних відбувається одним керуючим пристроєм. Для вирішення поданої проблеми було модифіковано стандартну бібліотеку.

```
Connected
Mode: STA
PHY mode: N
Channel: 1
AP id: 0
Status: 5
Auto connect: 1
SSID (12): TP-Link_C2D4
Passphrase (8)
BSSID set: 0
```

```
Connected to TP-Link_C2D4
IP address: 192.168.0.162
MDNS responder started
HTTPS server started
Setup final. HEAP: 27744
nan|nan
4808
nan|nan
4824
nan|nan
4824
nan|nan
```

Рисунок 1 – Залишається менше 5 Кб пам'яті

Іншою проблемою з обмеженим об'ємом оперативної пам'яті – є вразливість до DOS атак. Задля унеможливлення такого типу атак – було додано затримку на всі елементи керування, щоб запобігти флуду командами.

Подані проблеми не є всіма, з якими можна зіткнутися при побудові системи керування на базі малих, дешевих, хоча і стабільних у роботі чіпах. Є три шляхи модернізації поданої системи.

Перший – використання більш сучасних плат розробника на базі чипів ESP32, вони мають підтримку WiFi та Bluetooth, обладнані більш сучасними одно- або двох ядерними процесорами з частотою від 80 до 160 МГц, 384 Кб ОЗП та 4 Мб флеш-пам'яті. Таке рішення є актуальним лише для, так би мовити, стабілізації роботи системи у поточному стані, тобто не планується розширювати набір функцій.

Другий – розбити роботу системи на 2 керуючих пристрої. Перший пристрій – мікроконтролер, що використовується для збору та переробки даних у зручний для надсилання вигляд, у якості такого пристрою можна використовувати будь-який мікроконтролер від PIC18/PIC16 серії, до Arduino Nano, Mega. Другий пристрій – відповідає за пересилання даних та підтримку HTTP сервера на якому розгорнути панель керування. Таким чином, можна обійти проблему зберігання кодів для інфрачервоного світлодіода, оскільки за керування всіма діями відповідатиме окремий пристрій, а другий лише за зв'язок.

Третій шлях – найбільш доцільний з точки зору майбутнього розширення системи. Він полягає у використанні в якості головного керуючого пристрою міні-пк, як наприклад, Orange Pi, Banana Pi, Raspberry Pi. Такий шлях дозволить не лише розширити спектр потенційного функціоналу систему, а й надати альтернативу використання бездротових технологій зв'язку. З точки зору безпеки, кабельна лінія є більш стабільною ніж радіоканал.

Висновки. В роботі було проаналізовано розроблену захищену систему віддаленого контролю кліматичних параметрів у серверних приміщеннях. Описано можливі шляхи модернізації розробленої системи. Використання малих плат розробників та окремих Wi-Fi чипів. Не дивлячись на їх дешевизну та легкість опанування, сьогодні вони є досить

слабкими за технічними характеристиками та не можуть забезпечити потужностями усі необхідні функції. Існує три шляхи вирішення даної проблеми – використання більш сучасних версій, розділення виконуваних функцій на 2 мікроконтролери (один відповідає за передачу даних, другий за збір та обробку даних з датчиків), перехід на іншу архітектуру системи з використанням міні-ПК. Система зібрана на базі міні-ПК має більше можливостей для розширення функціоналу та модернізації. Такі системи можуть використовуватися, і як просто керуючий пристрій, що входить до складу загальної системи, і як окремий автономний пристрій. Також, такі системи є досить легкими у опануванні та дозволяють відійти від використання бездротових технологій, що може бути доцільно у питаннях інформаційної безпеки.

Список літератури:

1. Стефанюк Ю.О. Аналіз ринку та основні рекомендації щодо безпеки пристроїв IoT // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2023. [Електронний ресурс]. URL: <https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf> (дата доступу: лютий 2024).
2. Мікроконтролери в електричних системах – Режим доступу: <https://ela.kpi.ua/bitstream/123456789/19120/2/%D0%9C%D0%9F%D0%A22-95-184.pdf>
3. Orange Pi PC: [Електронний ресурс]. URL: <http://www.orangepi.org/html/hardWare/computerAndMicrocontrollers/details/Orange-Pi-PC.html>
4. Мікропроцесорна техніка [Електронний ресурс]: навчальний посібник для студентів усіх форм навчання та студентів-іноземців напряму підготовки 6.050701 “Електротехніка та електротехнології” / НТУУ «КПІ»; уклад. В. В. Кирик. – Київ: Політехніка, 2014. – 184 с.

ОЦІНКА ТА АДАПТАЦІЯ СТІЙКОСТІ ІНФОРМАЦІЙНО КОМУНІКАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ОБ'ЄКТУ

Автор: Стефанюк Ю.О., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Передерій В.І., д.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

За останні роки сформувався новий пріоритетний підхід, який пов'язаний із забезпеченням стійкості в інформаційно-комунікаційних системах критичних об'єктів.

Властивість стійкості розглядається, як можливість складної технічної системи, успішно завершити поставлене завдання при регламентованому числі змін в стані самої системи, тобто зберегти її працездатність після прояву припустимого числа відмов і зовнішніх дестабілізуючих впливів, до яких можна віднести наприклад DDos атаки.

Оскільки теорія стійкості перебуває в стадії розвитку тому формування основних показників є важливим напрямком наукових досліджень. Отже, можна зробити висновок, що ідея забезпечення властивості стійкості до кібернетичних загроз є актуальною, оскільки існуюча теорія для розподілених інформаційних систем не розглядає такий вид дестабілізуючих чинників як кіберзагрози.

На сьогодні існують різні Стандарти методів оцінки рівня інформаційної та кібербезпеки, такі як Cybersecurity Assessment Standard for Information Technology, CSET, розроблений Національним інститутом стандартів і технологій (NIST) США [1,2], які дозволяють оцінити кібербезпеку в конкретній організації та є простішим за інші підходи. Однак методологія є тривалою та складною у використанні. Стандарти ISO/IEC 27001 від Міжнародної організації зі стандартизації (ISO) є всесвітньо визнаною та прийнятою на міжнародному рівні; він адаптований до різних типів організацій і різних стандартів безпеки. Однак його розробка та впровадження потребують значних зусиль і ресурсів.

Виходячи з результатів аналізу вимог [1,2] зазначено що на стійкість інформаційно комунікаційних систем критичного об'єкту

найбільш значний вплив мають фактори інформаційної та кібербезпеки, фактори вразливості та стан ризику критичного об'єкту. До основних цих факторів відносяться:

Фактори інформаційної безпеки: DC – узгодженість даних; AD – доступність даних; DP – конфіденційність даних, DI – цілісність даних.

Фактори кібербезпеки: EI – зовнішній вплив; SF – відмови програмного забезпечення; DS – захищеність даних; SQL – ін'єкції; ILC – захищеність каналу витоку інформації.

До основних типів вразливостей:

1. Фізичні вразливості $PV = f_1(Pa, Ae, Cd)$: Недостатній захист від віддаленої фізичної атаки (Pa); Недостатній контроль доступу до обладнання (Ae); Несанкціоноване копіювання даних (Cd).

2. Вразливості мережі $NV = f_2(Np, Cr, Nd)$: Використання незахищених мережевих протоколів (Np); Недостатній контроль доступу до ресурсів (Cr); Вразливості мережевих пристроїв (Nd.)

3. Вразливості програмного забезпечення $SV = f_3(Vd, Ve, Aa)$: Вразливості валідації введених даних (Vd); Вразливості в шифруванні (Ve); Вразливості автентифікації та авторизації (Aa).

Для оцінки та визначення оперативного стану стійкості інформаційно комунікаційної системи критичного об'єкту від впливу зазначених факторів розроблена інформаційно-логічна модель представлена на рис.1 [3,4].

Особливістю зазначених факторів є неможливість їх безпосереднього виміру і запису в числовому виді. Для цього існують різні тести для оцінки, однак вони вимагають затрат часу і можуть представляти результат з деякою мірою невизначеності.

Для рішення вказаних проблемних питань, та кількісної оцінки оперативного стану стійкості ІКСКО пропонується застосування ймовірнісного математичного апарату з використанням Байєсовської мережі довіри (БСД), зображену на рис.2.

БМД це імовірнісна графічна модель, що є набором випадкових величин та їх умовних ймовірностей за допомогою ациклічного орієнтованого графа [5].

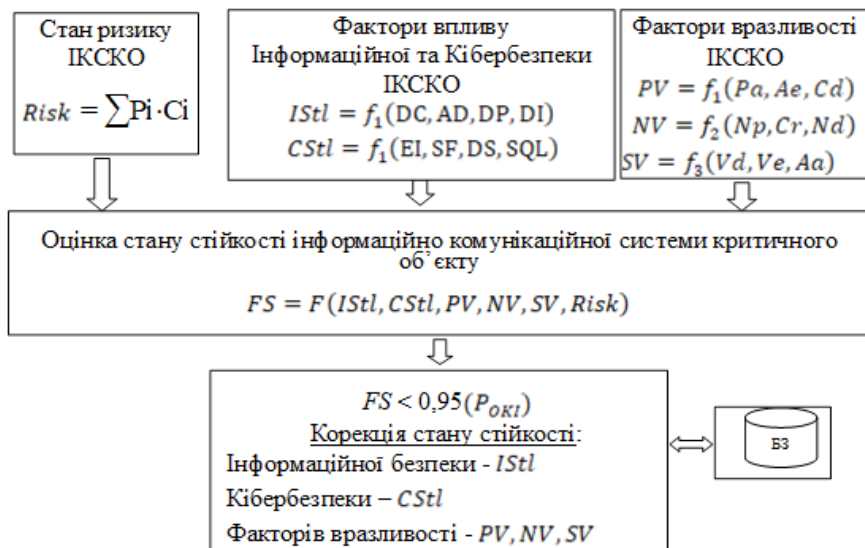


Рис. 1 – Інформаційно-логічна модель оцінки та адаптації оперативного стану стійкості ІКСКО.

Для будь-якої множини випадкових величин (вершин) $A_1, A_2, \dots, A_n$ БМД ймовірність спільного розподілу обчислюється за умовними ймовірностями за ланцюговим правилом наступним чином:

$$P(A_1, \dots, A_n) = \prod_{i=1}^n P(A_i | Parents(A_i)), \quad (1)$$

де $Parents(A_i)$ – змінні – предки змінної A_i .

Для обчислення ймовірності того, що змінна B набуває значення b_j на БМД, що складається з вершин $B, A_1, \dots, A_n$ використовується формула:

$$P(B = b_j) = \sum_{A_1, \dots, A_n} P(B = b_j, A_1, A_2, \dots, A_n) \quad (2)$$

Секція 2. **Захист інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах**

де підсумовування здійснюється за всіма значеннями змінних $A_1, A_2, \dots, A_n$.

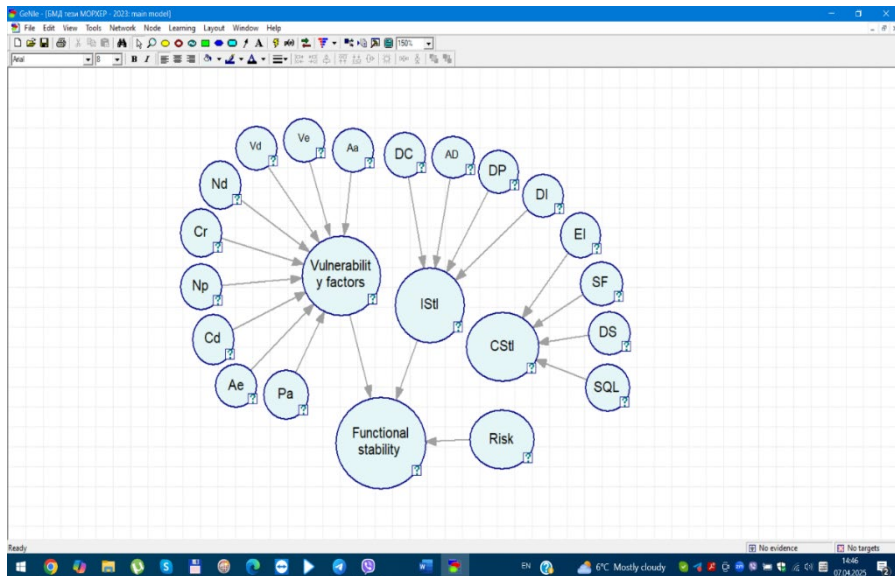


Рис.2. – Байесовської мережі довіри оцінки оперативного стану стійкості ІКСКО.

При побудові структури даної БСД та заповнення таблиць умовних ймовірностей для змінних мережі використовувалися вимоги нормативних документів, та знання експертів.

Розрахунки проводились за допомогою системи Genie 2.0 з використанням типу "Noisy MAX".

Висновки.

На основі проведеного аналізу визначенні основні фактори впливу на стійкість інформаційно комунікаційних систем критичного об'єкту та запропоновано інформаційно-логічну модель оцінки його оперативного стану стійкості.

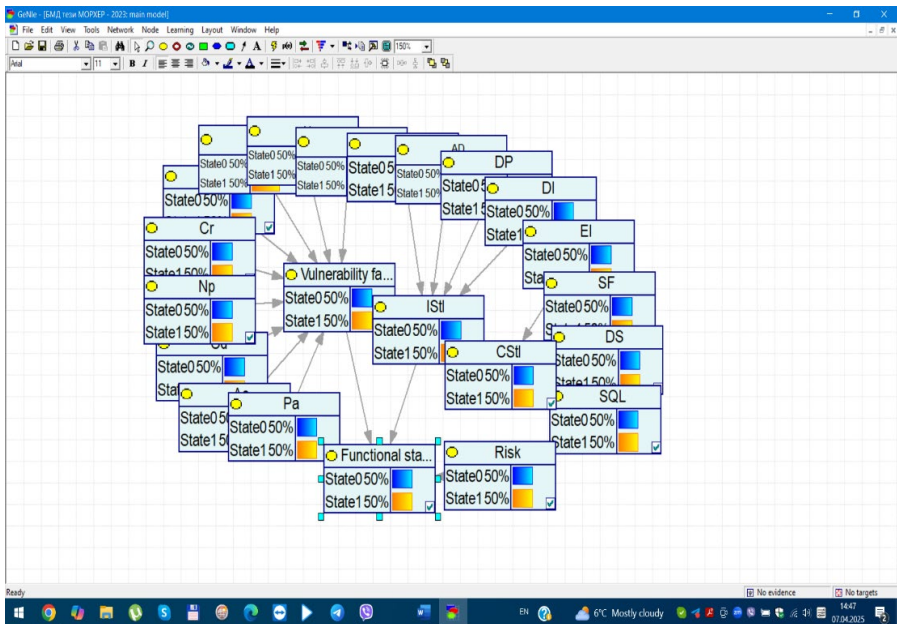


Рис.2. – Приклад розрахунку Байєсовської мережі довіри оцінки оперативного стану стійкості ІКСКО.

Для кількісної оцінки оперативного стану стійкості ІКСКО запропоновано ймовірнісний математичний апарат з використанням Байєсовської мережі довіри, яка на сьогодні є однією з найбільш доцільних моделей, призначених для роботи з неповною, неточною та суперечливою інформацією.

При побудові структури даної БСД та заповнення таблиць умовних ймовірностей для змінних мережі використовувалися вимоги нормативних документів, та знання експертів. Розрахунки проводились за допомогою системи Genie 2.0 з використанням типу "Noisy MAX".

Список літератури:

1. Cybersecurity Evaluation Tool, CSET. <https://www.nist.gov/cyber-framework/cybersecurity>

2. International Organisation for Standardization (ISO).
<https://www.nist.gov/cyberframework/cybersecurity>

3. Evaluation of the influence of environmental factors and cognitive parameters on the decision-making process in human-machine systems of critical application / [V. I. Perederyi, E. Y. Borchik, V. V. Zosimov, O. S. Bulgakova,] // Radio Electronics, Computer Science, Control. – 2024. – № 1 – P. 77-84. DOI 10.15588/1607-3274-2024-1-7.

4. Perederiy V., Borchik E. Information technology for determination, assessment and correction of functional sustainability of the human-operator for the relevant decision-making in human-machine critical application systems. Theoretical and practical aspects of the development of modern science: the experience of countries of Europe and prospects for Ukraine: monograph. Riga, Latvia: "Baltija Publishing", 2019. – Pp. 490-509

5. Murphy K. A brief introduction to graphical models and Bayesian networks / Technical report 2001-5-10, department of computer science, University of British Columbia, Canada, May 2001. – 19p.

ПРОГРАМНЕ МОДЕЛЮВАННЯ КОЛЬОРОВИХ ФРАКТАЛІВ З ПОЛІНОМІАЛЬНОЮ ФУНКЦІЄЮ ПЕРЕТВОРЕННЯ ТА ДОСЛІДЖЕННЯ ЇХ ПАРАМЕТРИЧНОЇ ЧУТЛИВОСТІ

***Автори:** Суліма М.М., к.т.н, доцент кафедри інформаційних технологій та фундаментальної підготовки; Корчевський Д.О., д.пед.н., професор кафедри інформаційних технологій та фундаментальної підготовки; Данилець Є.В., к.т.н, доцент, доцент кафедри інформаційних технологій та фундаментальної підготовки; Новак С.М., к.т.н, доцент, доцент кафедри інформаційних технологій та фундаментальної підготовки; Самойленко Д.М., к.ф.-м.н., доцент, завідувач кафедри інформаційних технологій та фундаментальної підготовки, Приватний заклад вищої освіти «Одеський технологічний університет «Шаг»», м. Одеса, Україна*

У роботі [1] проведено постановку задачі використання кольорових фракталів у задачах безпеки комунікаційних протоколів, досліджено вплив на безпекові параметри окремих параметрів фрактального перетворення. Зокрема, проведено досліді зі змінами головного ступеня перетворення. Дана робота присвячена дослідженню впливу параметрів ступенів перетворення, менших за головну.

Математичною моделлю фракталу у роботі є узагальнення множини Жюліа, яке містить у правій частині комплексну функцію перетворення у вигляді поліному степені N

$$z_{k+1} = \sum_{n=0}^N C_n z_k^n. \quad (1)$$

Множники C_n у цих поліномах, а також величина головного ступеня перетворення N формують множину конфіденційних даних (паролів) користувачів. Це значить, що паролем є масив величин $\{N, C_N, C_{N-1}, \dots, C_0\}$, що може мати більшу інформаційну ентропію при обмеженому бітовому представленні чисел, ніж класичний набір $\{N, C\}$ у фракталах Жюліа. З практичної точки зору збільшена множина паролів надає більш широкі можливості для дослідження на їх вплив різних параметрів перетворення.

Традиційно, належність точки до фракталу визначається фактом розбіжності чи збіжності перетворення (1). Але слід зауважити, що практичної можливості повторювати перетворення нескінченну кількість разів реалізувати неможна. Очевидно, що при програмному моделюванні використовується гранична величина ітерацій.

У якості кольору точки на площині $z = (x, y)$ розуміється кількість ітерацій, протягом якої послідовність не розбігається. Практичним критерієм розбіжності при скінченній кількості ітерацій $k_{\max}$ виступатиме певне граничне значення для модуля комплексного числа

$$|z_k| > R_{\max}, \quad (2)$$

де $R_{\max}$ – дійсне число, за якого гарантується подальша розбіжність послідовності (теоретична межа - $\sqrt{2}$). Оскільки практичний розрахунок модуля комплексного числа вимагає машинно-складного обчислення квадратного кореня, умову розбіжності можна замінити на більш просту з точки зору програмної реалізації [1].

$$|\operatorname{Re} z_k| + |\operatorname{Im} z_k| = |x| + |y| > r_{\max}, \quad (3)$$

де $r_{\max}$ – число, яке удвічі перевищує $R_{\max}$. Конкретні значення $k_{\max}$ та $r_{\max}$ також можна додати до параметрів алгоритмів.

Для практичного дослідження було обране перетворення третього ступеня

$$z_{k+1} = z^3 + C_2 z^2 + C_1 z^1 + C_0 \quad (4)$$

Основний акцент зроблено на недосліджені раніше коефіцієнти C_2 та C_1 . У таблиці 1 зведено результати моделювання фракталів зі змінами величин коефіцієнтів відносно центрального значення. Величина C_0 залишалась незмінною з величиною (0,4; 0,4).

За результатами аналізу наведених у таблиці даних можна зробити наступні висновки

- додавання параметрів менших ступенів зміщує центр фракталу, що ускладнює його криптоаналіз за симетрією;

- кількість «рукавів» полюсів фракталу не відповідає величині максимального ступеня. Це також робить фрактал більш стійким до виявлення його параметрів

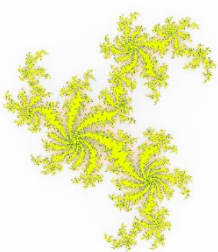
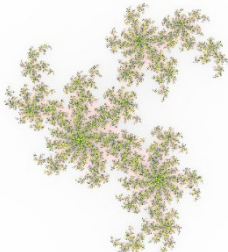
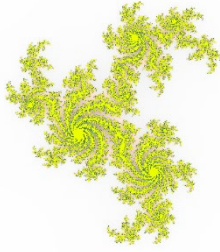
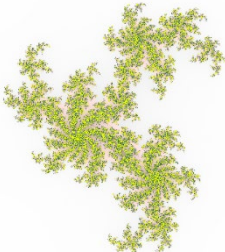
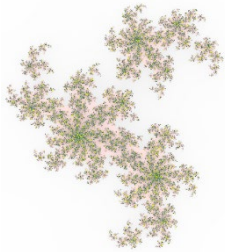
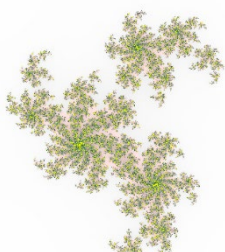
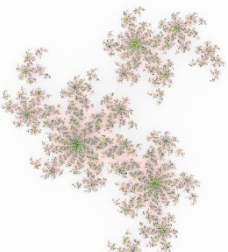
- форма фракталу зазнає менших змін, ніж його колір; при відносній схожості образів за формою, їх колір відрізняється практично для всіх точок. З точки зору прямого порівняння значень – це однозначна відмінність;

- чутливість до параметра першого ступеня (C_1) значно більша, ніж для другого (C_2). Приблизно однакові масштаби змін відбуваються при $\Delta C_1 = 0,05$ та $\Delta C_2 = 0,2$

Список літератури:

1. Samoilenko, D. (2024). Determining optimal parameters of algebraic fractals in zero-knowledge authentication protocols. *Eastern-European Journal of Enterprise Technologies*, 5(9 (131), 79–87. <https://doi.org/10.15587/1729-4061.2024.313471>

Таблиця 1 – Зміна образу фрактальної множини при зміні параметрів перетворення

 $C_2 = 0.18, C_l = 0.295$	 $C_2 = 0.2, C_l = 0.295$	 $C_2 = 0.22, C_l = 0.295$
 $C_2 = 0.18, C_l = 0.3$	 $C_2 = 0.2, C_l = 0.3$	 $C_2 = 0.22, C_l = 0.3$
 $C_2 = 0.18, C_l = 0.305$	 $C_2 = 0.2, C_l = 0.305$	 $C_2 = 0.22, C_l = 0.305$

УДК 621.314

СИСТЕМИ БЕЗПЕРЕБІЙНОГО ЖИВЛЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

***Автори:** Трибулькевич С.Л., ст. викладач; Трибулькевич В.В., викладач; Трешнюк А.І., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Системи безперебійного живлення (СБЖ) є ключовим елементом забезпечення стабільної та безперервної роботи комп'ютерних мереж. Вони дозволяють підтримувати функціонування мережевих пристроїв під час відключення або нестабільності електропостачання, що є критично важливим як для підприємств, так і для особистих користувачів, особливо в умовах сучасних технологічних викликів.

Особливе значення безперебійні джерела живлення набувають в Україні, де за останні роки спостерігається постійна напруга в енергетичному секторі. Військові конфлікти, зростаюча потреба в електроенергії та старіння інфраструктури електропостачання впливають на стабільність енергосистеми. Постійні аварії, часті відключення світла і надзвичайні ситуації змушують організації, підприємства та навіть звичайних споживачів звертати увагу на інструменти, які можуть забезпечити безперервну роботу мереж, серверів та інших важливих інформаційних систем.

В умовах відсутності стабільного енергопостачання, СБЖ забезпечують критичні функції: від захисту апаратури від перепадів напруги до забезпечення роботи серверних і мережевих центрів у режимі резервного живлення. В Україні саме зараз актуальність цих систем зростає, і їхнє використання стає незамінним у різних сферах діяльності, від бізнесу до державних установ, освітніх та медичних закладів. Сучасні технології дозволяють значно покращити ефективність роботи таких систем, мінімізуючи ризики, пов'язані з перебоями в енергозабезпеченні.

Таким чином, питання безперебійного живлення комп'ютерних мереж набуває не тільки технічного, але й стратегічного значення, зокрема в умовах нестабільного енергетичного забезпечення країни.

Джерело безперебійного (безперервного) живлення (ДБЖ) (англ. UPS – Uninterruptible Power Supply) дозволяє приєднаному до нього

обладнанню деякий час (для комп'ютерних мереж, здебільшого нетривалий – декілька хвилин) працювати від вбудованих акумуляторів у разі зникнення електричного струму в електромережі, або відхилення його показників (параметрів) від допустимих норм (насамперед рівнів напруги на які налаштовано електронну схему ДБЖ, приблизно 170...255 В).

За типом архітектури поділяються на:

1. резервні;
2. лінійно-інтерактивні;
3. неперервної дії.

У ДБЖ використовуються Li-Ion та Lead-Acid батареї, які можна класифікувати наступним чином:

1. Li-Ion:

- Lithium nickel manganese cobalt oxide NMC, $\text{LiNi}_x\text{Mn}_y\text{Co}_z\text{O}_2$
- Lithium nickel cobalt aluminum oxide NCA, LiNiCoAlO_2
- Lithium nickel cobalt manganese aluminum oxide NCMA,

$\text{LiNi}_{0.89}\text{Co}_{0.05}\text{Mn}_{0.05}\text{Al}_{0.01}\text{O}_2$

- Lithium manganese oxide LMO, LiMn_2O_4
- Lithium iron phosphate LFP, LiFePO_4
- Lithium cobalt oxide LCO, LiCoO_2

2. Lead-Acid

- VRLA (Valve Regulated Lead-Acid) Battery
- AGM (Absorbent Glass Mat) Sealed Lead-Acid Battery
- GEL Sealed Lead-Acid Battery:
- Deep Cycle Lead-Acid Battery
- High-Rate Lead-Acid Battery
- OPzV Tubular Battery
- OPzS Lead-Acid Battery
- Start-Stop or Engine Start Lead-Acid Batteries

Порівняння характеристик зазначених вище батарей наведено в таблиці 1.

