



**НАУКОВО-ТЕХНІЧНІ  
КОНФЕРЕНЦІЇ**

Національний університет кораблебудування  
імені адмірала Макарова

## СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

# МАТЕРІАЛИ

**ХІ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ  
КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ**

**23-24 листопада 2023 р.**



Науково-дослідна частина  
Національного університету  
кораблебудування  
імені адмірала Макарова

54025, м. Миколаїв,  
пр. Героїв України, 9  
Тел.: (0512) 70-91-04  
<http://conference.nuos.edu.ua>  
e-mail: [conference@nuos.edu.ua](mailto:conference@nuos.edu.ua)

Навчально-науковий інститут  
автоматики та електротехніки  
Національного університету  
кораблебудування  
імені адмірала Макарова

54021, м. Миколаїв,  
пр. Центральний, 3  
Тел.: (0512) 47-70-95  
<http://iae.nuos.edu.ua>  
e-mail: [university@nuos.edu.ua](mailto:university@nuos.edu.ua)

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ  
імені адмірала Макарова

**Миколаїв ■ НУК ■ 2023**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ  
імені адмірала Макарова

**СУЧАСНІ ПРОБЛЕМИ  
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ  
НА ТРАНСПОРТІ**

**СПІБТ–2023**

**МАТЕРІАЛИ**

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

23–24 листопада 2023 року

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



МИКОЛАЇВ • НУК • 2023

УДК 004  
У 45

**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. – Миколаїв : НУК, 2023. – 223 с.

У збірнику подано матеріали XI 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, системи Інтернет речей (IoT), 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, 2023

## СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТРАНСПОРТНИХ ЗАСОБІВ І СИСТЕМ

УДК 004.056.53

### РОЗРОБКА СИСТЕМИ ВІДДАЛЕНОГО КЕРУВАННЯ КАМЕРОЮ НА БАЗІ МЕСЕНДЖЕРА «ТЕЛЕГРАМ»

*Автори:* Байдиков А.О., студент; Білець О.О., студентка; Вовк Є.Р., 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 сучасному світі, де безпека та доступ до інформації стають ключовими аспектами повсякденного життя, інноваційні технології в галузі відеоспостереження вирішують важливі завдання забезпечення безпеки та зручності.

Велика частина систем захисту повинна мати можливість сигналізувати про можливий перетин захищеної зони на великі відстані по телефонним лініям або мобільному зв'язку. Така сигналізація надає обмежену кількість інформації про порушника та має можливості хибних спрацювань, що призведе до затрат часу виявлення причин спрацювання сигналізації.

**Метою роботи** є опис системи керування камери відеоспостереження з можливістю управління через телеграм-бота, спрямованої на створення ефективного і зручного інструменту для нагляду та безпеки.

**Основна частина.** Проект має на меті забезпечити користувачів можливістю віддалено отримувати відеодані, контролювати режими та виконувати дії через інтуїтивний інтерфейс телеграм-бота, сприяючи простоті використання та забезпечуючи надійний засіб забезпечення безпеки в різних контекстах, таких як домашнє середовище, офісні приміщення або комерційні об'єкти.

Завдяки поєднанню передових технологій зі зручністю та доступністю, наш проект ставить за мету надати користувачам потужний інструмент для віддаленого контролю та управління відеоспостереженням. Використання телеграм-бота як інтерфейсу дозволяє отримувати

дані та керувати системою з будь-якого місця, забезпечуючи високий рівень зручності та ефективності.

Цей проєкт стає відповіддю на сучасні виклики в галузі безпеки, забезпечуючи віддалений доступ до важливої інформації та можливість реагування в реальному часі. Поєднуючи технологічні досягнення з простотою у використанні, ми прагнемо створити інноваційне рішення, яке відповідає потребам у безпеці та зручності в сучасному світі.

Проєкт із створення камери з віддаленим доступом та управлінням через телеграм-бота є ефективним і зручним рішенням для відеоспостереження. Його основна перевага полягає в тому, що користувач може отримувати зображення та відео, а також керувати камерою з будь-якого місця через телеграм-бота, що робить систему легко доступною.

Використання телеграм-бота як інтерфейсу дозволяє користувачам миттєво отримувати інформацію та взаємодіяти з системою в реальному часі, навіть якщо вони знаходяться віддалено від місця розташування камери. Це робить систему зручною для використання в різних сценаріях, таких як домашнє використання, офіси чи інші місця.

Основою даної системи є модуль ESP32-CAM який включає в себе роботу з камерою та вбудований модуль WiFi, що значно пришвидшило розробку системи. Для написання програми яка буде забезпечувати контроль над роботою камери та обробляти і виконувати команди, надіслані телеграм ботом ми вирішили використати мову програмування C++. Оскільки вона є достатньо швидкою та низькорівневою, щоб працювати з апаратною частиною камери.

В якості середовища розробки ми обрали Arduino IDE, оскільки воно надає широкий спектр бібліотек, які необхідні для коректної роботи програми та має широкий функціонал. Також підтримується великою спільнотою розробників, що в подальшому надало змогу використовувати готові рішення при реалізації системи.

Модуль роботи з телеграм-ботом було взятий код з сайту GitHub [1] за авторством користувача “amarnathkr” та підлаштовано для потреб системи.

Для написання функціонала бота була використана мова програмування Python. Обране середовище розробки – програма PyCharm, а створення самго бота використали вбудовані можливості телеграма, а саме телеграм бота BotFather.

Недоліками проєкту на даній стадії можна вважати погану якість фотографій, які робить камера, відсутність можливості запису відео, та невеликий об'єм внутрішньої пам'яті камери.

В перспективі проєкт може бути розширений для включення додаткових функцій, таких як розпізнавання обличчя або виявлення руху, або ж можливість додання автономного живлення, що може дозволити розміщення камери в різноманітних місцях. Також слід звернути увагу на аспекти безпеки, забезпечуючи шифрування даних та надійний механізм автентифікації для запобігання несанкціонованому доступу.

### **Висновки.**

Загалом, цей проєкт є привабливим для різних груп користувачів і може забезпечити ефективний та зручний засіб відеоспостереження з віддаленим доступом та управлінням.

### **Список літератури:**

1. FastBot: github.com сайт: URL: [https://github.com/amarnathkr/ESP32-Cam-Telegram/blob/main/Esp32\\_Cam\\_Telegram.ino](https://github.com/amarnathkr/ESP32-Cam-Telegram/blob/main/Esp32_Cam_Telegram.ino)

## **СУЧАСНІ ЗАВДАННЯ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ СТІЙКОСТІ НА ВОДНОМУ ТРАНСПОРТІ**

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

Згідно Концепції забезпечення національної системи стійкості [1] національна система стійкості – це комплекс цілеспрямованих дій, методів та механізмів взаємодії органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, інститутів громадянського суспільства, які гарантують збереження безпеки і безперервності функціонування основних сфер життєдіяльності суспільства і держави до, під час і після настання кризової ситуації.

Україні приділяє значну увагу комплексу завдань щодо успішної реалізації Концепції забезпечення національної системи стійкості в

рамках відповідного «Плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року» [2]. У зв'язку з цим ключовою місією Національного університету кораблебудування імені адмірала Макарова має бути розробка та реалізація (в межах своєї компетенції) теоретичного підґрунтя системи стійкості воднотранспортної складової держави, а саме – забезпечення безпеки об'єктів морської критичної інфраструктури (МКІ).

До таких об'єктів відносяться:

- водний транспорт (Т) – морський, річковий, озерний;
- водні транспортні шляхи (Ш) – морські транспортні коридори, якірні стоянки, річкові фарватери та канали, судноплавні маршрути на водосховищах та озерах;
- морські та річкові порти і перевантажувальні комплекси (П);
- морські стаціонарні платформи, підводні трубопроводи та інші стаціонарні споруди, які розташовані на морському шельфі (С);
- суднобудівні та судноремонтні заводи (З);
- військово-морські бази (Б).

Впроваджувана складова національної системи стійкості має передбачати забезпечення функціонування таких базових елементів:

1) гарантована дієвість та спроможність до повноцінного функціонування системи державних органів, у сфері відповідальності яких знаходяться об'єкти МКІ;

2) безпека та захищеність власне об'єктів МКІ, зокрема:

стійке постачання продовольства, водопостачання, енергопостачання, постачання теплової енергії;

стійке функціонування транспортних систем;

кібербезпека;

захищеність та безперебійне функціонування інформаційних та комунікаційних послуг;

забезпечення оборони та правопорядку;

3) спроможність єдиної державної системи цивільного захисту до дій в умовах загрози чи виникнення надзвичайних ситуацій на об'єктах МКІ;

4) здатність ефективно реагувати на неконтрольоване масове переміщення людей;

5) суспільна стійкість, зокрема, до інформаційних впливів;

6) фінансово-економічна стійкість, зокрема, безперервність основних бізнес-процесів.

Важливою складовою реалізації місії університету є ідентифікація загроз об'єктам МКІ, виявлення вразливостей, оцінювання та пріоритизація загроз безпеці таким об'єктам, зокрема:

проведення фундаментальних і прикладних наукових досліджень за всіма складовими водогосподарського комплексу держави з подальшим включенням результатів досліджень до програм підготовки та підвищення кваліфікації державних службовців, а також до програм створення нових технічних засобів захисту таких об'єктів;

забезпечення освітньо-науково-методичного супроводу фахівців, відповідальних за забезпечення кіберзахисту об'єктів кібербезпеки та кіберзахисту об'єктів МКІ;

оновлення професійних стандартів для працівників, що забезпечують функціонування національної системи кібербезпеки з урахуванням вимог Агентства ЄС з мережевої та інформаційної безпеки (ENISA);

оновлення освітніх програм за напрямом “Кібербезпека”, розроблення і запровадження освітніх програм за напрямом “Безпека і захист критичної інфраструктури” з урахуванням нових (оновлених) професійних стандартів;

розроблення та впровадження разом з Миколаївським управлінням ДССЗІ програм підвищення кваліфікації для службовців, працівників державних органів, що входять до складу сектору безпеки та оборони, посадових осіб органів управління та органів місцевого самоврядування з питань кібербезпеки та захисту критичної інфраструктури.

Очевидно, що практичну реалізацію наведених завдань доцільно організувати на принципах проектного підходу, основним принципом побудови якого є концепція проекту – створення нового інноваційного продукту.

Розглянемо моделі управління проектами фізичної та інформаційної безпеки об'єктів МКІ з єдиних позицій системного підходу, отримані науковцями наукової школи НУК «Підводна техніка» на протязі 2010-2023 рр. [3-5].

У загальному випадку, множина об'єктів МКІ, наведена вище, може бути розширена за рахунок:

- розгляду окремих видів вказаних вище основних об'єктів МКІ (наприклад, для стаціонарних споруд (С), які розташовані на морському шельфі, таке розширення може включати морські стаціонарні платформи (С1), підводні трубопроводи (С2) тощо;

- уведення у систему безпеки й інших об'єктів особливої важливості (причальні споруди для спеціальних вантажів  $P_{\text{пс}}$ , підводні кабелі зв'язку  $P_{\text{к}}$ , плавучі судноремонтні майстерні  $P_{\text{м}}$ , плавдоки  $P_{\text{д}}$  тощо).

Відповідно, проекти безпеки цих видів МКІ у сукупності можна представити у вигляді програми проєктів  $PP_{\text{МКІ}}$  у складі  $L$  базових проєктів (індекси відповідають наведеним вище аббревіатурам):

$$PP_{\text{МКІ}} = \{P_{\text{т}}; P_{\text{ш}}; P_{\text{п}}; P_{\text{с}}; P_{\text{з}}; P_{\text{б}}; P_{\text{пс}}; P_{\text{к}}; P_{\text{м}}; P_{\text{д}}; \dots P_{\text{і}}; \dots P_{\text{л}}\}. \quad (1)$$

Розробку системи захисту об'єктів МКІ доцільно проводити з залученням відомих принципів системного підходу [6], який передбачає комплексне врахування особливостей функціонування матеріальної, енергетичної та інформаційної складових цих об'єктів, а також урахування людського фактору як складової їх ефективної експлуатації.

Відносно захисту об'єктів МКІ пропонується наступна множина основних підпроєктів  $UP_{\text{МКІ}}$  для кожного з базових проєктів програми (1), управління виконанням якими реалізується на основі системного підходу до класифікації видів безпеки:

$$UP_{\text{МКІ}} = \{UP_{\text{о}}; UP_{\text{е}}; UP_{\text{і}}; UP_{\text{к}}\}, \quad (2)$$

де:  $UP_{\text{о}}$  – підпроєкт «Фізична безпека», який включає заходи щодо унеможливлення несанкціонованого фізичного доступу на об'єкти МКІ та до їх інформаційних ресурсів;

$UP_{\text{е}}$  – підпроєкт «Енергетична безпека», який включає заходи щодо гарантованого енергозабезпечення об'єктів МКІ у мирний час та в особливий період;

$UP_{\text{і}}$  – підпроєкт «Інформаційна безпека», який включає заходи щодо захисту систем комунікацій та документообігу на об'єктах МКІ;

$UP_K$  – підпроект «Кадрова безпека», який включає заходи щодо управління розробкою та реалізацією кадрової політики на об'єктах МКІ.

В окремих випадках вказана множина може бути розширена за рахунок додаткових підпроектів спеціального спрямування – фінансової безпеки  $UP_\Phi$ , безпеки закупівель  $UP_{Ц}$ , нормативно-правового забезпечення проєктів  $UP_{Ю}$  тощо.

Тоді позначивши через  $M$  загальну кількість основних підпроектів, вираз (2) запишемо у вигляді:

$$UP_{MKI} = \{UP_O; UP_E; UP_I; UP_K; UP_\Phi; UP_{Ц}; UP_{Ю}; \dots UP_m; \dots UP_M\}. \quad (3)$$

Пропонується також для кожного з вказаних основних підпроектів увести множину  $J_{MKI}$  типових процесів, які мають охоплювати повний комплекс заходів зі створення системи захисту та управління виконанням якими забезпечить захист об'єктів МКІ.

Виходячи з принципів системного підходу до процесу створення системи захисту об'єктів МКІ, така множина процесів має охоплювати

$$J_{MKI} = \{J_X; J_B; J_{T3}; J_{Pr}\}, \quad (4)$$

де:  $J_X$  – процеси з визначення переліку усіх значущих характеристик об'єктів МКІ, які підлягають захисту (матеріальних цінностей, енергетичного, інформаційного та кадрового забезпечення об'єктів МКІ);

$J_B$  – процеси з визначення тих характеристик імовірних порушників, від яких слід будувати систему захисту (для підпроекту  $UP_O$  – терористів, несанкціонованих відвідувачів та їх технічних засобів; для підпроекту  $UP_E$  – характеристик загроз системі енергетичного забезпечення об'єктам МКІ; для підпроекту  $UP_I$  – хакерів та несанкціонованих користувачів; для підпроекту  $UP_K$  – характеристик персоналу об'єктів МКІ, які утворюють загрози фізичній, енергетичній та інформаційній складовим їх діяльності, а також породжують ризики, пов'язані з інтелектуальним потенціалом персоналу та трудовими відносинами);

$J_{T3}$  – процеси з визначення технологій захисту, які необхідно застосувати для унеможливлення протиправних дій порушника (інформаційних, технічних та силових впливів);

$J_{\text{Пр}}$  – процеси з організації практичної реалізації проєктів захисту об'єктів МКІ (проєктування, будівництво, введення в експлуатацію та супровід експлуатації).

Очевидно, що запропонована множина  $J_{\text{МКІ}}$  типових процесів також ґрунтується на системному підході до створення

системи захисту МКІ, оскільки охоплює роботи по встановленню властивостей об'єктів захисту та характеру загроз,

а також роботи по вибору необхідних технологій захисту і практик їх практичного створення.

Позначивши через  $N$  загальну кількість типових процесів, запишемо їх множину у вигляді:

$$J_{\text{МКІ}} = \{J_X; J_B; J_{T_3}; J_{\text{Пр}}; J_H; J_L; \dots J_n; \dots J_N\}. \quad (5)$$

Залежності (1), (3) і (5) утворюють генеральну множину  $Q_{\text{МКІ}}$  проєктів, підпроєктів і процесів програми проєктів захисту об'єктів МКІ, кожний елемент якої  $q_{l,m,n}$   $Q_{\text{МКІ}}$  являє собою окрему  $n$ -ту роботу, управління процесами виконанням якої забезпечить захист  $l$ -го об'єкта МКІ за  $m$ -ю ознакою виду безпеки:

$$Q_{\text{МКІ}} = \{PP_{\text{МКІ}}; UP_{\text{МКІ}}; J_{\text{МКІ}}\} \quad (6)$$

Отримана генеральна множина  $Q_{\text{МКІ}}$  являє собою класифікацію базових проєктів, основних підпроєктів і типових процесів програми проєктів захисту об'єктів МКІ.

З математичної точки зору множина  $Q_{\text{МКІ}}$  є тривимірною матрицею (тривимірним масивом завдань для менеджера проєкту безпеки об'єкта МКІ), первинне заповнення якої створює шаблони для однотипних проєктів.

Така матриця дає змогу ефективно працювати з базами даних артефактних проєктів, використовуючи їх при плануванні проєктів захисту об'єктів МКІ та доповнюючи їх новими проєктами і процесами.

### **Висновки та пропозиції.**

1. Прийнятий Урядом України «План заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року» вказує на необхідність розробки заходів щодо подальшого розвитку навчального процесу і наукових досліджень за актуальним для України напрямком “Безпека і захист критичної інфраструктури України».

У рамках цього напрямку пропонується започаткувати в НУК нову спеціалізацію з метою підготовки фахівців (бакалаврів та/чи магістрів) та підвищення кваліфікації державних службовців, працівників державних органів, що входять до складу сектору безпеки та оборони, посадових осіб органів управління та органів місцевого самоврядування.

2. Вбачається доцільним започаткування нового напрямку прикладних наукових досліджень НУК за напрямком “Безпека і захист критичної інфраструктури України», результати досліджень за яким використовувати при підготовці PhD-аспірантів за акредитованими в НУК спеціальностями третього (освітньо-наукового) рівня.

Теоретичним підґрунтям таких досліджень можуть слугувати результати досліджень наукових шкіл НУК «Підводна техніка» (науковий керівник – д.т.н., професор Блінцов В.С.), «Механізми управління соціально-економічним розвитком Причорноморського регіону» (науковий керівник – д.е.н., професор Іртищева І.О.) та «Управління проектами та програмами» (науковий керівник – д.т.н., професор Харитонов Ю.М.), отримані на протязі 2010-2023 рр.

### **Список літератури:**

1. Концепція забезпечення національної системи стійкості. Затверджено Указом Президента України від 27 вересня 2021 року № 479/2021.

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

3. Управління успішними проектами створення складної техніки : Монографія / Г. В. Бабкін, В. С. Блінцов, Є. А. Дружинін, С. Г. Кійко, Н. Р. Книрик, К. В. Кошкін, Д. М. Крицький, С. С. Рижков, С. О. Слободян, Т. А. Фаріонова. – Миколаїв : Видавництво Торубари В. В., 2017. – 336 с.

4. V. Blintsov, G. Babkin. Theoretical Basis of Design and Production of Marine Robotics. Collective monograph “Prospects and priorities of re-

search in science and technology” ∴ Vol. 1. Riga, Latvia : “Baltija Publishing”, 2020. Pages 25-43.

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.

6. Проектування засобів морської робототехніки на основі системного підходу : монографія : у 3 ч. / за ред. д-ра техн. наук, проф. В. С. Блінцова. – Миколаїв : Іліон, 2023. Ч. 1 : Самохідні прив’язні підводні системи / В. С. Блінцов, О. П. Клочков, В. А. Надточій, А. В. Надточій. – 2023. – 164 с.

**УДК 004.056**

## **OSINT-МЕТОДОЛОГІЯ РОЗВІДКИ У КІБЕРПРОСТОРІ**

***Автори:** Божаткін С.М., ст. викладач; Пасюк Б.Б., аспірант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

На сучасному етапі розвитку інформаційного суспільства на тлі інноваційного розвитку інформаційних технологій кібербезпеки набуває особливого значення у глобалізованому світі. Кіберпростір визнано одним з можливих театрів військових дій [1], тому безпека кіберпростору розглядається як запорука національної безпеки. В різних країнах створюється новий рід військ – кібервійська [2], завданнями котрих [3] є забезпечення захисту об’єктів критичної інформаційної інфраструктури власної країни від кібератак і виведення з ладу аналогічних об’єктів країн-супротивників, проведення превентивних наступальних операцій у кіберпросторі тощо. Підготовчим етапом до такої діяльності є розвідка, яка дозволяє визначити цілі атак, особливості їх функціонування і захисту, конкретизувати ключові задачі і способи проведення операцій.

У сучасному кіберпросторі спостерігається тенденція до зростання інтенсивності міждержавного протидержавного, розвідувально-підбивної діяльності, конкурентної кіберрозвідки [4] посилення державного контролю за сегментами мережі Інтернет, що мають значення для забезпечення національної безпеки, розширення кола соціальних груп і окремих осіб, які ви-

користовують кіберпростір для власних потреб, починаючи з простого обміну інформацією, під час якого може бути випадково розголошена конфіденційна інформація, і закінчуючи цілеспрямованими злочинними діями, такими як організація продажу зброї і передавання розвідданих.

Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму є однією з цілей, визначених Планом реалізації Стратегії кібербезпеки України [5]. При цьому набуватиме поширення розроблення інструментарію, що передбачає накопичення великих масивів інформації щодо поведінки людини, соціальних груп та використання сучасних досягнень у сфері штучного інтелекту [6].

**Метою даної роботи** є визначення особливостей OSINT-методології проведення розвідки у сучасному кіберпросторі.

Для досягнення поставленої мети необхідно визначити місце розвідки у алгоритмі проведення атак, поширені інструменти проведення розвідки і особливості їх використання, особливості OSINT-методології.

Для підвищення рівня кібербезпеки сучасних інформаційно-комунікаційних систем (ІКС), що використовуються, у першу чергу, в сферах критичної інфраструктури (КІ) держави, необхідно розуміти всі кроки розвитку кібератаки з точки зору її виявлення і захисту. Це дозволяє розвідці діяти превентивно, попередньо моделюючи можливість кібератаку на такі об'єкти. Атака може бути описана за моделлю Cyber Kill Chain від Lockheed Martin (рис.1), яка містить сім стадій.

Спершу порушник (атакуюча сторона) здійснює зовнішню розвідку – шукає уразливу жертву для атаки зі списку об'єктів КІ. На даному етапі виконується збирання даних про вразливості за межами мережі організації (невдоволені працівники, що згодні бути колаборантами – insider threat; цифрові ресурси, доступ до яких неправильно сконфігуровано з точки зору кібербезпеки; фішинг), що потенційно може дозволити атакуючій стороні обрати методи експлуатації, відповідно для кожної програмної або апаратної вразливості, визначеної для конкретної цілі. На даній стадії зазвичай використовуються два найбільш дієві та поширені методи: фішинг за допомогою електронних листів і соціальна інженерія. Після використання цих методів порушник з вірогідністю 80% знаходить точку входу до мережі. Це може бути зроблено за допомогою крадіжки паролів або зараження комп'ютера співробітника шкідливим ПЗ в мережі цільового об'єкта КІ.

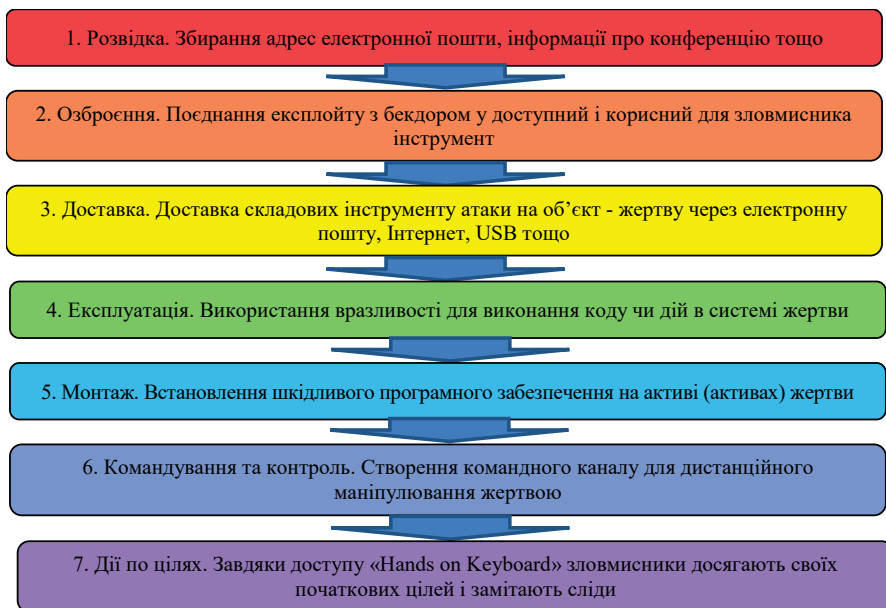


Рисунок 1 – Стадії кібератаки згідно моделі Cyber Kill Chain

На наступному кроці (Озброєння, англ. *Weaponization*, сканування) атакуюча сторона досліджує слабкі місця інформаційно-комунікаційної системи, що були виявлені на етапі розвідки. Сканування включає використання різних програмних інструментів для пошуку критичних міiskonфігурацій, які можна використовувати для організації майбутньої атаки. Серед доступних інструментів сканування можуть використовуватися:

- NMap – мережева утиліта з відкритим початковим кодом для платформ Windows, Linux і macOS, що використовує звичайні IP-пакети (виявляє пристрої, підключені до цільової мережі, їх відкриті порти та банери сервісів за ними; ідентифікуються операційні системи, використовувані хостами та ін.);
- Metasploit – фреймворк з колекцією експлойтів для злому різних програмних сервісів на базі ОС Linux, що надає можливість відразу експлуатувати типову вразливість цільової системи;

- John the Ripper – утиліта для злому паролів в ОС Linux і Windows (в тому числі – захешованих), яка використовується для здійснення словникових атак (dictionary attack). Застосовується для знаходження реальних паролів користувачів із зашифрованих баз даних як персональних комп’ютерів, так і веб-систем і застосунків;

- THC Hydra – утиліта злому паролів в ОС Windows, Linux і macOS. Використовує словникові атаки і повний перебір для атаки на веб-сторінки авторизації;

- Wireshark – утиліта сканування трафіку в мережі – збирає пакети даних в цільовій мережі, відображає їх в детальному форматі, зручному для читання, і дозволяє фахівцям ретельно аналізувати мережевий трафік до рівня перевірки окремих пакетів;

- Aircrack-NG – набір програмних засобів, що використовується для злому паролів безпроводних мереж. Він включає такі атаки, як FMS (отримання хешів RC4), KoreK (атаки на точки доступу з WEP-шифруванням каналу) і PTW (злам захищених мереж Wi-Fi з шифруванням WEP і WPA);

- Nikto – сканер вразливостей веб-сайтів на основі Linux. Утиліта сканує веб-сервери на наявність найбільш вживаних експлуатованих уразливостей (майже 6800 вразливостей), а також сканує версії веб-серверів, в яких не виправлені вразливості на більш ніж 250 платформах. Утиліта також перевіряє наявність помилок в конфігураціях файлів на веб-серверах (бекапи файлів, наприклад);

- Cain and Abel – утиліта для зламу паролів, яка ефективна проти ОС Microsoft. Зламає паролі, використовуючи атаку за словниками (dictionary attack). Дозволяє записувати розмови, які йдуть через VoIP, розшифровувати паролі, розкривати кешовані паролі і аналізувати протоколи маршрутизації внутрішньої мережі.

Третій крок атаки (доставка, експлуатація, встановлення, командування та контроль) має на меті створення технічних умов проведення атаки. Наприклад, зловмисником здійснюється доступ до цільової системи і підвищення привілеїв до Адміністратора (Windows OS) або root (Linux OS). Основними завданнями атакуючої сторони є збереження доступу до зламаной системи і переміщення по мережі жертви, залишаючись при цьому непоміченим. Для цього порушник має попередньо підвищити привілеї зламаного акаунту, що може бути викона-

но такими способами: вертикальним (атакуюча сторона може змінити зламаний аканут на привілейований) і горизонтальним (атакуюча сторона використовує той же обліковий запис, але підвищує свої привілеї шляхом хибних конфігурацій безпеки певних сервісів або файлів всередині системи).

На четвертому кроці зловмисник реалізує проникнення і витік даних з цільової системи – на даному етапі починається основна атака: атакуюча сторона може безперешкодно пересуватися по мережі жертви, маючи доступ до усіх її систем, хостів і даних (англ. sensitive data), що підлягають захисту. На даному етапі порушники викрадають величезні масиви даних, які в результаті можуть бути або продані третім особам чи організаціям, або опубліковані з метою компрометації репутації жертви.

На п'ятому кроці зловмисник створює умови для майбутніх злочинних дій і проведення багатоетапних атак. Наприклад, для того щоб сховати свою присутність, зловмисники встановлюють руткіти до систем своїх жертв, що надає їм змогу отримати доступ до комп'ютерів і систем жертви у будь-який час. Таким чином, атакуюча сторона виграє час для себе, щоб підготуватися до більш небезпечної атаки, ніж просто витік даних.

Шостий крок атаки (штурм) є найнебезпечнішою стадією будь-якої кібератаки. На даному етапі атакуюча сторона (вже попередньо маючи привілейований доступ до потрібних хостів та сервісів) завдає ушкоджень апаратним одиницям жертви. Можливе відключення назавжди комп'ютерного або серверного обладнання, можлива зміна роботи дороговартісного устаткування. За більш гірших обставин, атакуюча сторона фокусується на знищенні апаратного забезпечення, керованого скомпрометованими системами. Прикладом може бути атака Stuxnet на іранську атомну станцію. Це була перша зареєстрована цифрова зброя, яку було використано для руйнування фізичних ресурсів.

Заключним сьомим кроком атаки є обфускація (маскування, «замітання слідів»). Метою даного етапу є приховування слідів свого перебування в мережі жертви. Для цього використовуються різні методи з метою заплутати, утримати або відвернути процес розслідування (фо-

рензики, англ. *forensics*), який слідує за кібератакою: стирання або підміна логів, знищення операційних систем, шифрування файлів тощо.

Враховуючи вищесказане, цілком зрозуміло, що перший етап побудови будь якої серйозної атаки – це розвідка на основі відкритих джерел (англ. *open source intelligence*, OSINT), під час якої отримуються дані для реалізації наступних стадій атаки.

OSINT – це технологія добування будь якої військової, політичної, економічної та іншої інформації з відкритих джерел. Такі дані можуть бути в тому числі й засекреченими, але через програмні хибні конфігурації – за певних обставин, зловмисник може отримати до них доступ. Для вдалої OSINT-розвідки необхідно мати спеціалізоване програмне забезпечення, яке, в ідеалі, може збирати інформацію не тільки з відкритих, а й із закритих джерел (наприклад, з опіон-форумів DarkNet) [7-12].

За допомогою сучасних технологій, штучного інтелекту можна досить швидко дізнатися інформацію про те, що, як і де відбувається. Даними для збору подібної інформації можуть бути Google-карти, фотографії, які є в мережі, відео чи пости в соціальних мережах, закритих пабліках або ж чатах, усе, що пов'язано з місцевістю (геолокація), метадані файлів (фото- та відеоматеріалів) [7].

Передусім OSINT-розвідка сьогодні дуже важлива через те, що за її допомогою можна розкривати злочини. Також можна прослідкувати, де перебуває тяжка військова техніка ворога [7, 11, 12]

Однією з особливостей OSINT-розвідки є те, що її можуть здійснювати не тільки співробітники певних спецслужб, а й ентузіасти, які мають достатні навички розвідники у галузі інформаційних технологій і здатні знаходити в мережі Інтернет корисні матеріали, зіставляти інформацію, визначати і використовувати прихований вміст файлів. Станом на сьогодні, враховуючи ситуацію з повномасштабним вторгненням на територію України, OSINT-розвідники тісно співпрацюють з розвідкою та Службою Безпеки України.

### **Висновки**

Таким чином, в даній роботі визначено місце розвідки у алгоритмі проведення атак за моделлю Cyber Kill Chain від Lockheed Martin, визначені поширені інструменти проведення розвідки і особливості їх використання на різних кроках моделі, особливості OSINT-методології проведення розвідки у сучасному кіберпросторі.

### Список літератури:

1. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука безпечного розвитку країни. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n7>
2. Кібервійська. URL: <https://www.dw.com/uk/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B2%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0/t-45117632>
3. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. – Київ: Видавничий дім «Кондор», 2019. – 272 с. . URL: <http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf>
4. Додонов А. Г. Компьютерная конкурентная разведка: [монография] / А. Г. Додонов, Д. В. Ландэ, В. В. Прищепа, В. Г. Путятин ; НАН Украины, Институт проблем регистрации информации. – Киев : ТОВ "Інжиніринг", 2021. – 354 с. URL: <http://dwl.kiev.ua/art/kkr/kkr.pdf>
5. План реалізації Стратегії кібербезпеки України. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>
6. Турти М., Єрмакова О. Прогнозування інформаційної безпеки в інформаційних системах та технологіях: 8-а Міжнародна науково-технічна конференція IST-2019: ХНУРЕ, Харків – Коблево, 2019. – С.260-265.
7. ESET. Як здійснюються атаки соціальної інженерії [URL]: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/>
8. Активна розвідка OSINT [URL]: <https://gridinsoft.ua/osint>
9. Дослідження на основі відкритих джерел або OSINT: де використовується і в чому небезпека. [URL]: <https://eset.ua/ua/blog/view/117/issledovaniye-na-osnove-otkrytykh-istochnikov-ili-osint-gde-ispolzuyetsya-i-v-chem-opasnost>
10. Пасивна розвідка OSINT. [URL]: <https://gridinsoft.ua/osint>
11. Уфімцева О.С. Використання OSINT в умовах збройної агресії РФ проти України [URL]: <http://dspace.onua.edu.ua/bitstream/handle/11300/19841/%D0%A3%D1%84%D1%96%D0%BC%D1%86%D0%B5%D0%B2%D0%B0%20%D0%9E%D0%BB%D0%B5%D0%BD%D0%B0%20%D0%A1%D0%B5%D1%80%D0%B3%D1%96%D1%97%D0%B2%D0%BD%D0%B0.pdf?sequence=1&isAllowed=y>

12. Як працює OSINT-розвідка. Від бізнес-аналізу до оборони України. [URL]: <https://www.issp.training/post/yak-pratsyuye-osint-rozvidka-vid-biznes-analizu-do-oborony-ukrayiny>

**УДК 004.056.53**

## **КЛАСИФІКАЦІЯ СИСТЕМ ІНТЕРНЕТ РЕЧЕЙ**

***Автор:** Бондар О.О., магістрант, 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.** Інтернет речей (IoT) описує пристрої з датчиками, здатністю обробки, програмним забезпеченням та іншими технологіями, які підключаються та обмінюються даними з іншими пристроями та системами через Інтернет або інші комунікаційні мережі. Інтернет речей охоплює електроніку, комунікацію та інформатику. «Інтернет речей» вважався неправильним, оскільки пристрої не потрібно підключати до публічного Інтернету, їх потрібно лише підключити до мережі та мати індивідуальну адресацію[1].

Існує низка занепокоєнь щодо ризиків, пов'язаних із розвитком технологій і продуктів IoT, особливо в сферах конфіденційності та безпеки, і, отже, індустрія та уряд вжили заходів для вирішення цих проблем, включаючи розробку міжнародних і місцевих стандартів, керівних принципів та нормативно-правової бази [2].

**Метою роботи** провести загальний аналіз вразливостей систем Інтернет речей та основні засоби захисту.

**Основна частина.** Аналіз каналів витоку інформації в системах Інтернету речей (IoT) є критичним завданням для забезпечення безпеки та конфіденційності даних, які обробляються та передаються в таких системах. Це особливо важливо, оскільки IoT зазвичай збирає і обробляє великі обсяги особистої та конфіденційної інформації.

Основні канали витоку інформації в системах IoT включають:

1. Несанкціонований доступ до пристроїв IoT. Вітік інформації через несанкціонований доступ до пристроїв IoT відбувається, коли злоумисники отримують фізичний або дистанційний доступ до пристроїв IoT без дозволу або авторизації. Це може мати серйозні наслідки для безпеки та конфіденційності даних, які обробляються цими пристроями.

2. Комунікація по мережі. Витік інформації через комунікацію по мережі в системах IoT відбувається, коли зловмисники отримують доступ до даних, які передаються між пристроями IoT та іншими частинами мережі. Це може стати наслідком низки потенційних атак та загроз, і вимагає ретельного аналізу та заходів для забезпечення безпеки комунікаційного процесу.

3. Вразливості пристроїв. Витік інформації через вразливості пристроїв в системах IoT відбувається, коли зловмисники використовують програмні або апаратні слабкості у пристроях IoT для отримання доступу до даних або виконання несанкціонованих операцій. Ці вразливості можуть бути використані для витоку чутливої інформації або для атак на систему в цілому.

4. Виток інформації через додатки та сервіси. Витік інформації через додатки та сервіси в системах Інтернету речей (IoT) відбувається, коли зловмисники отримують доступ до даних, які зберігаються або передаються через додатки або сервіси, призначені для управління та моніторингу пристроїв IoT. Це може стати наслідком низки можливих загроз та атак, і вимагає ретельного аналізу та заходів для забезпечення безпеки цих додатків і сервісів.

5. Фізичний доступ до даних. Витік інформації через фізичний доступ до даних в системах Інтернету речей (IoT) відбувається, коли зловмисники фізично отримують доступ до фізичних пристроїв або інфраструктури системи IoT і копіюють, викрадають, змінюють або завдають шкоду даній апаратурі чи пристрої. Це може призвести до витоку чутливої інформації, порушення безпеки системи, а також може стати загрозою для фізичної безпеки інфраструктури IoT.

Для захисту від витоку інформації через фізичний доступ до даних в системах IoT, слід вживати наступні заходи:

1) Фізична безпека: Забезпечте надійну фізичну безпеку для пристроїв та інфраструктури IoT, включаючи встановлення відповідних систем контролю доступу.

2) Шифрування даних: Використовуйте шифрування для захисту даних, які зберігаються на пристроях IoT.

3) Фізичний моніторинг: Моніторіть фізичний доступ до пристроїв і виявляйте будь-які незвичайні активності або спроби несанкціонованого доступу.

4) Аудит безпеки: Проводьте аудит безпеки обладнання та інфраструктури для виявлення вразливостей.

5) Освіта персоналу: Навчайте персонал та користувачів про безпеку та методи захисту від фізичного доступу до даних.

### **Висновки:**

Системи Інтернет речей все більше використовуються в повсякденному житті, при цьому наявність незахищеного каналу передачі даних (бездротові мережі, обов'язковий зв'язок з Інтернетом) надає більше вразливостей ніж іншим системам передачі даних. Аналіз витоків інформації дає комплексне розуміння відносно побудови системи безпеки включаючи в себе програмні, апаратні та організаційні засоби захисту.