Lead-Acid: хороші для малобюджетних або тимчасових рішень, або якщо UPS використовується рідко. Li-Ion: ідеальні для критичних систем, де важлива довговічність, економія простору і швидкий заряд.

Таблиця 1. Порівняння Li-Ion і Lead-Acid в UPS

Критерій	Lead-Acid (VRLA, AGM, Gel)	Li-Ion
Ціна	Низька початкова вартість	Вища, але знижується
Розміри і вага	Важкі та громіздкі	Легкі, компактні
Термін служби	3–5 років (часто менше у високих температурах)	8–15 років
Кількість циклів	~300–500	1000–3000+
Обслуговування	Потрібен моніторинг стану	Мінімальне
Температурна стабільність	Краще переносять низькі температури	Гірше працюють у холоді
Час перезарядки	6–12 годин	1–3 години
Ризик займання/вибуху	Мінімальний	Потребує BMS для захисту
Гнучкість установки	Обмежена через вагу та вентиляцію	Більше варіантів встановлення
ТСО (загальна вартість володіння)	Вища через часту заміну батарей	Нижча в довгостроковій перспективі

Виробники ДБЖ виготовляють серійно моделі як з Lead-Acid так і з Li-Ion акумуляторами. Для порівняння (рис. 1) можна звернутись до одного з найпоширеніших виробників APC. У порівняння додані моделі однакової потужності. Слід звернути увагу, що напруга акумуляторної збірки з Lead-Acid батареї набагато вища ніж напруга збірки з Li-Ion батареї. Також слід відзначити, що час перезаряду Li-Ion батареї менше ніж Lead-Acid, що також впливає на потужність зарядного пристрою.

Досвід експлуатації ДБЖ з Lead-Acid батареями показує, що в сучасних умовах в Україні термін служби таких батарей складає 2 – 3 роки. Тому стає актуальним питанням переобладнання вже існуючих ДБЖ на використання Li-Ion акумуляторів.

Ключові аспекти можливості переобладнання наступні:

☒



SRTL3KRM1UC
APC Smart-UPS Ultra On-Line, 3000VA, Lithium-ion, Rack/Tower 1U, 120V, 5x 5-20R, 1x L5-30R NEMA...

In stock

\$5,425.00

 **Add to Cart**

☐



Featured
SRT3000RMXLA
APC Smart-UPS On-Line, 3kVA, Rackmount 2U, 120V, 8x 5-20R+1x L5-30R NEMA outlets, SmartSlot,...

In stock

\$3,875.00

 **Add to Cart**

 Documents ^

 Documents ^

Battery Type	Li-Ion (Lithium Ion)	Lead-Acid battery
Battery Voltage	50 V	96V
Included Battery Modules		1
Typical recharge time	1.5 h	3 h
Battery life		3...5 year(s)
Replacement battery	 APCRBC173-LI	 APCRBC152
Battery Charge Power (Watts)	448 W	151 W rated

Рисунок 1 – Порівняння серійних моделей APC Smart UPS

1. Електрична сумісність:

- Li-Ion модулі повинні мати таку саму напругу, як і свинцево-кислотні (наприклад, 12V, 24V, 48V).
- повинна бути не меншою за наявну (А·г).
- Li-Ion батарея має витримувати пусковий/піковий струм, що дуже важливо, тому що, в Lead-Acid батареях піковий струм

web-site: conference.nuos.edu.ua | email: conference@nuos.edu.ua; tel (+380512) 709444; 709105|

обмежений лише внутрішнім опором акумулятора, а Li-Ion – обмежений в налаштування BMS та часто складає половину ємності АКБ.

– Тип зарядного пристрою: стандартні UPS розраховані на Lead-Acid – їх зарядні контролери не завжди сумісні з Li-Ion.

2. Безпека:

Потрібен надійний BMS: захист від перенапруги, перегріву, короткого замикання.

LiFePO₄ – найбезпечніший тип серед Li-Ion (термічно стабільний, важко загоряється).

3. Юридичні та гарантійні обмеження:

Переобладнання UPS може анулювати гарантію виробника.

При проектуванні нових систем є сенс звернути увагу на гібридні мережеві інвертори, які працюють з будь яким типом АКБ та мають доволі гнучкі налаштування (рис. 2).

У порівнянні з готовими рішеннями ДБЖ, гібридний інвертор з LiFePO₄ акумулятором коштує набагато дешевше ніж ДБЖ з аналогічними характеристиками. Але статистики використання інверторів у якості ДБЖ на сьогоднішній день поки що немає. Окрім того немає стандартного програмного забезпечення для моніторингу параметрів інвертору, який працює у якості ДБЖ, для завершення роботи операційних систем при розряді акумулятору, а таке кросплатформне програмне забезпечення, як Network UPS Tools (NUT) не підтримує протоколи гібридних інверторів. Тому для надійної та довготривалої (в умовах відключень електроживлення) роботи серверного та телекомунікаційного обладнання може використовуватись схема живлення обладнання від стандартного ДБЖ, який живиться від системи зберігання енергії (гібридний інвертор з АКБ), яка в свою чергу має можливість запуску генератору при довготривалих відключеннях. (рис. 3.)

Висновки. У сучасних умовах функціонування комп'ютерна мережа потребує стабільного та надійного електроживлення. Традиційні джерела безперебійного живлення (ДБЖ), які базуються на свинцево-кислотних акумуляторах, залишаються популярними через свою доступність, проте мають низку обмежень — велику масу, невеликий ресурс, обмежену кількість циклів та потребу в регулярному обслуговуванні.



Резервний, автономний режим	
Потужність, Вт	6000
Максимальна потужність, Вт	6600
Пікова потужність не більше 10 с, Вт	12000
Вихідний струм, А	27.3
Максимальний струм транзиту, А	40
Вихідна частота, Гц	50/60
Тип мережі	1ф (L / N / PE)
Коефіцієнт гармонік, %	THD <3% (лінійне навантаження <1,5%)

Рисунок 2 – Характеристики гібридного інвертору

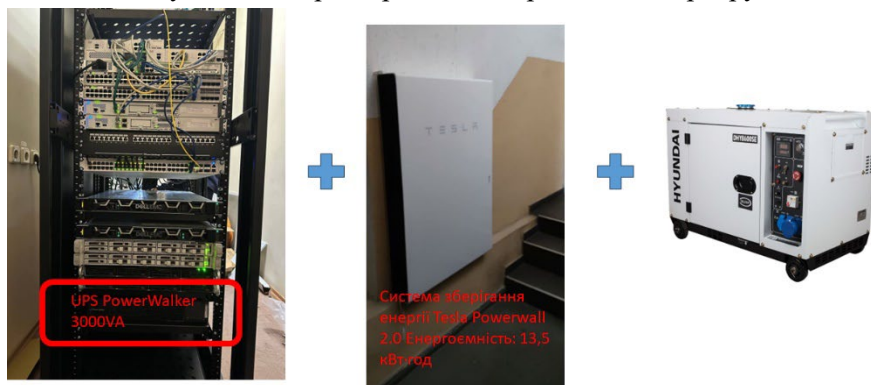


Рисунок 3 – Схема резервного електроживлення

Зі зростанням вимог до ефективності та надійності, все більше уваги приділяється літій-іонним акумуляторам, зокрема на базі LiFePO_4 . Вони мають низку переваг: високу щільність енергії, тривалий термін служби, швидке заряджання, зменшену вагу та відсутність необхідності в обслуговуванні. Хоча початкова вартість Li-Ion рішень є вищою, в довгостроковій перспективі вони забезпечують економічно вигідніше та стабільніше резервне живлення.

Окрему увагу заслуговує можливість використання ****гібридних інверторів**** у ролі джерел безперебійного живлення. Вони поєднують функції інвертора, контролера заряду та часто мають вбудований автоматичний перемикач живлення (ATS), що дозволяє забезпечити живлення критичних навантажень як від електромережі, так і від альтернативних джерел (сонячні панелі, акумулятори). Завдяки високій гнучкості, розширюваності та підтримці роботи з Li-Ion АКБ, гібридні інвертори стають перспективним напрямом розвитку систем ДБЖ, особливо у поєднанні з відновлюваними джерелами енергії.

Список літератури:

1. Гібридний інвертор Deye SUN-6k-SG05LP1-EU 6kW, 1ф, 48V – DeyeUkraine. DeyeUkraine – Сонячні інвертори Deye. URL: <https://deye.com.ua/product/gibridnij-invertor-deye-sun-6k-sg05lp1-eu-6kw-1f-48v/> (дата звернення: 10.10.2024).
2. Учасники проєктів Вікімедіа. Джерело безперебійного живлення – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Джерело_безперебійного_живлення (дата звернення: 10.10.2024).
3. APC Smart-UPS On-Line, 3kVA, Rackmount 2U, 120V, 8x 5-20R+1x L5-30R NEMA outlets, SmartSlot, Extended runtime, W/ rail kit – SRT3000RMXLA | APC USA. Access Denied. URL: <https://www.apc.com/us/en/product/SRT3000RMXLA/> (date of access: 10.10.2024).
4. APC Smart-UPS Ultra On-Line, 3000VA, Lithium-ion, Rack/Tower 1U, 120V, 5x 5-20R, 1x L5-30R NEMA outlets, SmartConnect, Extended runtime, W/rail kit – SRTL3KRM1UC | APC USA. APC, a flagship brand of Schneider Electric – APC USA. URL: <https://www.apc.com/us/en/product/SRTL3KRM1UC/apc-smartups-ultra-online-3000va-lithiumion-rack-tower-1u-120v-5x-520r-1x-l530r-nema-outlets-smartconnect-extended-runtime-w-rail-kit/> (date of access: 10.10.2024).

5. Contributors to Wikimedia projects. Lead–acid battery – Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Lead-acid_battery (date of access: 10.10.2024).

6. Contributors to Wikimedia projects. Lithium-ion battery – Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Lithium-ion_battery (date of access: 10.10.2024).

7. Network UPS Tools – Documentation. Network UPS Tools – Welcome. URL: <https://networkupstools.org/documentation.html> (date of access: 10.10.2024).

8. What are the types of lead-acid batteries?. JYC Battery. URL: <https://www.jycbattery.com/what-are-the-types-of-lead-acid-batteries/> (date of access: 10.10.2024).

УДК 004.2

ОЦІНКА ЗАЛЕЖНОСТІ КОНСОЛІДАЦІЇ ІНФОРМАЦІЙНОГО WEB РЕСУРСУ ВІД ВПЛИВУ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

***Автори:** Хавело Д.С., магістрант; Пархоменко Б.І., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Передерій В.І., д.т.н, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. Роль інформаційної та кібернетичної безпеки в системах конкурентної розвідки набуває особливої ваги в сучасному бізнес-середовищі, де інформація виступає як ключовий актив. В контексті конкурентної розвідки, інформаційна та кібернетична безпека відіграє критичну роль у захисті цінної комерційної та стратегічної інформації, а також у забезпеченні цілісності і конфіденційності даних.

Однак, в контексті зростання обсягів інформації від різних джерел, виникає потреба в ефективному забезпеченню інформаційною та кібернетичною безпекою цієї різноманітності даних.

Тому інформаційна та кібернетична безпека відіграє вирішальну роль у захисті аналітичних систем конкурентної розвідки, які обробляють конфіденційні дані та інформацію, критичну для бізнес-стратегій організацій. На відміну від традиційних ІТ-систем, які зосереджені на забезпеченні цілісності, доступності та конфіденційності даних, аналітичні системи конкурентної розвідки також мають забезпечувати достовірність та актуальність інформації, яка є важливою для прийняття рішень на вищому рівні управління [1].

Метою роботи є запропонувати технологію оцінки залежності консолідації інформаційного WEB ресурсу від інформаційної та кібернетичної безпеки з урахуванням людського фактору.

Основна частина Технології консолідації інформаційного WEB ресурсу дозволяють об'єднувати та інтегрувати різноманітні джерела інформації з мережі для забезпечення цілісності та актуальності даних.

Важливим аспектом забезпечення стійкої інфраструктури є: захист від втрати даних, захист від несанкціонованого доступу, захист від зовнішніх атак, забезпечення конфіденційності, забезпечення цілісності даних, надійність апаратних та програмних засобів, а також готовність до швидкого виявлення та реагування на можливі інциденти в області інформаційної та кібернетичної безпеки.

Використання передових технологій для забезпечення безпеки даних є стратегічно важливим аспектом у контексті сучасних викликів кібербезпеки.

Однак, вирішення цих завдань повинно враховувати не тільки технічні питання, але й враховувати людський фактор та вдосконалення процесів управління безпекою. Тільки комплексний підхід до цих викликів дозволить забезпечити надійний, ефективний та безпечний процес консолідації інформаційного WEB ресурсу в аналітичних системах конкурентної розвідки [2].

Для часткового рішення цих проблем пропонується Інформаційна модель оцінки впливу інформаційної та кібернетичної безпеки на процес консолідації інформаційного WEB ресурсу, яка дозволяє оцінити та визначити рівень захищеності системи консолідації веб ресурсу виходячи з якості роботи модулів безпеки та когнітивного стану користувача (рис.1).

Таким чином, динамічні фактори, що впливають на захищеність системи консолідації інформаційного Web ресурсу можуть бути розподілені на дві категорії [3]:

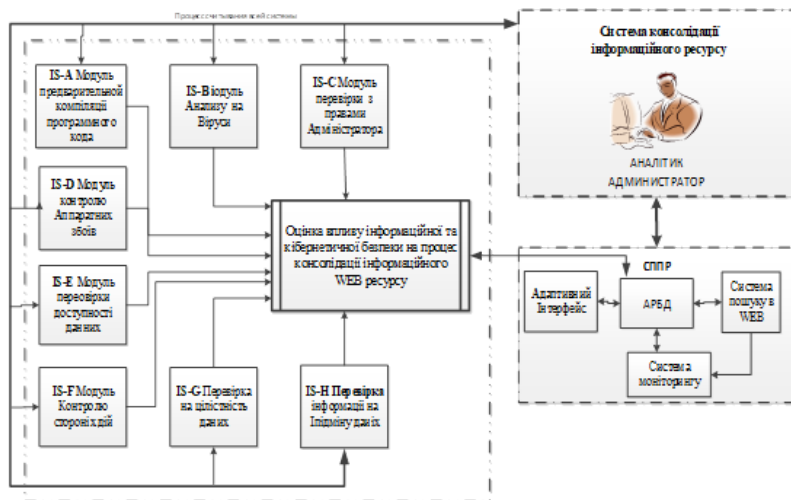


Рисунок 1 – Інформаційна модель оцінки впливу інформаційної та кібернетичної безпеки на процес консолідації інформаційного WEB ресурсу.

- фактори, пов'язані зі станом користувача: такі як психофізіологічні та когнітивні аспекти;
- робота модулів контролю пов'язаних з забезпеченням інформаційної та кібернетичної безпеки системи консолідації інформаційного веб ресурсу.

Робота модулів захисту системи охоплює комплекс технологій та процедур, призначених для забезпечення безпеки системи консолідації інформаційного веб-ресурсу. Модулі захисту включають функції, як-от шифрування даних, аутентифікація користувачів, захист від вірусів та шкідливого ПЗ, фільтрація трафіку та моніторинг аномалій у мережі. Вони відіграють критичну роль у виявленні, запобіганні та реагуванні на кіберзагрози, забезпечуючи захист від зовнішніх та внутрішніх вторгнень. Ефективність цих модулів залежить від їхньої спроможності

адаптуватися до постійно змінюваного ландшафту загроз, а також від регулярних оновлень та підтримки.

Для оцінки стану захищеності системи консолідації WEB ресурсу, використовуються Байесовські мережі довіри (БМД), які дозволяють моделювати складні взаємозалежності між численними факторами безпеки та захищеності. Такі мережі допомагають передбачити ймовірність виникнення певних загроз та визначити, які контрзаходи будуть найбільш ефективними для запобігання або мінімізації наслідків атак.

Виходячи з цього, на підставі схеми інформаційної моделі (рис.1), для оцінки факторів впливу інформаційної і кібернетичної безпеки з урахуванням психофізіологічних та когнітивних аспектів на процес консолідації інформаційного WEB ресурсу побудована БСД (рис. 2). При побудові її структури та таблиць умовних ймовірностей використовувалися експериментальні дані та знання експертів [4].

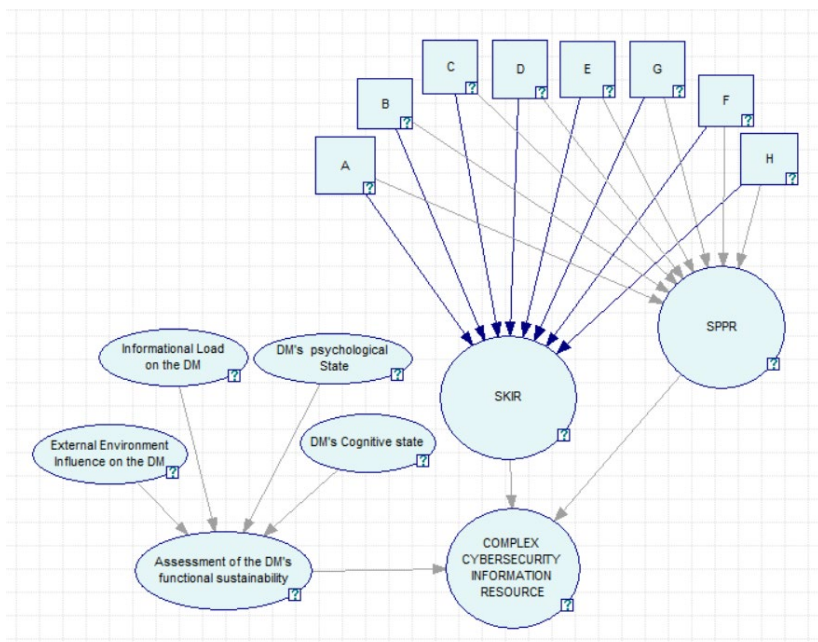


Рисунок 2 – БМД оцінки стану захищеності системи консолідації WEB ресурсу.

У моделі застосовано ймовірнісний математичний підхід і розроблена БМД яка представляє собою графічні моделі, що ґрунтуються на принципах теорії ймовірностей та теорії графів. Вони складаються з пар $\langle G, B \rangle$, де G – це спрямований ациклічний граф, що представляє випадкові змінні, а B – набір параметрів, які визначають структуру системи.

Повна загальна ймовірність БМД обчислюється по формулі (1)

$$P_B(X^{(1)}, \dots, X^{(N)}) = \prod_{i=1}^N P_B(X^{(i)} | P_A(X^{(i)})) \quad (1)$$

де A – множина станів модулів безпеки; $N = (x_1, \dots, x_N)$ – вектор параметрів їх розподілів.

Умовна ймовірність події визначається співвідношенням (2)

$$p(E | H_k) = \frac{p(E \cap H_k)}{p(H_k)}, \quad (2)$$

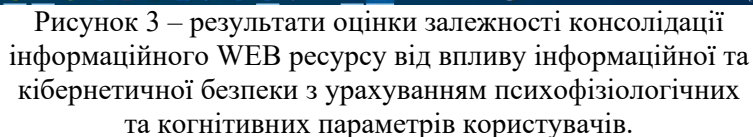
де E й H_k – зв'язані між собою змінні. Ця залежність дозволяє визначити, яка буде ймовірність події E , якщо має місце конкретна подія H_k . Взаємовиключні події формують вичерпну множину у випадку зображеному формулою (3)

$$U_{i=1}^n E_i = \Omega \quad (3)$$

де $\sum P$ – сума значень ймовірностей значення i -го фактору, при різних заданих значеннях вихідної змінної. Очевидно, що чим вище коефіцієнт максимальної зміни ймовірностей, тим більше чутлива система до даного вхідного параметра, отже, значимість даного параметра буде більш вагомою.

Використовуючи результати експертних оцінок обчислення ймовірностей по БМД проводилось за допомогою спеціалізованого

програмного пакета Genie 2.0. На рис. 3 наведений приклад результатів оцінки факторів впливу інформаційної і кібернетичної безпеки з урахуванням психофізіологічних та когнітивних параметрів користувачів [5].



Висновки. В роботі розроблено та запропоновано технологію оцінки залежності консолідації інформаційного WEB ресурсу від впливу інформаційної і кібернетичної безпеки з урахуванням психофізіологічних та когнітивних параметрів користувачів з застосуванням сучасних новітніх інтелектуальних та інформаційно – когнітивних технологій.

1. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2021) (Україна). <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

web-site: conference.nuos.edu.ua | email: conference@nuos.edu.ua; tel (+380512) 709444; 709105|

3. Jain P., Pasman H. J., Waldram S., Pistikopoulos E. N., Mannan M.S. Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. Journal of Loss Prevention in the Process Industries. 2018. V. 53. P. 61–73.

4. V. Peredery, M. Voronenko, E. Borchik and J. Krejci, "Information Technology of Operative Formation and Evaluation of Relevant Alternatives of Decision-Making in Human-Machine Systems of Critical Application," 2018 IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2018, pp. 33-36, doi: 10.1109/STC-CSIT.2018.8526750.

5. Передерій В.І. Інтелектуальні та інформаційно-когнітивні технології підтримки прийняття рішень: Навчально-методичний посібник / В.І. Передерій, С.М. Нужний – Миколаїв: НУК, 2024. – 137 с. (Затверджено Грифом Вченої ради НУК, протокол № 2 від 23.02.2024 року)

СЕКЦІЯ 3. ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 004.056.5;057.2

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО РАНЖУВАННЯ ЗАГРОЗ ЗА ISO/IEC 27005:2022

Автор: Іванюк А.О., магістриня, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Турти М.В., к.т.н., доцентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Організаційно-технічна модель кіберзахисту 2021 року [1], Стратегія кібербезпеки України [2] і планів її реалізації [3, 4] передбачають розвиток систем виявлення та реагування на кіберзагрози з метою ефективного управління ризиками інформаційної безпеки (РІБ) і забезпечення кіберготовності та кіберстійкості об'єктів інформаційної діяльності (ОІД), особливо об'єктів критичної інфраструктури.

Захист кіберпростору передбачає організацію ефективної протидії актуальним загрозам, визначення котрих передбачає проведення моніторингу і аналізу стану кіберпростору, створення і застосування ефективної системи індикаторів кіберзагроз, прогнозування появи загроз різних типів, їх очікуваних наслідків і визначення відповідних ризиків.

На даний час прийнято проводити аналіз факторів РІБ і оцінювання ризиків шляхом евристичних експертних оцінок. При цьому можуть застосовуватися десятки методів оцінки ризиків [5], вибір серед яких складно здійснити [6]. Визначення РІБ проводиться на основі прийнятих дослідником класифікації загроз, моделі загроз і методів оцінки ризиків, які мають узгоджуватися з діючими нормативними документами. Цим питанням присвячені роботи багатьох науковців та практиків як в Україні, так за кордоном [6-14], однак залишається невирішеною задача автоматизації процесів визначення рангів загроз за їх критичністю згідно із відповідності з міжнародними стандартами.

Метою даної роботи є розробка системи підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- провести аналіз відкритої нормативно-правової бази і визначити принципи та процедури ранжування загроз;
- визначити критерії і правила прийняття рішень щодо рангів загроз;
- розробити основні алгоритми і структуру системи підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022.

Ранжування загроз – це процес віднесення загроз до певного поіменованого діапазону заданого критерію. Ранг загрози визначається за асоційованою із загрозою мірою ризику. Міра ризику може бути кількісною або якісною. Існує багато кількісних мір ризиків, які різняться як за розрахунковими формулами, так і за розмірністю: можуть бути виражені у грошовій або безрозмірній формі. Ризик, асоційований із загрозою, у кількісній формі є очікуваним збитком в разі успішної реалізації загрози. Якісна міра ризику є поіменованим діапазоном кількісної міри, наприклад, «високий», «середній», «низький», тобто фактично визначає ранг ризику з міркувань його критичності. Таким чином, для визначення рангів загроз необхідно сформувати перелік загроз, які підлягатимуть аналізу, обрати міру ризику і спосіб її визначення. Для складання переліку загроз необхідно прийняти певну класифікацію загроз. На даний час існує багато класифікацій загроз, наприклад, виділяють:

- в НД ТЗІ [15]: загрози конфіденційності, цілісності, доступності і спостережуваності інформації;
- в моделі STRIDE [16]: підміна мережевих об'єктів, модифікація даних, відмова від авторства, розголошення інформації, відмова в обслуговуванні, несанкціоноване підвищення рівня привілеїв;
- загрози, що характерні для певної предметної галузі, наприклад: загрози безпеці державних інформаційних ресурсів [14], загрози соціального інжинірингу [9], загрози критичній інфраструктурі [11], загрози для соціально-економічних процесів [13] тощо;
- в ISO/IEC 27005 [17], якому відповідає ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT), ідентифікація ризику передбачає обов'язкову ідентифікацію джерел ризику, подій, їх причин та потенційних наслідків,

а також може включати історичні дані, теоретичний аналіз, інформовані та експертні думки та потреби стейкхолдерів. Наприклад, джерелом загроз може бути людина, яка створює загрозу цілеспрямовано або внаслідок випадкової помилки, або природа, дії якої не є цілеспрямованими. В ISO/IEC 27005:22 передбачено, що від певних джерел можуть надходити загрози різних типів, наприклад: технічні відмови; втрата необхідних сервісів; компрометація інформації і функцій; несанкціоновані дії тощо;

- в моделі загроз DSECCT компанії Digital Security [18]: загрози класифікуються за характером загрози, видом впливу, джерелами та за цільовими об'єктами загрози;

- в моделі OCTAVE [19]: передбачено різний ступінь деталізації первинного опису загроз і ризиків для великого і малого бізнесу тощо.

В даній роботі за основу прийнято класифікацію загроз, наведену в [12].

Оскільки ранжування загроз здійснюється за рівнем асоційованих з ними ризиків, то воно може бути проведене тільки після оцінювання ризиків як процедура перевірки належності відповідного ризику певному діапазону чи групі діапазонів ризиків. Після цього за правилами, визначеними в процесі менеджменту ризиків на етапах визначення контексту та ідентифікації ризиків, загрози певних рангів визнаються критичними у різному ступені.

Таким чином, входними даними для СППР ранжування загроз є дані, які мають бути отримані на етапі визначення контексту та ідентифікації ризиків, зокрема:

- сфера управління ризиками і джерела загроз;
- перелік інформаційних активів із визначеною цінністю, з переліками наявних вразливостей; і переліків асоційованих з ними загроз;
- перелік сценаріїв виникнення і реалізації загроз із визначеними джерелами загроз, активами-об'єктами атаки, ймовірностями виникнення кожного сценарію.

Опис сценаріїв також включає в себе:

- оцінки ймовірностей виникнення кожної загрози, асоційованої з певним активом;
- оцінки ймовірностей експлуатації кожною загрозою певних вразливостей, асоційованих з певним активом;

- оцінки ймовірностей успіху реалізації загроз при експлуатації певних вразливостей кожного активу;
- оцінки наслідків успіху реалізації загроз при експлуатації певних вразливостей кожного активу.

Визначення, оцінювання і аналіз ризиків здійснюється для кожного сценарію. Аналіз ризиків може здійснюватися для всієї множини обчислених ризиків або для окремої вибірки, яка формується за заданим ОПР критерієм, наприклад, ризики для певного активу або ризики, що асоційовані із загрозою порушення цілісності даних. Ранжовані ризики є основою для визначення рангів загроз, після чого СППР формує і видає ОПР звіт про отримані результати. На підставі цього звіту ОПР приймає рішення або про обробку ризиків або про проведення повторного аналізу загроз за більш детальним сценарієм.

Узагальнений алгоритм ранжування загроз за міжнародним стандартом ISO/IEC 27005:2022 наведено на рис.1.

Ранжування ризиків здійснюється за алгоритмом, наведеним на рис.2. При цьому користувач має задати кількість рангів ризиків NR і граничні значення ризиків a_n, b_n , що відповідають кожному n -ому рангу. На вхід блоку ранжування ризиків подається множина ризиків $\{R_{ijk}\}$, де i – номер активу, j – номер загрози, k – номер вразливості за рахунок успішної експлуатації котрої реалізується загроза. Ці номери визначаються із опису сценаріїв.

Ранжування загроз здійснюється за алгоритмом, наведеним на рис.3, який передбачає, що аналіз проводиться для певного активу. Кількість рангів загроз NZ задається ОПР. Послідовно переглядаються всі загрози і їх ранг визначається як m при умові, що сумарний ризик, асоційований із загрозою потрапляє в діапазон, обмежений значеннями $c_m = 1 + (m-1) \frac{NR}{NZ}$ і $d_m = c_m \frac{NR}{NZ}$. Ранги присвоюються у порядку зрос-

тання ризиків, тому, якщо загроза за різними сценаріями може експлуатувати різні вразливості, що матиме різні наслідки і, відповідно, ризики, то ранг цієї загрози буде перевизначатися. Остаточню загрозу буде присвоєно ранг, що відповідатиме максимальному ризику.

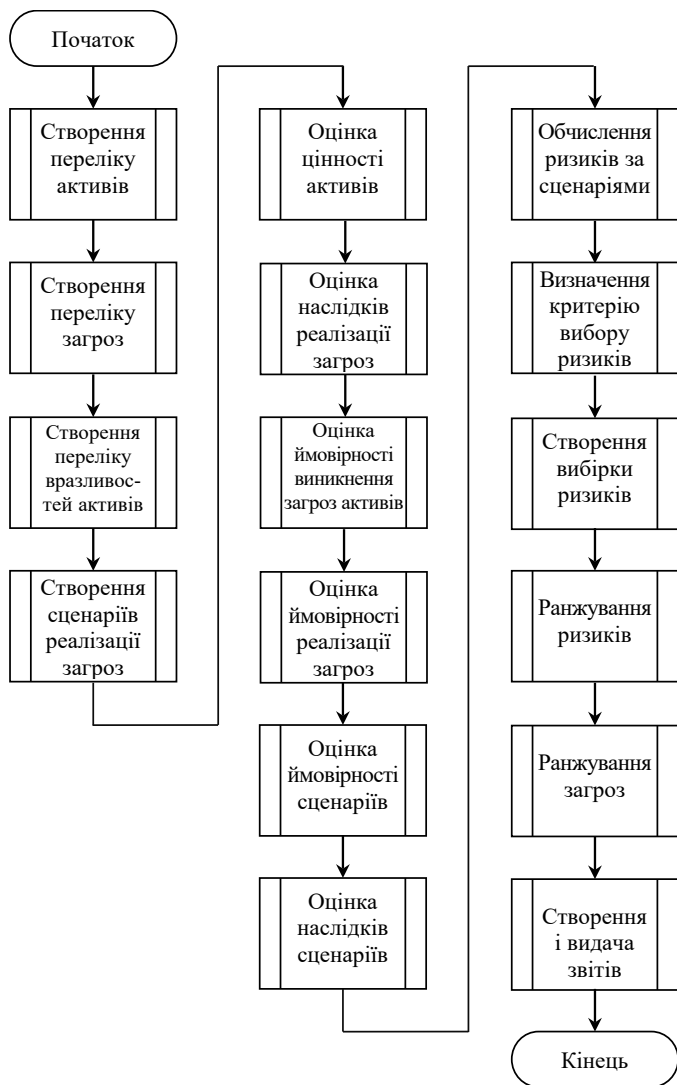


Рисунок 1 – Узагальнений алгоритм ранжування загроз за міжнародним стандартом ISO/IEC 27005:2022

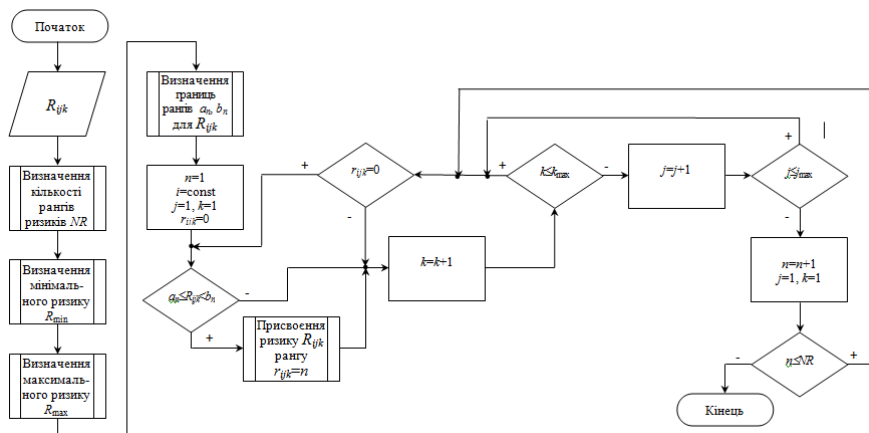


Рисунок 2 – Алгоритм блоку «Ранжування ризиків»

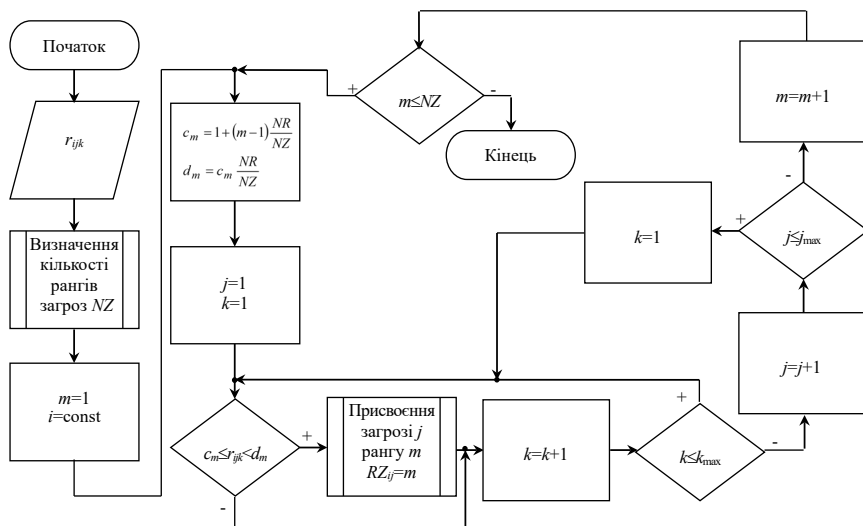


Рисунок 3 – Алгоритм блоку «Ранжування загроз» для i-го активу

2. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука безпечного розвитку країни. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n7>
3. План реалізації Стратегії кібербезпеки України. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>
4. План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України URL: <https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text>
5. ДСТУ EN IEC 31010:2022 Керування ризиками – методи оцінки ризиків (EN IEC 31010:2019, IDT; IEC 31010:2019, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=100889
6. Карпович І., Гладка О., Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки. *Технічні науки та технології*. 2021. №1(23). С.62–68. URL: <http://tst.stu.cn.ua/article/view/233549/232282>
7. Carfora M., Martinelli F. Cyber Risk Management: An Actuarial Point of View. *Journal of Operational Risk*. 2021. Vol.4. №4. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3778061
8. Top 10 emerging cyber-security threats for 2030. URL: <https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030>
9. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. К.: ДУТ, 2015. 288 с. URL: http://www.dut.edu.ua/uploads/p_r_303_79299367.pdf
10. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія. Київ: ЦП «Компринт», 2017. 435 с.
11. Салієва О.В., Яремчук Ю.Є. Визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури ранжуванням загроз. *Реєстрація, зберігання і обробка даних*. 2020. Т. 22. № 2. С.63-76. URL: <http://drsp.ipri.kiev.ua/article/view/211279>
12. Турти М.В.; Доценко В.В. Інформаційна модель ранжування загроз за BS ISO/IEC 27005:2011. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали X Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК, 2022. С.134-140.

URL: <https://www.nuos.edu.ua/wp-content/uploads/2023/05/SPIBT-2022-Materiali-s-obkladinkoju.pdf>

13. Шандрівська О. Є., Шинкаренко Н. В. Прикладна оцінка ризиків у системі забезпечення безпеки соціально-економічних процесів у кіберпросторі. *Вісник Національного університету “Львівська політехніка”*. Серія “Проблеми економіки та управління”. 2020. №2(8). С.94-104.

14. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія. К.: НАУ, 2015. 214 с. URL: https://er.nau.edu.ua/bitstream/NAU/31911/1/Monogr_klas_zagroz_Yudin_Buchyk.pdf

15. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. URL: <http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342>

16. Зубок В.Ю. Оцінювання ризиків глобальної маршрутизації. *Електронне моделювання*. 2019. Т.41. №2. С.97-109. URL: <https://www.emodel.org.ua/images/em/41-2/Zubok.pdf>

17. ISO/IEC 27005:2022(en) Information security, cybersecurity and privacy protection — Guidance on managing information security risks URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-4:v1:en>

18. Лисенко І. А. Методичні вказівки до виконання практичних робіт з навчальної дисципліни “Основи управління кібербезпекою”. Кропивницький: ЦНТУ, 2018. 64 с. URL: <https://dspace.kntu.kr.ua/server/api/core/bitstreams/3256be49-4ce2-4178-a396-1c1136b8a237/content>

19. Alberts C., Dorofee A., Stevens J., Woody C. Introduction to the OCTAVE® Approach. Pittsburgh, Pennsylvania, United States: Carnegie Mellon University. 2003. 27 p. URL: <https://www.itgovernanceusa.com/files/Octave.pdf>

УДК 004.056.5

НОРМАТИНО-ПРАВОВА БАЗА КІБЕРБЕЗПЕКИ ГАЛУЗІ ВОДНОГО ТРАНСПОРТУ

Автор: Хван Ю.В., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Турти М.В., к.т.н., доцентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Бурхливий розвиток цифровізації усіх галузей господарства, суспільного і політичного життя, військової справи зумовлює актуальність захисту інформації у всіх сферах людської діяльності. Водний транспорт є важливою складовою сучасних логістичних систем, належить до критичної інфраструктури і має велику кількість стейкхолдерів. Відповідно, кібербезпеки в цій галузі регламентується нормативно-правовими актами, що видаються законодавчими і виконавчими органами влади, міжнародними організаціями, галузевими відповідальними органами, місцевими органами влади, керівництвом окремих портів, судноплавних компаній тощо [1-12]. Кількість цих документів постійно зростає. Крім того, розвитком теоретичних основ кібербезпеки водного транспорту займаються займаються вітчизняні і зарубіжні науковці [13-17], які у своїх роботах визначають проблеми захисту інформації в галузі і пропонують методи для їх вирішення. Таким чином, актуальною задачею управління кібербезпекою в галузі водного транспорту є систематизація інформації щодо нормативно-правових актів, що є чинними для вирішення прикладних задач в галузі, і розробка засобів обробки цієї інформації.

Метою даної роботи є розробка структури бази даних відкритих нормативно-правових актів в галузі водного транспорту.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- провести аналіз відкритих літературних джерел і визначити типи інформаційних блоків, які мають бути включені в базу даних, і їх

параметри, що можуть використовуватися при вирішенні конкретних прикладних задач кібербезпеки у галузі водного транспорту;

- визначити перелік типових запитів до розроблюваної бази даних;
- розробити структуру бази даних відкритих нормативно-правових актів в галузі водного транспорту.

Інформацію, яка має бути представлена в базі даних можна умовно поділити на дві частини – нормативно-правові акти і публікації у відкритих джерелах. З метою нормалізації бази даних доцільно інформацію, яка може використовуватися для описів документів чи відповідати на деякі типові запити, винести в окремі допоміжні таблиці.

В базі даних має бути представлена інформація щодо нормативно-правових актів, які стосуються різних аспектів управління інформаційною безпекою на водному транспорті:

- опису загроз і вразливостей інформаційної безпеки для портів і суден, наприклад, на підставі [2-4, 6];
- вимог стейкхолдерів, країн, міжнародних і національних організацій до забезпечення кібербезпеки, наприклад, на підставі [1-12];
- вимог щодо обробки ризиків, наприклад, на підставі [2, 3, 8-12];
- рекомендацій щодо найкращих практик забезпечення кібербезпеки в галузі водного транспорту [2-4, 6, 7];
- опису процесів інформаційного обміну в галузі [5].

Наприклад, ISO 24060:2021 Ships and marine technology — Ship software logging system for operational technology (укр. Судна та морська технологія — Програмна система реєстрації суден для операційної технології) є міжнародним стандартом [5], виданим Міжнародною організацією із стандартизації, який визначає систему реєстрації і моніторингу стану програмного забезпечення (ПЗ) судна, зокрема:

- реєструє версії програмного забезпечення для судового обладнання;
- встановлює порядок реєстрації в журналі фактів встановлення обладнання або виявлення ПЗ, порядок автоматичної реєстрації звітів, надісланих обладнанням, і порядок розміщення у сховищі електронних звітів про послуги, пов'язаних із записами журналу.

ISO 24060:2021 вимагає, щоб ПЗ було зареєстроване, і можна було б отримати інформацію про його поточний робочий стан, що з точки

зору кібербезпеки є корисним для виявлення причин кіберінцидентів, пов'язаних із використанням певного ПЗ, певного судового операційного технологічного обладнання та інтегрованих систем, включаючи, системи електрогенерації, контролю і сигналізації, навігації та зв'язку, рульового керування тощо.

Розроблювана база даних повинна формувати звіти за результатами типових запитів, зокрема, надавати користувачу відповіді на наступні питання:

- які нормативні документи і/або публікації пов'язані із вирішуваною користувачем задачею (за ключовими словами, що задаються користувачем);
- які документи є обов'язковими/рекомендованими для виконання в заданій сфері;
- чи є певний документ чинним і в якій сфері, і з якого часу;
- ким і коли був затверджений/відмінений документ;
- чи були наявні попередні версії документів і коли вони були чинними або на заміну якому документу був прийнятий даний документ; чи планується і коли видання нової версії.

База даних повинна дозволяти користувачу отримувати переліки нормативно-правових актів, рекомендацій і публікацій, що є і/або були чинними у певній сфері; визначати органи, які випускали нормативні акти у заданій сфері, науковців і практиків, що займаються розробкою теорії і засобів кібербезпеки у заданій сфері; ознайомлюватися з оригіналами нормативно-правових актів і рекомендацій, їх перекладами, науковими публікаціями і практичними рекомендаціями, а у разі відсутності оригіналів у вільному доступі – з описами і умовами отримання; планувати власну діяльність на підставі інформації про заплановані зміни нормативно-правових актів.

Для вирішення цих завдань опис документу має містити наступну інформацію:

- назва документу;
- посилання на документ: посилання на документ мовою оригіналу, посилання на переклад/переклади документу;

- стан документу: чинний/ не чинний;
 - сфера дії: опис;
 - обов’язковість: обов’язковий для сфери дії, рекомендації;
 - ключові слова: перелік;
 - зміст: опис;
 - відповідальний орган: група [18] (Верховна Рада, Президент України, Кабінет міністрів України, Адміністрація Держспецзв’язку, Національний банк України, міністерство, служба, агентство, інспекція, ЦОВВ зі спеціальним статусом, колегіальні органи, інші центральні органи виконавчої влади, місцеві органи влади, міжнародна організація, зарубіжна організація, група організацій тощо), орган, країна/країни;
 - затверджуючий документ: тип (Закон України, міжнародний стандарт, ДСТУ, НД ТЗІ, Постанова кабінету міністрів України, Розпорядження Кабінету міністрів України, Указ Президента України, Наказ Адміністрації Держспецзв’язку, Наказ Міністерства (назва)), дата прийняття документу (день, місяць, рік), номер документу, введення в дію (день, місяць, рік);
 - втрата чинності: дата (день, місяць, рік), підстава (опис документу);
 - пов’язані документи: перелік і посилання;
 - пов’язані публікації: перелік і посилання (підручники, наукові статті, тези доповідей на наукових конференціях, web-публікації тощо);
 - версії документа: попередні версії (назва, часові рамки чинності, посилання), заплановане оновлення (дата, джерело інформації).
- Опис публікацій повинен мати реквізити згідно з [19], наприклад для книги – автори, назва, місце публікації, видання, рік, кількість сторінок, гіперпосилання.

Структура бази даних наведена на рис.1.

Висновки

В даній роботі проведено аналіз відкритих літературних джерел і визначені типи інформаційних блоків в базі даних і їх параметри, типові запити до розроблюваної бази даних; розроблена структура бази даних відкритих нормативно-правових актів в галузі водного транспорту.

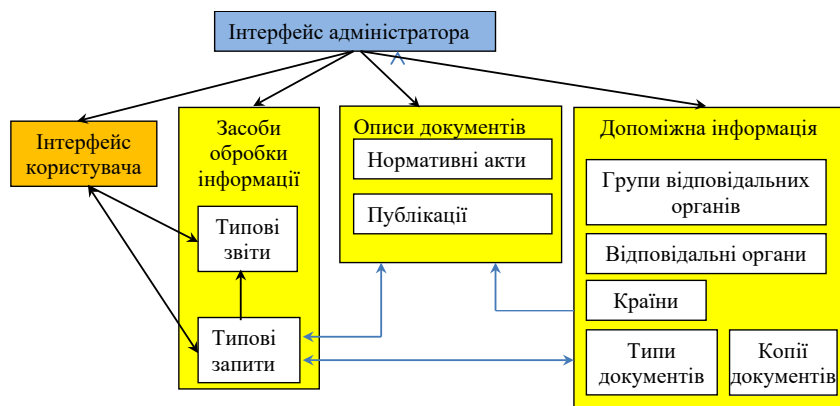


Рисунок 1 – Структура бази даних

Список літератури:

1. IACS E22. Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e22_rev.3_june_2023_ul.pdf
2. IACS UR E26 Cyber resilience of ships. URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf
3. IACS UR E27 Cyber resilience of on-board systems and equipment. URL: <https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103854/UR-E27-Rev.1-Sep-2023-UL.pdf>
4. IAPH Cybersecurity Guidelines for Ports and Port Facilities. URL: https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf
5. ISO 24060:2021 Ships and marine technology — Ship software logging system for operational technology. URL: <https://www.iso.org/ru/standard/77678.html>
6. Recommendation on Cyber Resilience No.166. URL: <https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/24150438/rec-166-corr2-apr-2022-ul.pdf>
7. Rules for the survey and construction of steel ships. Part X. Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/rules/465_part_x_e_202406.pdf

8. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. URL: https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400

9. Наказ № 23 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів КІ». URL: <https://zakon.rada.gov.ua/rada/show/v0023519-21#Text>

10. Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг Постанова № 4 Правління Національного банку України від 16.01.2021 URL: <https://zakon.rada.gov.ua/laws/show/v0004500-21#Text>

11. Про критичну інфраструктуру. Закон України URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

12. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука безпечного розвитку країни. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n7>.

13. Juan Ignacio Alcaide, Ruth Garcia Llave. Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*. 2020. Volume 45. Pages 547–554. URL: <https://www.sciencedirect.com/science/article/pii/S2352146520302209>

14. Баронова О., Турти М., Ганчо С. Визначення рівня впливу кіберзагроз на розвиток морської галузі. *Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ICT-2020»*. Харків: ХНУРЕ, 2020. С.275-278.

15. Веремчук В.С. Міжнародно-правове регулювання кібербезпеки у морській галузі: сучасний стан та перспективи розвитку. *Вісник Одеського Національного ун-ту. Серія: Правознавство*. 2024. Т.26. Випуск 1(38). С.112-117. URL: <https://journals.visnyk-onu.od.ua/index.php/law/article/view/472/462>

16. Грищенко С.Л. Принципи інтелектуального управління інформаційною безпекою корпоративної мережі порту. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК,

2023. С.168-175. URL: <https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf>

17. Трофименко А.О., Майданевич С.Б., Войченко Т.О., Дорофєєва З.Я. Деякі проблемні питання впровадження стандартів кібербезпеки на морському транспорті. *Водний транспорт*. №.1(37). 2023. С.179–188. URL: <https://vt.duit.in.ua/index.php/home/article/view/267/224>

18. Інші органи виконавчої влади <https://www.kmu.gov.ua/catalog>

19. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення. URL: https://dnaop.com/html/61984/doc-ДСТУ_3008_2015

СЕКЦІЯ 4. МОДЕЛЮВАННЯ ОБ'ЄКТІВ І ПРОЦЕСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.5: 534.[784: 835]: 621.391.883

ОЦІНЮВАННЯ ЗВУКОІЗОЛЯЦІЇ АКУСТИЧНИХ СИГНАЛІВ ОГОРОДЖУВАЛЬНИМИ КОНСТРУКЦІЯМИ РЕЖИМНИХ ПРИМІЩЕНЬ

***Автори:** Касьянов Ю.І., ст. викладач; Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. Оскільки мова є акустичним сигналом, то захист мовної інформації з обмеженим доступом на об'єктах інформаційної діяльності, як правило починається з перевірки можливих акустичних і віброакустичних каналів витоку і розробки заходів захисту для їх закриття. Роботи з побудови системи захисту при цьому перш за все ґрунтуються на оцінці існуючої та забезпечення необхідної звукоізоляції виділених приміщень (ВП).

Існуючі методики оцінки ефективності звукоізоляції, в тому числі в області інформаційної безпеки, побудовані на співставленні рівня сигналу до і після огорожувальної конструкції в октавних смугах мовного діапазону [1] або індексу звукоізоляції повітряного шуму [2, 3]. Однак оцінка ефективності звукоізоляції огорожувальних конструкцій режимних приміщень потребує комплексного підходу.

Метою роботи є розробка основ методики оцінювання ізоляції акустичних (мовних) сигналів огорожувальними конструкціями, що відокремлюють режимні приміщення від інших приміщень, за частотними характеристиками і індексом ізоляції повітряного шуму.

Основна частина. Захист мовної інформації є досить дорогим і складним заходом, тому на підприємствах і в установах облаштовуються спеціальні виділені приміщення (ВП) з гарантованим захистом акустичної інформації.

Виділені (режимні) приміщення, як об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом (ІзОД) підлягають обов'язковому категоріюванню,

яке здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації на об'єкті [4]. При цьому ознакою, за якою здійснюється категоріювання є ступінь обмеження доступу до інформації, що обробляється та/або озвучується на об'єкті інформаційної діяльності (ОІД). В Україні встановлено 4 категорії виділених приміщень залежно від правового режиму доступу до інформації [5].

Категорії щодо ступеня захищеності інформації з обмеженим доступом у виділених приміщеннях означають [6]:

- приховання факту проведення закритих заходів;
- приховання предмету закритих заходів;
- приховання змісту закритих заходів;
- приховання змісту переговорів від ненавмисного прослуховування.

Щодо захисту мовної інформації звукоізоляція виділених приміщень вирішує подвійну задачу. По-перше, вона спрямована на локалізацію акустичної інформації з обмеженим доступом усередині ВП і виключення витоку цієї інформації по прямому акустичному та вібраційному каналах (забезпечує конфіденційність інформації). По-друге, забезпечує захист інформації в процесі мовної комунікації від спотворення чи втрат в результаті дії зовнішніх шумів, тобто цілісність інформації. Ця задача подібна до задачі, що вирішується в будівельній та санітарній практиці.

При формуванні конкретних технічних вимог до звукоізоляції виділених приміщень виходять з норм, що відповідають категорії ВП, рівнів інформативних акустичних сигналів у даному приміщенні, рівнів фонових акустичних шумів та місця знаходження приміщення. В табл.1 наведено вимоги, взяті з відкритих джерел [7].

Було проаналізовано існуючі методики оцінювання ефективності звукоізоляційних конструкцій [1-3], які брались за основу для розробки методики оцінювання ізоляції акустичних (мовних) сигналів огорожувальними конструкціями, що відокремлюють режимні приміщення від інших приміщень, за частотними характеристиками і індексом ізоляції повітряного шуму.

Таблиця 1– Вимоги до звукоізоляції різних категорій приміщень

Частота, Гц	Категорія виділеного приміщення та ступінь звукоізоляції, дБ		
	1 категорія	2 категорія	3 категорія
500	53	48	43
1000	56	51	46
2000	56	51	46
4000	55	50	45

В розробленій методиці вимірювання ізоляції повітряного шуму внутрішніми огорожувальними конструкціями полягає у порівнянні середніх рівнів звукового тиску в приміщеннях високого і низького рівнів та розрахунку звукоізоляції огорожувальної конструкції у смугах частот.

Приміщенням високого рівня є приміщення, що захищається від витоку акустичної (мовної) інформації (виділене приміщення). Приміщенням низького рівня є суміжне з ним приміщення, в якому можливим є знімання інформації.

Джерело тестового сигналу, що імітує інформативний (небезпечний) сигнал у виділеному приміщенні, повинно створювати у приміщенні високого рівня дифузне звукове поле. В якості джерела використовується акустична система з генератором шуму та підсилювачем.