### **Список літератури:**

1. Lea, P. (2018) Internet of Things for Architects. 1st edn. PacktPublishing. Available at: <https://www.perlego.com/book/578809/internet-of-things-for-architects-pdf> (дата звернення: 01.11.2023).

2. Жураковський Б. Ю., Зенів І. О. Технології інтернету речей: навчальний посібник. Київ: КПП ім. Ігоря Сікорського, 2021. 271 с.

**УДК 004.056**

## **РОЛЬ STF-ЗМАГАНЬ В КІБЕРБЕЗПЕЦІ**

***Автор:** Іванов.В.І., магістрант, 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 стрімкій сфері кібербезпеки, де загрози розвиваються з безпрецедентною швидкістю, оволодіння мистецтвом захисту стало більш важливим, ніж будь-коли. Змагання STF – це захоплюючі виклики кібербезпеки, які відображають складність реальних сценаріїв безпеки. Похідні від традиційної гри на відкритому повітрі, де команди змагаються за захоплення прапора суперника, STF у сфері кібербе-

зпеки є цифровими полями битви, де учасники перевіряють свої навички, інтелект і здатність вирішувати проблеми.

У CTF перед учасниками постає низка цікавих і різноманітних викликів, які охоплюють широкий спектр сфер кібербезпеки. Ці виклики ретельно розроблені, щоб імітувати реальні вразливості, загрози та вектори атак, з якими організації стикаються в цифровому середовищі. Кульмінацією кожного завдання є виявлення та вилучення «прапора» – унікального коду або маркера, який підтверджує успішне завершення.

Мета роботи: дослідження ролі CTF-змагань в здобутті необхідних навичок в сфері інформаційної безпеки

Основна частина: CTF (Capture the flag або Захоплення прапора) – це командні змагання у сфері комп'ютерної (інформаційної) безпеки, в яких «прапори» таємно ховаються в навмисно вразливих програмах або веб-сайтах. «Прапори» – це бітові дані, які повідомляють системи, що ви виконали поставлені завдання. Зазвичай прапор є рядком випадкових даних або тексту в певному форматі [1].

Завдання Capture the Flag (CTF) у сфері кібербезпеки часто бувають різних типів, кожен з яких призначений для перевірки різних наборів навичок злому/ухилення від безпеки. Еволюція CTF була динамічною подорожжю від простих текстових викликів до складних багатограних подій, які перевіряють широкий спектр навичок кібербезпеки.

Для учасників змагання CTF – це потужний спосіб привернути увагу потенційних роботодавців. На відміну від традиційного процесу працевлаштування, коли резюме відбирають у відділі кадрів, перш ніж передати їх відповідному відділу, на змаганнях CTF учасники часто спілкуються безпосередньо з майбутнім керівником, який може брати таку ж участь у цьому змаганні в іншій команді.

Одним із найвидатніших аспектів CTF є їх здатність імітувати реальні проблеми безпеки. Ці виклики охоплюють широкий спектр сценаріїв, від використання вразливостей веб-додатків і зворотного проектування шкідливого програмного забезпечення до розшифровки криптографічних головоломок і аналізу цифрової криміналістики. CTF сприяють глибокому розумінню тонкощів кіберзагроз і механізмів захисту.

CTF створюють умови для того, щоб учасники думали як супротивники. Таке хакерське мислення є ключовим активом у світі кібербезпеки, що дозволяє професіоналам передбачати потенційні загрози та протидіяти їм. Учасники розвивають інстинкт виявлення слабких місць і розробки інноваційних рішень – навички, незамінні для захисту цифрових активів.

Є кілька типів викликів CTF, з якими можуть зіткнутися команди. Деякі з найпоширеніших включають [2]:

- двійковий аналіз – у цьому завданні ви повинні проаналізувати певний двійковий код, щоб виявити вразливості та використати їх для отримання доступу до системи.

- експлуатація веб-сайтів – це завдання передбачає виявлення та використання вразливостей у веб-додатках для отримання несанкціонованого доступу до конфіденційних даних.

- криптографія – у цьому завданні ви повинні використовувати криптографічні методи для розшифровки зашифрованих даних або зламати алгоритми шифрування, щоб отримати доступ до конфіденційної інформації.

- реверсивне проектування – ви повинні провести реверсивне проектування зловмисного або іншого програмного забезпечення, щоб зрозуміти, як воно працює, і визначити потенційні вразливості.

- безпека мережі – це завдання передбачає захист мережі від потенційних загроз і її захист від несанкціонованого доступу.

Хоча CTF має деякі подібності з іншими дисциплінами кібербезпеки, є кілька ключових відмінностей, які відрізняють його. Наприклад:

- тестування на проникнення – хоча CTF і тестування на проникнення мають спільне використання імітованих кібератак, вони відрізняються за своїми основними цілями. Тестування на проникнення в основному спрямоване на виявлення вразливостей і слабких місць у системі, щоб відтворити реальні сценарії атак і надати рекомендації щодо зменшення ризиків. На відміну від CTF, де метою часто є виявлення позначок у конкретних викликах, тестування на проникнення наголошує на цілісній оцінці стану безпеки та потенційних проблемних областей.

- оцінка вразливості – Оцінка вразливості передбачає систематичне визначення та класифікацію потенційних вразливостей у системі.

Однак, на відміну від CTF, оцінка вразливості не поширюється на використання цих вразливостей для отримання несанкціонованого доступу. Замість цього він зосереджений на створенні повного переліку слабких місць, які організації потім можуть визначити пріоритети для виправлення. CTF, з іншого боку, охоплює ширшу сферу застосування практичних навичок, крім просто ідентифікації.

– Етичне хакерство – Етичне хакерство, яке часто називають білим хакерством, узгоджується з CTF у своїй меті виявлення вразливостей у системах. Однак воно розходиться за призначенням. Етичний хакерство має на меті підвищити безпеку системи шляхом виявлення слабких місць і надання дієвих рекомендацій щодо покращення. Це контрастує з фокусом CTF на захопленні прапорів і демонстрації володіння навичками кібербезпеки через вирішення різноманітних проблем.

CTF – це унікальна дисципліна з кібербезпеки, яка поєднує в собі елементи різних інших дисциплін, таких як тестування на проникнення, оцінка вразливості та етичне хакерство, з особливим акцентом на захопленні прапора та демонстрації майстерності володіння навичками кібербезпеки.

**Висновок:** CTF змагання дуже корисні для здобуття, вдосконалення та перевірки навичок по різних напрямкам з кібербезпеки, де постійно виникають нові загрози, до яких потрібно вміти швидко підбирати ефективні способи рішення. Здобуті на CTF-змаганнях навички спеціаліст може в майбутньому використати на практиці, бо CTF відображає реальні сценарії в роботі, з якими зіштовхуються спеціалісти в області кібербезпеки.

### **Список літератури:**

1. «Capture The Flags, or CTFs, are computer security competition. [Електронний ресурс]. Режим доступу: <https://ctf101.org/>
2. «Змагання CTF – ключ до успішної кар'єри у сфері кібербезпеки». [Електронний ресурс]. Режим доступу: <https://dou.ua/forums/topic/43810/>

**УДК 004.056.5:004.738.5**

**ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ  
ВІДДАЛЕНОМУ КЕРУВАННІ ЛАБОРАТОРНИМ  
ОБЛАДНАННЯМ СТЕНДУ «ЦИФРОВИЙ АВТОМАТ»**

***Автор:** Клеошин С.К., студент, 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*

**Метою роботи** є дослідження проблем інформаційної безпеки, які виникають при віддаленому керуванні лабораторним обладнанням стенду “Цифровий автомат” та аналіз загроз, пов’язаних з цим видом роботи, а також розробка заходів для їх уникнення.

У сучасному світі швидкість змін та технологічних розробок безперервно зростає, що ставить перед науково-дослідними та навчальними установами нові виклики щодо ефективного використання лабораторного обладнання. Одним із відповідей на ці виклики стало впровадження систем віддаленого керування лабораторним обладнанням.

Віддалене керування лабораторним обладнанням відкриває широкі можливості для досліджень, навчання та інженерних проєктів, дозволяючи використовувати дорогоцінне обладнання з будь-якого місця, де є доступ до Інтернету. Це особливо важливо в умовах сучасної пандемії, коли віддалена робота та навчання стали необхідністю.

Однак разом з безсумнівними перевагами віддаленого керування приходять і нові виклики, зокрема у сфері інформаційної безпеки. Забезпечення захисту систем віддаленого доступу до лабораторного обладнання стає пріоритетним завданням для забезпечення конфіденційності, цілісності та доступності даних.

У цьому контексті вивчення проблем інформаційної безпеки при віддаленому керуванні лабораторним обладнанням набуває особливого значення, адже воно спрямоване на розуміння потенційних загроз та розробку ефективних стратегій захисту, що дозволить максимально використовувати переваги віддаленого доступу без ризику порушення безпеки.

Проблеми інформаційної безпеки при віддаленому керуванні лабораторним обладнанням можуть включати:

– Несанкціонований доступ: ризик отримання несанкціонованого доступу до системи через віддалене підключення. Це може призвести до втрати конфіденційної інформації або навіть зміни параметрів обладнання.

– Збій зв'язку: віддалене керування вимагає стабільного зв'язку між користувачем і обладнанням. Відсутність зв'язку може призвести до неправильної роботи або навіть аварії.

– Конфіденційність даних: передача даних через мережу може бути підвергнута ризику перехоплення або несанкціонованого доступу. Важливо забезпечити шифрування та захист даних.

– Цілісність даних: ризик зміни даних під час передачі або керування. Заходи повинні бути вжиті для запобігання незаконним змінам.

З історії інтернету виокремлюються декілька видатних хакерських атак на системи автоматики та інформаційні системи:

– Взлом Міжнародної космічної станції (МКС): У 1999 році 15-річний хакер Джонатан Джеймс вламав сервери NASA, отримавши доступ до системи життєзабезпечення МКС. Це був серйозний інцидент, який вимагав посилення заходів безпеки.

– **Вірус Stuxnet**, виявлений у 2010 році, спрямований на іранську ядерну програму. Він вразив системи керування промисловими процесами, такими як центрифуги для збагачення урану.

– **Ukraine Power Grid Attack (2015-2016)**. Ця атака сталася в грудні 2015 та січні 2016 року і призвела до вимкнення електроенергії в певних районах України. Хакери використовували шкідливе програмне забезпечення, щоб перехопити системи керування енергомережею та заблокувати їх роботу.

– **Triton / Trisis**: Ця атака була виявлена в 2017 році і спрямована на системи керування виробничою безпекою. Хакери використовували шкідливе програмне забезпечення, щоб змінити програмне забезпечення контролерів безпеки, що призвело до небезпеки для робітників та можливого аварійного виробництва.

– **Dragonfly (Havex)**: Ця атака, також відома як **Energetic Bear**, спрямована на системи керування електромережею та інші промислові системи в окремих країнах. Хакери використовували різні методи,

включаючи фішинг та використання вразливостей програмного забезпечення, щоб отримати доступ до систем керування та спостереження.

Керування обладнанням через глобальну мережу вимагає використання різних методів та засобів для забезпечення безпеки та ефективності, таких як забезпечення безпечних тунелів між віддаленими пристроями через глобальну мережу, шифрування та аутентифікація (використання SSL/TLS для шифрування даних під час передачі, встановлення паролів, двофакторної аутентифікації та інших методів для захисту доступу).

Вирішення проблем інформаційної безпеки при віддаленому керуванні лабораторним обладнанням стенду "Цифровий Автомат" вимагає комплексного підходу та застосування різноманітних заходів забезпечення безпеки:

1. Захист мережі: забезпечення безпеки мережі за допомогою захисту мережевого периметру, використання файрволів, інтранетів, VPN тунелів та інших засобів.

2. Сильні паролі та аутентифікація: від користувачів вимагається використання складних паролів, двофакторної аутентифікації та регулярної зміни паролів.

3. Шифрування даних для захисту передаваних даних через мережу, особливо у випадку чутливої інформації.

4. Моніторинг та журналювання для виявлення незвичайних активностей або спроб несанкціонованого доступу.

5. Обмеження доступу: доступ до лабораторного обладнання надається лише авторизованим користувачам та обмежуються їхні права доступу згідно з принципом найменших привілеїв.

6. Захист від вірусів та шкідливих програм: використання антивірусного програмного забезпечення та інші заходи захисту від шкідливих програм.

7. Планування кризових ситуацій: розроблення плану дій у випадку порушення безпеки, який включає в себе процедури реагування та відновлення після інциденту.

8. Навчання користувачів: проведення навчання з питань інформаційної безпеки для користувачів, щоб вони були усвідомлені та вміли виявляти можливі загрози.

9. Аудит безпеки для оцінки ефективності заходів безпеки та виявлення нових загроз.

**Висновки.** Забезпечення безпеки при віддаленому доступі до лабораторних систем є надзвичайно важливим завданням. Підвищення популярності віддалених робочих середовищ, супроводжується зростанням ризиків та загроз інформаційній безпеці.

У результаті дослідження встановлено, що ключовими проблемами безпеки при віддаленому керуванні є незахищені мережеві підключення, вразливість систем та відсутність ефективних механізмів аутентифікації та авторизації. Для ефективного рішення цих проблем рекомендується впровадження комплексу заходів, таких як захист мережі, сильні паролі та аутентифікація, шифрування даних, регулярні оновлення, моніторинг та журналювання, обмеження доступу, захист від вірусів та шкідливих програм, планування кризових ситуацій, освіта та навчання користувачів та аудит безпеки.

Враховуючи ці рекомендації, можна значно підвищити рівень інформаційної безпеки при віддаленому керуванні лабораторним обладнанням стенду "Цифровий Автомат", що дозволить зменшити ризики зловживання та зберегти конфіденційність, цілісність та доступність даних.

### **Список літератури:**

1. Клік, М. (2017). "Кібербезпека виробничих систем керування: загрози та заходи захисту". Комп'ютерні науки та інформаційні технології, 4, 22-31.
2. Петренко, О., & Сімонов, В. (2018). "Кібератаки на промислові системи керування: аналіз та захист". Інформаційно-керуючі системи на залізничному транспорті, 2(26), 101-109.
3. Кравченко, О., & Шевчук, В. (2019). "Захист від кібератак на системи автоматизації виробничих процесів". Інформаційні технології та комп'ютерна інженерія, 3(69), 81-88.
4. Грінюв, Д. (2020). "Кібербезпека в промислових системах керування: актуальні проблеми та заходи захисту". Інженерія безпеки, 2(43), 42-48.

5. Барановський, О., & Гончаренко, С. (2016). "Загрози та заходи захисту від кібератак на системи автоматизації промислових підприємств". Інформаційні технології та комп'ютерна інженерія, 1(63), 106-113.
6. Stouffer, K., Falco, J., & Scarfone, K. (2011). "Guide to Industrial Control Systems (ICS) Security". NIST Special Publication 800-82.
7. Langner, R. (2011). "Stuxnet: Dissecting a Cyberwarfare Weapon". IEEE Security & Privacy, 9(3), 49-51.
8. Klick, M. (2017). "Cybersecurity Threats to Manufacturing Control Systems - An Overview". IEEE Xplore.
9. Slay, J., & Higgins, G. (2016). "The Cyber Security of Industrial Control Systems - What Does It Mean?" International Journal of Critical Infrastructure Protection, 14, 53-75.
10. Lodi, G., & Zanero, S. (2016). "An Empirical Study of the Reliability of Windows Filtering Platform for the Detection of SCADA-specific Network Traffic". Computers & Security, 62, 78-91.
11. Lee, J., & Kim, H. (2015). "Advanced Persistent Threats and Zero-day Attacks in Industrial Control Systems". International Journal of Control, Automation and Systems, 13(2), 295-302.
12. Bianco, M., Frigieri, F., & Oliva, A. (2017). "Industrial Control System Cyber-Physical Security: A Taxonomy". IFAC-PapersOnLine, 50(1), 4810-4817.
13. Hansman, J., Paulraj, A., & Saberi, S. (2015). "Cyber Physical System Security for Industrial Control Systems". Proceedings of the IEEE, 103(5), 835-848.
14. Luijff, H., & Chotinaiwattarakul, W. (2013). "Cyber Security in the Energy Sector: Why It's Crucial & How to Improve It". Journal of Critical Infrastructure Policy, 1(1), 97-109.
15. Perrow, C. (2007). "The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters". Princeton University Press.

УДК 004.056

## СУЧАСНІ ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В ГАЛУЗІ МОРСЬКИХ ПЕРЕВЕЗЕНЬ

*Автор: Кучер В.С., магістрант, 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.** До пандемії COVID-19 комерційне судноплавство охоплювало близько 80 відсотків світового обсягу торгівлі за вантажами, та понад 70 відсотків світової торгівлі за цінністю. У 2016 року понад 61 відсоток світових поставок нафти та інших рідких енергоносіїв у світі було доставлено морським транспортом [1]. Жоден інший вид транспорту не може перевезти таку кількість товарів за конкурентною ціною.

Проте ризики морської кібербезпеки залишаються недооціненими. Зростання кількості кібератак, націлених на морську сферу, включає в себе як традиційні загрози, відомі іншим галузям, зокрема атаки націлені на знищення або заволодіння даними, так і специфічні для галузі – на операційні технології суден і в портів. За трирічний період до 2020 року кількість звітів про атаки збільшилась на колосальні 900 відсотків [2].

У своєму поточному стані морська галузь є однією з найскладніших для реалізації ідеальної системи безпеки, враховуючи велику кількість портового обладнання, механізмів та постійної ротації персоналу різних рівнів вкупі з швидкою модернізацією інформаційних систем. Це створює ризики для інформаційної безпеки що потребують регулярного дослідження.

**Метою роботи** є дослідження сфери морських вантажоперевезень на актуальні загрози для інформаційних систем портів та суден.

**Основна частина.** Морська галузь складається з різномірних, складних і часто застарілих систем. Системи перебувають у стані постійної еволюції. Як стаціонарні, так і мобільні елементи інфраструктури взаємозалежні та взаємопов'язані. За своєю суттю вони керуються

розмаїттям систем що варіюється від загальних ІТ-пристроїв і пристроїв ОТ, до більш вузькоспеціалізованих елементів, характерних для морської екосистеми.

Потенційними цілями і жертвами є судна, порти, пасажирські і вантажні судноплавні лінії, суднобудівники, виробники морської техніки і так далі.

Морська сфера може зіткнутися з такими атаками:

- крадіжка, знищення або підробка конфіденційних і критичних даних, наприклад про місцезнаходження контейнерів ;
- "людина в посередині". Перехоплення зв'язку між портом і різними зацікавленими сторонами;
- шпигунство через сканування портових систем для перехоплення даних;
- викрадення сеансу, тобто використання вразливостей системи для отримання тих же прав доступу, що і цільові клієнти;
- мережева розвідка і маніпулювання трафіком для компрометації цільових портових системи;
- використання фішингових атак для компрометації мереж;
- незаконна контрабанда людей і наркотиків через організовані злочинні угруповання які розглядають порти як майданчик для контрабанди;
- можливість відключення всіх систем порту шляхом компрометації портових систем. Наприклад диверсії;
- атаки з метою шахрайства, саботажу, вандалізму, крадіжку, тероризму або з корупційною метою.

З 2017 року всі чотири найбільші морські судноплавні компанії світу – A. P. Moller-Maersk (Maersk, як відомо, є частиною A. P. Moller Group), China Ocean Shipping Company (COSCO) Group і Mediterranean Shipping Company (MSC) – зазнали значних кібератак[3]. Операційні системи Maersk були зруйновані, коли шкідливе програмне забезпечення NotPetya поширилося з інфікованого українського програмного забезпечення для підготовки податкових декларацій під назвою MeDoc. Компанія витратила понад 300 мільйонів доларів США, щоб повернутися до повноцінної роботи після десяти днів ремонту та відновлення [4].