Тестовий сигнал представляє собою широкосмуговий шум із неперервним спектром. Рекомендується застосовувати "білий" або "рожевий" шум. Можливе використання широкосмугового шуму зі спектром довготривалої мови, тобто його рівні в третьоктавних чи октавних частотних смугах повинні відповідати рівням довготривалого мовленнєвого сигналу заданого інтегрального рівня сигналу.

Відстань між джерелом шуму і огорожувальними конструкціями приміщення високого рівня повинна бути не меншою ніж 0,7 м, а між джерелом шуму і випробовуваною конструкцією – не меншою ніж 2,5 м.

Вимірювання рівнів звукового тиску в приміщеннях високого і низького рівнів треба проводити не менше ніж у шести точках.

Точки вимірювань (точки розташування мікрофонів) у приміщеннях високого і низького рівнів повинні бути рівномірно розподіленими по всьому об'єму, але при цьому не повинні знаходитися на відстані, меншій ніж 0,5 м від поверхонь огорожувальних конструкцій або дифузорів і не меншій ніж 1 м від випробовуваної конструкції і джерел шуму. Відстань між окремими позиціями мікрофонів повинна бути не меншою ніж 0,7 м.

Вимірювання рівнів звукового тиску в кожній точці приміщень високого і низького рівнів треба проводити в третиннооктавних смугах з середньгеометричними частотами 100, 125, 160, 200, 250, 315, 400, 500, 630, 800, 1000, 1250, 1600, 2000, 2500, 3150 Гц. За необхідності отримання додаткової інформації частотний діапазон вимірювань може бути розширеним у бік низьких частот (смуги з середньгеометричними частотами 50, 63, 80 Гц) і у бік високих частот (смуги з середньгеометричними частотами 4000, 5000 Гц). Допускається проведення вимірювань в октавних смугах частот. При цьому вимірювання треба проводити у смугах з середньгеометричними частотами 125, 250, 500, 1000, 2000, 4000, 8000 Гц.

Середні рівні звукового тиску L_i , дБ у кожній i -й смузі частот у приміщеннях високого і низького тиску визначають за формулою

$$L_i = 10 \lg \left(\frac{1}{n} \sum_{k=1}^n 10^{0,1 L_k} \right), \quad (1)$$

де L_k – рівень звукового тиску в k -й вимірювальній точці, дБ; n – кількість точок вимірювання.

Ізоляцію повітряного шуму огорожувальною конструкцією R , дБ, визначають у кожній i -й смузі частот за формулою, що враховує підвищення заміряного рівня звукового тиску у суміжному приміщенні за рахунок відбивання від його конструкцій,

$$R_i = L_{1i} - L_{2i} + 10 \lg \frac{S}{A_2}, \quad (2)$$

де L_{1i} – середній рівень звукового тиску в i -й смузі частот у приміщенні високого рівня; L_{2i} – середній рівень звукового тиску в i -й смузі частот у приміщенні низького рівня; S – площа поверхні випробовуваної конструкції; A_2 – еквівалентна площа звукопоглинання в приміщенні низького рівня.

Еквівалентну площу звукопоглинання у приміщенні низького рівня визначають у кожній смузі частот за формулою

$$A_2 = \frac{0,16 \cdot V}{T_2}, \quad (3)$$

де V – об'єм приміщення низького рівня, м^3 ; T_2 – час реверберації в приміщенні низького рівня, с (вимірюють у відповідності до ГОСТ 24146).

За результатами вимірювань і розрахунків будується частотна характеристика звукоізоляції і робляться висновки, щодо забезпечення нормативних значень.

Індекси ізоляції повітряного шуму R_w або R'_w огорожувальної конструкції визначаються на основі частотних характеристик звукоізоляції, отриманих за результатами вимірювань шляхом їх порівняння зі стандартною оціночною частотною характеристикою ізоляції повітряного шуму, побудованою в тих же координатах (рис.1).

Розрахунок виконується за ДСТУ Б В.2.6-85:2009 [2].

Результати вимірювань треба надавати у протоколі випробувань у вигляді таблиці і графіка для всього діапазону вимірювальних частот.

Висновок: Розроблено основи методики оцінювання ізоляції акустичних (мовних) сигналів огорожувальними конструкціями, що відокремлюють режимні приміщення від інших приміщень, за частотними характеристиками і індексом ізоляції повітряного шуму. Проведено її апробацію.

Методика дає можливість комплексно оцінити ефективність звукоізоляційних конструкцій режимних приміщень.

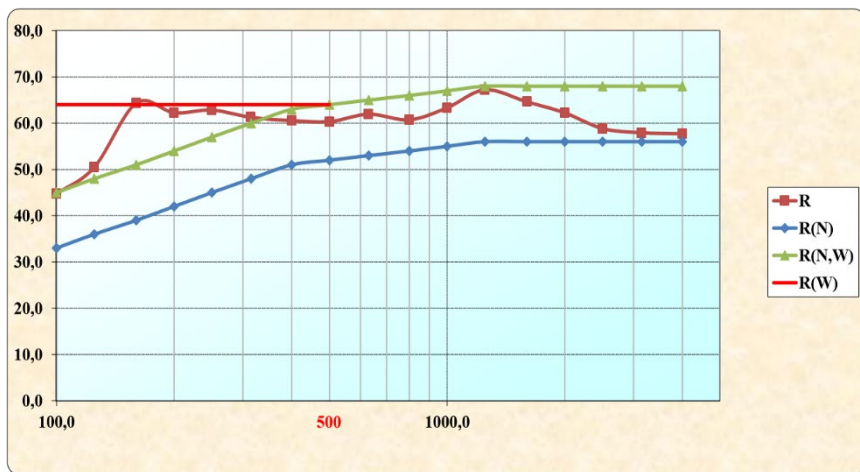


Рисунок 1 – Частотні характеристики звукоізоляції

Список літератури:

1. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. – М.: ООО "Издательство Машиностроение", 2009 – 508 с.
2. ДСТУ Б В.2.6-85:2009 "Конструкції будинків і споруд. Звукоізоляція огорожувальних конструкцій. Методи оцінювання." – Київ: Мінрегіонбуд України, 2010. – 30 с.
3. ДСТУ-Н Б В.1.1-34-2013. Настанова з розрахунку та проектування звукоізоляції огорожувальних конструкцій житлових і громадських будинків. – Київ: Мінрегіон України, 2014. – 88 с.
4. НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці». – Режим доступу: <http://dstszi.kmu.gov.ua>.
5. Комплексні системи захисту інформації: навчальний посібник / Ю.Є. Яремчук, П.В. Павловський, В.С. Катаєв, В.В. Сінюгін – Вінниця: ВНТУ, 2018. – 118 с.

6. Хорев А.А. Способы и средства защиты речевой (акустической) информации от утечки по техническим каналам / А.А.Хорев // Специальная техника. – 2005. – № 5. – С. 54 – 59, № 6. – С. 54 – 62.

7. Торокин А. А. Основы инженерно-технической защиты информации / А.А. Торокин. — М.: Издательство «Ось-89», 1998. — 336 с.

УДК 004.056.53: 534.781

УЗАГАЛЬНЕННЯ СПЕКТРІВ ДОВГОТРИВАЛИХ МОВЛЕННЄВИХ СИГНАЛІВ З ВИКОРИСТАННЯМ МОЖЛИВОСТЕЙ МАТЛАВ

***Автори:** Касьянов Ю.І., ст. викладач; Щербаков М.С., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. Наразі нормування і оцінювання захищеності мовної інформації від витoku акустичними каналами виконується за двома критеріями: відношення сигнал/шум і розбірливості мови в точках можливого знімання інформації (контрольних точках).

Критерій сигнал/шум базується на маскувальній дії шумової завади, використовується вже давно і норми за цим критерієм прив'язані до завади типу «білого шуму» чи фонового транспортного шуму. Його перевагами є простота і оперативність, оскільки дані отримуються простими інструментальними вимірюваннями. Цей критерій поки що використовується і в Україні. Однак, як показав ряд досліджень, даний критерій є неінваріантним до виду шумової завади, тобто при одних видах завад нормоване значення може бути надлишковим, а при інших – недостатнім [1-4]. Тому в провідних країнах світу в практику нормування і оцінювання захищеності мовної інформації впроваджено критерій словесної розбірливості мови, який вже певний час використовувався для оцінювання якості засобів мовного зв'язку та акустики приміщень. Він є первинним чисельним показником зрозумілості мовного повідомлення і норма залишкової словесної розбірливості в точці прослуховування не залежить від виду завади [3]. В сертифікованих методах оцінювання захищеності мовної інформації за критерієм розбірливості формантними методами використовується узагальнений спектр

довготривалої мови. Такі спектри для російської та англійської мови приведені в [5].

Враховуючи, що впровадження критерію розбірливості мови в практику нормування і оцінювання захищеності мовної інформації в Україні видається лише питанням часу, а також те, що службові інформаційні потоки в Україні стали практично україномовними, стоїть задача отримання спектру довготривалої української мови. Дослідження в цьому напрямку та їх результати описані в [6, 7]. Однак при спробі дослідити українські мовленнєві спектри за допомогою програмних спектроаналізаторів виникла проблема їх узагальнення [8].

Метою роботи є розробка і дослідження можливості використання розроблених програмних процедур в середовищі MatLab для узагальнення спектрів довготривалих українських мовленнєвих сигналів.

Основна частина. Узагальнений спектр довготривалих (не менше 15 с) мовленнєвих сигналів отримують шляхом статистичного усереднення спектрів ряду різних дикторів (чоловіків і жінок), тобто шляхом проведення статистичного експерименту.

Дослідження спектрів мовленнєвих сигналів можна проводити у 3 способи [9]:

1) Проведенням акустичних експериментів (інструментально-вимірювальні);

2) Проведенням спектрального аналізу з використанням швидкого перетворення Фур'є в програмних математичних середовищах Mathcad, MatLab тощо.

3) Дослідженнями з використанням спеціальних програм обробки звуку, таких як Sound Forge, SpectraLab, Praat тощо або окремих програмних спектроаналізаторів.

В першому випадку задача узагальнення спектрів вирішується просто, оскільки отримані в результаті інструментальних вимірювань спектри представляють собою масиви даних, які легко обробляються програмними математичними середовищами типу Mathcad. Це підтверджується дослідженнями, описаними в [6, 7], в яких спектри представлялися обвідними середньоквадратичних рівнів звукового тиску в семи октавних смугах мовного діапазону відкладених на

середньоеометричних частотах октавних смуг 125, 250, 500,1000, 2000, 4000, 8000 Гц. Узагальнений спектр визначався як обвідна середньоарифметичних значень рівнів звукового тиску на цих частотах.

В [9] було описано розроблені в Mathcad програмні процедури для отримання узагальнюючого спектру довготривалої мови шляхом обробки зображень спектрів окремих довготривалих мовленнєвих сигналів, отриманих в програмі обробки звуку Sound Forge, оскільки дана програма не має функції узагальнення (усереднення) кількох спектрів і не має навіть можливості виводу чи експорту спектрів у вигляді файлів (масивів) даних, які б можна було використати для подальшої обробки. Однак в процесі такого узагальнення мала місце втрата ряду відліків, коли окремі спектри пересікались, або швидко змінювались. Причому кількість таких втрат різко зростала з ростом кількості спектрів, які узагальнюються.

Тому було розроблено алгоритми і програмні процедури в MatLab, що забезпечували зчитування фонограм, їх нормалізацію, спектральний аналіз з використанням швидкого перетворення Фур'є і узагальнення спектрів шляхом статистичної обробки масивів даних. Було проведено апробацію розроблених засобів для узагальнення 5-ти спектрів довготривалих мовленнєвих сигналів. Використано ті ж фонограми, що і в [9].

Процес отримання узагальненого графіка АЧХ відбувався наступним чином:

1. Здійснювався імпорт п'яти фонограм довготривалих мовленнєвих сигналів тривалістю 15-20 с (зчитування артикуляційних таблиць українських слів) у форматі .wav. Ці файли завантажувалися й аналізувалися по черзі.

2. Розробленими і стандартними програмними засобами виконувалася спектральний аналіз і створювались масиви для зберігання різних даних, необхідних для отримання узагальненого спектра.

3. Розраховувався узагальнений спектр шляхом усереднення.

4. Для кожного файлу виконувалася побудова спектру. Після чого виводився інтерпольований і згладжений узагальнений спектр на загальний графік.

5. У середовищі MatLab на графік так само додано підпис усіх спектрів для кожної з фонограм, а так само підписи осей, заголовок і легенда.

Результат роботи програми наведено на рис.1. Чорна лінія відповідає узагальненому спектру.

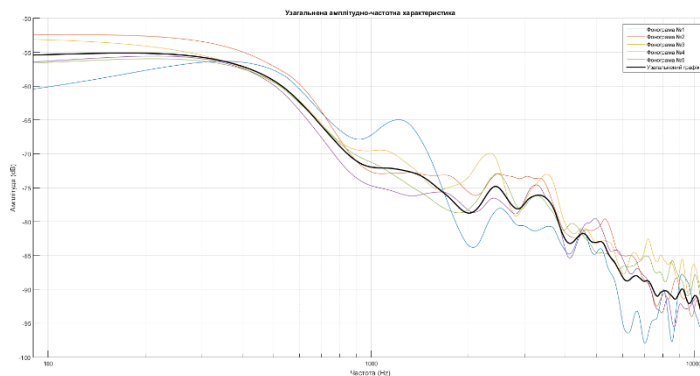


Рисунок 1 – Спектри дикторів та узагальнений спектр

На відміну від процедури обробки зображень, цей метод дає змогу отримати «чистий» графік узагальненого спектру довготривалих мовленнєвих сигналів.

Висновок. 1. Відсутність вбудованих процедур узагальнення та можливості експорту спектру у вигляді масиву даних обмежує використання апаратних і програмних спектроаналізаторів для узагальнюючих статистичних досліджень спектрів. 2. Середовище MatLab дозволяє отримати узагальнюючі спектри для множини довготривалих мовленнєвих сигналів, хоч це і потребує великих масивів у кілька сотен тисяч відліків сигналів.

Список літератури:

1. Хорев А.А. (2001) Методы защиты речевой информации и оценки их эффективности. Специальная техника, № 4, С. 22 – 33.
2. Дидковский В.С., Дидковская М.В., Продеус А.Н. (2008) Акустическая экспертиза каналов речевой коммуникации. Монография. Киев, Имэкс-ЛТД, 420 с.

3. Касьянов Ю.І., Нужний С.М. (2016) Оцінювання ефективності генератора реальної мовоподібної завади за критерієм розбірливості мови. Вісник Нац. ун-ту "Львівська політехніка": Автоматика вимірювання та керування, №.852, С. 105 – 110.

4. Blintsov, V., Nuzhniy, S., Parkhuts, L., Kasianov, Y. (2018). The objectified procedure and a technology for assessing the state of complex noise speech information protection. Eastern-European Journal Of Enterprise Technologies, 5 (9 (95)), 26–34. doi: <http://dx.doi.org/10.15587/1729-4061.2018.144146>

5. Покровский Н.Б. (1962) Расчет и измерение разборчивости речи. Москва, Гос. изд-во литературы по вопросам связи и радио, 392 с.

6. Касьянов Ю.І., Плютенко В.В. (2019) Спектр довготривалої української мови в оцінюванні захищеності мовної інформації за критерієм розбірливості. Інформаційні системи та технології ICT-2019: Матеріали 8-ї міжнародної науково-технічної конференції. Харків, ХНУРЕ, С. 243–245.

7. Yurii Kasianov, Viktoriia Khivrich, Anastasiia Mykhailychenko. (2021) Research of the Ukrainian speech signal spectrum to assess the security of speech information. Proceedings of the VIII-th International science and technical conference «Information Security and Information Systems Security» ISSS-2021. – Lviv: Lviv Polytechnic Publishing House, pp.117–118. – <https://drive.google.com/drive/folders/18xwh1x6hp2ggE14Znhf4Ckn1164FRyi?usp=sharing>.

8. Касьянов Ю.І. (2023) Проблема узагальнення спектрів тривалих нестаціонарних сигналів // Інновації в суднобудуванні та океанотехніці: Матеріали XIV міжнародної науково-технічної конференції. – Миколаїв: НУК. – С. 395 – 398.

9. Касьянов Ю.І. Узагальнення спектрів довготривалих мовленнєвих сигналів з використанням процедур обробки зображень /Ю.І. Касьянов, М.С. Щербаков, С.С. Трощенко // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI всеукраїнської науково-технічної конференції з міжнародною участю. - Миколаїв: НУК, 2023. – С. 110-115.

УДК 004.934: 534.8

ВРАХУВАННЯ ХАРАКТЕРИСТИК СЛУХУ В СИСТЕМАХ ЦИФРОВОГО ЗВУКУ

Автор: Лях О.Д., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Касьянов Ю.І., старший викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Вступ. В природі звук існує у вигляді коливань і розповсюджується у вигляді акустичних хвиль, тобто є сигналами неперервними в часі і за рівнем (має аналоговий характер). Такий же характер має звук і після перетворення його в електричний сигнал. Однак обробка, передача та збереження звукової інформації в аналоговому вигляді пов'язана зі значними складнощами, втратами якості і спотворенням через дію шумових і інших завад. Тому ще з часів появи перших комп'ютерів звукові сигнали намагаються перевести в цифрові сигнали, що не мають або суттєво зменшують вказані недоліки.

Розвиток цифрових аудіотехнологій тісно пов'язаний з дослідженням особливостей людського слуху. Врахування характеристик слуху дозволяє створювати аудіосистеми з високою якістю звучання, зменшувати обсяг даних для зберігання та передачі звуку без втрати суб'єктивної якості.

Метою роботи є аналіз врахування характеристик слуху в системах цифрового звуковідтворення для забезпечення і покращення якості звуку.

Основна частина. Дослідження здатності слухової системи сприймати і перетворювати в певні слухові відчуття (гучність, висоту, тембр та ін.) основні об'єктивні параметри звукового сигналу (інтенсивність звуку, її динамічний діапазон, частотний діапазон, часові характеристики), є головним завданням сучасної психоакустики [1, 2].

Людський слух має кілька ключових характеристик, які потрібно враховувати при створенні систем цифрового звуку та при його обробці.

Людське вухо сприймає звуки в діапазоні від 20 Гц до 20 кГц [1–5]. Це є основою для визначення стандартів цифрового звуку, таких як частота дискретизації, яка відповідно теореми Котельникова повинна більш ніж у 2 рази перевищувати верхню частоту діапазону, щоб забезпечити відновлення сигналу без втрат. У стандарті CD прийнята частота дискретизації 44,1 кГц, що дозволяє відтворювати весь спектр чутих частот.

Обрана частота дискретизація повинна забезпечити не тільки сприйняття потрібного діапазону частот, але і злитність сприйняття звуку. Слуховий апарат людини є інерційним – при зникненні звуку слухове відчуття зникає не відразу, а поступово, зменшуючись до нуля. Час, протягом якого відчуття по рівню гучності зменшується на 9...10 фон називається сталою часу слуху і складає 30...50 мс [1, 2, 5]. Експериментально встановлено, що два відліки звукового сигналу одного рівня сприймаються як один звук, якщо час між ними не перевищує 50 мс, тобто злитність звуку забезпечується вже при дискретності в 20 Гц. На використанні цієї ж властивості слуху побудовано створення штучної реверберації (луна) в результаті подачі одного й того ж відліку звукового сигналу з певною затримкою.

Важливою особливістю слухової системи людини є сприйняття гучності звуку не пропорційно зміні звукового тиску, а за логарифмічним законом, що потребує реалізації регуляторів гучності з відповідними характеристиками. Окрім того відчуття гучності звуку залежить від його частоти на високих і особливо на низьких частотах слухова система має меншу чутливість ніж на середніх, що характеризується кривими рівної гучності. Цей фактор зумовлює створення і використання еквалайзерів для налаштування бажаного звучання під своє індивідуальне сприйняття.

Слух має обмежену роздільну здатність за рівнем звуку, від 0,5 до 1 дБ (менше - на середніх частотах і більше - на низьких і високих частотах). Це відповідатиме 150...250 градаціям гучності. Таким чином для запису звуку з широким динамічним діапазоном в режимі «моно» достатньо 8 біт на відлік, а в режимі «стерео» 16 біт на відлік.

Маскування звуку є інструментом для зменшення впливу небажаних звуків, особливо в умовах, де присутні сильні звуки, які можуть

маскувати слабкіші. Це дозволяє зменшити обсяг аудіоданих, зберігаючи при цьому якість звуку.

Вплив рекреаційного шуму, наприклад, від прослуховування музики через персональні музичні плеєри, може зменшити сприйняття мови в шумі та чутливість до високих частот.

Дослідження показують, що різні частотні компоненти можуть впливати на сприйняття просторових характеристик звуку, таких як дифузність, рух, розщеплення зображення та екстерналізація. Наприклад, високочастотні канали можуть впливати на сприйняття просторових атрибутів звуку, особливо при використанні динамічної компресії.

Бінауральний ефект є властивістю здатності слуху визначати напрямок на джерело звуку. Цей процес базується на обробці звукових сигналів, що надходять до обох вух і використовується в системах звуковідтворення для створення стереоефекту.

MP3 та AAC є популярними форматами стиснення із втратами, які роблять вибір маскування звуку для зменшення розміру файлів. Ці формати видають частини аудіосигналу, менш помітні для людського слуху, що дозволяє значно зменшити обсяг даних без значного зниження якості звуку. MP3 є одним із найрозширеніших форматів, але сучасні дослідження показують, що AAC може бути більш ефективним у певних випадках, забезпечуючи кращу якість звуку при меншому розмірі файлу [6, 7].

PCM та FLAC є прикладами форматів стиснення без втрат, які зберігають оригінальну якість звуку, враховуючи частотний діапазон слуху. FLAC, зокрема, є одним із найпопулярніших форматів без втрати, що дозволяє зберегти аудіо без втрати якості, що робить його ідеальним для архівування та професійного використання. Дослідження показують, що FLAC має найшвидший час кодування разом з іншими форматами без втрати, наприклад, як MPEG-4 ALS, хоча останній може мати вищий коефіцієнт стійкості.

Еквалайзери використовують для налаштування звуку, враховуючи індивідуальні переваги слухачів. Дослідження показують, що в автомобільних аудіосистемах користувачі часто відрізняються рівнів звуку та підсилення низьких частот залежно від умов шуму, що показав

про значні індивідуальні відмінності в уподобаннях. Це підкреслює важливість персоналізації налаштування еквалайзера для досягнення оптимального звучання.

Динамічна компресія (DRC) широко використовується в пристроях для слуху для адаптації звукових рівнів до зниженого динамічного режиму слухачів із внутрішнього слуху. Вона підсилює тихі звуки більше, ніж гучні, що може привести до спотворення в шумних середовищах. У музичній індустрії DRC використовується для підвищення привабливості музики для слухачів з нормальним слухом. Важливо відзначити, що динамічна компресія може впливати на просторові атрибути звуку, такі як дифузність і зовнішність, особливо при швидкій компресії на високих частотах. Це може мати слідки для використання компресії в пристроях для слуху, особливо в динамічних ситуаціях.

Висновки. Врахування характеристик слуху є основою для створення ефективних цифрових аудіосистем. Це дозволяє підвищити якість звучання, зменшити обсяг даних і забезпечити природність сприйняття звуку. Подальший розвиток технологій передбачає більш глибоку персоналізацію аудіосистем та розширення їх можливостей у сферах розваг, комунікації та медицини.

Список літератури:

1. Алдошина И.А. Основы психоакустики. [Электронный ресурс] – KLEX. Книжный архив – Режим доступа: <https://www.klex.ru/6n5>.
2. Вологдин Э.И. Слух и восприятие звука: Курс лекций. – СПб.: СТ "Факультет ДВО", 2004. – 36 с.
3. Сапожков М.А. Электроакустика: учебник для вузов. – М.: Связь, 1978. – 272 с.
4. Акустика слуху: навч. посіб. / К. С. Дрозденко, О. І. Дрозденко. – Київ: КПІ ім. Ігоря Сікорського, 2020. – 99 с.
5. Алдошина И., Приттс Р. Музыкальная акустика. Учебник. – СПб.: Композитор Санкт-Петербург, 2006. – 720 с.
6. Ковалгин Ю. А., Вологдин Э. И. Аудиотехника. Учебник для вузов. – М.: Горячая линия – Телеком, 2013. – 742 с.
7. Продеус А.М. Основы компьютерной обработки музыки та мови: навчальний посібник. – Київ: КПІ ім. Ігоря Сікорського, 2022. – 324 с.

СЕКЦІЯ 5. СТВОРЕННЯ ПІДВОДНО-ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ ЗАХИСТУ МОРСЬКИХ ОБ'ЄКТІВ ТА АКВАТОРІЙ

УДК 629

СТЕНД ДЛЯ ВИПРОБУВАНЬ УСТАНОВОК ГРЕБНИХ ЕЛЕКТРОПРИВОДІВ

Автор: Большаков Є.Д., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Бабкін Г.В., к.т.н., доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Електричний привід відіграє важливу роль у житті сучасної людини, оскільки це привід розроблений для виконання технологічних та виробничих операцій у промисловості, сільському господарстві та повсякденному житті. Однак перед тим, як пристрій електричного приводу буде працювати в реальних умовах, необхідно зробити складні тести, які експериментально визначають кількісні та якісні характеристики функціонування об'єкта. Для вирішення проблеми створюється найрізноманітніші комплекси, що складаються з набору трибун, які є спеціальним обладнанням, з яким продукт піддається певним навантаженням та впливам. Такі пристрої використовуються в галузях високої технології, наприклад, автомобільної, суднобудівної та літальної промисловості для досягнення високої надійності, безпеки та ефективності продукції.

Що стосується суднобудування, то у зв'язку з розвитком океанів, збірки вантажних перевезень, здійснених морським та річковим транспортом. Набір електричних накопичувачів, які є комплексними складними випробуваннями. Але окремо варто відзначити про електричний привід встановлення веслування, оскільки цей об'єкт знаходиться на голові всіх пристроїв електричного приводу, присутнього на кораблі, тому що Він споживає найбільшу силу, і її неправильна робота чи відмова призводить до неминучих наслідків. Тому тест цього пристрою вимагає спеціальної об'єктивності, ретельності, а результати – надійності.

З цією метою створюється найрізноманітніші стенди для різних типів випробувань, включаючи тестування установок для веслувальних електроприводів, цей пристрій проходить ряд перевірок для підтвердження міцності, механічних, електричних та інших властивостей. Однак, з точки зору електричного приводу, випробування на навантаження, спрямовані на вивчення здатності досліджуваного гребного електричного двигуна, представляють особливий інтерес до подолання електромагнітного моменту, прикріпленого до його валу.

Відповідність обраної теми полягає в тому, що сьогодні за допомогою сучасних інструментів автоматизації можна створити тестові стенди, які можуть утворювати різні характеристики навантаження, тим самим моделюючи різні умови та обставини плавання корабля. Як результат, перевіряються не лише заявлені кількісні та якісні характеристики, але й розвиток позаштатних ситуацій запобігається.

У цій роботі було зроблено розробку випробувального стенду гребних рушіїв, побудованих на основі двох частот, що користуються електричними приводами та системами управління. Цей пристрій за допомогою вибраних технічних та програмних засобів може імітувати навантаження, що відповідає типовим характеристикам навантаження гвинт -гвинта на валу досліджуваного об'єкта. В результаті цих заходів параметри веслування визначаються на основі яких приймається рішення щодо задоволення тих чи інших передбачуваних норм та вимог, встановлених у методології тестування.

У процесі розробки випробувального стенду одним із головних завдань було реалізація на основі асинхронного електричного двигуна функції управління на основі певних графічних залежностей. Ця проблема була вирішена за допомогою сучасних технічних та програмних засобів, таких як перетворювач частоти з векторним управлінням, який генерує момент у машині, модульний програмований логічний контролер.

В результаті роботи було розроблено тестовий стенд, який може виконувати завдання з високим ступенем автоматизації, точності та надійності, тоді як з мінімальними фінансовими та часом витрат на обслуговування.

УДК 629

СИСТЕМА КЕРУВАННЯ ПРОСТОРОВИМ РУХОМ ДИСТАНЦІЙНО КЕРОВАНОГО АПАРАТУ

***Автор:** Верещака О.І., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Бабкін Г.В., к.т.н., доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Системам автоматичного управління польотом на існуючих літальних апаратах приділяють велику увагу. Якщо такі системи відсутні з тих чи інших причин, то оперативне застосування авіаційних та космічних літальних апаратів, а також усіх типів ракет неможливо.

Управління польотом літального апарату (ЛА) полягає у підтримці заданої траєкторії руху його центру мас (ЦМ), а також стабілізації та орієнтації відносного центру мас. Вирішення цих завдань покладається на автоматичні або напіваавтоматичні системи керування.

Автоматичним керуванням літального апарату можна назвати процес програмної зміни та стабілізації окремих параметрів руху літального апарату або цілеспрямоване керування траєкторією польоту, яке здійснюється за допомогою інструментів автоматики, тобто. без впливу пілота на органи управління.

З усього вищесказаного можна дійти невтішного висновку, що ЛА далеко непростий об'єкт автоматичного управління. Тому необхідно мати математичний опис (математичну модель) досліджуваного літального апарату, щоб можна було зробити синтез системи автоматичного управління з метою отримання рішень щодо вибору перетворювальних, виконавчих та інших пристроїв.

Метою даної роботи є розробка системи програмного руху ЛА для забезпечення польоту заданою траєкторією. Для досягнення поставленої мети необхідно було вирішити такі завдання:

- 1) розробити математичну модель руху літального апарату;

2) розробити програмні моделі у пакеті MATLAB Simulink, серед яких: модель поздовжнього руху ЛА, модель бічного руху літального апарату, модель просторового руху літального апарату;

3) розробити систему управління каналами нищпорення і тангажу;

4) дослідити динаміку просторового руху літального апарату із застосуванням розробленої системи управління;

5) розробити систему програмного наведення літального апарату на точку у просторі, що задається трьома координатами;

6) провести аналіз отриманих результатів та зробити висновок про точність спроектованої системи виходячи з промахів наведення по кожній координаті.

Висновки:

1. При аналізі синтезованої моделі просторового руху літального апарату виявили взаємний вплив кожного з каналів один на одного і зроблено висновок про те, що цей вплив перехресних зв'язків – незначне, т.к. аеродинамічні коефіцієнти, що пов'язують поздовжнє та бічне рух – малі.

2. Моделі незалежного руху використані до створення лабораторного практикуму з дисципліни: «Динаміка рухливих об'єктів». На даний момент цей лабораторний практикум впроваджений і користуються студентами. У процесі користування було внесено деякі зміни до програми лабораторних робіт, а саме додано функцію побудови графіка в окремому вікні, для зручності прикріплення його до звіту.

3. Синтез системи управління просторовим рухом ЛА проводився з урахуванням підбору коефіцієнта регулятора. Це було реалізовано за допомогою блоку "Signal constraint" у Simulink. Перехідні процеси, що виходять, не задовольняли вимогам по динаміці і коливальності, тому було прийнято рішення поставити в контур регулятора ПІД-регулятор, коефіцієнти якого були підібрані емпіричним шляхом. Підсумкові перехідні процеси по куту тангажу і куту нищпорення вже мали більш швидкі перехідні процеси і коливання швидше загасали у випадку з кутом нищпорення, а у випадку з кутом тангажу – перехідний процес став монотонним.

4. Для зручності проектування просторової системи програмного наведення були розроблені окремі моделі наведення в площинах XZ і XY. Отримані результати задовольняли вимоги завдання. Далі,

об'єднаємо, дві моделі наведення, отримали модель, здатну наводитися на ціль у просторі із заданою точністю. Таким чином, отримана просторова модель програмного наведення впоралася з поставленим завданням.

Рекомендації: Надалі необхідно:

1. Розробити модель просторового руху літального апарату, яка була б меншою, щоб скоротити машинний час на інтегрування диференціальних рівнянь, а також більш точну, щоб відтворювати більш точну динаміку руху ЛА.

2. Розробити зручний інтерфейс лабораторних робіт, для ще зручнішого і зрозумілішого відображення отриманої, під час моделювання, інформації.

3. Спроекувати систему програмного наведення, що має швидшу динаміку. Цього можна досягти шляхом збільшення точності, складеної в першому розділі моделі просторового руху літального апарату.

УДК 629

РОЗРОБКА АЛЬТЕРНАТИВНОГО ДЖЕРЕЛА ЕЛЕКТРОЕНЕРГІЇ НА ОСНОВІ СОНЯЧНИХ ЕЛЕМЕНТІВ ТА ВІТРОГЕНЕРАТОРНОЇ УСТАНОВКИ

***Автор:** Малишев Б.Г., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Бабкін Г.В., к.т.н., доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

На початку XXI століття людству довелося зіткнутися з проблемою вирішення енергетичних проблем, спрямованих на майбутнє, пов'язаних зі швидким вичерпанням традиційних джерел енергії та зміною в гірший бік екологічного стану Землі. У промислово розвинених країнах звертають велику увагу на розробку систем, в основі яких лежать відновлювані джерела енергії, зокрема енергія Сонця та вітру.

Найзручнішим для використання у виробництві та побуті видом енергії, безумовно, є електрична енергія. Тому перше місце на

нинішньому етапі розвитку альтернативних технологій займає виробництво електроенергії за допомогою поетапного перетворення енергії вітру, води та сонячного світла.

Ця тема широко відкрита для досліджень та різноманітних рішень. Сонячна та вітроенергетика – дуже перспективні напрямки у нетрадиційній електроенергетиці.

Тому метою даної роботи є поглиблення знань у галузі альтернативної енергетики, проектування комбінованої сонячної електростанції, а також подання оптимальних рішень для будівництва цієї електростанції.

Сонячна енергетика є однією з найбільших частин альтернативної енергетики та галузі використання відновлюваних джерел енергії (ВІЕ). В наш час розрізняються три основні способи використання енергії сонця: генерування електроенергії, отримання зосередженої теплової енергії для подальшого електрогенерування або пряме нагрівання теплоносія (зазвичай – водного).

Сонячна енергія знаходить застосування у різноманітних сферах діяльності:

- промислові тепло- та електростанції;
- станції постачання теплової та електричної енергії різного роду будівель та приміщень;
- економічно вигідні установки для приватних будинків;
- застосування еластичних сонячних батарей як будівельний матеріал;
- резервні джерела живлення в товарах масового споживання: калькулятори, годинники, ноутбуки, ліхтарі, акумулятори та ін.;
- резервні джерела живлення транспортних засобів;
- освітлення у темний час доби дорожніх знаків та іншого за рахунок накопиченої енергії сонця.

Вітрогенератори, у свою чергу, теж набирають популярності. Вони використовуються не тільки як додаткове джерело електрики, а часто і як основне джерело завдяки надійній конструкції, комфорту при експлуатації. Вітрогенератор (вітроелектрична установка (ВЕУ)) – система перетворення кінетичної енергії потоку вітру в механічну енергію обертання ротора з подальшим перетворенням цієї енергії на електричну.

На початку роботи було вивчено переваги та потенціал альтернативної енергетики на сьогоднішній день. Актуальність розробки досить висока, т.к. можна одержати екологічно чисте джерело енергії з низькою вартістю виробництва електроенергії. У ході виконання роботи було спроектовано дві схеми комбінованої електростанції. Однак обраний був перший варіант схеми як найбільш технічно та економічно доцільний. Постачальник електроенергії повинен не тільки забезпечити електрикою споживачів, але й зобов'язаний дотримуватися та контролювати його якість, щоб уникнути аварій та позаштатних ситуацій. Для цього представлені вимоги державного стандарту на якість електричної енергії та можливі методи контролю якості ЕЕ.

УДК 629

РОЗРОБКА АЛГОРИТМІВ КЕРУВАННЯ СИСТЕМИ РУХОМ МОБІЛЬНОЇ РОБОТОТЕХНІЧНОЇ УСТАНОВКИ

Автор: Назаров В.Ю., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Бабкін Г.В., к.т.н., доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

На сьогоднішній день роботи все частіше беруть участь у нашому повсякденному житті. В результаті прискореного розвитку технологій, останні кілька років, використання робототехнічних комплексів зростає експоненційно.

Роботи використовуються в різних областях: в автомобільній промисловості; у медичній промисловості роботи, де роботи можуть виконувати хірургічні операції, щоб уникнути появи людського фактору; у військовій промисловості, видалення наземних мін, знешкодження бомб, ліквідація небезпечних техногенних зон; у космічній промисловості; у побуті, для збирання приміщень.

Існують роботи, які потребують особливої уваги – це автономні мобільні роботи. Даний тип роботів створений для вирішення задач навігації, планування, локалізації.

Дослідні інститути, університети та промисловість вкладають багато ресурсів та часу на дослідження в цій галузі. Вони намагаються залучити студентів та дослідників до вивчення у цій галузі.

Розробка мобільних роботів є складним завданням, пов'язаним з необхідними ресурсами та навичками у багатьох галузях, такі як розробка програмного забезпечення, штучний інтелект, механічне проектування, електротехніка, сигнал обробки сенсорної техніки або теорії управління. Сучасні мобільні робототехнічні системи найчастіше є монолітними.

В даний час велика увага приділяється розробці робототехнічних комплексів з високою пристосовністю до руху складними траєкторіями і складними поверхнями. У всьому світі ведуться розробки подібних апаратів для реалізації таких завдань, як проведення знешкодження вибухових пристроїв, локалізація зони надзвичайної ситуації (НС). З цими завданнями багато хто з існуючих апаратів не справляється. У цій роботі найбільша увага була приділена робототехнічним комплексам, що використовують гібридний спосіб пересування – колісного.

Мобільні робототехнічні системи (РТС) використовуються в різних сферах діяльності, як забезпечення безпеки на роботах у зоні небезпечних для життя людей, підвищення продуктивності різних технологічних операцій порівняно з продуктивністю ручної праці. При створенні мобільних робототехнічних систем неможливо не враховувати особливості умов навколишнього середовища, в якому надалі використовуватиметься РТС.

Враховуючи всі особливості РТС, стає необхідним створення опорної конструкції мобільної робототехнічної платформи малих розмірів та маси з використанням блочно-модульного принципу побудови. Це дає можливість швидко та своєчасно проводити ремонт технологічного обладнання, вузлів та механізмів ходової частини та силової частини РТС для швидкого пристосування робота до умов експлуатації при швидкій зміні зовнішнього середовища функціонування та зміні початкових завдань.

Головна проблема автоматизації при конструюванні мобільних робототехнічних систем є завдання пристосованості робота до змін зовнішнього середовища функціонування. Мобільні робототехнічні системи використовуються в умовах відсутності інформації про довкілля.

Важливо, що це інформація не визначається коли РТС перебуває у статичному становищі, і при переміщенні робота, що створює труднощі для робота виконувати поставлені йому завдання автономно, без участі людини.

Робототехнічні комплекси, що мають невелику власну вагу, використовують переважно для пересування гусеничний або колісний тип переміщення. Незважаючи на те, що такий клас роботів показує хороші результати щодо проходження різних видів поверхні, існує ряд завдань, які для даних робототехнічних комплексів вирішити неможливо. Завдання створення інноваційних моделей робототехнічних комплексів є актуальним на сьогоднішній день. Для вирішення такого завдання потрібно розробити нестандартні типи рушіїв, зміну їхньої конструкції та масогабаритних показників. Це все обумовлено вирішенню пріоритетних завдань для підвищення показників ґрунтової та профільної прохідності.

Принцип таких роботів наступний: робот переміщається ландшафтом, який він визначає за допомогою визначального пристрою, розміщення кожної ноги в бажаному місці, що визначається керуючим пристроєм, а потім переміщуючи тіло вперед, щоб змінити його положення.

УДК 629

ІНТЕЛЕКТУАЛЬНА СИСТЕМА КЕРУВАННЯ ДИСТАНЦІЙНО КЕРОВАНИМ РОБОТОМ

***Автор:** Новиков А.Ю., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Бабкін Г.В., к.т.н., доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Робототехніка є науково-дослідним напрямком багатьох країн. Однією з найважливіших завдань завдання розробки алгоритмів управління промислових роботів. Роботи-маніпулятори широко використовуються для промислового виробництва. Їхня технологія є добре вивченою. Тим не менш, порівняно мало робіт присвячено моделюванню

рухомих важелів робота-маніпулятора, розташованих на рухомій основі. Однак, маніпулятори з вільною рухомою основою мають важливе значення. Тому, з розвитком технології їх проектування, вони широко застосовуватимуться у сфері промислового виробництва, наукових досліджень тощо.

Завдання роботи містять:

1. Розпізнавання об'єктів та його просторового становища.
2. Розв'язання прямої та зворотної задачі кінематики робота.
3. Розробка моделі робота.
4. Реалізація алгоритмів керування роботом на «залізі».

Модель поведінки робота включає наступне: закони фізики приводу на два колеса, замкнута система з двигунами постійного струму по куту з ПД-регуляторами, 3D-модель робота в середовищі 3D Animation. Розробка алгоритмів управління роботом включає наступне: розпізнавання об'єктів за кольором, визначення просторових координат об'єктів, наближення до об'єкта, підняття об'єкта за допомогою руху маніпулятора, перевезення об'єкта та розміщення його у вказане місце. Реалізація апаратного забезпечення робота полягає в тому, щоб реалізувати зв'язки між мікрокомп'ютером та мікроконтролером, розробити програми для мікроконтролера управління двигунами постійного струму маніпулятора та виконання розпізнавання образів у мікрокомп'ютері.

У цьому проекті виконані такі задачі:

1. Вивчення алгоритмів та теорем управління роботом.
2. Доказ того, що алгоритми, що використовуються, коректні і реалізовані за допомогою Matlab і Python.
3. Описано вибори елементів, що застосовуються в системі управління роботом.
4. Розробка електронної схеми системи керування роботом на «залізі».
5. Розробка алгоритмів управління роботом на «залізі» Raspberry Pi B+ та Ардуїно Uno.

Висновок: хоча виконали завдання даного проекту, не виконано ще глибше вивчення. Наприклад, використання кращих алгоритмів розпізнавання об'єктів, визначення просторового становища об'єкта, інших рішень зворотного завдання кінематичного маніпулятора та реалізації системи управління роботом іншому «залізі».

УДК 629

СИСТЕМА КЕРУВАННЯ ДИСТАНЦІЙНО КЕРОВАНИМ РОБОТОМ

Автор: Пашкевич А.В., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Бабкін Г.В., к.т.н., доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Через попит, що постійно збільшується, на перевезення у сучасного суспільства з кожним роком зростає проблема завантаженості доріг. Це призводить до втрати часу в дорозі та величезних соціальних та економічних витрат. Одним із можливих рішень цієї проблеми, але менш здійсненним через обмеженість ресурсів, може бути будівництво нових доріг. Альтернативним рішенням може бути модернізація існуючої інфраструктури, що включає як удосконалення транспортної системи, так і модифікацію транспортних засобів.

Мета цієї роботи – розробка системи управління автономним рухом чотириколісного транспортного засобу.

Завдання

1. Огляд існуючих розробок у галузі автономного руху чотириколісних транспортних засобів.
2. Складання математичного опису чотириколісного транспортного засобу з кермовим керуванням Аккермана.
3. Розробка принципу керування приводами прототипу чотириколісного транспортного засобу.
4. Розробка принципу формування траєкторії руху із використанням технологій комп'ютерного зору.

Предмет роботи: система управління автономним рухом чотириколісного мобільного робота, що дозволяє коректно здійснювати маневри з дотриманням існуючих правил дорожнього руху.

Цей транспортний засіб має наступні переваги:

- здатність перевозити вантажі у небезпечних зонах, під час природних та техногенних катастроф чи воєнних дій;

- зниження вартості транспортування вантажів та людей за рахунок економії на заробітній платі водіїв;
- більш економічне споживання палива та використання доріг за рахунок централізованого керування транспортним потоком;
- можливість самостійно переміщатися транспортним засобом людям з обмеженими можливостями.
- мінімізація аварій та жертв;
- підвищення пропускну здатність доріг за рахунок оптимізації руху потоків транспортних засобів.

Крім переваг автономний транспортний засіб має низку недоліків:

- не формалізовано на законодавчому рівні відповідальність за завдання шкоди;
- працездатність багато в чому залежить від надійності програмного забезпечення;
- відсутність досвіду водіння у водіїв при виникненні необхідності перемикання в ручний режим керування в критичній ситуації;
- втрата робочих місць людьми, робота яких пов'язана з водінням транспортних засобів;
- етичне питання наділення відповідальності за скоєний маневр транспортний засіб.

Дослідження систем автономного руху транспортних засобів показують, що такі системи можуть зменшити стрес, який отримує водій, і рівень втоми, що призведе до значного зменшення кількості аварій та пригод зі смертельним наслідком. Система автономного керування транспортним засобом є подальшою модифікацією адаптивного круїз-контролю.

В результаті виконання роботи було проведено огляд існуючих розробок у галузі автономного руху транспортних засобів та вивчено загальну термінологію даної тематики, складено математичний опис чотириколісного транспортного засобу з кермовим керуванням Аккермана, при цьому враховано вплив встановлених диференціалів у конструкції мобільного робота. На базі ралійної моделі WR8 Flux було зібрано прототип мобільного робота, призначений для перевірки та налагодження створених у рамках роботи алгоритмів управління. Система управління мобільним роботом складається з двох рівнів: нижній рівень – мікроконтролерна система управління приводами робота,

верхній рівень – система комп'ютерного зору на базі одноплатних комп'ютерів Raspberry Pi 2. На базі прототипу реалізовані завдання розпізнавання знаків дорожнього руху та дорожньої розмітки, що повністю задовольняє вимогам до системи управління.

Результати випробувань виявили коректність запропонованих рішень. Розроблена система управління дозволяє здійснити підтримку руху в смузі, розпізнавання знаків дорожнього руху та здійснення коректних маневрів відповідно до змісту знака, а також здійснення перпендикулярного паркування в обмеженому просторі.

УДК 629

РОЗРОБКА СИСТЕМИ ЕЛЕКТРОЖИВЛЕННЯ ТА ВНУТРІШНЬОГО КОНТРОЛЮ МОБІЛЬНОГО РОБОТОТЕХНІЧНОГО КОМПЛЕКСУ

***Автор:** Яровий М.С., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Бабкін Г.В., к.т.н., доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Світовий досвід створення та застосування робототехнічних систем наземного призначення показує, що вони є потужним інструментом у вирішенні таких завдань, як:

- проведення аварійно-рятувальних робіт (пошук та порятунок людей, розбирання завалів, гасіння пожеж);
- проведення вибухотехнічних робіт (пошук та діагностика вибухових пристроїв, знищення або евакуація вибухових пристроїв, розпорядження або знешкодження вибухових пристроїв);
- проведення хімічної та радіаційної розвідки об'єктів та територій та очищення та дезактивації місцевості та територій;
- допомога у проведенні антитерористичних операцій (постановка радіоелектронних перешкод, димових та спеціальних завіс, доставка та застосування спецзасобів нелетальної дії, приховане проникнення на

захоплені та об'єкти, що охороняються, ведення радіоелектронної аудіо- та відео-розвідки об'єктів і територій, руйнування перешкод: двері ведення відволікаючого вогню, виявлення вогневих точок противника, захист бійців спецпідрозділів);

- при охороні об'єктів (патрулювання території чи периметра об'єкта, припинення спроб проникнення об'єкт, нейтралізація порушників);

- при проведенні будівельних робіт (земляні роботи, вантажопідйомні роботи), особливо у небезпечних для людини умовах;

- у військових цілях (проведення розвідки, загороджувальний вогонь, розвідка боєм, руйнування загороджень, вивезення поранених, супровід підрозділів та перевезення спорядження) тощо;

Зазначені операції можуть проводитись на різних об'єктах та в різноманітних умовах:

- на об'єктах громадського транспорту (міський транспорт, залізничний, авіаційний, морський, автомобільний);

- у місцях проживання та життєдіяльності людей (квартири, будинки, офіси та ін.);

- на промислових об'єктах (об'єкти хімічної промисловості, ядерного технологічного циклу та ін.);

- на об'єктах міської інфраструктури (каналізація, теплові та атомні станції, водопровід тощо);

- на відкритій місцевості, сильно пересіченій місцевості, у лісах тощо. До мобільного роботу, у складі самохідного шасі (або робототехнічної транспортної платформи) із встановленим на ньому спеціальним або універсальним обладнанням, пред'являються такі вимоги: -мобільний робот повинен мати високі рухливість і прохідність у міських умовах (можливо і всередині будівель та споруд), в зонах руйнувань, на пересіченій місцевості, як на твердих і гладких покриттях, так і на ґрунтових і сипучих підставах, що деформуються; -мобільний робот повинен надійно діяти як у непередбачених природних умовах, у тому числі на завалах, так і в середовищі, спеціально пристосованому для проживання людини (всередині будинків, у транспортних комунікаціях), вписуватись у міські транспортні потоки або рухатися у складі транспортних колон; -конструкція робота повинна забезпечувати його високу мобільність та швидке розгортання при виконанні спецоперацій. Сучасна мобільна

робототехніка, здатна допомогти людині, а також захистити або замінити людину в небезпечних для неї завданнях, роботах або умовах – це перспективний науково-технічний напрямок, що комплексно охоплює проектування, розробку, виробництво та експлуатацію робототехнічних систем і активно розвивається в таких країнах, як США, Росія, Китай, Канада, Великобританія, Франція, Німеччина, Ізраїль та ін.

СЕКЦІЯ 6. ПІДГОТОВКА КАДРІВ У ГАЛУЗІ ЗНАНЬ «ІНФОРМАЦІЙНА БЕЗПЕКА»

УДК 004.4

ЗАСТОСУВАННЯ БІБЛІОТЕКИ OPENCV В ОХОРОННИХ СИСТЕМАХ

***Автор:** Курманський В.В., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. У сучасному світі безпека та спостереження стають дедалі важливішими аспектами повсякденного життя. Оскільки технології продовжують розвиватися, комп'ютерне бачення стали потужними інструментами у сфері спостереження та безпеки.

Комп'ютерний зір – це галузь дослідження, спрямована на те, щоб дозволити машинам інтерпретувати та розуміти візуальні дані з навколишнього світу. OpenCV, бібліотека комп'ютерного бачення з відкритим кодом, є популярним інструментом, який використовується для розробки програм комп'ютерного бачення в реальному часі. Завдяки широкому спектру функцій і алгоритмів OpenCV став важливим інструментом для розробників і дослідників, які працюють у сфері комп'ютерного зору.

Мета роботи провести огляд кінцевого застосування бібліотеки OpenCV для задач комп'ютерного зору охоронних систем.

Основна частина.

Бібліотека комп'ютерного бачення з відкритим кодом, відома як OpenCV, написана мовами C і C++ і працює в Linux, Windows і Mac OS X. Незважаючи на те, що Intel запустила OpenCV, бібліотека завжди призначена для безкоштовного комерційного та дослідницького використання. OpenCV може використовувати переваги багатоядерних процесорів, оскільки він написаний на оптимізованому C. Йде активна розробка інтерфейсів для Python та інших мов.

Одним із найважливіших застосувань комп'ютерного зору та OpenCV у сфері спостереження та безпеки є розпізнавання обличчя.

Аналізуючи шаблони рис обличчя та відображаючи їх у базі даних відомих людей, алгоритми комп'ютерного зору можуть швидко й точно ідентифікувати людей у реальному часі. Технологія розпізнавання обличчя стала важливим інструментом у правоохоронних органах, що дозволяє більш ефективно та точно ідентифікувати підозрюваних.

Ще одним важливим застосуванням комп'ютерного зору та OpenCV у сфері спостереження та безпеки є виявлення об'єктів. Аналізуючи шаблони у візуальних даних, алгоритми комп'ютерного зору можуть швидко ідентифікувати та відстежувати цікаві об'єкти, наприклад транспортні засоби чи зброю. Технологія виявлення об'єктів стала важливим інструментом у безпеці аеропорту та прикордонному контролі, що дозволяє більш ефективно та точно перевіряти людей та їхні речі.

Виявлення рухомих об'єктів широко використовується для різноманітних додатків, починаючи від охоронного спостереження й закінчуючи моніторингом руху. Це важливий виклик у сфері комп'ютерного зору, що постійно розвивається. Бібліотека OpenCV із відкритим кодом, відома своїм повним набором інструментів для комп'ютерного зору, надає надійні рішення для виявлення рухомих об'єктів. У цій статті ми розглядаємо комбінацію виявлення контурів і віднімання фону, які можна використовувати для виявлення рухомих об'єктів за допомогою OpenCV розпізнавання облич.