Повідомлення про 400-відсоткове збільшення кількості морських кібератак протягом 2020 року, а також 900-відсоткове збільшення кі-

лькості атак на судна та портові системи за попередні три роки вказують на те, що морська галузь перебуває під прицілом кіберзловмисників. Список потенційних порушників та їх цілі наведено в таблиці 1.

Таблиця 1. Види кіберзлочинців, що зацікавлені в атаці морської інфраструктури

| Види кіберзлочинців | Кіберзлочинці                             | Кіберактивісти                               | Терористи                           | Організації, що фінансуються державою                      | Державні суб'єкти                             |
|---------------------|-------------------------------------------|----------------------------------------------|-------------------------------------|------------------------------------------------------------|-----------------------------------------------|
| Цілі                | фінансова або інша матеріальна винагорода | Філософія, політика та інші немонетарні цілі | Терористичні акти, фінансова вигода | Фінансове, промислове, політичне і дипломатичне шпигунство | Шпигунство, диверсії та інші стратегічні цілі |

Існують прецеденти, коли кіберподії з великими наслідками спричиняли перебої в роботі морській сфері. У листопаді 2020 року порт Кенневік, США, зазнав комплексної атаки з вимогою викупу, яка змусила персонал відновлювати цифрові файли з резервних копій.[5]

Також є поширеним кібершпигунство, в основному у формі збору розвідувальних даних і крадіжки Інтернет-протоколів (IP). Кібершпигунство є проміжним видом діяльності, який може бути корисним як для злочинців, так і для державних суб'єктів. Наприклад, у березні 2019 року фінансовані державою китайські хакери, за повідомленнями, націлилися на університети по всьому світу, а також ВМС США з метою викрадення морських технологій.[6] Китай також має власність і/або оперативну присутність у десятках великих портів по всьому світу, що надає широкі можливості для збору інформації про порти, суд-

на і вантажі. Крім того, супротивники можуть розглянути можливість зламу мережі для того щоб у потрібний момент вплинути на роботу інфраструктури. До більш складних атак можна віднести кібератаку Ізраїлю в травні 2020 року на іранський порт Шахід Раджаї в Бандар-Аббасі у відповідь на кібератаку Ірану на систему водопостачання Ізраїлю.[7] Цілеспрямовані підробки та глушіння систем GPS, навігації та синхронізації з боку Росії, Китаю, Ірану та Північної Кореї є додатковими загрозами, що впливають на морський сектор.

В останні роки морська індустрія наполегливо прагне до технологічної інтеграції, більшої автоматизації та впровадження нових систем. Зміни створюють нові значні проблеми з безпекою. Брак кваліфікованих технічних знань на борту кораблів посилює технологічну складність.

Наприклад, у 2019 році есминець ВМС США "Джон С. Маккейн" зіткнувся з нафтовим танкером "Алнік МС" під прапором Ліберії. Після розслідування слідчі встановили, що основними причинами зіткнення стали надто складна система керування з сенсорним екраном і недостатній рівень підготовки.

У звіті Національної ради з безпеки на транспорті (NTSB) зазначалося, що "конструкція сенсорного екрану системи керування та контролю тяги на кораблі "Джон С. Маккейн" збільшила ймовірність помилок оператора, які призвели до зіткнення".[8]

Цей приклад привертає увагу до потенційного ризику, пов'язаного з дедалі ширшим застосуванням надто складних технологій у морській сфері.

Існує ряд ключових причин і проблем, з якими стикаються порти на шляху до забезпечення ефективної кібербезпеки:

- консервативність в цифровій трансформації сфери, що призводить до недостатнього пріоритету кібербезпеки під час впровадження нових технологій.
- недостатній рівень навчання щодо кібербезпеки;
- відсутність розуміння того, який час і бюджет слід виділяти на заходи кібербезпеки;
- недостатня кількість кваліфікованих ІТ-спеціалістів в сфері інформаційної безпеки, нестача навичок;
- відсутність балансу між ефективністю бізнесу, цифровою трансформацією та кібербезпекою;

– проблеми ланцюга поставок: відсутність контролю над рівнем кібербезпеки постачальників також створює проблеми кібербезпеки для портів;

– тісні взаємозалежності між портовими системами та зовнішніми службами з інших секторів(наприклад інфраструктурних);

**Висновок:** В даній роботі було проведено аналіз актуальних загроз для інформаційних систем портів та суден, розглянуто актуальні типи зловмисників та кібератак на існуючих прецедентах. Визначено перелік основних перепон до забезпечення ефективної кібербезпеки у сфері морських вантажоперевезень.

**Список літератури:**

1. “World Oil Transit Chokepoints,” US Energy Information Administration (EIA)
2. “Maritime Cyber Attacks Increase by 900% in Three Years,” Hellenic Shipping News, July 21, 2020
3. Catalin Cimpanu, “All Four of the World’s Largest Shipping Companies Have Now Been Hit by Cyberattacks,” ZDNet, September 28, 2020
4. Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” Wired, August 22, 2018
5. Martyn Wingrove, “Cyber Attack Shuts Down US Port Servers,” Riviera news hub, Riveria Maritime Media, November 23, 2020
6. Emily Price, “Chinese Hackers Targeted 27 Universities to Steal Maritime Research, Report Finds,” Fortune, March 5, 2019
7. Ronen Bergman and David M. Halbfinger, “Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks,” New York Times, May 19, 2020
8. “Collision between US Navy Destroyer John S McCain and Tanker Alnic MC, Singapore Strait, 5 Miles Northeast of Horsburgh Lighthouse, August 21, 2017” National Transportation Safety Board, Report Adopted June 19, 2019

УДК 004.056.53

## ОПТИМІЗАЦІЯ ТА КОНТРОЛЬ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРАТАКИ SOC-ЦЕНТРУ

*Автор:* Михайличенко А.В., магістрантка, 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 світі, де кожна організація стикається з постійно зростаючими кіберзагрозами та широким застосуванням зловмисного програмного забезпечення, особливу увагу слід звернути на критичну інфраструктуру країни. Розуміння та своєчасна реакція на ці кіберзагрози стають вирішальними факторами для забезпечення надійного захисту інформаційних систем.

Правильно налаштовані та оптимізовані процеси виявлення та реагування на кібератаки, а також постійний професійний ріст операторів дозволять знизити час реагування на кіберінциденти та мінімізувати їхній вплив на інформаційні системи організації. Крім того, це забезпечить стійкість та надійність функціонування центру та допоможе забезпечити безпеку інформаційних активів організації.

**Метою роботи** є аналіз сучасних підходів до ефективної організації операційного центру безпеки.

**Основна частина.** Операційний центр безпеки (SOC) – це одна з команд ефективного реагування на інциденти комп'ютерної безпеки [1].

Розгорнута розробка процедур та ролей для ефективної роботи Центру операцій з безпеки дуже важлива для забезпечення безпеки інформації та реагування на кібератаки в організації. Кожен інженер повинен мати свою специфікацію, оскільки встановлення чітких ролей і обов'язків для членів SOC-команди допомагає забезпечити ефективну роботу. Приклади ролей включають:

- 1) Аналітик безпеки: Відповідає за аналіз інцидентів і виявлення загроз;
- 2) Інцидент-менеджер: Координує реакцію на інциденти та комунікацію з іншими відділами;

3) Інженер з безпеки: Відповідає за впровадження заходів забезпечення безпеки та реагування на інциденти.

Також важливо встановити внутрішні процедури для управління SOC, включаючи процеси звітності, відстеження прогресу та оцінку продуктивності. Менеджмент SOC повинен бути відповідальним за надання директив, моніторинг процесів та прийняття рішень на основі об'єктивних даних. Керівник відділу зацікавлений в постійному розвитку навичок своїх підлеглих для підвищення безпеки систем, тому регулярні навчання і тренінги для персоналу SOC є необхідними [2].

Потрібні плейбуки, структуровані документи, які містять кроки та процедури для реагування на різні види інцидентів, задля спрощення роботи інженерів. Розробка плейбуків включає в себе:

- 1) опис типових інцидентів, включаючи їхні симптоми та індикатори;
- 2) кроки, які повинні бути вжиті для виявлення, аналізу і реагування на інцидент;
- 3) ролі та обов'язки персоналу на кожному етапі обробки інциденту.

Інтеграція різних систем моніторингу та реагування допомагає виявляти загрози та реагувати на них автоматично, а автоматизація рутинних завдань і реагування на типові інциденти зменшує навантаження на персонал і забезпечує швидку реакцію на загрози. Наприклад, можна налаштувати та автоматизувати інцидент менеджмент в SIEM, що буде самостійно оброблювати події при надходженні. Звичайно, все навантаження з інженера даний інструмент не забере, проте дасть можливість приділити уваги більш значним інцидентам.

Важливо проводити регулярні аудити та перевірки для перевірки ефективності процесів SOC і дотримання стандартів безпеки, оскільки аудити допомагають виявляти можливість вдосконалення та коригування процедур на основі виявлених проблем.

Усі ці елементи допоможуть створити ефективний SOC, який зможе ефективно реагувати на кіберзагрози і інциденти, забезпечуючи безпеку інформації в організації. Безпека – це процес, і правильно налаштований SOC грає важливу роль у захисті організації від кіберзагроз.

Розробка метрик і показників ефективності є ключовим завданням для оцінки процесів виявлення та реагування на кібератаки в

Центрах операцій з безпеки. Ці метрики і показники допомагають виміряти продуктивність SOC і забезпечити об'єктивну оцінку їхньої ефективності. Нижче наведено приклади таких метрик і показників:

1) Середній час виявлення (Mean Time to Detect, MTTD): ця метрика вимірює середній час, який потрібен SOC для виявлення кібератаки після того, як вона стала активною. Менше значення MTTD вказує на більш ефективний процес виявлення.

2) Середній час реагування (Mean Time to Respond, MTTR): MTTR визначає середній час, який потрібен SOC для прийняття та впровадження заходів щодо відповіді на кібератаку після її виявлення. Швидший відгук (менший MTTR) може позитивно вплинути на обмеження збитків.

3) Кількість FP: Цей показник вимірює, скільки разів SOC помиляється, вважаючи, що звичайна активність є загрозою. Низька кількість хибних позитивів допомагає уникнути витрат на надмірне реагування.

4) Кількість виявлених загроз: Вимірює кількість реальних загроз, які були виявлені SOC протягом певного періоду часу. Велика кількість виявлених загроз може свідчити про більш високий рівень активності загроз в організації.

5) Рівень попереджень (Alert Accuracy): Визначає точність попереджень SOC, тобто відсоток інцидентів, які були правильно виявлені та визнані як загрози.

6) Час для аналізу інцидентів: Ця метрика вимірює середній час, який потрібен SOC для аналізу інциденту після його виявлення. Швидший аналіз дозволяє швидше реагувати на загрози.

7) Результати тестування плейбуків: Вимірює ефективність і точність застосування плейбуків під час обробки інцидентів.

8) Загальний обсяг даних, які обробляються: Вимірює кількість подій та дані, які SOC аналізує та обробляє.

9) Кількість оновлень інцидент-планів: Вказує на актуальність і гнучкість інцидент-планів SOC. Більше оновлень може вказувати на більшу адаптивність до нових загроз.

Ці метрики та показники можуть варіюватися в залежності від потреб вашої організації і специфічних цілей SOC. Важливо визначити ті, які найкраще відображають ефективність процесів виявлення та

реагування на кібератаки в контексті вашої організації і регулярно оцінювати їх для вдосконалення безпеки інформації.

Використання засобів моніторингу і звітності в Центрі операцій з безпеки допомагає забезпечити контроль і покращення процесів виявлення та реагування на кібератаки. Ці інструменти дозволяють збирати дані, аналізувати їх та надавати інформацію для прийняття рішень. Важливі аспекти використання засобів моніторингу і звітності в SOC включають:

1) Моніторинг загроз і активності:

- Використовуйте спеціалізовані системи моніторингу, які можуть виявляти незвичайну або підозрілу активність в мережі та на системах;

- Налаштуйте спостереження за індикаторами компрометації (IoCs) і аномаліями у відповідях системи, наприклад, MISP.

2) Збір та аналіз журналів подій (Log Management):

- Збирайте і зберігайте журнали подій з усіх важливих систем і пристроїв у мережі;

- Використовуйте системи SIEM для аналізу цих журналів і виявлення підозрілих або вразливих місць.

3) Аналіз трафіку (Network Traffic Analysis):

- Моніторинг мережевого трафіку допомагає виявляти аномалії і незвичайну активність;

- Використовуйте інструменти для аналізу пакетів та виявлення можливих атак.

4) Захист від витоку даних (Data Loss Prevention, DLP):

- Використовуйте системи DLP для виявлення та блокування спроб витоку чутливої інформації з мережі, наприклад, Symantec.

5) Системи виявлення вторгнень (Intrusion Detection Systems, IDS, та Intrusion Prevention Systems, IPS):

- Встановлюйте IDS та IPS для виявлення та блокування небажаних мережевих атак.

6) Засоби звітності і аналітики (Reporting and Analytics):

- Створюйте звіти і аналітику на основі зібраних даних для спостереження за активністю, виявлення трендів та аналізу результатів.

- Використовуйте дашборди (наприклад, такий продукт як PowerBI від Microsoft) для візуалізації інформації та підвищення розуміння поточного стану безпеки.

7) Автоматизована обробка інцидентів (Incident Response Automation):

- Використовуйте засоби автоматизації для реагування на типові інциденти шляхом виконання автоматичних заходів забезпечення безпеки.

8) Метрики та KPI (Key Performance Indicators):

- Встановіть метрики та KPI для оцінки продуктивності SOC, які дозволяють визначити, наскільки ефективні ваші процеси обшуку та реагування;

- Метрики можуть включати середній час виявлення, середній час реагування, кількість виявлених загроз і т. д.

Засоби моніторингу і звітності допомагають SOC отримувати реальну інформацію про загрози і вчасно реагувати на них. Результати аналізу даних і звітності можуть служити основою для вдосконалення процесів безпеки та прийняття рішень для захисту організації від кібератак [3].

**Висновки:**

SOC-центр є критичною складовою захисту організації від кіберзагроз. Наявність ретельно розроблених процедур, ролей та плейбуків, регулярні аудити та використання інтегрованих систем моніторингу роблять його ефективним інструментом безпеки.

Розробка метрик ефективності є ключовою для оцінки роботи SOC-центру. Метрики, такі як час виявлення та реагування, точність інцидент-попереджень та оновлення інцидент-планів, визначають продуктивність та гнучкість системи. Важливо обирати та оцінювати ті метрики, що найкраще відповідають потребам організації для постійного удосконалення безпеки інформації.

Важливі аспекти включають моніторинг загроз, аналіз журналів подій, мережевий аналіз, захист від витоку даних та системи виявлення вторгнень. Ці засоби також допомагають встановлювати метрики та KPI для оцінки ефективності SOC. Автоматизація обробки інцидентів і регулярна звітність покращують реагування на загрози і забезпечують вдосконалення безпеки інформації в організації.

**Список літератури:**

1. "Computer Security Incident Handling Guide" by National Institute of Standards and Technology (NIST). [Електронний ресурс]. Режим доступу: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
2. "Security Operations Center: Building, Operating, and Maintaining your SOC" by Joseph Muniz, Gary McIntyre, Nadhem AlFardan
3. "The Practice of Network Security Monitoring: Understanding Incident Detection and Response" by Richard Bejtlich

**УДК 004.056.53**

**КЛАСИФІКАЦІЯ СИСТЕМ ІНТЕРНЕТ РЕЧЕЙ**

***Автор:** Рукінов В.А., магістрант, 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.** Інтернет речей (IoT) – це мережа взаємопов'язаних пристроїв, які з'єднуються та обмінюються даними з іншими пристроями IoT і хмарою. Пристрої IoT, як правило, оснащені такими технологіями, як датчики та програмне забезпечення, і можуть включати механічні та цифрові машини та споживчі об'єкти. Організації в різних галузях все частіше використовують IoT, щоб працювати ефективніше, надавати покращене обслуговування клієнтів, покращувати процес прийняття рішень і підвищувати цінність бізнесу.

**Метою роботи** є класифікація систем Інтернет речей з точки зору захисту інформації для подальшого визначення вимог системи їх захисту.

**Основна частина.** Системи IoT на даний момент є досить новим явищем з точки зору нормативно правової бази та вимог до реалізації їх систем захисту. Систему захисту інформації пропонується розробляти виходячи з призначення даної системи та можливості здійснення збитків. Відповідно до призначення системи можуть бути:

– особисті – системи, що призначенні для використання одною людиною або невеликою групою людей. Прикладом такої системи є розумний будинок або кіберсистема особистих смарт об’єктів (розумний годинник, транспорт, побутові прибори). Такі системи зазвичай не вимагають складних налаштувань та повинні працювати «з коробки». Система захисту в таких об’єктах повинна бути передбачена виробниками та ввімкнення за замовчуванням.

Вихід з ладу таких систем рідко може привести до значних збитків екології та здоров’ю людини. Головною загрозою в при компрометації таких систем є викрадення особистих даних користувача, що може привести до матеріальних втрат (у випадку викрадення фінансових даних), моральної та репутаційної шкоди (при викраденні та незаконній експлуатації приватних даних).

Не зважаючи на вказані загрози безпеки більш пріоритетним в системі захисту є саме доступність інформації, так як саме отримання інформації та керованість пристроями є забезпечення основним аргументом при використанні систем ІоТ в особистому керуванні.

– наукові – системи для віддаленого моніторингу та обробки отриманих даних. Дані системи характеризуються датчиками, що можуть знаходитись на великій відстані один від одного або розміщені на рухомій платформі. Віддаленість та велика кількість вузлів один від одного зазвичай свідчить про те, що на кожен вузол має обмежені розрахункові можливості та наявність безпроводного каналу передачі даних.

Основні загрози в інформаційній безпеці викликані втратою сигналу через втрату датчиків, злонамірне втручання в дану систему може передавати хибні дані або дублювати їх для обробки власними силами, що призведе до потенційної втрати коштів.

Головними критеріями в інформаційній безпеці є цілісність даних, що передається оскільки, саме правильність отриманих даних надає повноту інформації про об’єкт дослідження.

– громадські – системи, що використовуються для роботи в громадських організаціях по прикладу системи «розумне» місто. Такі системи часто використовуються для роботи комунальних служб, служби громадських перевезень тощо. Дана система повинна мати розділений доступ для адміністраторів та власників даної мережі та загальнодоступний користувачів. Вихід з ладу системи може погіршити ро-

боту інфраструктури загального призначення але дана система не повинна мати високий рівень критичності.

Основний критерій для даної системи є достовірність та доступність отриманих даних.

– промислові – системи, що призначенні для віддаленого керування виробництвом. Системи повинні мати розподілені права та закриту структуру. Централізація мереж IoT створює єдину точку відмови, якою можуть скористатися хакери, а велика кількість взаємозалежних пристроїв ускладнює забезпечення їхньої безпеки.

Головною метою атак на дану систему може викрадення конфіденційної інформації, порушення роботи системи, все це може привести до значних матеріальних втрат підприємства.

Головними критеріями для промислових систем так як вказано і в НД ТЗІ 2.5-005 -99 є цілісність та доступність даних.

– системи спеціального призначення – дані системи мають спеціалізоване галузеве призначення, до таких систем відносяться системи критичної інфраструктури, банківські, військового та медичного призначення.

Вихід з ладу таких систем може призвести до серйозних екологічних, соціальних наслідків або можуть загрожувати життю людини. Загальні риси для таких систем є підвищена увага до конфіденційності, цілісності та доступності даних.

### **Висновки:**

Класифікація призначення систем IoT дасть змогу розмежувати вимоги до безпеки відносно їх призначення, що в подальшому буде сприяти розробці нових інструкцій та нормативно-правових актів для висування вимог для даних систем.

### **Список літератури:**

1. Uribe, Felix, The Classification of Internet of Things (IoT) Devices Based on Their Impact on Living Things (January 1, 2018). Available at SSRN: <https://ssrn.com/abstract=3350094> or <http://dx.doi.org/10.2139/ssrn.3350094>.

**УДК 004.056 : 629.12**

## **СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ ВОДНОГО ТРАНСПОРТУ, ЯК ОСНОВНИЙ МЕТОД ЗАХИСТУ**

***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*

Зростання комп'ютеризації і автоматизації водного транспорту, хоча і призводить до покращення ефективності та керованості суден, робить його більш вразливим перед кіберзагрозами, оскільки збільшує кількість точок доступу та атакованих поверхонь. Зростання кількості комп'ютеризованих систем призводить до появи багатьох функцій на одному судні чи в одному порту, що робить їх взаємопов'язаними. Це створює більше точок входу для потенційних кібератак і збільшує загальну поверхню атак. Сучасні системи навігації залежать від супутникових технологій, які, в свою чергу, можуть бути піддані інформаційним атакам, що може впливати на точність навігації і безпеку судноплавства. Морські порти використовують різноманітні електронні системи для управління вантажами, рухом суден та іншими процесами. Ці системи також є мішенню для кібератак, які можуть впливати на портові операції та безпеку.

**Метою даної роботи** є дослідження та оцінка систем виявлення вторгнення (СВВ), спрямованих на забезпечення безпеки та захисту на судні.

Для досягнення даної мети необхідно вирішити наступні задачі:

- визначити сучасні критичні завдання СВВ на суднах;
- провести аналіз специфічних компонентів СВВ, притаманних водному транспорту;
- оцінити перспективи використання існуючих СВВ на водному транспорті.

Захист інформаційної інфраструктури в морському транспорті, включаючи бази даних, системи відстеження вантажів та електронні системи безпеки, є критичним завданням для забезпечення цілісності та конфіденційності. Важливо забезпечити безпеку баз даних, які містять

критичну інформацію про судна, вантажі, екіпаж та інші аспекти морського транспорту. Застосування аутентифікації, авторизації та шифрування може бути ключовими заходами. Електронні системи відстеження вантажів мають бути захищені від несанкціонованого доступу та маніпуляцій. Крім того, важливо забезпечити цілісність та точність інформації про рух вантажів. Системи безпеки, такі як системи контролю доступу, відеоспостереження та інші, повинні бути захищені від кібератак, оскільки їх вразливість може призвести до серйозних наслідків для безпеки портових об'єктів і суден. Реалізація систем моніторингу та виявлення загроз дозволяє вчасно виявляти аномалії чи підозрілі активності в інформаційній інфраструктурі та швидко реагувати на них. Навчання персоналу з питань кібербезпеки та підвищення їх свідомості щодо можливих загроз є важливим для інформаційної безпеки.

СВВ, які застосовуються на водному транспорті, мають відмінності від звичайних СВВ які діють в «офісних» умовах. Система виявлення вторгнення для безпеки на водному транспорті – це комплекс технічних засобів, які використовуються для виявлення та відстеження можливих вторгнень або загроз безпеці на водних шляхах. Наприклад, ці системи можуть включати в себе:

- радари та системи відеоспостереження;
- автоматизовані ідентифікаційні системи. Системи, що базуються на розпізнаванні обличчя та інших біометричних параметрах.
- системи виявлення аномалій. Алгоритми, які аналізують звичайні патерни руху суден та виявляють будь-які аномалії або неправильності, які можуть свідчити про можливі вторгнення або інші загрози.
- системи глобального позиціонування (GPS). Використання GPS дозволяє в реальному часі відстежувати рух суден та контролювати їхнє місцезнаходження.
- системи виявлення та управління аварійними ситуаціями
- інші підсистеми.

СВВ які можуть включати захист специфічних компонентів, при-  
таманних водному транспорту називають, інтегрованими системами

виявлення вторгнень. Інтегровані системи захисту на морському транспорті об'єднують різні технічні засоби та програмні рішення для забезпечення безпеки суден, екіпажу та пасажирів. Ці системи можуть включати в себе різноманітні компоненти, спрямовані на виявлення та захист від різних загроз, таких як вторгнення, терористичні атаки, піратство, аварії та інші небезпеки.

Розглянемо на прикладі система Naval Dome. Системи, розроблені компанією Naval Dome, спрямовані на захист суден та морської інфраструктури від кіберзагроз, таких як хакерські атаки, віруси та інші кібер небезпеки. Захист кожного встановленого компоненту забезпечує кібербезпечне середовище між усіма захищеними системами. Зловмиснику необхідно здійснити окрему атаку на кожную систему виявлення вторгнень, і навіть якщо це вдасться, це залишиться локальним зломом, який легше локалізувати. Ця форма захисту має справу як з внутрішніми, так і з зовнішніми загрозами.

Основні компоненти, які Naval Dome може контролювати та захищати, включають:

- системи управління судном. Моніторинг та контроль за основними системами судна. Захист від несанкціонованого доступу до систем управління;
- системи зв'язку. Контроль за безпекою та цілісністю морських систем зв'язку;
- системи захисту від піратства. Виявлення та відстеження потенційних піратських загроз. Розробка заходів для попередження або подолання піратських атак;
- системи управління загрозами та кризового реагування. Системи, які аналізують та оцінюють рівень загроз та допомагають управляти ситуацією в реальному часі. Підготовка та виконання планів дій у випадку кризових ситуацій;
- системи антивірусного та анти шпигунського захисту. Захист від вірусів, шпигунського програмного забезпечення та інших шкідливих програм. Постійне оновлення бази даних для виявлення нових кіберзагроз;
- системи керування доступом. Контроль доступу до різних зон судна чи морської інфраструктури. Використання електронних ключів, карт чи біометричних методів для ідентифікації та автентифікації;

– системи виявлення та захисту від електронних загроз. Захист від електронних атак, включаючи атаки на системи зв'язку та електроніку судна. Моніторинг та виявлення недостовірних електронних сигналів.

Naval Dome та подібні компанії надають інтегровані рішення для забезпечення надійності та безпеки на водному транспорті, такі системи допомагають мінімізувати можливість атаки на критичні компоненти для забезпечення цілісності і конфіденційності інформації.

### **Висновки**

В даній роботі розглянуто специфіку систем захисту на водному транспорті, визначено основні критично важливі компоненти захисту, доведено важливість застосування інтегрованих СВВ для водного транспорту, задля забезпечення надійного захисту і контролю зі всіма компонентами системи, які необхідні для судна.

### **Список літератури:**

1. 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>
2. Brown A., Jones R. Integrated Intrusion Detection Systems for Maritime Cybersecurity. International Conference on Cybersecurity and Maritime Safety, Proceedings, 2020. P.45-56.
3. Naval Dome. URL: <https://navaldome.com/index.html>
4. Турти М.В, Книжник Р.О. Методика визначення оптимальності інформаційних моделей в галузі інформаційної безпеки //Матеріали III Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».- Миколаїв: НУК, 2013. – С.148-153.

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

**УДК 004.056.53**

**МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ У ТЕХНІЧНИХ  
КАНАЛАХ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ  
НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ**

***Автор:** Болтовський А.В., В/ч 3039 Національної гвардії України, 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*

Актуальність даної роботи обумовлена суттєвим збільшенням кількості інформації, зростанням попиту на неї, а отже і зростанням її цінності, у зв'язку з цим зростають і вимоги щодо її захисту.

З початку повномасштабного вторгнення російських загарбників кількість кібератак на об'єкти енергетичної інфраструктури України збільшилася на третину – до більш ніж 1,2 мільйонів порівняно з 0,9 мільйонами кібератак [1].

Про це повідомив заступник міністра енергетики з цифрового розвитку, цифрових трансформацій та цифровізації. Наразі росіяни продовжують намагатися "покласти" нашу енергосистему, застосовуючи і кібератаки, і прямі фізичні атаки ракетами та дронами. Загальна кількість кібератак за час повномасштабного вторгнення становить понад 1,4 млн. випадків. Кількість DDos-атак на сайти ключових енергетичних компаній та міністерства – 70, для порівняння з початку фіксації такого типу атак з 2019 року їх було лише п'ять, – сказав чиновник під час Energy Security Forum 2022.

**Вступ**

Витік будь-якої інформації може негативним чином відобразитись на діяльності організацій. Особливу роль відіграє інформація з обмеженим доступом (далі ІЗОД), втрата якої може спричинити великі зміни в самій організації та понести за собою матеріальні збитки. Вра-

ховуючи сучасні тенденції до поширення використання портативних джерел обробки інформації, які можна використовувати, актуальним є захист від витоку каналами ПЕМВН саме з таких пристроїв і саме в таких умовах. Неправомірне перекручування, знищення або розголошення ІзОД може нанести серйозні, а іноді й непоправні матеріальні або моральні втрати. У цьому випадку, досить важливим є забезпечення безпеки інформації з обмеженим доступом.

**Метою роботи** є розробка рекомендацій по удосконаленню методів та технологій захисту інформації від витоку технічними каналами на об'єктах інформаційної діяльності Національної гвардії України.

Для досягнення мети необхідно вирішити **наступні задачі**:

- проаналізувати наявні технічні канали витоку інформації об'єкта інформаційної діяльності Національної гвардії України;
- проаналізувати джерела витоку інформації по технічним каналам;
- розглянути методи і засоби захисту інформації від витоку технічними каналами;
- розробка рекомендацій по удосконаленню методів та технологій захисту інформації для об'єктів інформаційної діяльності Національної гвардії України.

### **1. Аналізувати технічних каналів витоку інформації для об'єктів інформаційної діяльності Національної гвардії України**

Однією з найнебезпечніших загроз для інформації, що озвучується на об'єктах інформаційної діяльності або обробляється технічними засобами, в тому числі і інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем, є витік інформації технічними каналами.

Під виток інформації розуміється неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання. Витік інформації відбувається відповідним каналом витоку. Оскільки засоби розвідки противника, як правило, технічні, то і канали витоку також називають технічними.

ТКВІ – сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засоби технічної розвідки (далі – ЗТР). Тобто, ТКВІ це фізичний шлях небезпечного сигналу (носія ін-

формації) від джерела небезпечного сигналу до противника. Також враховуються завади, що діють на вході ЗТР [2].

## **2. Методи і засоби захисту інформації від витоку технічними каналами**

Методи захисту інформації на практиці реалізуються із застосуванням засобів захисту. На рис.1 зображено пасивні та активні засоби захисту інформації.

Захист інформації від витоку технічними каналами досягається шляхом розробки та реалізації заходів, представлених на рис.2.



Рисунок 1 – Пасивні та активні засоби захисту інформації

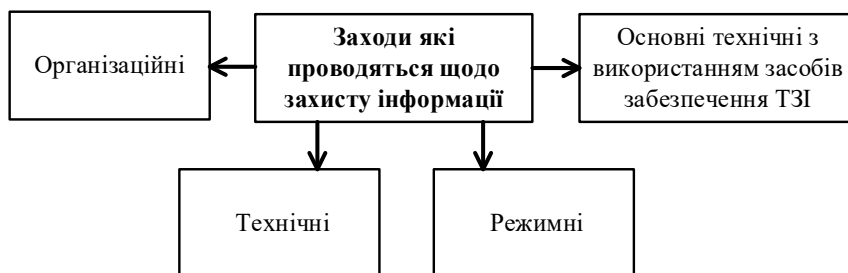


Рисунок 2 – Заходи щодо захисту інформації

Організаційні заходи захисту інформації – це комплекс адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом регламентації діяльності особового складу підприємства та порядку функціонування засобів (систем) за-

безпечення інформаційної діяльності та засобів (систем) забезпечення технічного захисту інформації (далі – ТЗІ).

До основних організаційних і режимним заходів належать [2]:

- залучення до проведення робіт із захисту інформації організацій, що мають ліцензію на діяльність в галузі технічного захисту інформації;
- категорювання та атестація об'єктів інформаційної діяльності (далі – ОІД) і виділених для проведення закритих заходів приміщень (далі виділених приміщень), щодо виконання вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідного обмеженого доступу;
- використання на об'єктах сертифікованих ОІД і допоміжних технічних засобів і систем (далі – ДТЗіС);
- встановлення контрольованої зони навколо ОІД та контрольованої території навколо ОІД НГУ;
- залучення до робіт з будівництва, реконструкції ОІД, монтажу апаратури організацій, що мають ліцензію на діяльність в галузі технічного захисту інформації;
- організація контролю і обмеження доступу на ОІД і в режимних приміщеннях;
- введення територіальних, частотних, енергетичних, просторових і часових обмежень в режимах використання технічних засобів, які підлягають захисту;
- відключення від ліній зв'язку на період закритих заходів технічних засобів, що мають елементи, що виконують роль електроакустичних перетворювачів.

Основні технічні заходи передбачають захист інформації шляхом блокування виявлених загроз із використанням спеціальних засобів ТЗІ.

Усі заходи розробляються одночасно і пов'язуються один з одним.

Організаційні заходи передбачають встановлення:

- окремих завдань захисту ІзОД;
- структури й технології функціонування ТЗІ;
- вимог до забезпечення ТЗІ при організації проектування будівництва (нового будівництва, розширення, реконструкції та капітального ремонту) будівель, споруд і окремих приміщень;

---

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

---

- порядку реалізації організаційних, первинних і основних технічних заходів ТЗІ;
- прав і обов'язків підрозділів і осіб, що беруть участь в обробці ІзОД;
- порядку придбання засобів забезпечення ТЗІ і необхідних нормативних документів;
- контролю й обмежень доступу до виділених приміщень;
- територіальних, частотних, енергетичних, просторових і тимчасових обмежень у режимах використання технічних засобів, що потребують захисту;
- порядку відключення на період проведення закритих заходів технічних засобів, які мають електроакустичні перетворювачі, від ліній зв'язку;
- порядку залучення до проведення робіт із захисту інформації організацій, які мають ліцензію на діяльність у сфері захисту інформації, видану відповідними органами (Держспецзв'язку);
- порядку впровадження захищених засобів обробки інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;
- порядку контролю функціонування СЗІ за її якісними характеристиками;
- порядку проведення атестації СЗІ з розробкою програми атестаційних випробувань [2].

### **Висновок**

На даний момент досить гостро поставлене питання стосовно збереження секретної інформації, та унеможливлення її витоків стороннім особам, оскільки в країні йде війна.

Розвиток сучасних технологій і технічних засобів сприяє постійному розширенню спектрів каналів витоку інформації, засобів знімання інформації, тому дослідження каналів витоку стає все більш актуальним, і складним завданням.

На ефективність систем безпеки впливають характеристики каналів витоку інформації, тому створення систем захисту має відбуватись з урахуванням особливостей реальних каналів. Усе визначається конкретним рівнем напруженості поля за межами КЗ й технічних можливостей противника, тому остаточний висновок про витік інформації

може зробити тільки кваліфікований фахівець, що використовує спеціальні технічні засоби.

Розглянуто можливі канали витоку інформації, та різноманітні методи подавлення несанкціонованого доступу до інформації з обмеженим доступом.

В роботі досліджено основні різновиди технічних каналів витоку інформації та визначені основні способи запобігання витоку інформації такими каналами. Значна увага приділена заходам по унеможливленню створення технічних каналів витоку інформації.

### **Список літератури:**

1. Кількість кібератак на енергетичну інфраструктуру з початку війни зросла на третину – Міненерго. [URL]: <https://www.epravda.com.ua/rus/news/2022/11/21/694084/>.
2. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С., Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навч. Посібник Київ 2016 – 104 с.
3. Бузов Г.А. Захист від витоку інформації по технічних каналах. Навч. посібник / Г.А. Бузов, С. В. Калинин, А.В. Кондратьев – М: 2005р. – 416 с.

**УДК 004.056.5**

## **АНАЛІЗ ЗАДАЧ ТА СТРУКТУРИ СИСТЕМИ ЗАХИЩЕНОГО ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ДЛЯ ОБ'ЄКТІВ ІНФОРМАТИЗАЦІЇ**

**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**

Двадцять другого серпня 2005 року Верховна Рада України затвердила конвенцію 1981 року від Ради Європи «Про захист осіб у

зв'язку з автоматизованою обробкою персональних даних». Крім основних правил і зобов'язань держави в цій конвенції йде мова про створення/прийняття нормативно-правових актів, які повинні гарантувати захист персональних даних громадян країни. Першого червня 2010 року Верховна Рада прийняла пакет законів, які зараз нам відомі як Закони України «Про захист персональних даних», які дають безліч визначень і пояснень у сфері захисту інформації. Особливого значення питання захисту інформаційних ресурсів надули з початком повномасштабного вторгнення російських загарбників в Україну.

### **Вступ**

Кількість інцидентів втрати інформації на об'єктах інформатизації невинно зростає, навіть з урахуванням усієї роботи, що ведеться постійно. Певна частина законів та нормативних актів – застаріли і повинні бути замінені. Процес навчання персоналу необхідно перебудувати та вдосконалювати, для цього необхідно включати в навчання сучасні курси з навчання співробітників із країн, які стоять вище за Україну в цьому питанні: Ізраїль, Канада, США.

**Метою роботи** є дослідження існуючих систем захисту інформації для об'єктів інформатизації та розробка комплексного підходу до їхнього розвитку.

### **1. Аналіз мети та задач, що вирішуються при впровадженні захищеного документообігу**

**1.1** При встановленні цілей та структури системи захищеного електронного документообігу інформаційних об'єктів важливо зосередитися на розумінні існуючих вразливостей, потенційних ризиках та розробці стратегій щодо мінімізації цих проблем. Так, наприклад, мету проекту можна виразити як триєдину ціль:

**Виявлення слабких місць** – виявлення та локалізація слабких місць, вразливостей та потенційних точок проникнення в існуючій системі.

**Оцінка ризиків** – проведення оцінки ризиків щодо потенційних впливів зламаного електронного документообігу на конфіденційність, цілісність та доступність інформаційних об'єктів.

**Аналіз архітектури системи** – проведення розгорнутого аналізу архітектури системи електронного документообігу для визначення потенційних точок збою та областей, вразливих до несанкціонованого доступу.

1.2 До основних задач, виконання яких забезпечить досягнення поставленої мети, можна віднести:

*Аналіз потоку даних* – проведення детального аналізу потоків інформації/даних усередині системи для виявлення потенційних точок перехоплення чи несанкціонованого доступу. Можна розглядати як розширені структурну та функціональну схеми інформаційної моделі потоків даних.

*Оцінка контролю доступу* – виконується оцінка ефективності наявних засобів контролю доступу та виявлення будь-яких прогалин, які можуть призвести до несанкціонованого доступу до конфіденційної інформації.

*Планування реагування на інциденти* – розробка плану/інструкцій/регламентів реагування на інциденти для швидкого та ефективного усунення потенційних інцидентів безпеки, мінімізуючи вплив на інформаційні об'єкти.

*Рекомендації щодо покращення* – розробка рекомендацій щодо посилення безпеки системи електронного документообігу, включаючи технологічні вдосконалення, зміни політики та навчання співробітників.

*Документування результатів* – розробка та введення в дію системи документування інцидентів, спостережень за розвитком інциденту і його розрішення та висновків, в яких описуються поточний стан системи електронного документообігу та пропонуються кроки щодо покращення.

## **2. Система організаційного забезпечення інформаційної безпеки об'єктів критичної інформаційної інфраструктури**

Сама по собі система забезпечення безпеки повинна включати в себе реалізацію комплексу заходів по недопущенню загроз інформаційної безпеки, по припиненню загроз і по ліквідації наслідків реалізованих загроз.