Система пожежної сигналізації з використанням OpenCV – це рішення на основі комп'ютерного зору, призначене для раннього виявлення пожеж у відеопотоках у реальному часі. Пожежі становлять суттєву загрозу як безпеці людей, так і майну, що підкреслює важливість своєчасного втручання. Ця система використовує OpenCV, потужну бібліотеку комп'ютерного зору, для ідентифікації моделей полум'я та диму у відеокдрах, викликаючи попередження після виявлення. Отже, ми пропонуємо метод виявлення диму та вогню на основі мережі YOLOv5 як рішення для вирішення цієї проблеми.

Системи підрахунку відвідувачів призначені для врахування кількості людей, які пройшли через певний прохід за певний проміжок часу. Також іноді важливо визначити напрямок руху, проте найчастіше системи обмежуються поділом людей, що проходять, на два класи:

вхідні та виходять. Точність підрахунку безпосередньо залежить від досконалості використовуваної технології. Система підрахунку, як правило, встановлюється на вході до приміщення, дозволяючи стежити за кількістю відвідувачів.

Висновки

Загалом, комп'ютерний зір і OpenCV відіграють дедалі важливішу роль у сфері спостереження та безпеки. Від розпізнавання обличчя до виявлення предметів ці технології змінюють наш підхід до громадської безпеки. Оскільки технології продовжують розвиватися, цілком імовірно, що комп'ютерне бачення та OpenCV стануть ще більш важливими інструментами в галузі.

Список літератури:

1. Open Source Computer Vision: веб сайт URL: <https://docs.opencv.org/4.x/index.html>
2. G. Bradski and A. Kaehler, Learning OpenCV: Computer vision with the OpenCV library. O'Reilly Media, 2008.
3. Chetana Patil, Vaishnavi Andhalkar, Janhavi Dandavate, Pranjali Pokharkar, Suresh Lora A Survey: Fire Detection Alarm System Using OpenCV. *International Journal for Research in Applied Science & Engineering Technology*. Volume 11, Nov 2023- Available at www.ijraset.com

УДК 004.056.53

АНАЛІЗ ІСНУЮЧИХ СИСТЕМ ДЛЯ ОТРИМАННЯ НАВИЧОК ПЕНТЕСТИНГУ ДЛЯ СТУДЕНТІВ

Автори: *Логачов М.В.; Орел О.С., студенти, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ

У сучасному світі кібербезпека стає однією з найважливіших галузей через вплив цифрової трансформації на всі сфери діяльності. Загрози у цифровому просторі вимагають від фахівців високого рівня

підготовки для протидії кіберзлочинцям. Однією з ключових навичок є пентестинг – процес моделювання кібератак для виявлення вразливостей. Проте практикування пентестингу на реальних системах без дозволу є незаконним і може мати серйозні юридичні наслідки.

З цієї причини з'явилася потреба у спеціалізованих навчальних платформах, які дозволяють легально розвивати навички пентестингу. Однією з таких платформ перевірки навичок в засобах кіберзахисту є завдання Capture the Flag (CTF). Учасники отримують контрольований доступ до віртуальних серверів і мереж для практики виявлення вразливостей без порушення закону.

Метою роботи є аналіз існуючих систем, що дозволяють безпечно та легально практикувати навички пентестингу, які можна впровадити в навчальний процес.

Основна частина

Тест на проникнення (англ. penetration test, pentesting) – метод оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу).

Цей процес включає активний аналіз системи з виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативне відставання в процедурних чи технічних контрзаходах. Цей аналіз проводиться з позиції потенційного нападника і може включати активне використання вразливостей.

У процесі навчання пентестингу важливо мати доступ до практичних завдань, які дозволяють відточити навички зламування без порушення законодавства. Наприклад, Hack The Box та TryHackMe є одними з найбільш популярних платформ для таких тренувань, надаючи можливість працювати з реальними вразливостями в контрольованому середовищі. Ці ресурси дозволяють практикувати різні методи зламування, вивчати експлойти та захисти від них, що є важливою частиною підготовки до пентестингу.

Справжній пентестинг вимагає ґрунтовних знань про різні інструменти, такі як Metasploit, які широко використовуються для тестування вразливостей в реальних умовах.

Типи тестів на проникнення, що можуть протестувати студенти, можна виділити:

- веб-додаток (Web Pentesting). Використовується для виявлення вразливості в безпеці та інших проблем в декількох варіантах вебдодатків і сервісів, які розміщені на боці клієнта чи сервера;
- мережева служба (Network Pentesting). Тестування проникнення в мережу для виявлення можливості доступу хакерів чи інших неавторизованих об'єктів;
- клієнтська частина. Тест використовується для тестування додатків, встановлених на клієнтському сайті / додатку;
- віддалене підключення. Тестування wrp чи аналогічного об'єкта, який може забезпечити доступ до підключеної системи;
- бездротові мережі. Тест призначений для бездротових додатків і сервісів, включаючи їх різні компоненти та функції (маршрутизатори, фільтраційні пакети, шифрування, дешифрування і т. д.);
- тестування системи автоматичного контролю та збору інформації (SCADA Pentesting).

Існують спеціальні платформи для практики етичного хакерства, які надають вам доступ до "практичних" машин, які вам дозволяється взламувати в межах визначених умов. Ось декілька таких навчальних платформ :

1) Hack The Box — це єдина платформа, яка об'єднує підвищення кваліфікації, розвиток робочої сили та орієнтацію на людину в індустрії кібербезпеки. Дана платформа дає можливості проходити власні курси з підвищення кваліфікації, проведення тестування на взлом та режим «Шерлок», який дає можливість розслідування інциденту, що вже виникнув проаналізувавши дані журналів. Особливістю платформи є великий поріг входу.

2) TryHackMe – альтернатива Hack The Box, особливо для початківців. Це веб-браузерна навчальна платформа з кібербезпеки з навчальним контентом, який охоплює всі рівні навичок від початківця до досвідченого хакера.

3) VulnHub – це бібліотека вразливих віртуальних машин, які можна завантажити і використовувати локально. Вони розроблені для тренувань із пентестингу у безпечному середовищі.

Деякі компанії, такі як Google, Facebook, GitHub, проводять програми баг-баунті, де вони заохочують дослідників безпеки знаходити вразливості в їхніх системах в обмін на винагороду. Це дозволяє тестувати комп'ютери та програми на вразливості, але виключно в межах цих програм.

Висновки:

Треба завжди пам'ятати про етичні принципи та законність дій при проведенні тестів. Тестування без дозволу на комп'ютерах або в мережах, що вам не належать, є порушенням закону в багатьох країнах.

Список літератури:

1. Miller, J. M., & Roggenhofer, E. (2020). The Hacker Playbook 3: Practical Guide To Penetration Testing. Hacker House.
2. Harrison, D., & Harris, A. (2016). Mastering Metasploit: Penetration Testing and Ethical Hacking with the Metasploit Framework. Wiley.
3. Skoudis, E., & Liston, T. (2006). Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall.

УДК 004.4

АНАЛІЗ МОЖЛИВОСТЕЙ CYBER ICE BOX PLATFORM ДЛЯ ПРОВЕДЕННЯ CTF ЗМАГАНЬ

Автор: Момченко О.В., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Вступ. В умовах зростаючих кіберзагроз та потреби в підготовці кваліфікованих фахівців з кібербезпеки, CTF (Capture the Flag) змагання стають важливим інструментом для навчання та розвитку навичок захисту інформаційних систем. В Україні проведення CTF змагань є особливо актуальним через необхідність зміцнення кібероборони

здатності. Платформа Cyber ICE Box забезпечує гнучке та безпечне середовище для проведення змагань різного рівня складності, з використанням технологій контейнеризації та оркестрації на базі Kubernetes. Це дозволяє створювати реалістичні сценарії кіберзагроз для навчання як новачків, так і професіоналів.

Мета роботи є вивчення можливостей та переваг використання Cyber ICE Box Platform для проведення CTF змагань.

Основна частина.

Cyber Ice Box — це спеціалізована платформа для організації CTF змагань із використанням сучасних контейнерних технологій, що базується на Docker та Kubernetes. Платформа забезпечує високу гнучкість та масштабованість, дозволяючи організаторам легко налаштовувати середовища для завдань.

Контейнеризація Cyber Ice Box Platform використовує Docker та Kubernetes, які забезпечують ізоляцію та керування середовищами. Контейнери ізолюються за допомогою механізмів namespaces, що дозволяє запускати їх на одній операційній системі без ризику конфліктів. Cgroups (Control Groups) регулюють ресурси, що надаються кожному контейнеру, запобігаючи перевантаженню системи.

- Namespaces: поділяються на PID, Network, IPC та User, що забезпечують незалежність мереж, процесів та файлів між контейнерами;
- UnionFS: контейнерні образи використовують Union File System для зберігання багатопланових файлових систем, що забезпечує ефективність використання ресурсів;
- Оркестрація за допомогою Kubernetes: Kubernetes автоматизує розгортання контейнерів, об'єднуючи їх в Pod-и, розподіляючи навантаження між Node-ами в кластері, що дозволяє масштабувати середовище в залежності від кількості учасників та завдань.

Безпека є одним з ключових аспектів для будь-якої платформи CTF, через те що в змаганні бере участь велика кількість учасників. Важливим аспектом є те що учасники не повинні заважати один одному і не повинні мати змогу бачити роботу одне одного. Це може бути досягнуто за рахунок:

- контейнеризації: кожне завдання виконується в окремому контейнері, що ізолює його від інших, мінімізуючи ризик стороннього доступу або порушення роботи інших компонентів системи;

– системі контролю доступу: підтримує розмежування прав для різних ролей (учасників, адміністраторів, організаторів), дозволяючи налаштовувати рівні доступу до ресурсів платформи;

– моніторингу безпеки: інтеграція з системами для відстеження активності, що дозволяє виявляти аномалії в режимі реального часу, запобігаючи несанкціонованим діям або атакам на платформу.

Крім безпеки, платформа також забезпечує інтеграцію з різними системами для створення цілісного середовища змагань:

– інтеграція з CI/CD системами: підтримка інтеграції з інструментами безперервної інтеграції (наприклад, Jenkins або GitLab CI), що дозволяє швидко розгортати та оновлювати завдання;

– API для керування платформою: організатори можуть автоматизувати різні процеси через API, включаючи управління завданнями та моніторинг результатів учасників;

– Інтеграція з системами обліку результатів: підтримка лідербордів та автоматизованого відстеження прогресу команд, що робить змагання більш динамічними та зручними для глядачів і суддів.

Cyber Ice Vox Platform побудована на Kubernetes, що забезпечує автоматичне масштабування та надійність навіть під час великих змагань. Основні функції масштабування включають:

– автоматичне масштабування: Kubernetes дозволяє автоматично збільшувати або зменшувати кількість контейнерів в залежності від навантаження, підтримуючи стабільну роботу системи.

– балансування навантаження: зменшує ризик перевантаження окремих компонентів і забезпечує рівномірний розподіл ресурсів для оптимальної продуктивності.

– резервування та відновлення: платформа підтримує регулярне резервне копіювання та швидке відновлення, що гарантує стабільність навіть при технічних неполадках.

Cyber Ice Vox підтримує командні змагання, дозволяючи учасникам створювати та працювати в команді. Це сприяє розвитку командної взаємодії та спільному розв'язанню завдань, що імітує реальні ситуації кіберконфліктів. Кастомізація платформи забезпечується через:

- налаштування середовищ: організатори можуть адаптувати контейнери під конкретні завдання та вимоги, що забезпечує високу гнучкість;
- гнучка система завдань: завдяки можливостям Docker та Kubernetes, можна створювати завдання різної складності, що охоплюють різні аспекти кібербезпеки (наприклад, криптографію, веб-безпеку тощо);
- інтеграція з іншими платформами: через відкритий API Cyber Ice Vox можна з'єднати з інструментами моніторингу загроз, аналітики безпеки або навіть навчальними платформами для глибшого навчання учасників.

Висновки

Cyber Ice Vox Platform пропонує комплексне рішення для проведення CTF змагань на високому рівні безпеки, гнучкості та масштабованості. Платформа забезпечує організаторів інструментами для автоматизації процесів, контролю за ресурсами та безпекою, що є важливим під час проведення змагань із кібербезпеки.

Використання Kubernetes дозволяє адаптувати платформу до будь-якої кількості учасників, а також інтегрувати її з іншими системами для покращення навчання та моніторингу. Cyber Ice Vox є оптимальним вибором для організаторів, які прагнуть створити реалістичні та безпечні умови для змагань, що сприяють розвитку навичок кіберзахисту в Україні та на міжнародному рівні.

Список літератури:

1. Capture the flag (CTF): веб-сайт. URL: [https://uk.wikipedia.org/wiki/Capture_the_flag_\(CTF\)](https://uk.wikipedia.org/wiki/Capture_the_flag_(CTF))
2. CTF: веб-сайт. URL: <https://www.linkedin.com/pulse/ctf-digialert>
3. Overview | Kubernetes: веб-сайт. URL: <https://kubernetes.io/docs/concepts/overview/#why-you-need-kubernetes-and-what-can-it-do>

УДК 004.4

АНАЛІЗ ІНСТРУМЕНТІВ СИСТЕМИ МОНІТОРИНГУ GRAFANA

Автор: Подгайний О.М., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Вступ. Системи моніторингу – це апаратний або програмний компонент, який використовується для моніторингу системних ресурсів і продуктивності комп’ютерної системи. Серед проблем керування використанням інструментів моніторингу системи є використання ресурсів і конфіденційність. Моніторинг може відстежувати як вхідні, так і вихідні значення та події систем.

Зазвичай потужні системи моніторингу та візуалізації даних є платними або націлені на конкретний вид діяльності, наприклад, SIEM системи для менеджменту безпеки інформації. Використання таких систем надає інформацію про захищену систему в зручному для користувача вигляді, що забезпечує ефективне керування інцидентами в сфері кіберзахисту.

Grafana – це мультиплатформенний веб-додаток для аналітики та інтерактивної візуалізації з відкритим кодом. Він може створювати діаграми, графіки та сповіщення для Інтернету при підключенні до підтримуваних джерел даних. Існує дві версії даної системи це безкоштовна та комерційна Grafana Enterprise з додатковими можливостями, яка продається як самостійна інсталяція або через обліковий запис у хмарному сервісі Grafana Labs.

Мето роботи є аналіз інструментів системи Grafana для моніторингу безпеки та керування подіями.

Основна частина.

Однією з основних задач, що накладаються на систему моніторингу є візуалізація даних. В системі Grafana це забезпечується за допомогою спеціалізованих інформаційних панелей (dashboards).

Інформаційна панель Grafana складається з панелей, які відображають дані у вигляді красивих графіків, діаграм та інших візуалізацій. Ці панелі створюються за допомогою компонентів, які перетворюють необроблені дані з джерела даних у візуалізації. Процес передбачає передачу даних через три шлюзи: плагін, запит і додаткове перетворення.

Джерело даних відноситься до будь-якої сутності, яка складається з даних. Це може бути база даних SQL, Grafana Loki, Grafana Mimir або API на основі JSON. Це може бути навіть простий файл CSV. На інформаційних панелях ви можете бачити різні джерела даних, візуалізовані в одному модулі, що полегшує загальне розуміння даних.

Плагін Grafana – це програмне забезпечення, яке додає нові можливості Grafana. Вони бувають багатьох типів, але зараз ми розглянемо плагіни джерела даних. Завдання плагіна джерела даних Grafana полягає в тому, щоб прийняти запит, на який ви хочете отримати відповідь, отримати дані з джерела даних і узгодити відмінності між моделлю даних джерела даних і моделлю даних панелей інструментів Grafana. Для цього використовується уніфікована структура даних, яка називається кадром даних.

Запити дозволяють скоротити всі ваші дані до певного набору даних, забезпечуючи більш керовану візуалізацію. Вони допоможуть відповісти на ваші запитання щодо системи та операційних процесів. Працюючи з джерелами даних, дуже важливо розуміти, що кожне з них має свою окрему мову запитів.

Якщо формат даних у візуалізації не відповідає вашим вимогам, ви можете застосувати перетворення, яке маніпулює даними, повернувши запитом.

Після отримання даних, їх запитів і трансформації вони переходять на панель, яка є останніми воротами на шляху до візуалізації Grafana. Панель – це контейнер, який відображає візуалізацію та надає різні елементи керування для керування нею. У конфігурації панелі ви вказуєте, як ви хочете бачити дані. Наприклад, ви використовуєте спадне меню у верхньому правому куті панелі, щоб вказати тип візуалізації, який ви хочете побачити, як-от гістограма, секторна діаграма або гістограма.

Крім основних функцій візуалізації даних можна використовувати наступні можливості без встановлення додаткових плагінів:

– використовуючи Grafana Alerting, ви створюєте запити та вирази з багатьох джерел даних – незалежно від того, де зберігаються ваші дані

– це дає вам можливість об'єднувати дані та сповіщати про показники та журнали новими та унікальними способами;

– створення та керування звітами – дає змогу автоматично генерувати PDF-файли з будь-якої панелі інструментів і надсилати їх електронною поштою Grafana зацікавленим сторонам за розкладом. Це доступно в Grafana Cloud і Grafana Enterprise.

Розширення функціоналу Grafana забезпечується встановленням додаткових плагінів: Grafana Loki, Grafana Tempo, Grafana Mimir, Grafana Pyroscope, Grafana OnCall та Grafana Cloud

Висновки

Створення інформаційної панелі Grafana – це процес, який починається з визначення вимог до інформаційної панелі та визначення джерел даних, які підтримують ці вимоги. Якщо ви хочете інтегрувати спеціалізовану базу даних із інформаційною панеллю Grafana, ви повинні переконатися, що встановлено правильний плагін, щоб можна було додати джерело даних для використання з цим плагіном.

Визначивши джерело даних і встановивши плагін, ви можете написати свій запит, перетворити дані та відформатувати візуалізацію відповідно до ваших потреб.

Ця компонентна архітектура є частиною того, що робить Grafana настільки потужним і загальним. Враховуючи плагін джерела даних і абстракцію кадру даних, будь-яке джерело даних, до якого ви можете отримати доступ, може працювати з тим самим загальним підходом.

Список літератури:

1. Introduction of Grafana and its Usage: веб сайт URL: <https://www.cisco.com/c/en/us/support/docs/wireless/policy-suite-mobile/214788-introduction-of-grafana-and-its-usage.pdf>

УДК 004.4

МОДЕРНІЗАЦІЯ НАВЧАЛЬНО-НАУКОВОЇ ЛАБОРАТОРІЇ "БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИЙ СИСТЕМ"

Автор: Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Вступ. В останні роки все більше набуває актуальності та популярності підготовка спеціалістів з галузі кібербезпеки. Суттєвим поштовхом для цього стала цифровізація українського суспільства через епідемію коронавірусу в 2020 та підвищення актуальності захисту цифрових ресурсів в наслідок вторгнення Російської Федерації в 2022 році.

Реакцією на дані проблеми в Україні були проведено ряд змін в підході до кібербезпеки до них можна віднести:

- впровадження ЄДКІ;
- підвищена популярність змагань з кібербезпеки CTF;
- співробітництво з агентством з міжнародного розвитку USAID;
- відкриття нових спеціальностей з напрямку кібербезпеки в вищих навчальних закладах України;
- підключення міжнародних організацій до ініціатив в сфері кібербезпеки.

Для підтримання високого рівня підготовки спеціалістів перед кафедрою постають наступні виклики:

- зміна підготовки напрямку безпеки інформаційного-комунікаційних систем у відповідності до вимог ЄДКІ;
- підготовка студентів та створення команди для участі в змаганнях CTF;
- підтримка наукової діяльності студентів;
- підготовка студентів та готовність організації бригад для кіберклінік.

Мета роботи. Для подолання вищезазначених викликів пропонується модернізація лабораторії "Безпеки інформаційно-комунікаційних систем" для вивчення, аналізу та впровадження рішень з питань:

- адміністрування та захист комп'ютерних мереж;
- аналіз та балансування мережевого трафіку;
- сканування та виявлення вразливостей веб-застосунків та елементів комп'ютерних мереж;

- захист персональних комп'ютерів;
- виявлення мережових атак та протидія їм;
- моніторинг мережових ресурсів;
- засоби віддаленого контролю.

Основна частина.

Структура лабораторії повинна розбиватися на дві складові: фізична та віртуальна.

Фізична складова лабораторії включає в себе апаратне забезпечення лабораторії, що не виходить за її межі. До фізичних пристроїв відносяться персональні комп'ютери, мереже обладнання та засоби демонстрації (проектор або монітор з великою діагоналлю).

Віртуальна складова лабораторії включає в себе засоби моделювання (Cisco Packet Tracer, Oracle VirtualBox), віддалені робочі місця для роботи з вибагливими задачами, тестовий web-сервер та поштовий сервер, віртуальні робочі машини з відомими вразливостями, тестовий сервер для проведення CTF та сторонні сервери тестування навичок (Hack The Box, TryHackMe).

Фізична структура лабораторії в свою чергу повинна поділятися на дві мережі: тестова мережа та загальна мережа.

Являє собою ізольовану локальну мережу з 4 комп'ютерами, 3 маршрутизаторами та 1 міжмережовим екраном.

Задачею даної локальної мережі є надання студентам навичок налаштування маршрутизаторів, виявлення вразливостей реальних персональних комп'ютерів, локальні змагання червоної та синьої команди кіберзахисту без можливості завдання шкоди загальній мережі кафедри та університету.

Комп'ютери в даній мережі використовуються для перевірки працездатності мережі або як цілі для мережових атак.

Маршрутизатори в даній мережі повинні надавати студентам навичок з налаштувань мережових операційних систем різної складності:

– Cisco IOS – програмне забезпечення, що використовується в маршрутизаторах і мережових комутаторах Cisco. В Cisco IOS є специфічний інтерфейс командного рядка (command line interface, CLI), який був скопійований багатьма іншими мережевими продуктами. Інтерфейс IOS пропонує набір

багатослівних команд, відповідно до обраного режиму і рівню привілеїв користувача. Global configuration mode надає можливість для зміни налаштувань системи і мережевих інтерфейсів, даних;

- Router OS – це спеціалізована операційна система, призначена виключно для побудови багатофункціональних маршрутизаторів, фаєрволів, бриджів, базових станцій, vpn-серверів, web-серверів та інших пристроїв керування мережами;

- OpenWrt – це проект із відкритим вихідним кодом для вбудованих операційних систем на базі Linux, який переважно використовується на вбудованих пристроях для маршрутизації мережевого трафіку.

Загальна мережа необхідна для взаємодії студентів з глобальною мережею Інтернет та доступу до віртуальних навчальних ресурсів та повинна складатися не менше ніж з 6 комп'ютерів та одного комутатора.

Віртуальні складова лабораторії може бути реалізована, як на сервері кафедри так і за її межами. На сервері кафедри пропонується використання віртуальних робочих місць з операційними системами Windows та Kali Linux. Що забезпечить роботу практично з всім необхідним програмним забезпеченням.

Для демонстрації вразливостей веб застосунків пропонується використання веб серверу з відомим набором вразливостей, що дасть студентам поняття як саме працюють дані вразливості.

Розгортання поштового серверу та налаштування систем захисту та здійснення атак на нього.

Для забезпечення системи безпеки операційної системи користувачу повинні бути надані права адміністратора, тому для того щоб студент не зміг нашкодити програмному забезпеченню кафедри необхідно для тестування системи безпеки розгортати віртуальні машини за допомогою програмного забезпечення Oracle VirtualBox.

Додатково планується використання Cisco Packet Tracer для моделювання роботи комп'ютерних мереж та систем Cyber Ice Box platform і Hack The Box для підготовки студентів до CTF змагань.

Висновки. Розвиток лабораторії дасть змогу покращити навчання студентів в напрямку кібербезпеки та ставить нові завдання перед викладацьким складом до яких відносяться: складання переліку необхідного програмного забезпечення; підготовка методичних вказівок; підготовка тестових завдань.

ВИКОРИСТАННЯ СИСТЕМ МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ В УМОВАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Автори: Трибулькевич С.Л., ст. викладач; Трибулькевич В.В., викладач; Титарчук В.В., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

В умовах швидкого розвитку інформаційних технологій та необхідності адаптації освітнього процесу до нових реалій, зокрема в умовах дистанційного навчання, важливу роль відіграють інструменти для ефективного моделювання комп'ютерних мереж. Застосування систем моделювання комп'ютерних мереж дозволяє створювати віртуальні моделі реальних мережевих інфраструктур, тестувати різні сценарії роботи та оптимізувати мережеві ресурси без необхідності фізичного втручання. У рамках дистанційного навчання ці системи стають незамінним інструментом для студентів та викладачів, адже вони дозволяють поглиблено вивчати складні аспекти мережевих технологій, не маючи доступу до реальних фізичних лабораторій.

Існує велика кількість систем моделювання комп'ютерних мереж, які використовуються для дослідження, проектування та аналізу мережевих топологій та протоколів. За можливістю багатокористувацького доступу системи моделювання можна поділити на такі, що встановлюються індивідуально, та системи моделювання з доступом через Web-сервер (рис. 1).

Однею за найвідоміших програм для моделювання мереж є Packet Tracer – симулятор мережі передачі даних, що випускається фірмою Cisco Systems. Дозволяє створювати працездатні моделі мережі, налаштовувати маршрутизатори та комутатори, взаємодіяти між кількома користувачами (через хмару). Інтерфейс програми показано на рис. 2.