Такий поділ поєднаний з тим, що міри недопущення можуть працювати не тільки на одному етапі, а й на двох або трьох. Наприклад, можна привести сучасне антивірусне ПЗ, які не тільки захищає ОС від проникнення небажаних троянів, але і допомагає впоратися з ними, якщо вони все ж таки потрапили в вашу систему. Роботу по забезпеченню інформаційної безпеки необхідно починати з розробки плану

реалізації заходів. Такий план включає в себе: повне найменування робіт, строки їх виконання і відповідальність за виконання кожного пункту. Далі йде схема витрат на реалізацію плану реалізації заходів, від якого вже роблять корекцію плану в більш реальний бік. Розподіл коштів повинен відбуватися таким чином, щоб все було виконано в мінімальні строки, а з іншого боку – фінансувати необхідно спочатку вкрай необхідні частини.

### **3. Морська кібербезпека**

Морська кібербезпека – це набір інструментів, політик, концепцій безпеки, заходів безпеки, інструкцій, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій і технологій, які використовуються для захисту морських організацій, їхніх суден і кіберсередовища.

Багато з глобальних мереж та інфраструктур на морі все ще використовують застарілі технології, які не були створені для підключення до Інтернету. Ці складні мережі включають суміш систем інформаційних технологій (ІТ) і систем операційних технологій (ми розглянемо їх у наступному розділі), які використовуються внутрішньою командою та сторонніми постачальниками, розширюючи потенціал компрометації з боку хакерів або інсайдерів. погрози.

### **4. Аналіз проблеми кібербезпеки, що впливають на морську галузь**

Багато з поширених проблем кібербезпеки, які впливають на морську галузь, віддзеркалюють проблеми в інших галузях, які мають справу з ІТ-мережами:

- Немає чіткого розуміння всіх систем і пристроїв у мережі ОТ у парку чи операції
- Відсутність видимості мереж ОТ кожного судна
- Відсутність моніторингу в реальному часі або сегментації мережі ОТ
- Ненавмисно підключені ІТ та ОТ мережі
- Використання незахищених бездротових мереж
- Цілодобовий віддалений доступ, наданий стороннім OEM-виробникам
- Відсутність видимості сторонніх мереж OEM (чорний ящик)

- Поганий контроль фізичної безпеки
- Відсутність поінформованості про кібербезпеку серед команди, співробітників і підрядників

### **5. Структура системи захищеного електронного документообігу для об'єктів критичної інформаційної структури**

Зберігання документів: система потребує безпечного центрального репозиторію для зберігання зашифрованих документів. Цей репозиторій має бути доступний лише авторизованим користувачам, яким надано відповідні права доступу.

Шифрування та дешифрування: система повинна використовувати надійні алгоритми шифрування, такі як AES-256, для шифрування документів перед їх збереженням у репозиторії.

Аутентифікація та авторизація: система повинна використовувати надійні методи аутентифікації та авторизації, щоб гарантувати, що лише авторизовані користувачі можуть отримати доступ до зашифрованих документів.



Рисунок 1 – Структура системи електронного документообігу

Відстеження та аудит документів: система повинна вести журнал усіх дій з документами, включаючи створення, зміну та доступ. Цей журнал слід регулярно перевіряти для виявлення будь-яких спроб несанкціонованого доступу.

Інтеграція з іншими системами: система має бути здатна інтегруватися з іншими поліцейськими системами, такими як система управління справами, щоб забезпечити безпечний обмін документами між системами.

Резервне копіювання та аварійне відновлення. Система повинна включати надійний план резервного копіювання та аварійного відновлення, щоб забезпечити можливість відновлення зашифрованих документів у разі системного збою або аварії.

Навчання та підтримка: система повинна забезпечувати навчання та підтримку користувачів тому, як безпечно та ефективно використовувати систему. Це буде включати регулярне навчання з питань безпеки, щоб переконатися, що користувачі обізнані про потенційні ризики безпеки та про те, як їх уникнути.

### **Висновки**

Аналіз завдань системи управління захищеного електронного документообігу для критичних інформаційних об'єктів виявив значні вразливості та потенційні ризики в існуючій структурі. Вивчення різних компонентів, включаючи відображення завдань, потік даних, контроль доступу, методи шифрування та автентифікацію користувачів, дало цінну інформацію про слабкі сторони поточної системи.

Оцінка ризику підкреслює потенційний вплив скомпрометованого електронного документообігу на конфіденційність, цілісність і доступність критичних інформаційних об'єктів. Вкрай важливо негайно вирішувати ці проблеми, щоб зменшити ризики, пов'язані з несанкціонованим доступом і потенційними порушеннями даних.

Для підвищення рівня безпеки системи запропоновано:

1) Впровадження надійних засобів контролю доступу за рахунок покращення методів та засобів контролю доступу, а саме запровадження багатофакторної автентифікації та регулярний аудит та оновлення дозволів користувачів.

2) Регулярний аудит безпеки – проведення регулярні перевірки безпеки з метою своєчасного виявлення нових загроз та вразливостей, їх усунення.

3) Програми навчання та підвищення кваліфікованої роботи користувачів з інформацією в системі електронного документообігу – запровадження комплексних навчальних програми, щоб ознайомити користувачів з використаними в системі методами безпеки, наголошуючи на важливості захисту електронних документів і розпізнаванні потенційних загроз безпеці.

4) План реагування на інциденти – розроблення та регулярне оновлення плану реагування на інциденти, що сприяє швидкому та ефективному реагуванню на інциденти безпеки та мінімізує потенційні збитки.

#### **Список літератури:**

1. Maritime Cyber Security: A Comprehensive Approach. OT Native Zero Trust Security | Mission Secure. URL: <https://www.mission-secure.com/maritime-security-perspectives-for-a-comprehensive-approach>

2. Why maritime cyber security is so important? | Hellenic Shipping News Worldwide. Hellenic Shipping News Worldwide | Hellenic Shipping News Worldwide, Online Daily Newspaper on Hellenic and International Shipping. URL: <https://www.hellenicshippingnews.com/why-maritime-cyber-security-is-so-important/>

3. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.1981 р.: станом на 6 лип. 2010 р. URL: [https://zakon.rada.gov.ua/laws/show/994\\_326#Text](https://zakon.rada.gov.ua/laws/show/994_326#Text)

4. Hellenic Shipping News Worldwide | Hellenic Shipping News Worldwide, Online Daily Newspaper on Hellenic and International Shipping. Hellenic Shipping News Worldwide | Hellenic Shipping News Worldwide, Online Daily Newspaper on Hellenic and International Shipping. URL: <https://www.hellenicshippingnews.com>

УДК 004.056

## **ПОРУШЕННЯ БЛОКУЮЧИХ ІНСТРУКЦІЙ В АСИНХРОННИХ МЕТОДАХ JAVA**

***Автор:** Самойленко Д.М., к.ф.-м.н., доцент, завідувач кафедри інформаційних технологій та фундаментальної підготовки, ПВНЗ "Одеський технологічний університет ШАГ", м. Одеса, Україна*

Асинхронне програмування упевнено прийшло на зміну звичайному імперативному підходові у більшості сучасних мов програмування. Навіть персональні комп'ютери чи мобільні смартфони на сьогодні мають у процесорному блоці декілька окремих процесорів які, у свою чергу, можуть містити декілька обчислювальних ядер. Використати повну потужність таких систем можна лише за допомогою паралельних алгоритмів, частиною яких є асинхронний підхід.

Мова програмування Java, хоч і не є новою, беручі свій початок з 1996 року, але залишається поширеною у застосунках практично усіх типів – мобільних, десктопних, серверних тощо. Причому у деяких галузях обіймає чільне місце [1].

Однією з найбільш поширених задач асинхронного програмування є одержання даних з віддаленого джерела – бази даних, веб API чи з файлової системи. Подібні завдання виконуються за допомогою спеціалізованого функціонального інтерфейсу «Supplier<T>» [2]. Більш того, у ряді випадків робота у синхронному режимі просто забороняється [3], що свідчить про актуальність проведення досліджень у даній галузі, особливо, у контексті безпеки і надійності кодів з асинхронними викликами.

У якості демонстрації роботи з описаною задачею використаємо імітацію тривалого процесу шляхом блокуючої потік операції «sleep». З метою виявлення особливостей роботи коду додамо хрономітки за допомогою системної інструкції «System.nanoTime()». Повний код прикладу наведено далі, наведемо його пояснення. Об'єкт «supplier» інтерфейсу Supplier<String> є головним учасником, що імітує тривалу роботу з одержання даних. У його тілі створюється блокування потоку на 500 мілісекунд після чого відбувається повернення константного результату «Result of Supply». У тілі основної програми створюються дві задачі («task1» і «task2») шляхом поміщення об'єкту до пулу потоків

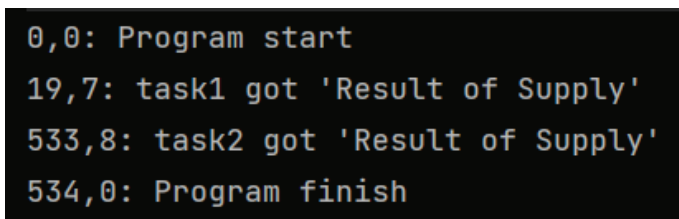
«threadPool». Для гарантії того, що ці дві задачі будуть виконуватись паралельно пул потоків створено з місткістю у 3 одночасні потоки. Але використання результатів задач має відмінності – результат задачі «task1» відразу виводиться на екран (у тілі метода «System.out.printf»), тоді як результат задачі «task2» спочатку зберігається у проміжній локальній змінній «res» і далі в інструкції виведення фігурує вже ця змінна.

У коді здійснюється виведення контрольних точок роботи програми, що дозволяє візуально оцінювати її перебіг. З метою зменшення впливу похибок визначення часу використано достатньо тривалий час блокування (500 мс).

```
import java.util.concurrent.*;
import java.util.function.Supplier;
public class App
{
    private static final ExecutorService threadPool =
Executors.newFixedThreadPool(3) ;
    static Supplier<String> supplier = () -> {
        try {
            TimeUnit.MILLISECONDS.sleep( 500 ) ;
        } catch (InterruptedException ex) {
            System.err.println( "Supplier error: " + ex.getMessage() );
            return "Error result";
        }
        return "Result of Supply";
    };
    public static void main( String[] args )
    {
        long t = System.nanoTime() ;
        System.out.printf( "%.1f: Program start\n", (System.nanoTime() – t) /
1e6 );
        Future<String> task1 = CompletableFuture.supplyAsync( supplier,
threadPool ) ;
        Future<String> task2 = CompletableFuture.supplyAsync( supplier,
threadPool ) ;
```

```
try {  
    System.out.printf( "%.1f: task1 got '%s'\n", (System.nanoTime() - t)  
/ 1e6, task1.get() );  
    String res = task2.get();  
    System.out.printf( "%.1f: task1 got '%s'\n", (System.nanoTime() - t)  
/ 1e6, res );  
} catch( InterruptedException | ExecutionException ex ) {  
    System.err.println( ex.getMessage() );  
}  
System.out.printf( "%.1f: Program finish\n", (System.nanoTime() - t)  
/ 1e6 );  
threadPool.shutdown();  
}  
}
```

Результати роботи наведеної програми ілюстровано на наступному рисунку.



```
0,0: Program start  
19,7: task1 got 'Result of Supply'  
533,8: task2 got 'Result of Supply'  
534,0: Program finish
```

Рисунок 1 – Результат виконання програми

Як видно з рисунку, результат роботи задачі «task1» з'являються значно раніше за очікувані 500 мс, тоді як результати «task2» надходять ближче до очікуваного часу. Зауважимо, що звернення до задач повністю ідентичне «taskN.get()» і воно передбачає очікування результату з блокуванням потоку з викликом.

Також слід зауважити, що при зміні викликів місцями результати роботи програми змінюються і відповідають очікуваним результатам:

```
String res = task2.get();  
System.out.printf( "%.1f: task2 got '%s'\n", (System.nanoTime() - t) /  
1e6, res );
```

```
System.out.printf( "%.1f: task1 got '%s'\n", (System.nanoTime() - t) /  
1e6, task1.get() ) ;
```

```
0,0: Program start  
522,0: task2 got 'Result of Supply'  
522,4: task1 got 'Result of Supply'  
522,6: Program finish
```

Рисунок 2 – Результат при зміненому порядку операцій

Більш того, якщо результат задачі «task1» також помістити у проміжну змінну, аналогічно до схеми роботи з «task2», то її час виконання буде теж близьким до 500 мс у будь-якому порядку очікування задач.

Звертає на себе увагу певний парадокс, відповідно до якого правильний результат роботи задачі одержуться раніше, ніж завершується блокування потоку методом «sleep». Переривання даного методу передбачене системою, але у такому разі програма має піти шляхом блоку виключення і повернути результат-помилку «Error result», доповнивши його повідомленням про виключення. Тоді як реальний хід роботи відповідає нормальному шляху.

Пояснення описаного явища вимагає більш ґрунтовних досліджень алгоритмів роботи середовища JRE і на даному етапі ще не завершене.

У якості **висновків** можна зазначити, що робота з асинхронними задачами вимагає уважного тестування і може призвести до неочікуваних результатів. Висловимо рекомендацію щодо надання переваги створенню додаткової змінної для результату асинхронної задачі, такий підхід показує більш адекватну роботу.

### Список літератури:

1. Руслан Шевченко, Ігор Яновський *Рейтинг мов програмування 2022*. (2023) Retrieved from <https://dou.ua/lenta/articles/language-rating-2022/>
2. Oracle Documentation: *Class CompletableFuture<T>*. (2023) Retrieved from <https://docs.oracle.com/javase/8/docs/api/java/util/concurrent/CompletableFuture.html>

3. Google for developers: *NetworkOnMainThreadException*. (2023)  
Retrieved from <https://developer.android.com/reference/android/os/NetworkOnMainThreadException>

**УДК 004.056.5;057.2**

## **ВДОСКОНАЛЕННЯ ЗАХИЩЕНОСТІ БЕЗДРОТОВИХ ТОЧОК ДОСТУПУ В МЕРЕЖІ WI-FI**

*Автор: Соболев В.В., магістрант, 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*

Тенденція розвитку сучасних Wi-Fi пристроїв полягає в активному впровадженні нових, більш безпечних протоколів Wi-Fi, в результаті чого нові протоколи безпеки і традиційні моделі набувають більшого значення.

Метою даної роботи є дослідження перспектив застосування протоколів бездротової мережі Wi-Fi і їх захисту.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- провести аналіз всіх протоколів;
- визначити типові напрями атаки які можуть використовуватися;
- визначити методи покращення безпеки;

На цей час, існує не так багато протоколів безпеки Wi-Fi, а саме: WEP, WPA, WPA2, WPA3.

- Протокол WEP. Протокол WEP, представлений у 1999 році, є першою версією сімейства протоколів безпеки бездротової мережі IEEE 802.11. Через два роки після його впровадження цей протокол був зламаний через його довжину ключа та погану структуру та криптографічний алгоритм.

- Протокол WPA. Введено для вирішення проблем попередніх протоколів, а саме WEP. Цей протокол оснащено більш надійним шифруванням протоколу часової цілісності ключа (TKIP), а його довжина ключа становить 128 біт замість ключа на 40 біт.

- Протокол WPA2. Замінив протокол WPA в 2004 році. Цей протокол був оснащений ланцюгом блоків шифрування в режимі лічиль-

ника (CCMP) з алгоритмом AES. Є найпопулярнішим протоколом у даний час. З 2017 року став ненадійним після публікації атаки Krack.

- Протокол WPA3 Найсучасніший протокол безпеки, котрий покриває майже всі недоліки минулого зразку, але ще не набув тієї популярності в розповсюдженні. Оскільки головна уразливість приховувалася у чотирьохсторонньому рукоштовуванні, у WPA3 додалася обов'язкова підтримка більш надійного методу захисту SAE, також відомого як Dragonfly. У цьому разі довжина ключа може становити 192, для автентифікаційного шифрування 256(GCMP-256) для захисту цілісності кадрів – VIP-GMAC-256, а для передачі і підтвердження ключів використовується HMAC з хешами SHA-384.

Розглянемо більш детально стандарт WPA3 в його режимах роботи.

#### 1. WPA3-SAE (Simultaneous Authentication of Equals):

- Основна ідея: WPA3-SAE базується на протоколі SAE (Simultaneous Authentication of Equals), який використовує варіант протоколу Діффі-Хеллмана для створення безпечного ключа обміну даними між точкою доступу та клієнтом.

- Переваги: Захищає мережу від атак, таких як атаки перехоплення пароллю, і забезпечує високий рівень безпеки.

- Використання: Підходить для використання в домашніх та малих бізнес-мережах.

#### 2. WPA3-OWE (Opportunistic Wireless Encryption):

- Основна ідея: WPA3-OWE (або Enhanced Open) забезпечує шифрування безпеки з'єднань без необхідності введення пароля чи проведення автентифікації. Це особливо корисно для громадських Wi-Fi мереж.

- Переваги: Забезпечує шифрування для відкритих мереж без необхідності обміну паролем.

- Використання: Ідеальний для громадських мереж, де користувачі можуть приєднуватися до мережі без обміну автентифікаційними даними.

#### 3. WPA3-Enterprise:

- Основна ідея: WPA3-Enterprise використовує індивідуальні автентифікаційні дані для кожного користувача на мережі, зазвичай че-

рез сервер аутентифікації, такий як RADIUS. Користувачі можуть використовувати свої унікальні паролі або інші методи аутентифікації, такі як сертифікати.

- Переваги: Забезпечує високий рівень безпеки через індивідуальну аутентифікацію для кожного користувача.

- Використання: Рекомендується для корпоративних мереж та великих організацій.

#### **4. WPA3-PSK (Pre-Shared Key):**

- Основна ідея: WPA3-PSK використовує спільний (однаковий для всіх пристроїв) попередньо встановлений ключ (пароль) для аутентифікації точок доступу і клієнтів.

- Переваги: Легко встановлюється та керується, підходить для домашніх та невеликих мереж.

- Використання: Зручно використовувати в домашніх та невеликих мережах, де простота важлива.

Підвищити безпеку наявних протоколів можна звичайними методами: Основне наразі це використання сучасних протоколів безпеки, таких як WPA3-PSK або WPA3-Enterprise Приховування/зміна SSID мережі; Вибір надійного пароля та часта його зміна; Обмеження доступу до конфігурації роутера; В жодному разі не використовувати кнопку WPS на Wi-Fi роутері, використання цього засобу дуже сильно знижує безпеку Wi-Fi роутеру і дає можливість дуже простого захоплення контролю небажаним людям; Оновлення бездротового пристрою; Використання фільтрації MAC-адрес. Відімкнення непотрібних служб та портів; Ввімкнення файрволу; А з боку користувача додатковим посиленням безпеки користування буде використання VPN для додаткового шифрування свого трафіку.

#### **Висновки**

В даній роботі проведено аналіз протоколів мереж Wi-Fi, методів їх злому та обходу захисту, визначені типові методи підвищення безпеки. WEP і WPA це дуже ненадійні протоколи, через невелику довжину ключа, тому отримується доступ як до самої мережі, так і до пакетних даних які ви використовуєте. WPA-2 можна використовувати але на свій страх і ризик, це не досить надійний протокол на даний час. Еталоном надійності і захищеності можна вважати WPA-3.

### Список літератури:

1. I. ul Naq, and A. Kh. Tamim, "Penetration frameworks and development issues in secure mobile application development: A Systematic Literature Review", IEEE Access, vol. 9, pp. 87806–87825, 2021.
2. M. Mohammadi, et al. "Energy-aware key management and access control for the internet of things", World Wide Web, pp.1-32, 2021.