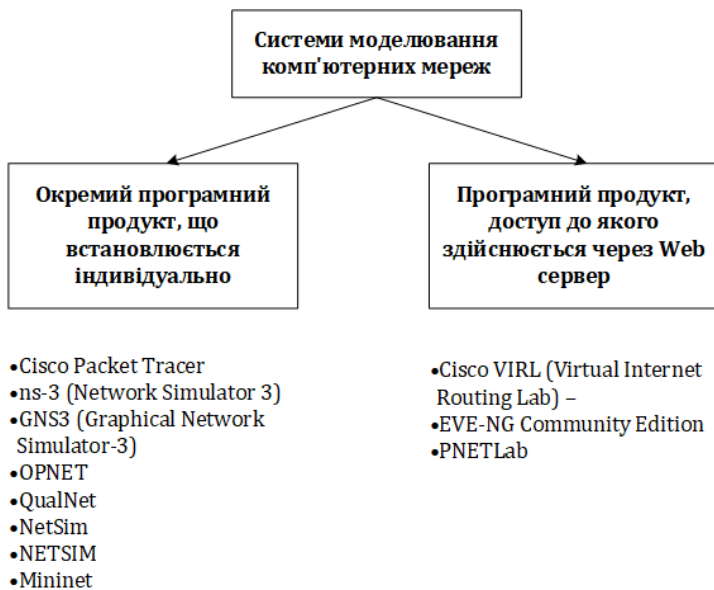


Рисунок 1 – Класифікація систем моделювання за можливістю багатокористувацького доступу

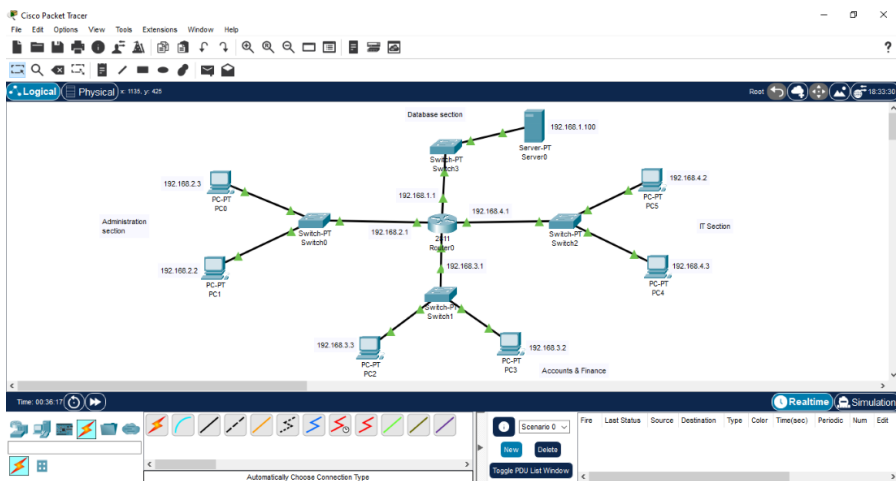


Рисунок 2 – Інтерфейс Cisco Packet Tracer

Packet Tracer в основному орієнтований на учасників Програми Мережевої Академії Cisco в якості безкоштовного навчального посібника, який допомагає їм вивчити основні концепції сертифікації Cisco. До переваг слід віднести широкий спектр обладнання Cisco, що підтримується, водночас, до недоліків слід віднести те, що підтримується обладнання лише фірми Cisco.

NS (від симулятор мережі) – назва низки мережевих симуляторів дискретних подій, зокрема, NS-1, NS-2 та NS-3. Всі вони є дискретно-подієвими комп'ютерними мережевими тренажерами, в основному використовується в дослідженнях і викладанні. NS-3-це безкоштовна програма, у відкритому доступі під ліцензією GNU gplv2 — ліцензія на дослідження, розробку і використання.

ns-1 розробка більше не ведеться,

ns-2 розвивається не активно (активна розробка припинена в 2010 році, але добровольці зі спільноти користувачів, як і раніше, розвивають його)

ns-3 активно розвивається (але не сумісний для роботи на ns-2).

Як і NS-2, NS-3 є також трудомістким в освоєнні і використанні, в порівнянні з симуляторами на основі GUI.

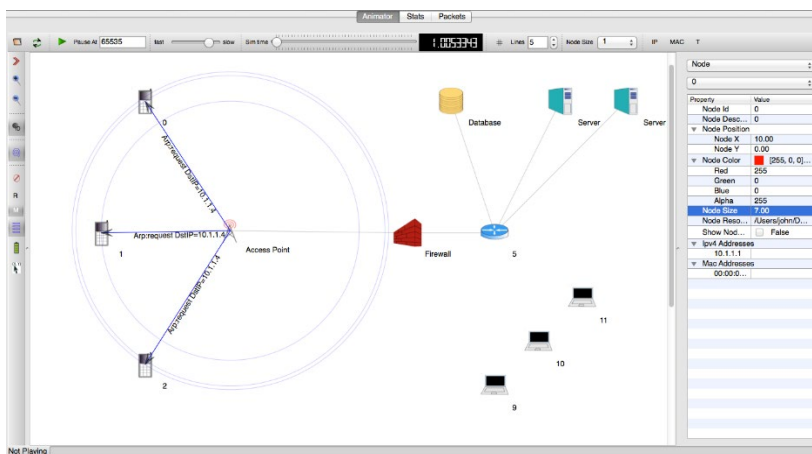


Рисунок 3 – Анімація в симуляторі NS-3

GNS3 (Graphical Network Simulator-3) – потужний емулятор, що дозволяє змоделювати реальні мережеві пристрої за допомогою віртуальних машин. GNS3 (Graphical Network Simulator-3) – це програмний емулятор комп'ютерної мережі. На відміну Cisco Packet Tracer, котрий націлений на симуляцію процесу побудови та конфігурування мереж Cisco, GNS3 дозволяє емулювати складні комп'ютерні мережі, комбінуючи реальні та віртуальні мережеві пристрої.

Серед віртуальних пристроїв з яких може складатися мережа є віртуальні машини QEMU, VirtualBox, VMware, Docker-контейнери, vpcs, запущені через dynamips реальні образи маршрутизаторів Cisco та IOU (IOS on UNIX) образи від Cisco. Також у сам GNS3 вбудована емуляція найпростіших комутаторів першого та другого рівня моделі OSI.

GNS3 написаний на мові програмування Python і використовує бібліотеку Qt для відображення графічного інтерфейсу, що робить це програмне забезпечення кроссплатформовим.

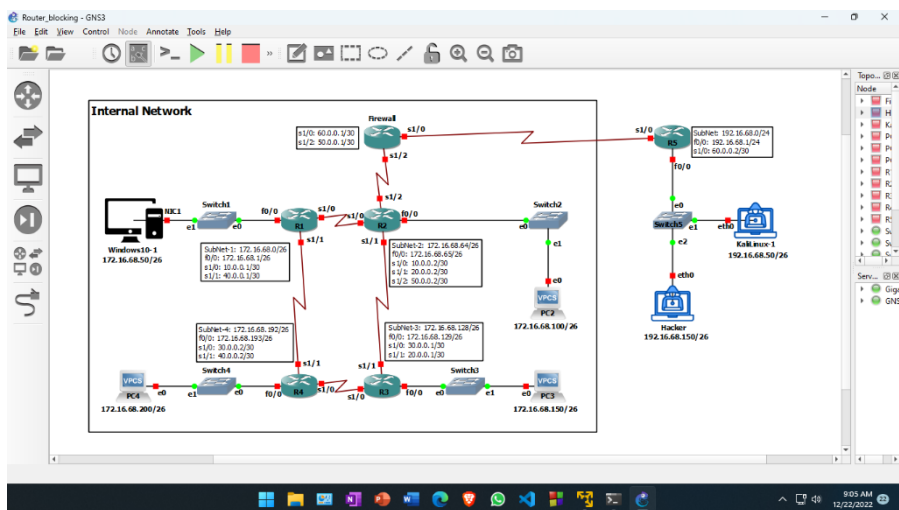


Рисунок 4 – Інтерфейс GNS3 (Graphical Network Simulator-3)

OPNET – комерційний програмний продукт, що надає широкий спектр інструментів для моделювання та аналізу комп'ютерних мереж. Набір протоколів/пристроїв є фіксованим – ви не можете створювати нові протоколи або змінювати поведінку існуючих.

web-site: conference.nuos.edu.ua | email: conference@nuos.edu.ua; tel (+380512) 709444; 709105|

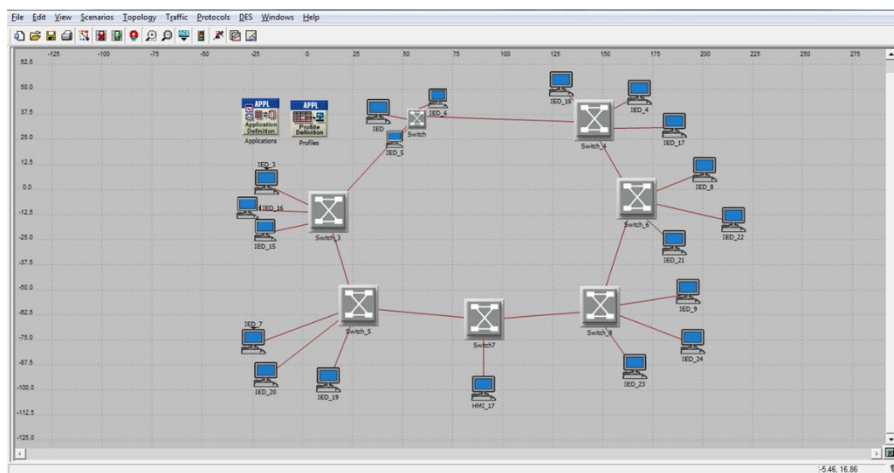


Рисунок 5 – Інтерфейс OPNET

QualNet – ще один комерційний симулятор, який надає можливості для моделювання мобільних, бездротових і проводових мереж.

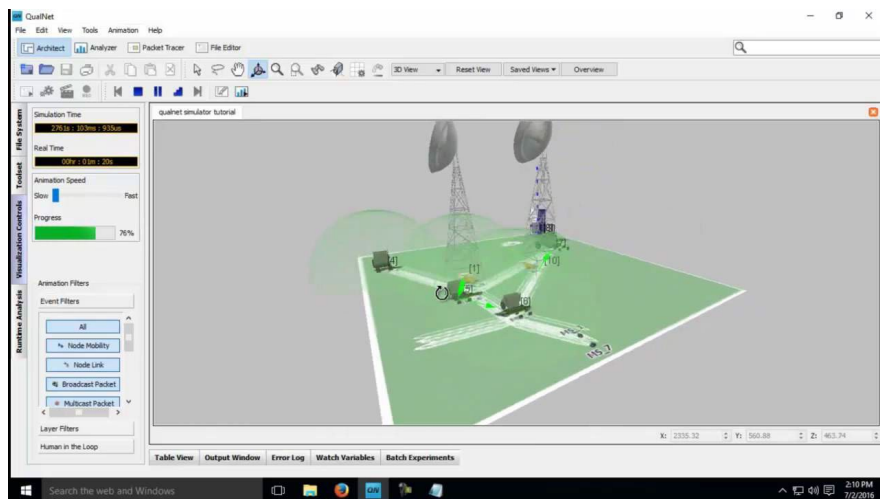


Рисунок 6 – Інтерфейс QualNet

Секція 6. Підготовка кадрів у галузі знань «Інформаційна безпека»

NetSim – симулятор, який підтримує різні мережеві технології та протоколи, що дозволяє вивчати мережі різного рівня складності.

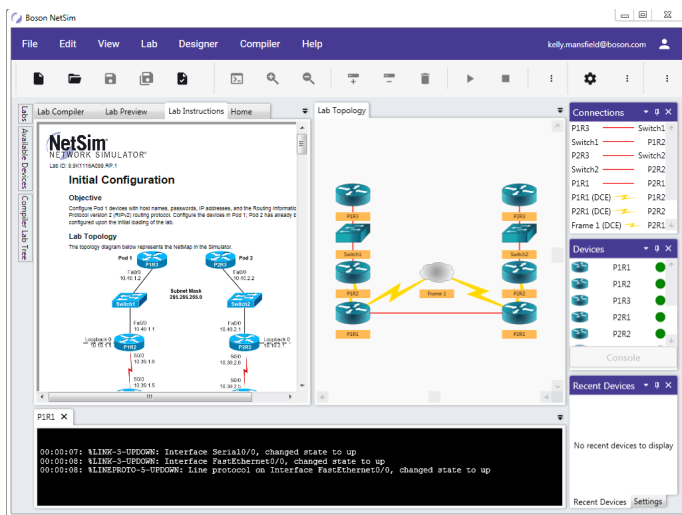


Рисунок 7 – Інтерфейс NetSim

NETSIM – симулятор, який підтримує різні мережеві технології та протоколи, що дозволяє вивчати мережі різного рівня складності.

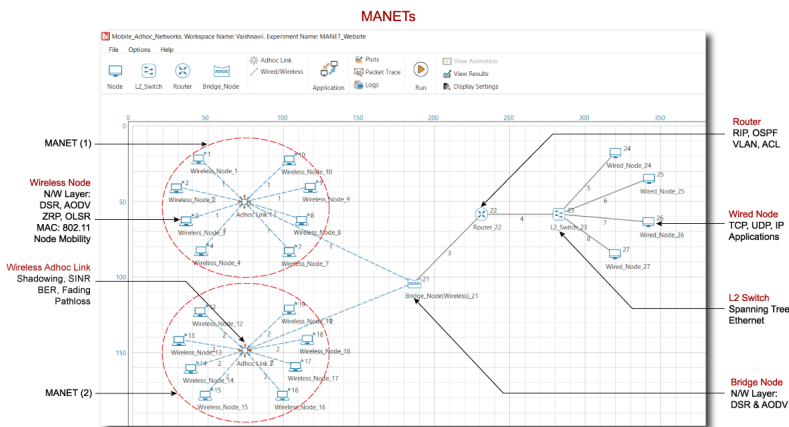


Рисунок 8 – Інтерфейс NETSIM

Mininet – легка платформа для створення і тестування віртуальних мереж в середовищі Linux. Підходить для розробників і дослідників, які хочуть експериментувати з SDN (Software Defined Networking).

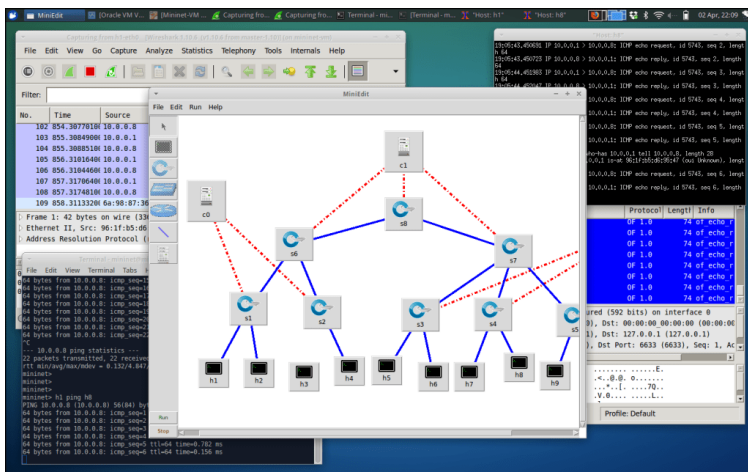


Рисунок 9 – Інтерфейс Mininet

Cisco VIRL (Virtual Internet Routing Lab) – платформа для віртуального моделювання, що дозволяє створювати та тестувати мережеві топології з використанням Cisco IOS та інших образів.

EVE-NG Community Edition – безкоштовна версія EVE-NG, яка також дозволяє створювати віртуальні мережі та є популярною серед студентів та фахівців.

EVE-NG Community Edition (Emulated Virtual Environment Next Generation) – це безкоштовна версія потужної платформи для віртуалізації та моделювання комп'ютерних мереж, яка дозволяє створювати складні топології мереж і симулювати роботу мережевих пристроїв. EVE-NG Community Edition надає можливість для навчання, тестування та вдосконалення мережевих навичок без необхідності в фізичному обладнанні. Ця версія платформи є ідеальним інструментом для студентів, професіоналів і тих, хто готується до сертифікацій Cisco, Juniper, VMware та інших провідних виробників мережевого обладнання.

|web-site: conference.nuos.edu.ua | email: conference@nuos.edu.ua; tel (+380512) 709444; 709105|

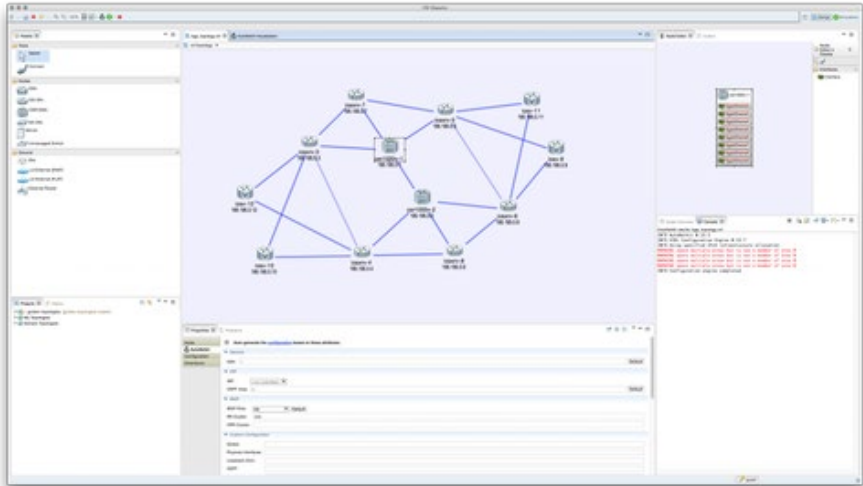


Рисунок 10 – Інтерфейс Cisco VIRL

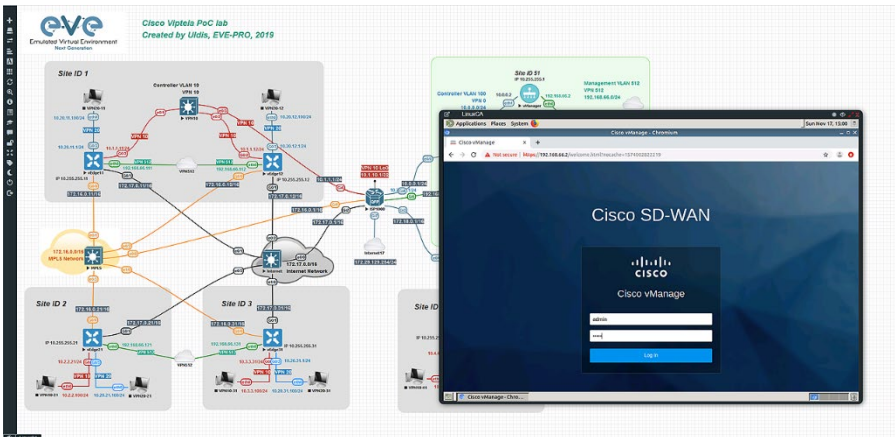


Рисунок 11 – Інтерфейс EVE-NG Community Edition

Основні характеристики EVE-NG Community Edition:

1. EVE-NG дозволяє створювати віртуальні мережі з використанням різноманітних мережевих пристроїв, таких як маршрутизатори,

комутатори, брандмауери, сервери та інші. Користувачі можуть працювати з топологіями, що складаються з багатьох вузлів і підключених пристроїв, що дозволяє тестувати реальні сценарії налаштування та оптимізації мереж.

2. Платформа підтримує віртуальні образи пристроїв різних виробників, таких як Cisco, Juniper, Arista, Dell і багато інших. Це робить EVE-NG потужним інструментом для навчання роботи з мережами різних типів і виробників.

3. EVE-NG має простий і зручний веб-інтерфейс, що дозволяє легко створювати топології, налаштовувати пристрої, підключати їх між собою та управляти мережею. Інтерфейс також дозволяє зручно запускати і зупиняти віртуальні машини, а також здійснювати доступ до них для конфігурації.

4. В EVE-NG можна симулювати роботу багатьох мережевих протоколів, таких як TCP/IP, OSPF, EIGRP, BGP, MPLS, VLAN, NAT, VRF, а також різноманітні технології віртуалізації, такі як VMware, Docker, VirtualBox тощо.

5. EVE-NG використовує KVM (Kernel-based Virtual Machine) для віртуалізації, що забезпечує високу продуктивність та ефективність при моделюванні мереж. Це дає змогу запускати великі та складні мережеві топології навіть на стандартних комп'ютерах.

6. Одна з переваг EVE-NG — це підтримка колективної роботи. Кілька користувачів можуть працювати над однією топологією одночасно, що корисно для групових навчальних занять або роботи над проектами в команді.

7. Окрім віртуальних пристроїв, EVE-NG підтримує інтеграцію з реальними мережевими пристроями через серійний порт або через консольний доступ, що дає змогу тестувати реальні конфігурації без необхідності наявності фізичного обладнання.

8. EVE-NG Community Edition є безкоштовною для особистого і навчального використання, що робить його доступним для широкого кола користувачів, включаючи студентів, викладачів і самонавчальних фахівців.

PNETLab – дозволяє створювати віртуальні мережі та є популярною серед студентів та фахівців. — це потужна платформа для

моделювання комп'ютерних мереж, яка дозволяє створювати віртуальні мережі з використанням різноманітних мережевих пристроїв та технологій. Вона є популярним інструментом серед студентів, викладачів і фахівців, які бажають здобути практичний досвід у налаштуванні та управлінні комп'ютерними мережами без необхідності використання фізичного обладнання. PNETLab, подібно до інших систем моделювання, таких як EVE-NG, дає можливість створювати складні топології мереж і тестувати різноманітні мережеві конфігурації в умовах віртуального середовища.

Основні характеристики PNETLab:

1. PNETLab дозволяє створювати віртуальні мережі, включаючи маршрутизатори, комутатори, брандмауери, сервери та інші пристрої, які можна з'єднувати для побудови складних мережевих топологій. Користувачі можуть налаштовувати різні мережеві протоколи та технології, наприклад, маршрутизацію, VLAN, VPN, NAT, QoS тощо.

2. Платформа підтримує віртуальні образи пристроїв різних постачальників, таких як Cisco, Juniper, Arista, Fortinet і багато інших. Це дозволяє створювати реалістичні лабораторії, які допомагають студентам і професіоналам освоювати роботу з пристроями різних виробників.

3. PNETLab має простий у використанні веб-інтерфейс, що дозволяє легко створювати і управляти мережевими топологіями. Користувачі можуть додавати пристрої, налаштовувати їх, зв'язувати їх у мережу та запускати конфігурації в кілька кліків.

4. PNETLab дає змогу моделювати різноманітні мережеві протоколи, такі як OSPF, BGP, EIGRP, RIP, MPLS, STP, а також протоколи безпеки, VPN та інші. Це дозволяє студентам і професіоналам розв'язувати складні задачі з налаштування мереж і тестувати роботу мережевих протоколів в умовах реального середовища.

5. Однією з переваг PNETLab є можливість використання реальних образів операційних систем, таких як Cisco IOS, Juniper JunOS, FortiOS, а також образів для віртуалізації, таких як VMware ESXi або KVM. Це дає змогу працювати з реальними операційними системами мережевих пристроїв, що є важливим для професіоналів, які готуються до сертифікаційних іспитів або працюють у реальних проектах.

6. PNETLab інтегрується з платформами віртуалізації, такими як VMware та VirtualBox, що дозволяє використовувати зовнішні

віртуальні машини для симуляції більш складних інфраструктур. Це відкриває додаткові можливості для створення багатокомпонентних мережевих середовищ.

7. PNETLab підтримує роботу на різних операційних системах, таких як Linux та Windows. Це дає можливість використовувати платформу на різних комп'ютерах без прив'язки до конкретної ОС.

Переваги використання PNETLab:

1. Простий веб-інтерфейс і потужний функціонал роблять PNETLab дуже зручним для навчальних цілей. Студенти можуть легко створювати та налаштовувати мережеві топології, виконувати лабораторні роботи та тестувати різноманітні сценарії, не витрачаючи час на налаштування фізичного обладнання.

2. Завдяки можливості використання реальних образів мережевих пристроїв, а також підтримці багатьох мережевих протоколів, PNETLab дає змогу моделювати реальні умови роботи мережі. Це допомагає студентам і фахівцям здобути практичні навички, які можуть бути корисними при роботі з реальними мережами.

3. PNETLab є відмінним інструментом для підготовки до сертифікаційних іспитів таких, як CCNA, CCNP, JNCIA та інших. Моделюючи мережі та протоколи, студенти можуть отримати практичні навички, необхідні для успішного складання іспитів.

4. PNETLab дозволяє кільком користувачам працювати над однією лабораторією або проектом, що є корисним для групових навчальних завдань та проектної роботи. Взаємодія між студентами та викладачами в реальному часі дозволяє ефективно вирішувати завдання та обговорювати результати.

5. PNETLab охоплює широкий спектр мережевих технологій, від основних протоколів маршрутизації до складних налаштувань безпеки та віртуалізації мереж. Це дозволяє студентам освоювати не лише базові аспекти, а й більш складні технології, що застосовуються в реальних мережах.

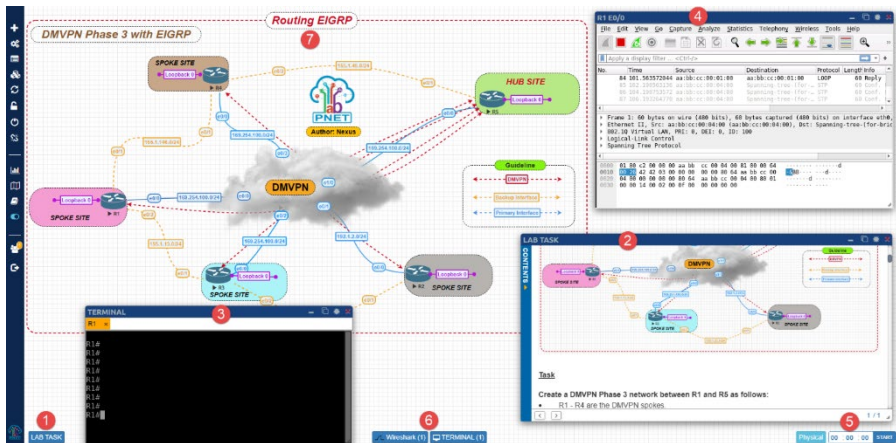


Рисунок 12 – Інтерфейс PNETLab

Висновки. Проведено огляд систем моделювання комп'ютерних мереж, проаналізовано їх переваги та недоліки, а також можливість використання в умовах дистанційного навчання.

Використання таких платформ, як EVE-NG та PNETLab, дає змогу викладачам і студентам створювати складні топології мереж і налаштовувати різноманітні сценарії без обмежень, пов'язаних з фізичними пристроями. Це відкриває безліч можливостей для вивчення складних мережевих конфігурацій у межах дистанційного навчання. EVE-NG і PNETLab дозволяють моделювати реальні умови роботи мережі, що дає можливість студентам отримувати практичний досвід у налаштуванні мережевих пристроїв, маршрутизації, віртуалізації мереж та інших складних технологій. Це дозволяє створювати умови, максимально наближені до реальних, що є важливим для якісної підготовки майбутніх фахівців.

Список літератури:

1. Учасники проєктів Вікімедія. Ns (simulator) – Вікіпедія. *Bikinedia*. URL: [https://uk.wikipedia.org/wiki/Ns_\(simulator\)](https://uk.wikipedia.org/wiki/Ns_(simulator)) (дата звернення: 10.10.2024).
2. Cisco packet tracer. *Cisco Networking Academy: Learn Cybersecurity, Python & More*. URL: <https://www.netacad.com/cisco-packet-tracer> (date of access: 10.10.2024).

3. Cisco virtual internet routing lab (VIRL PE). *Cisco Learning Network*. URL: <https://learningnetwork.cisco.com/s/virl> (date of access: 10.10.2024).