УДК 004.056.5;057.2

## СИСТЕМА АНАЛІЗУ ЗАХИЩЕНОСТІ ТОЧОК ДОСТУПУ WI-FI

*Автори: Соболев В.В., магістрант; Козирев С.С., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Тенденція розвитку сучасних Wi-Fi пристроїв полягає в активному впровадженні нових, більш безпечних протоколів Wi-Fi, в результаті чого нові протоколи безпеки і традиційні моделі набувають більшого значення.

Метою даної роботи є покращення безпеки застосування протоколів бездротової мережі Wi-Fi.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- провести аналіз всіх протоколів;
- створити методи покращення безпеки;

На цей час, існує не так багато протоколів безпеки Wi-Fi, а саме: WEP, WPA, WPA2, WPA3.

• Протокол WEP. Представлений у 1999 році, є першою версією сімейства протоколів безпеки бездротової мережі IEEE 802.11. Через два роки після його впровадження цей протокол був зламаний через його довжину ключа та погану структуру та криптографічний алгоритм.

• Протокол WPA. Введено для вирішення проблем попереднього протоколу. Цей протокол оснащено більш надійним шифруванням протоколу часової цілісності ключа (TKIP), а його довжина ключа становить 128 біт замість ключа на 40 біт.

- Протокол WPA2. Замінив протокол WPA в 2004 році. Цей протокол був оснащений ланцюгом блоків шифрування в режимі лічильника (CCMP) з алгоритмом AES. Є найпопулярнішим протоколом у даний час. З 2017 року став ненадійним після публікації атаки Krack.

- Протокол WPA3 Найсучасніший протокол безпеки, котрий покриває майже всі недоліки минулого зразку, але ще не набув тієї популярності в розповсюдженні. Оскільки головна уразливість приховувалася у чотирьохсторонньому рукоштовуванні, у WPA3 додалася обов'язкова підтримка більш надійного методу захисту SAE, також відомого як Dragonfly. У цьому разі довжина ключа може становити 192, для автентифікаційного шифрування 256 (GCMP-256) для захисту цілісності кадрів – BIP-GMAC-256, а для передачі і підтвердження ключів використовується HMAC з хешами SHA-384.

Підвищити безпеку наявних протоколів можна звичайними методами: Основне наразі це використання сучасних протоколів безпеки, таких як WPA3-PSK або WPA3-Enterprise Приховування/зміна SSID мережі; Вибір надійного пароля та часта його зміна; Обмеження доступу до конфігурації роутера; В жодному разі не використовувати кнопку WPS на Wi-Fi роутері, використання цього засобу дуже сильно понижує безпеку Wi-Fi роутеру і дає можливість дуже простого захоплення контролю небажаним людям; Оновлення бездротового пристрою; Використання фільтрації MAC-адрес. Відімкнення непотрібних служб та портів; Ввімкнення файрволу; А з боку користувача додатковим посиленням безпеки користування буде використання VPN для додаткового шифрування свого трафіку.

Для можливості оцінки системи яка використовується, була створена програма, яка оцінює стан захищеності і надійності підключеної мережі Wi-Fi.

Програма сканує підключену мережу Wi-Fi на предмет використання того чи іншого протоколу безпеки, дає відповідь на те чи безпечний протокол на даному підключенні, а також перевіряє складність паролю, якщо потрібно то рекомендує провести його покращення.

Робота програми зображена на Рисунку 1.

Код написаний на мові програмування C++ і створений для Windows 10/11.

```
Scanning...
You use WPA3 - highest level of protection.
Your password: 13Le@_Og
Password is strong.

[Program finished]
```

Рисунок 1.

Програма працює таким чином що спочатку збирає всі данні про підключену Wi-Fi мережу. Після збору необхідної інформації, на основі отриманої інформації проводиться аналіз про те яким протоколом ви користуєтесь та який він по захищеності, де WPA – низький рівень, WPA2 – середній рівень, а WPA3 – високий. Після чого ініціюється перевірка складності пароллю. Складність пароллю межується двома відповідями, складний або простий. Якщо в паролі буде відсутня одна з вимог до «складного» пароллю, то він буде автоматично записаний до простих. Звичайні вимоги парольної перевірки в даній програмі це наявність великих і малих літер, чисел та спеціальних символів. Рисунок 1 показує виконання програми на пристрої підключеному до мережі WPA3 з досить надійним паролем, в той самий час як Рисунок 2 показує підключення до Wi-Fi із протоколом WPA2, і досить простим паролем на що і наголошує після оцінки пароллю наша програма.

```
Scanning...
You use WPA2 - Medium level of protection.
Your password: 12345678
Password is weak.
Need to enhance your password.

[Program finished]
```

Рисунок 2.

### **Висновки**

В даній роботі проведено аналіз протоколів мереж Wi-Fi, методів їх злому та обходу захисту, визначені типові методи підвищення безпеки. WEP і WPA це дуже ненадійні протоколи, через невелику довжину ключа, тому отримується доступ як до самої мережі, так і до пакетних даних які ви використовуєте. WPA-2 можна використовувати але на свій страх і ризик, це не досить надійний протокол на даний час. Еталоном надійності і захищеності можна вважати WPA-3.

### **Список літератури:**

1. I. ul Haq, and A. Kh. Tamim, "Penetration frameworks and development issues in secure mobile application development: A Systematic Literature Review", IEEE Access, vol. 9, pp. 87806–87825, 2021.
2. M. Mohammedi, et al. "Energy-aware key management and access control for the internet of things", World Wide Web, pp.1-32, 2021.

**УДК 004.056.5; 004.89; 514.743.4**

## **АНАЛІЗ РИНКУ ТА ОСНОВНИХ РЕКОМЕНДАЦІЙ ЩОДО БЕЗПЕКИ ПРИСТРОЇВ IoT**

***Автор:** Стефанюк Ю.О., студент, 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*

Сучасний світ все більше нагадує велике павутиння. Кількість IoT-пристроїв – роутерів, камер, NAS-сховищ, компонентів «розумного дому» – росте з кожним роком. Зі збільшенням кількості таких пристроїв росте і необхідність їх захисту. «Організації в усьому світі перебувають під зростаючим тиском щодо захисту свої пристроїв Інтернету речей і підключених пристроїв, а також орієнтування в дедалі складнішому цифровому ландшафті, який вимагає абсолютної довіри», – каже Еллен Боем, старший віце-президент зі стратегії та операції IoT компанії Keyfactor. [1]

Метою даної роботи є збір та аналіз даних щодо розширення світу пристроїв «Інтернету речей» та вироблення універсальних порад щодо їх захисту.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- Проаналізувати статистичні дані та прогнози, щодо стану світу IoT у світі;

- Проаналізувати методичні рекомендації світових агентств з питань кібербезпеки, щодо захисту пристроїв IoT.

Поява такого поняття, як «Internet of Things» була передбачена ще Ніколом Теслою у 1926 році. Але розвиток цього напрямку відбувався досить повільно. У 1990 році Джон Ромки, один з творців протоколу ТСР/ІР, підключив свій тостер до Інтернету і змусив його включатися і вимикатися дистанційно. Цей пристрій і став першою в світі «інтернет-річчю». У період з 2008 по 2009 рік (точну дату вказати неможливо), за оцінкою аналітиків корпорації Cisco, кількість пристроїв, підключених до Всесвітньої павутини, перевищило чисельність населення Землі [2]. Лише у 1999 році засновник дослідницької групи Auto-ID Labs вперше сформулював концепцію та термін «Інтернету речей» у звичному для нас розумінні. Жовтень 2004 року став одним із головних років у світ «Інтернету речей». В цьому році у науково-популярному журналі Scientific American, була опублікована стаття, що наочно показувала можливості використання концепції «Інтернету речей» у побуті [3].

Станом на 2021 рік, кількість глобальних підключень IoT зросла до 35,82 мільярдів активних кінцевих точок та продовжила рости. У 2022 році, кількість підключень виросла порівняно з 2021 роком та досягла 42,62 млрд [4]. Очікувана кількість активних підключень у 2025 році може становити більше 70 млрд, це у 8 рази більше за загальну популяцію людей у світі. Такий стрімкий зріст відбувся зокрема через зацікавленість даною перспективною технологією не лише світовими ІТ країнами, а й країнами. Так, по оцінкам International Data Corporation очікується, що європейські організації витратять близько 227 млрд доларів на технологією Інтернету речей у 2023 році. Очікується, що витрати пов'язані з IoT, продовжать зростати з п'ятирічним середньорічним темпом зростання 11%, досягнувши майже 345 мільярдів доларів до 2027 року [5].

Глобальна проблема кібербезпеки пристроїв IoT почала поширюватися з появою дешевих китайських мікроконтролерів, при виробництві яких дуже мало приділялося уваги саме кібербезпеці. Пристрої на базі таких мікроконтролерів дуже швидко почали заповнювати світовий ринок та користуватися популярністю, через масовість їх виробництва та дешевизну. International Data Corporation прогнозує, що світові витрати на Інтернет речей до 2026 року перевищать 1 трильйон доларі, а провідним у цьому питанні стане Китай, обігнавши США на 13% за сукупним середньорічним темпом росту. [6]

Світові агентства з питань кібербезпеки почали проробляти законодавчі та рекомендаційні документи ще під час епідемії COVID-19. Так 4 грудня 2020 року був підписаний H.R.1668 – «Закон про покращення кібербезпеки IoT від 2020 року» [7, 8].

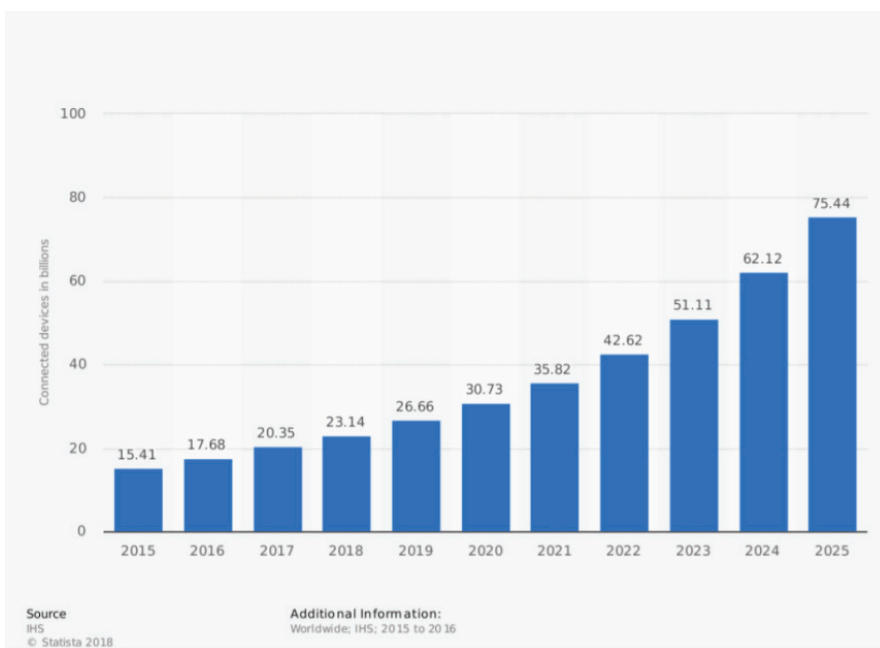


Рисунок 1 – Прогноз росту кількості активних підключень пристроїв IoT від компанії Statista [4]

Також планується у 2024 році ввести знак кібердовіри США. Цей знак буде допомагати користувачам визначати, чи відповідає цей продукт стандартам кібербезпеки чи ні. [9]

Європейське агентство з мережевої та інформаційної безпеки, 19 листопада 2018 року опублікувало дослідження спрямоване на вирішення проблем безпеки та конфіденційності, пов'язаних з еволюцією промислових систем і послуг, викликаних впровадженням інновацій IoT. [10]. На базі цього дослідження, 9 листопада 2020 року було представлено «Рекомендації щодо захисту Інтернету речей» [11].

Open Web Application Security Project (або скорочено OWASP) – відкритий проект забезпечення безпеки веб-додатків у 2018 році представив топ-10 вразливостей [12], які найчастіше дають змогу зловмисникам можливість зламати пристрій IoT.

**Висновки.** В роботі було проаналізовано статистичні дані та прогнози від світових компаній у IT сфері, щодо подальшого росту та розвитку світу «інтернету речей» у майбутньому. Проаналізовано методичні рекомендації світових агентств з кібербезпеки щодо налаштування захищених пристроїв IoT. Зокрема було проаналізовано методичні рекомендації Національного інститут стандартів та технологій, Європейського агентства з мережевої та інформаційної безпеки, топ-10 вразливостей пристроїв IoT від Open Web Application Security Project. На базі цих документів було розроблено універсальні рекомендації:

1. Необхідно приділяти увагу фізичному захисту пристрою, унеможливити доступ зловмисника до пристрою
2. Не залишати пристрої з налаштуваннями за замовчуванням.
3. Не нехтувати шифруванням та механізмами контролю доступу до конфіденційної інформації.
4. Надавати перевагу сертифікованим продуктам.
5. Вчасно оновлювати ПЗ пристроїв. Використання застарілого ПЗ може спричинити виникнення вразливостей.
6. Оновлювати ПЗ роутерів та маршрутизаторів мережі.
7. Надавати перевагу пристроям з механізмами Безпечного оновлення. Відсутність таких механізмів означає, що пристрій протягом невизначеного часу залишиться уразливим.

8. Перевіряти веб-інтерфейс, API, хмарні та мобільні інтерфейси в екосистемі поза пристроєм. Їх не належна захищеність може компрометувати пристрій або пов'язані з ним компоненти.

9. Непотрібні або небезпечні служби, запущені на пристрої ставлять під загрозу конфіденційність, цілісність, доступність інформації.

10. Не використовувати слабкі паролі та регулярно змінювати їх.

IoT є перспективною технологією, що дуже стрімко розвивається й з огляду на прогнози та тенденції та незважаючи на величезну кількість IoT пристроїв зараз, в неї досі є потенціал до росту та розвитку. Зокрема це пов'язано з їх головною функцією – підключенням до мережі, чим більше підключень до мережі – тим більше вразливостей. Тому зараз необхідно приділяти увагу не тільки боротьбі з вже відомими вразливостями, а й проробляти стратегії подальшого розвитку кібербезпеки у сфері IoT.

#### **Список літератури:**

1. Digital Trust Enables IoT Device Security | Ellen Boehm, SVP, IoT Strategy & Operations at Keyfactor. URL: <https://www.youtube.com/watch?v=aRCria65-gk> (дата звернення 17.11.2023).

2. Internet of Things, IoT. URL: <https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot> (дата звернення 19.11.2023).

3. The Internet of Things. Scientific American. URL: <https://cba.mit.edu/docs/papers/04.10.i0.pdf> (дата звернення 19.11.2023).

4. Statista GmbH. IoT: Number of Connected Devices Worldwide 2012-2025. Statista. URL: <https://www.statista.com/statistics/471264/iot-number-ofconnecteddevices-worldwide/> (дата звернення: 18.11.2023).

5. European IoT Spendind to Reach Nearly \$227 Billion in 2023, Despite Ongoing Market Uncertainly, Says IDC. URL: <https://www.idc.com/getdoc.jsp?containerId=prEUR250941023> (дата звернення: 18.11.2023).

6. Worldwide Spending on the Internet of Things is Forecast to Surpass \$1 Trillion in 2026, According to a New IDC Spending Guide. URL: <https://www.idc.com/getdoc.jsp?containerId=prUS50936423> (дата звернення: 18.11.2023).

7. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науководослідний інститут інформатики і права

НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2020 – №12 (грудень) .156 – 157 с. URL: <https://ippi.org.ua/sites/default/files/2020-12.pdf> (дата звернення: 21.11.2023).

8. H.R.1668 – IoT Cybersecurity Improvement Act of 2020. URL: [https://www.congress.gov/bill/116th-congress/house-bill/1668?\\_gl=1\\*1g68cst\\*\\_gcl\\_au\\*MTI5MTcxMTQ0LjE3MDA0ODQwMTk](https://www.congress.gov/bill/116th-congress/house-bill/1668?_gl=1*1g68cst*_gcl_au*MTI5MTcxMTQ0LjE3MDA0ODQwMTk). (дата звернення: 21.11.2023).

9. The White House details its IoT cybersecurity label plan. URL: <https://staceyoniot.com/the-white-house-details-its-iot-cybersecurity-label-plan/> (дата звернення: 21.11.2023).

10. Good Practices for Security of Internet of Things in the context of Smart Manufacturing. URL: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot?fbclid=IwAR1q-chv88kZRsIESHtGTEwbA0Mbx8mb9hV1Euqy-Y--IHVYvLuFhGuvi6o> (дата звернення: 21.11.2023).

11. Guidelines for Securing the Internet of Things. URL: <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things> (дата звернення: 21.11.2023).

12. OWASP Internet of Things TOP10 2018. URL: <https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf> (дата звернення: 21.11.2023).

**УДК 004.056.5**

### **ЗАХИСТ ПРОГРАМНИХ ПРОДУКТІВ ПІД ЧАС РОЗРОБКИ**

**Автор:** Тихонов О.Ю., магістрант, 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

Програмне забезпечення сучасних комп'ютерних систем є дуже складним виробом, при створенні і функціонуванні якого активно використовуються автоматизовані засоби його розробки і загальносис-

темне програмне забезпечення, об'єм і складність якого можуть перевищувати прикладне програмне забезпечення на порядки.

Істотних збитків виробникові програмних продуктів наносять несанкціоновані дії, які завдають значного етичного і матеріального збитку виробникам програмного забезпечення, а часто і легітимним споживачам програмного продукту. Тому багато розробників задаються питанням, чи можна разом з правовим і організаційним забезпеченням процесу розробки і експлуатації програм, здійснити і науково-технічні заходи, що дозволяють захищатися від подібних зловмисних дій[1].

Таким чином, фактор безпеки інформаційних ресурсів і послуг при розробці та експлуатації сучасних ІКСМ відіграє першорядну роль. Захист програмного забезпечення (ПЗ) – це комплекс заходів, спрямованих на захист ПЗ від несанкціонованого придбання, використання, поширення, модифікації, вивчення та відтворення аналогів [2].

Завдяки розвитку технологій програмного забезпечення системи захисту також постійно розвиваються.. Необхідність використання систем захисту ПЗ обумовлена списком проблем, серед яких слід виділити:

1. незаконне використання алгоритмів, що є інтелектуальною власністю автора, при написанні аналогів продукту (промислове шпигунство);
2. несанкціоноване використання ПЗ (крадіжка і копіювання);
3. несанкціонована модифікація ПЗ з метою впровадження програмних зловживань
4. незаконне розповсюдження та збут ПЗ (піратство);
5. втрата прибутку від реалізації продукту

Для захисту ПЗ використовується ряд методів та алгоритмів. Всі методи захисту можна розділити на апаратні та програмні.

До програмних відносяться методи, у яких не зачіпаються фізичні характеристики носіїв інформації, спеціальне обладнання і т.п.

До апаратних відносяться методи, що використовують спеціальне обладнання або фізичні особливості носіїв інформації, щоб ідентифікувати оригінальну версію програми і захистити продукт від нелегального використання.

До основних переваг захисту на програмному рівні можна віднести: гнучкість, низьку вартість, сумісність з уже існуючими системами.

Проте, великим недоліком виступає обмежена надійність. Недоліки апаратних методів захисту:

- підвищення вартості,
- несумісність з деякими уже існуючими системами,
- складнощі при передачі таких програмних продуктів, модернізації, технічному обслуговуванні та видачі.

Отже, апаратні засоби мають значно меншу гнучкість, ніж програмні.