4. Documenation. *PNETLab : Lab is Simple*. URL: <https://pnetlab.com/pages/documentation> (date of access: 10.10.2024).

5. Documentation. *EVE – The Emulated Virtual Environment For Network, Security and DevOps Professionals*. URL: <https://www.eve-ng.net/index.php/documentation/> (date of access: 10.10.2024).

6. Getting Started with GNS3. *GNS3 Documentation*. URL: <https://docs.gns3.com/docs/> (date of access: 10.10.2024).

7. Mininet documentation. *GitHub*. URL: <https://github.com/mininet/mininet/wiki/Documentation> (date of access: 10.10.2024).

8. NetSim network simulator & router simulator. *Network Simulator – Boson*. URL: <https://www.boson.com/netsim-cisco-network-simulator> (date of access: 10.10.2024).

9. OPNET network simulator – opnet projects. *Opnet Projects*. URL: <https://opnetprojects.com/opnet-network-simulator/> (date of access: 10.10.2024).

10. QualNet network simulator. *Keysight*. URL: <https://www.keysight.com/us/en/assets/3122-1395/technical-overviews/QualNet-Network-Simulator.pdf> (date of access: 10.10.2024).

11. Tetcos: netsim – network simulation software, india. *NetSim Home | Network Simulator for 5G, IoT, Military Communication, VANETs, Sat Comm., UWAN and more*. URL: <https://www.tetcos.com/index.html> (date of access: 10.10.2024).

СЕКЦІЯ 7. ШКОЛА МОЛОДИХ НАУКОВЦІВ
РОЗРОБКА КОМПЛЕКСНОГО ПРОГРАМНОГО
ЗАБЕЗПЕЧЕННЯ ДЛЯ АНАЛІЗУ, РОЗПІЗНАВАННЯ ТА
ІДЕНТИФІКАЦІЇ ДИКТОРА

Автор: Байдиків А.О., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Анотація

У сучасному світі голос стає важливим біометричним інструментом, який відкриває нові можливості для ідентифікації особистості, забезпечення безпеки та автоматизації процесів у різних галузях. Цей проект спрямований на створення комплексного програмного забезпечення, яке здатне аналізувати та розпізнавати диктора на основі акустичних параметрів голосу. Ідентифікація диктора є важливою складовою для забезпечення конфіденційності даних, персоналізації сервісів та автоматизації розпізнавання особистості без фізичного контакту.

Вступ

Голосові технології відіграють все більш значущу роль, стають невід'ємною частиною цифрової екосистеми. Завдяки стрімкому розвитку обчислювальних потужностей і алгоритмів машинного навчання, стало можливим ефективно використання голосу не лише як засобу комунікації, але і як унікального біометричного інструменту. Голосові системи широко застосовуються у сферах кібербезпеки, банківських послуг, телекомунікацій, охорони здоров'я та розваг, забезпечуючи автоматизацію процесів, зручність та високий рівень персоналізації.

Ідентифікація диктора, тобто розпізнавання особистості за голосовими характеристиками, є однією з найбільш перспективних галузей досліджень і розробок у цій сфері. Унікальні особливості голосу кожної людини дозволяють створювати надійні системи безпеки, зменшувати залежність від традиційних методів автентифікації (паролів чи PIN-кодів) і підвищувати рівень конфіденційності даних.

Робота спрямована на розробку комплексного програмного забезпечення для аналізу, розпізнавання та ідентифікації диктора, яке

базується на сучасних технологіях обробки мовлення, машинного навчання та біометрії. Розробка такого продукту є важливим кроком для подальшого впровадження інновацій у системи безпеки, аналітику та автоматизацію.

Мета роботи

Розробити програмне забезпечення, яке буде використовувати передові методи аналізу мовного сигналу, алгоритми машинного навчання та нейронні мережі для забезпечення високої точності ідентифікації диктора.

Для досягнення цієї мети були визначені такі **завдання**:

1) ***Дослідження та аналіз наявних підходів***: аналіз сучасних методів розпізнавання мовлення та дикторів, визначення їхніх сильних і слабких сторін.

2) ***Збір та обробка даних: створення бази мовних зразків***, що включає записи голосів різних дикторів за умов різноманітного фону та акустики.

3) ***Розробка алгоритмів: реалізація передових методів обробки мовного сигналу***, зокрема:

- Виділення спектральних характеристик (MFCC, LPC, спектрограми).

- Аналіз акустичних параметрів голосу, таких як висота, тембр, інтонація та частотний діапазон.

1 Дослідження та аналіз наявних підходів

Ці підходи базуються на аналізі акустичних параметрів мовного сигналу:

- ***Метод коефіцієнтів частотної модуляції (MFCC)***: Один із найпоширеніших методів, який виділяє спектральні ознаки мовного сигналу, наближені до сприйняття людського вуха. MFCC дозволяє отримувати компактні та інформативні характеристики голосу.

- ***Лінійне прогнозування кодування (LPC)***: Метод, що використовує моделювання голосового тракту для визначення характеристик мовлення.

- ***Перетворення Фур'є та вейвлет-аналіз***: Використовуються для аналізу спектральних і тимчасових ознак мовлення.

Останніми роками глибокі нейронні мережі (DNN) стали основою сучасних систем ідентифікації диктора завдяки їхній здатності виявляти складні нелінійні закономірності в даних:

- **Глибокі згорткові нейронні мережі (CNN):** Використовуються для аналізу спектрограм голосу, що дозволяє враховувати просторові залежності між спектральними компонентами.

- **Рекурентні нейронні мережі (RNN) та їхні модифікації (LSTM, GRU):** Застосовуються для аналізу послідовності мовлення, враховуючи тимчасову динаміку голосових сигналів.

- **Трансформери:** Сучасні архітектури, такі як Wav2Vec або Whisper, здатні вчитися на величезних наборах даних безпосередньо з мовного сигналу, не покладаючись на традиційні методи вилучення ознак.

2 Збір та обробка даних

2.1 Формування вибірки

Для забезпечення точності ідентифікації необхідно зібрати різноманітний набір мовних записів, який враховує:

- **Різноманіття дикторів:** Зразки повинні включати голоси людей різного віку, статі, національності та діалектів.

- **Акустичні умови:** Записи мають бути зроблені за різних умов, включаючи тихе середовище, фоновий шум, різні типи мікрофонів і дистанцій запису.

- **Мовний контент:** Вибірка має містити як заздалегідь визначені фрази, так і довільне мовлення.

2.2 Джерела даних

- **Публічні бази даних:** Використання вже існуючих наборів даних, таких як LibriSpeech, VoxCeleb, TIMIT або Mozilla Common Voice.

- **Власні записи:** Організація збирання голосових зразків через мобільні додатки, веб-платформи чи польові дослідження.

- **Синтетичні дані:** Генерація голосів за допомогою TTS (Text-to-Speech) технологій для розширення бази, хоча їх використання обмежується через нестачу природності.

2.3 Етичні аспекти

- **Дотримання конфіденційності:** Збирання даних потребує отримання інформованої згоди від учасників.

- **Анонімізація:** Видалення особистих даних для захисту конфіденційності.

3 Розробка алгоритмів

Працюючи над цим проєктом, мені вдалося зібрати існуючі методи аналізу такі як:

- Поділ гармонійних (тональних) та ударних (перехідних) сигналів;
- Вилучення бітів – Beat;
- Нормалізовану енергію кольоровості (функції кольоровості, Chroma Energy Normalized (CENS));
- Мел-кепстральні коефіцієнти (MFCC);
- Спектрограми;
- Спектральний центроїд (Spectral Centroid);
- Спектральний контраст (Spectral Contrast);
- Спектральний спад (Spectral Rolloff);
- Спектральна ширина (Spectral bandwidth);
- Швидкість перетину нуля – Zero Crossing Rate

Зібравши все в один код, можна продемонструвати роботу цих методів (див. рис. 1, 2, 3). Для аналізу був використаний мій голос та фраза “Привіт. Як справи?”. Код був написаний мовою програмування Python.

Гармонічна складова сигналу містить тональні елементи, які мають чіткі частоти та довгі періоди. Перкусійна складова сигналу включає ударні та імпульсні звуки, які мають коротку тривалість і виражений час початку.

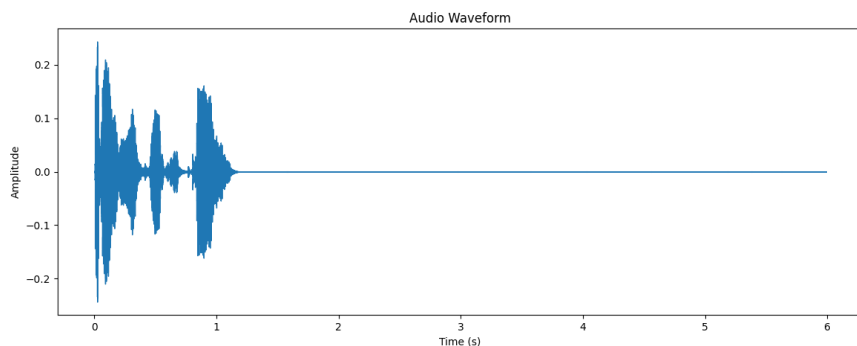


Рисунок 1 – Графічне представлення аудіо сигналу.

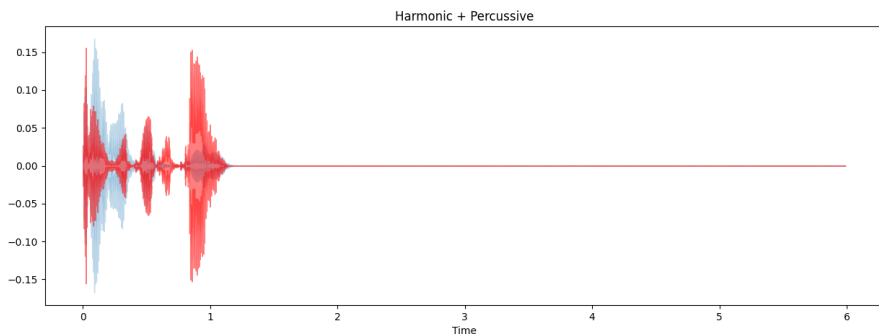


Рисунок 2 – Поділ гармонійних (тональних) та ударних (перехідних) сигналів.

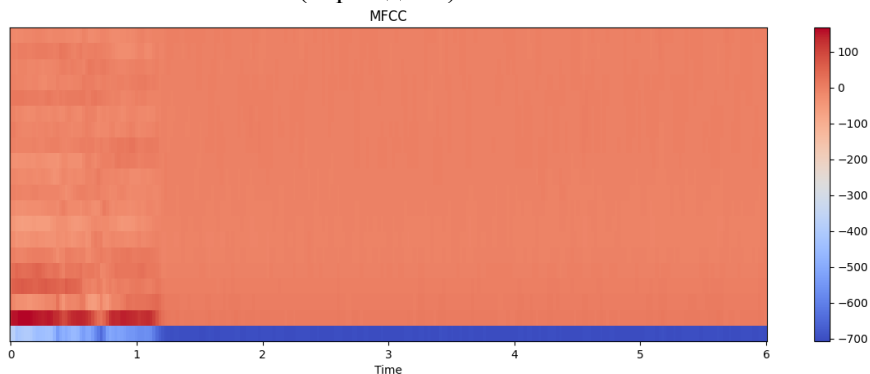


Рисунок 3 – Мел-кепстральні коефіцієнти (MFCC).

MFCC – являють собою набір ознак , які описують загальну форму спектральної огинаючої. Вони моделюють властивості людського голосу. MFCC – коефіцієнти частотної капсули, що підсумовують частотний розподіл за розміром вікна. Тому можна аналізувати як частотні, і тимчасові характеристики звуку. Перед побудовою графіка коефіцієнти нормалізуються.

4 Висновки

На початковому етапі розробки програмного забезпечення для аналізу, розпізнавання та ідентифікації диктора було виконано базові дослідження, визначено вимоги до системи та закладено фундамент для подальшої реалізації проекту.

Основні висновки цього етапу:

1) Сформульовано основну мету проекту – створення системи для розпізнавання дикторів на основі голосових характеристик. Виділено ключові завдання, такі як збір даних, розробка алгоритмів аналізу, побудова моделей і тестування системи.

2) Проведено огляд сучасних технологій розпізнавання диктора, включаючи традиційні методи обробки мовного сигналу (MFCC, LPC) та новітні підходи на основі глибокого навчання (CNN, RNN, трансформери). Виявлено, що найбільш перспективними для досягнення високої точності є методи, що поєднують традиційні алгоритми зі штучним інтелектом.

3) Проведено базові експерименти з виділення характеристик мовного сигналу (спектрограм, MFCC), що дозволило перевірити ефективність інструментів для обробки звуку та закласти основу для побудови моделей.

4) Окреслено технічні вимоги до програмного забезпечення:

- швидкодія для роботи в реальному часі;
- стійкість до шумів та зовнішніх перешкод;
- можливість масштабування для великих обсягів даних.

5) Проблеми та ризики. Виявлено потенційні ризики, пов'язані з доступністю якісних даних, необхідністю значних обчислювальних ресурсів і стійкістю моделей до різних умов.

Список літератури:

1. Audio analysis (part 1). URL: <https://habr.com/ru/articles/668518/>
2. Audio analysis (part 2). URL: <https://habr.com/ru/articles/670676/>
3. Чат GPT. URL: <https://chatgpt.com/g/g-mzFm1dKjW-chat-gpt>
4. Speech Recognition, Pyaudio и Libros. URL: <https://habr.com/ru/articles/577806/>
5. Аналіз аудіо. Ідентифікація голосу URL: <https://habr.com/ru/articles/572496/>
6. V.I. Solovyov, O.V. Rybalskiy, V.V. Zhuravel, N.V. Semyonova. Analyzing the models of speech recognition on the basis of neural networks of deep learning for examination of digital phonograms. Кібернетика та системний аналіз, 2021, том 57, № 1 URL: <http://www.kibernetika.org/volumes/2021/numbers/01/articles/13/13.pdf>

УДК 004.4

АЛГОРИТМИ ЗМЕНШЕННЯ РОЗМИТОСТІ ЗОБРАЖЕНЬ

Автор: Дацко О.Ю., студент, Національний університет кораблебудування імені адмірала Макарова, Миколаїв, Україна

Науковий керівник: Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Вступ. Погіршення зображення є однією з найсерйозніших проблем під час обробки зображень. Розмитість зображення — це несподіване зменшення пропускну здатності, яке погіршує якість зображення, і якого важко уникнути. Розмиття спричинене турбулентністю повітря або неправильним налаштуванням камери. Шум, крім ефектів розмиття, спотворює зняте зображення. Відновлення зображення — це техніка для усунення розмитості зіпсованого зображення та відновлення оригінального зображення. Розмиття може приймати різноманітні форми, наприклад розмиття за Гаусом, розмиття під час руху тощо. Останніми роками було представлено численні стратегії та методології для зменшення розмитості зіпсованого зображення. Існують спеціальні методи для усунення певних форм розмиття.

Мета роботи зробити огляд алгоритмів зменшення розмитості зображень.

Основна частина.

Проблема розмиття під час обробки зображень, яка знижує продуктивність і якість, є значною. Усунення розмиття усуває артефакти розмиття із зображень, зокрема розмиття від руху або розмиття через аберацію розфокусування. Розмиття часто описують як результат згортки (іноді змінної в просторі або часі) функції розповсюдження точки (PSF) із гіпотетичним чітким вхідним зображенням (яке потрібно отримати), де як різке вхідне зображення, так і функція поширення точок невідома.

Існує кілька методів видалення розмитості, які класифікуються як:

- алгоритм сліпої деконволюції. Якщо відомості про викривлення (розмиття та шум) невідомі, можна вважати ефективним алгоритм сліпої деконволюції. Метод одночасно відновлює зображення та функцію поширення точки. Кожна ітерація використовує прискорений

демпфованій алгоритм Річардсона-Люсі. Інші функції оптичної системи, наприклад камери, можна використовувати як вхідні параметри для покращення якості відновлення зображення. Обмеження PSF можуть передаватися функцією, визначеною користувачем;

- алгоритм Люсі-Річардсона. Коли відома функція розповсюдження точки PSF (оператор розмиття), але майже немає знань про шум, можна ефективно використовувати метод Люсі-Річардсона. Ітеративна, прискорена, демпфована техніка Люсі-Річардсона відновлює розмите та шумне зображення. Щоб підвищити якість відновлення зображення, додаткову оптичну систему (наприклад, камеру) можна використовувати як вхідні параметри;

- регуляризований фільтр. Коли на відновлене зображення накладаються обмеження (такі як гладкість) і мало відомо про додатковий шум, можна ефективно використовувати регуляризовану деконволюцію. Регуляризований фільтр і обмежений алгоритм відновлення найменших квадратів використовуються для відновлення розмитого та шумного зображення;

- Фільтр Вінера. Деконволюція Вінера може бути корисною, коли функція розкиду точок і рівень шуму відомі або можуть бути передбачені.

- пари розмитих/зашумлених зображень. Цей метод використовує шумове зображення для зменшення розмитості вихідного зображення. Основна перевага цього методу полягає в тому, що він використовує як зашумлені, так і розмиті зображення, у результаті створюючи високоякісне реконструйоване зображення.

- функція щільності руху. За допомогою функції щільності руху в цьому підході досягається зменшення розмитості зображення. Покладення цього методу на оцінки недосконалих просторово інваріантних методів усунення розмиття для ініціалізації є одним із його обмежень.

- обробка викидів. Ця техніка аналізує різні викиди, включаючи насиченість пікселів і негаусівський шум, а потім пропонує метод деконволюції, який включає явний компонент для моделювання викидів. Внутрішні та зовнішні пікселі – це дві основні категорії, які використовуються для класифікації пікселів зображення.

- алгоритм ADSD-AR. Цей метод представляє схему ASDS (Adaptive Sparse Domain Selection), яка вивчає деякі компактні підсловники та адаптивно призначає підсловник як розріджений домен для кожного локального патча.
- гіперспектральний. Щоб декорелювати зображення HS і відокремити інформаційний вміст від шуму, цей підхід спочатку використовує PCA. Більшу частину загальної енергії або інформації зображення HS можна знайти в перших k каналах PCA, тоді як решта $B-k$ каналів PCA (де B – кількість спектральних смуг HSI, а $B-k$) переважно містять шум.
- нейронні мережі. Тип багатопроцесорної комп'ютерної системи, відомий як нейронна мережа, має основні елементи обробки, високий рівень взаємозв'язку та адаптивну взаємодію між елементами. Завдяки своїй паралельній структурі нейронні мережі можуть функціонувати, навіть якщо один з їх елементів виходить з ладу.
- попереднє сліпе усунення розмиття. Це сліпа оцінка ядра та техніка видалення розмиття на основі попереднього градієнта $L0$. Підхід починається з оцінки ядра розмиття шляхом перемикавання між чітким прогнозом зображення за допомогою використання $L0$ перед градієнтним зображенням і багатомасштабною оцінкою ядра. Після оцінки ядра проектується чітке зображення за допомогою стандартного несліпого процесу деконволюції з попередньо встановленим ядром.

Висновки

Незважаючи на те, що методи зменшення розмиття (або відновлення) є давньою проблемою обробки зображень, дослідники та практики все ще цікавляться нею. Застосування алгоритмів відновлення зображень можна знайти в різних проблемах реального світу, від споживчих зображень до астрономії. Процес відновлення зображення може показати ширший клас зворотних проблем, які виникають у різних наукових, медичних, промислових і теоретичних проблемах.

ЗМІСТ

Секція 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТРАНСПОРТНИХ ЗАСОБІВ І СИСТЕМ..... 3

Загрози об'єктам морської критичної інфраструктури України та напрямки досліджень щодо їх нейтралізації <i>Блінцов В.С.; Буруніна Ж.Ю.</i>	3
Аналіз загроз системі інформаційного обміну між постом керування та дроном <i>Гололобов О.В.</i>	5
Оцінка безпеки баз даних NOSQL у системах відстеження та моніторингу транспорту <i>Євдокимов С.О.</i>	8
Перспективи комп'ютерного зору в задачах підводного моніторингу <i>Іванов В.А.</i>	13
Критерії вибору системи виявлення вторгнень для водного транспорту <i>Тотх М.</i>	15
Зважене оцінювання критичності об'єктів морського та річкового транспорту <i>Турти М.В.</i>	22
Критерії прийняття рішень щодо забезпечення кіберстійкості в морській галузі <i>Турти М.Ю.</i>	29

Секція 2. ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ..... 35

Система аналізу методів забезпечення безпеки у бездротових мережах <i>Бердніков В.В.</i>	35
Автоматизована система реєстрації відвідувачів на основі wi-fi підключення <i>Білець О.О.</i>	38
Модель прогнозування кібератак на основі аналізу поведінки <i>Божаткін С.М.; Гусєва-Божаткіна В.А.; Пасюк Б.Б.</i>	42
Дослідження використання прихованих каналів сучасних месенджерів <i>Восков К.П.</i>	46
Аналіз та виявлення мережових атак грубої сили на інтернет-сервіси <i>Десятов А.М.</i>	49

Дослідження функціонування системи захищеного електронного документообігу в підрозділах національної поліції України <i>Дзюбас Д.С.</i>	51
Розробка пакету документів для атестації АС-1 «Гермес-2» на IV категорію обмеження доступу кафедри КТІБ <i>Дибченко М.Є.</i>	59
Дослідження вразливостей протоколу керування безпілотним апаратом спеціального призначення <i>Душенко О.В.</i>	66
Система підтримки прийняття рішень щодо оцінювання ризиків глобальної маршрутизації <i>Єсипенко А.О.</i>	77
Система підтримки прийняття рішень щодо категоризації об'єктів критичної інфраструктури <i>Злочевська О.В.</i>	85
Аналіз системи захисту платформи BLYNK <i>Зобова Е.В.</i>	91
Розробка рекомендацій з покращення захисту інформації в АС-2 та АС-3 класів 4 категорії для об'єкту критичної інфраструктури <i>Мацibuра Д.О.; Мельничук О.Ю.; Шевченко В.В.</i>	94
Розробка системи моніторингу та інформування про відмови в роботі інтернет-сервісів <i>Ніколаєв В.Д.</i>	99
Систем захисту мовної інформації для об'єктів інформаційної діяльності <i>Нужний С.М.</i>	101
Організація захисту бази знань при роботі з хмарним сховищем <i>Письменюк В.А.</i>	108
Система підтримки прийняття рішень щодо вибору засобів захисту від DDoS-атак <i>Садалюк Є.О.</i>	113
Аналіз захищеної системи віддаленого контролю кліматичних параметрів серверних приміщень та можливі шляхи їх модернізації <i>Стефанюк Ю.О.</i>	120
Оцінка та адаптація стійкості інформаційно комунікаційної системи критичного об'єкту <i>Стефанюк Ю.О.</i>	124
Програмне моделювання кольорових фракталів з поліноміальною функцією перетворення та дослідження їх параметричної чутливості <i>Сулiма М.М.; Корчевський Д.О.; Данилець Є.В.; Новак С.М.; Самойленко Д.М.</i>	129
Системи безперебійного живлення комп'ютерних мереж <i>Трибулькевич С.Л.; Трибулькевич В.В.; Трешнюк А.І.</i>	133

Оцінка залежності консолідації інформаційного WEB ресурсу від впливу інформаційної та кібернетичної безпеки *Хавело Д.С.* ..140

Секція 3. ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 147

Система підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022 *Іванюк А.О.*147

Нормативно-правова база кібербезпеки галузі водного транспорту *Хван Ю.В.*..... 156

Секція 4. МОДЕЛЮВАННЯ ОБ'ЄКТІВ І ПРОЦЕСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ..... 163

Оцінювання звукоізоляції акустичних сигналів огорожувальними конструкціями режимних приміщень *Касьянов Ю.І.; Нужний С.М.* 163

Узагальнення спектрів довготривалих мовленнєвих сигналів з використанням можливостей MatLab *Касьянов Ю.І.; Щербаков М.С.* 169

Врахування характеристик слуху в системах цифрового звуку *Лях О.Д.,*..... 174

Секція 5. СТВОРЕННЯ ПІДВОДНО-ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ ЗАХИСТУ МОРСЬКИХ ОБ'ЄКТІВ ТА АКВАТОРІЙ..... 178

Стенд для випробувань установок гребних електроприводів *Большаков Є.Д.*..... 178

Система керування просторовим рухом дистанційно керованого апарату *Верещак О.І.* 180

Розробка альтернативного джерела електроенергії на основі сонячних елементів та вітрогенераторної установки *Малишев Б.Г.* 182

Розробка алгоритмів керування системи рухом мобільної робототехнічної установки *Назаров В.Ю.* 184

Інтелектуальна система керування дистанційно керованим роботом *Новиков А.Ю.* 186

Система керування дистанційно керованим роботом <i>Пашкевич А.В.</i>	188
Розробка системи електроживлення та внутрішнього контролю мобільного робототехнічного комплексу <i>Яровий М.С.</i>	190

**Секція 6. ПІДГОТОВКА КАДРІВ У ГАЛУЗІ ЗНАТЬ
«ІНФОРМАЦІЙНА БЕЗПЕКА»..... 193**

Застосування бібліотеки OpenCV в охоронних системах <i>Курманський В.В.</i>	193
Аналіз існуючих систем для отримання навичок пентестингу для студентів <i>Логачов М.В.; Орел О.С.</i>	195
Аналіз можливостей Cyber ICE Box Platform для проведення CTF змагань <i>Момченко О.В.</i>	198
Аналіз інструментів системи моніторингу Grafana <i>Подгайний О.М.</i>	202
Модернізація навчально-наукової лабораторії "Безпеки інформаційно-комунікаційних систем" <i>Сірівчук А.С.</i>	205
Використання систем моделювання комп'ютерних мереж в умовах дистанційного навчання <i>Трибулькевич С.Л.; Трибулькевич В.В.; Титарчук В.В.</i>	208

Секція 7. ШКОЛА МОЛОДИХ НАУКОВЦІВ 221

Розробка комплексного програмного забезпечення для аналізу, розпізнавання та ідентифікації диктора <i>Байдиков А.О.</i>	221
Алгоритми зменшення розмитості зображень <i>Дацко О.Ю.</i>	227

Наукове видання

**СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ НА ТРАНСПОРТІ**

СПІБТ–2024

**ХІІ Всеукраїнська науково-технічна конференція
з міжнародною участю**

12–13 грудня 2024 року

*Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв*

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(українською мовою)

Відповідальна за випуск В. В. Трибулькевич