На даний момент проблема збереження прав власності на вихідний код досить актуальна. Щоб обійти захист ПЗ, потрібно виконати аналіз принципу роботи його коду і того як він комунікує із захищеною програмою. Такий процес аналізу називають процесом реверсивної (зворотної) інженерії. На цей процес впливає особливість людської психіки, тому застосування цих властивостей дозволяє знизити ефективність процесу реверсивної інженерії.

Найвідомішим та найпопулярнішим способом захисту від реверс-інжинірингу є обфускація. Обфускацією програми називається деяке її перетворення, яке зберігає функціональність, але при цьому надає програмі таку форму, що вилучення програмного коду, ключової інформації щодо алгоритмів та структур даних, які були реалізовані у програмі, стає трудомістким завданням.

Заплутана (обфускована) програма виходить в результаті застосування до вихідної, не заплутаної програми заплутуючи перетворень (obfuscating transformations). Обфускація може використовуватися не тільки для захисту ПЗ, вона широко застосовується, наприклад, авторами вірусів, для захисту програмних продуктів.

Процес перетворення вихідного коду є процесом обфускації, якщо від задовольняє наступним вимогам:

- Візуально код модифікованої програми відрізняється від вихідного коду, але при тих самих вхідних даних повертає той самий результат.
- Аналіз модифікованого коду більш складний та трудомісткий, ніж аналіз вихідного коду.
- При кожному процесі модифікації результуючий код є різним.
- Зворотне перетворення коду є неефективним.

Суть обфускації програмного коду полягає в тому, щоб ускладнити розуміння та аналіз програмного коду та перешкодити цілеспрямованій його модифікації. Обфускованою програмою називається програма, яка після застосування обфускуючих перетворень на всіх прийнятних для вихідної програми вхідних даних показує той самий результат, що ж оригінальна програма, але більш складна для аналізу, розуміння та модифікації [3].

На сьогоднішній день відомо багато програм для обфускаційних перетворень, таких як: ThinApp, .NET Reactor, CilSecure, C# Source Code Obfuscator та ін. Більшість виконує лише такі перетворення як зміна порядку виклику даних/функцій, генерація нових імен змінних, вставка псевдокоду. Проте на сьогоднішній день цього вже недостатньо для забезпечення надійного захисту коду обфускаційними методами. Ефективність обфускації можуть забезпечити перераховані вище механізми, але вже в поєднанні з перетвореннями основних елементів коду, користуючись методами клонування, додаючи мертвий код, змінюючи тотожності та модифікуючи граф управління.

Сама по собі обфускація не рекомендована для забезпечення найбільш повного та продуктивного захисту програмних продуктів тому, що вона унеможливує запобігання нелегального використання програмного продукту. Тому обфускацію часто використовують разом з одним серед відомих методів захисту, це дає можливість значно посилити рівень захисту ПЗ в цілому.

Отже, обфускація є порівняно новим та перспективним методом захисту. Також вона відповідає принципу економічної доцільності, оскільки її застосування не істотно підвищує ціну програмного продукту та при цьому дає можливість зменшити втрати від піратства та плагіату в результаті крадіжки неповторного алгоритму роботи захищеного програмного продукту.

### **Список літератури:**

1. Давидов В. В. Моделі та методи підвищення безпеки програмного забезпечення (монографія). Харків, 2021. 146 с.
2. Бобало Ю.Я. Інформаційна безпека: навчальний посібник / Ю. Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарев, С.С. Войтусік, А.Я. Горпенюк, О.А. Нємкова, І.М. Журавель, Б.М. Березюк, Є.І. Яковенко, В.І. Отенко, І.Я. Тишик. Львів: Видавництво Львівської політехніки, 2019. – 580 с.

3. Обфускація і захист програмних продуктів [Електронний ресурс]. – Режим доступу : <http://www.citforum.ru/security/articles/obfus/>

**УДК 004.056.5:004.738.5**

## **ІНФОРМАЦІЙНА БЕЗПЕКА ВІДДАЛЕНОГО ДОСТУПУ ДО КОРПОРАТИВНИХ МЕРЕЖ**

***Автори:** Трибулькевич С.Л., ст. викладач; Трибулькевич В.В.,  
Національний університет кораблебудування імені адмірала  
Макарова, м. Миколаїв, Україна*

**Мета роботи** полягає у вивченні, аналізі та розробці стратегій та методів забезпечення захищеності корпоративних мереж під час віддаленого доступу. Основними завданнями є ідентифікація потенційних загроз та вразливостей, визначення ефективних заходів безпеки, розробка та впровадження політик безпеки, а також навчання персоналу щодо кращих практик забезпечення безпеки віддаленого доступу.

Віддалений доступ до корпоративних мереж став необхідною складовою сучасного бізнесу, особливо в умовах зростаючої мобільності та вимог до флексibility робочого процесу. Із розвитком технологій зв'язку та інформаційних систем, багато компаній надають своїм співробітникам можливість працювати з будь-якого місця, використовуючи віддалений доступ до корпоративних ресурсів.

Проте разом із зручністю віддаленого доступу приходять і нові виклики щодо безпеки інформації. Забезпечення конфіденційності, цілісності та доступності даних стає основною турботою для багатьох організацій, які використовують віддалені технології.

У цьому контексті робота з інформаційною безпекою віддаленого доступу до корпоративних мереж набуває особливого значення. Вона спрямована на вивчення та аналіз потенційних загроз безпеці, розробку та впровадження ефективних стратегій захисту, а також навчання персоналу щодо кращих практик безпеки віддаленого доступу.

Зловмисники активно використовують різноманітні методи та техніки для атак на системи віддаленого доступу з метою отримання

несанкціонованого доступу до конфіденційної інформації, розповсюдження шкідливого програмного забезпечення або нанесення шкоди бізнесу:

1. Перехоплення даних: зловмисники можуть використовувати методи перехоплення трафіку мережі для зламування віддалених сесій та отримання конфіденційної інформації, такої як паролі, дані корпоративних проектів тощо.

2. Brute Force атаки: зловмисники можуть використовувати програми для автоматичного перебору паролів, намагаючись відгадати пароль доступу до віддаленого облікового запису.

3. Фішинг: атаки фішингу можуть спрямовуватися на користувачів, які використовують віддалений доступ, з метою отримання їхніх облікових даних шляхом підмановання їх до натискання на шкідливі посилання або завантаження шкідливих вкладень.

4. Використання слабкостей програмного забезпечення: зловмисники можуть використовувати відомі або невідомі вразливості в програмному забезпеченні, що використовується для віддаленого доступу, для отримання несанкціонованого доступу до системи.

5. Перехоплення сесії (Session Hijacking): зловмисники можуть намагатися використовувати вразливості в мережевих протоколах або програмах для перехоплення сесії віддаленого доступу та отримання контролю над ним.

6. Атаки з використанням вразливостей в програмному забезпеченні: зловмисники можуть експлуатувати вразливості в програмному забезпеченні VPN клієнтів або серверів для отримання несанкціонованого доступу.

На сьогоднішній день найбільш популярні протоколи VPN наступні:

1. OpenVPN - відкритий протокол, який широко використовується для своєї надійності та безпеки. Він працює на основі SSL/TLS і підтримує різні типи шифрування.

2. L2TP/IPsec (Layer 2 Tunneling Protocol over IPsec) комбінує переваги IPsec для забезпечення безпеки та L2TP для створення тунелю. Цей протокол часто використовується на мобільних пристроях.

3. WireGuard вважається одним з найшвидших та найпростіших у використанні протоколів VPN. Він має менше коду порівняно з іншими протоколами, що сприяє зменшенню можливостей для вразливостей.

4. SSTP (Secure Socket Tunneling Protocol) - це інший протокол VPN, який забезпечує безпеку при передачі даних через віддалені з'єднання. Він розроблений компанією Microsoft і використовує SSL для шифрування трафіку між клієнтом і сервером

Якщо порівнювати OpenVPN з іншими протоколами VPN, то можна виділити наступне:

1. Безпека. OpenVPN забезпечує високий рівень безпеки завдяки шифруванню трафіку за допомогою сильних алгоритмів ідентифікації та шифрування. Він використовує SSL/TLS для аутентифікації і обміну ключами, що робить його дуже відповідним для захисту конфіденційності даних під час передачі через незахищені мережі.

2. Гнучкість. OpenVPN може працювати на різних портах і протоколах, що дозволяє йому обходити обмеження мережі та брандмауери. Він також підтримує різні методи аутентифікації, включаючи пароль, сертифікати та двофакторну аутентифікацію.

3. Швидкодія. Зазвичай OpenVPN забезпечує хорошу швидкодію, але в порівнянні з деякими іншими протоколами, такими як WireGuard, він може мати трохи більший наклад через складніші механізми шифрування.

4. Підтримка. OpenVPN підтримується на багатьох платформах, включаючи Windows, macOS, Linux, Android та iOS. Це робить його дуже універсальним і зручним для використання на різних пристроях та операційних системах.

Отже, якщо врахувати вищезазначені переваги, OpenVPN може бути вважаний одним із найбільш захищених та універсальних протоколів VPN, здатний забезпечити безпеку та приватність під час віддаленого доступу до корпоративних мереж.

Структурна схема системи віддаленого доступу наведена на рис. 1.

Вихід в інтернет здійснюється через головний маршрутизатор з білою IP адресою. Функції обробки запитів та безпеки покладено на OpenVPN сервер, який працює по протоколу UDP за допомогою тунельного (TUN) драйверу. На головному маршрутизаторі UDP порт 1194 (стандартний порт OpenVPN, для безпеки або приховування та маскуванню трафіку може бути змінений на будь-який інший, наприклад,

443) прокинуто у внутрішню мережу до сервера віддаленого доступу, на якому налаштовано маршрутизацію трафіку. Віддалені користувачі, у залежності від задач, можуть підключатися до віддаленого робочого столу до своїх власних робочих комп'ютерів або до термінальних серверів. При даній реалізації трафік проходить через тунель з шифруванням та відсутнє програмне забезпечення сторонніх розробників із закритим кодом, а також відсутній протокол RDP із прямим виходом у глобальну мережу.

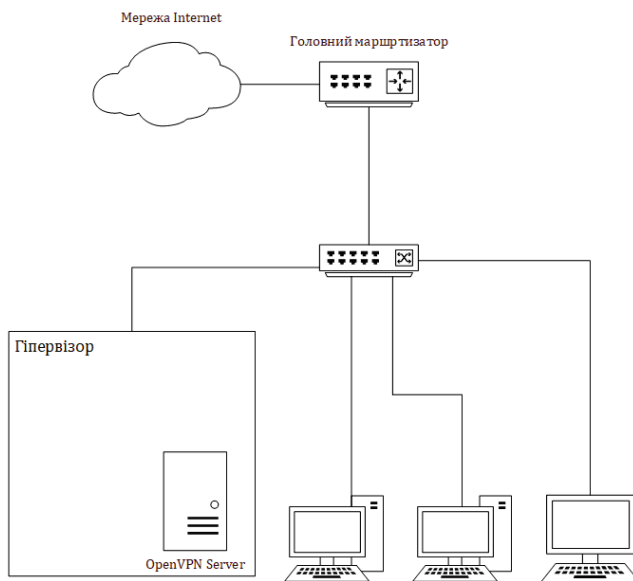


Рисунок 2.1 – Структурна схема системи

**Висновки.** Досліджено та проаналізовано питання безпеки під час використання віддаленого доступу до корпоративних мереж. Визначено основні загрози та ризики, пов'язані з цим процесом, а також розглянуто методи та стратегії захисту. Обрано OpenVPN як протокол VPN для забезпечення безпеки віддаленого доступу. OpenVPN відомий своєю надійністю, гнучкістю та високим рівнем шифрування, що робить його відмінним вибором для організацій, які прагнуть захистити свої корпоративні мережі під час віддаленої роботи.

Враховуючи усі аспекти слід зазначити, що ефективна інформаційна безпека віддаленого доступу до корпоративних мереж є важливою складовою для забезпечення безпеки та захисту конфіденційної інформації. Використання правильних інструментів та стратегій захисту, таких як OpenVPN, може допомогти організаціям забезпечити безпеку своїх даних у віддаленому режимі роботи.

**Список літератури:**

1. Александр Харкер. "OpenVPN Cookbook". Packt Publishing, 2017.
2. Майк Черчілло. "Mastering OpenVPN". Packt Publishing, 2015.
3. Майк МакКінлі. "OpenVPN: Building and Integrating Virtual Private Networks". O'Reilly Media, 2006.
4. Ерік Форті. "Virtual Private Networks, Second Edition". O'Reilly Media, 2005
5. Джон Вілкс. "SSL and TLS: Theory and Practice". Addison-Wesley Professional, 2009.
6. Найден Хібберт. "The Official (ISC)2 Guide to the CISSP CBK Reference, Fifth Edition". Sybex, 2019.
7. Хільбрукс Д.М., Сілва Л.М. "Кібербезпека: підручник". Видавництво КНЕУ, 2019.
8. Артем Остапець. "Безпека інформаційних технологій". Видавництво Національного університету "Львівська політехніка", 2018.
9. Дуглас Е. Комер. "Криптографія і безпека комп'ютерних мереж". Видавництво "ТОРСІНГ Плюс", 2019.
10. Б. Шнайдер. "SSL/TLS Essentials: Securing the Web". O'Reilly Media, 2000.

УДК 621.318; 004.056

## ЗАГРОЗИ ГЛОБАЛЬНІЙ МАРШРУТИЗАЦІЇ В СУЧАСНОМУ КІБЕРПРОСТОРІ

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

На даний час наявна тенденція до поширення практики зберігання даних окремими особами і організаціями в банках даних і хмарах, зростання кількості онлайн-сервісів та загального обсягу адресного передавання даних через Інтернет, який є незахищеним середовищем і регулюється тільки системою глобальної маршрутизації, на яку зловмисниками здійснюються тисячі атак щорічно [1].

Метою даної є розробка класифікації загроз глобальної маршрутизації.

Для досягнення поставленої мети необхідно шляхом аналізу відкритих літературних джерел визначити загрози та ризики глобальної маршрутизації, їх особливості та взаємозв'язки.

Прикладами інцидентів в системі глобальної маршрутизації є [2, 3]:

- 2018 рік: атака «викрадання префіксу» хмарного сервісу Amazon AWS і до якого були прив'язані його DNS сервери. Тривалість атаки – кілька годин. Метою викрадання інфраструктурного IP-префіксу Amazon AWS була фішингова атака на криптовалютний сервіс MyEtherWallet. В процесі атаки DNS-запити користувачів, що використовували DNS-сервери Amazon AWS, перенаправлялися на DNS-сервер зловмисників, де імена хостів з суфіксом, що відповідав криптовалютному сервісу, підмінялися IP-адресами фішингових сайтів, які працювали за протоколом HTTP і, на відміну від HTTPS, не дозволяли провести автентифікацію сервера. В результаті було викрадено значну кількість криптовалют і скомпроментовано дані користувачів;

- 2018 рік: збій в BGP-маршрутизації, що спричинив DoS-ефект щонайменше протягом 74 хвилин для таких сервісів Google як G Suite, Google Пошук і Google Аналітика, для внутрішніх систем Google і для сторонніх сервісів, в тому числі Spotify. Причиною збою стало анонсування 212 префіксів, що належали дата-центрам Google, невеликим нігерійським провайдером MainOne Cable Company сусіднім провай-

дерам. Хибна інформація поширилася серед інших провайдерів, один з яких – державний китайський провайдер China Telecom передав транзитом анонси до інших мереж, але сам зафільтрував трафік, що надходив до Google цими маршрутами. Тоді аналітики компанії Oracle і фахівці ряд дослідників США та Ізраїлю звинуватили China Telecom в навмисному улаштуванні BGP-збоїв і навмисно некоректній передачі трафіку західних країн;

– 2022 рік: крадіжка префіксів BGP, які належали південно-кореєській криптовалютній платформі, і крадіжка префіксу, який використовував Twitter. Префікс криптовалютної платформи було використано зловмисниками для крадіжки криптовалюти на суму 1,9 мільйона доларів шляхом видачі сертифікату на домен через ZeroSSL для обслуговування шкідливого файлу JavaScript;

– 2023 рік: були виявлені три нові уразливості в програмній реалізації протоколу BGP, які зловмисник може використати для організації DoS-атак на вразливі вузли BGP. Аналіз семи реалізацій BGP показав, що у версії 8.4 FRRouting, що є поширеним набором протоколів маршрутизації з відкритим кодом для платформ Linux і Unix і використовується декількома провайдерами, що створює умови для ланцюгової реакції збоїв, містяться вразливості читання поза межами під час обробки неправильно сформованого повідомлення BGP OPEN із опцією Extended Optional Parameters Length (CVE-2022-40302 (оцінка CVSS: 6,5) і CVE-2022-40318 (оцінка CVSS: 6,5)) та неправильно сформованого повідомлення BGP OPEN, яке раптово закінчується октетом довжини опції (CVE-2022-43681 (оцінка CVSS: 6,5)). Ці вразливості зловмисники можуть використати для досягнення умови DoS для вразливих однорангових вузлів BGP, припиняючи таким чином всі сеанси BGP, викривлюючи таблиці маршрутизації та переставляючи одноранговий пристрій на реакцію. При цьому стан DoS може бути продовжений на невизначений термін шляхом повторного надсилання неправильно сформованих пакетів. Крім того, зловмисник може підробити дійсну IP-адресу довіреного однорангового вузла BGP або використати інші недоліки та неправильні конфігурації, щоб скомпрометувати законний одноранговий вузол, а потім видати спеціально створене небажане повідомлення

BGP OPEN. Це досягається завдяки тому, що FRRouting починає обробляти повідомлення OPEN (наприклад, декапсуляцію додаткових параметрів) до того, як він отримає можливість перевірити ідентифікатор BGP і поля ASN вихідного маршрутизатора;

- 2023 рік: словацька компанія ESET (розробник NOD32 Antivirus) виявила, що старі маршрутизатори, які раніше використовувалися в бізнес-мережових середовищах, зберігають конфіденційні дані, включаючи корпоративні облікові дані, деталі VPN, криптографічні ключі та іншу важливу інформацію про клієнтів. Дані, зібрані із старих маршрутизаторів, включаючи дані клієнтів, ключі автентифікації між маршрутизаторами, списки програм та ін. є достатніми для кібератаки.

Причини поширення атак на глобальну маршрутизацію у сучасному кіберпросторі:

- ефект ланцюгової реакції – проблеми одного провайдера швидко поширюються на інших;

- теоретично необмежений вплив на мережу – помилки в адресації, допущені оператором чи провайдером або спричинені діями зловмисників за ланцюговою реакцією розповсюджуються на інших;

- висока ймовірність наявності недоліків налаштування роутерів, зокрема підтримки в діючому стані фільтрів маршрутів, хоча б одним провайдером;

- здатність атак на глобальну маршрутизацію завдати шкоди у великих масштабах – мільйонам мережових пристроїв та користувачів. В останні роки інциденти, пов'язані із глобальною маршрутизацією за масштабом перевищують розповсюджені DDoS-атаки на кілька порядків;

- відносна «дешевизна» атак на глобальну маршрутизацію порівняно із розподіленими атаками на відмову в обслуговуванні (DDoS) і використанням програм-вимагачів (Ransomware);

- наявність уразливостей у базових протоколах глобальної маршрутизації;

- складність усунення проблем глобальної маршрутизації, що вимагає узгодження дій в ідеалі всіх провайдерів і операторів.

Серед інцидентів інцидентів глобальної маршрутизації можна виділити типові атаки, наведені в табл.1 і комплексні атаки на базі по-

рушення безпеки глобальної маршрутизації, яке може створювати умови успішної реалізації зловмисником DDoS атак або відслідковування трафіку.

Таблиця 1 – Типові загрози глобальній маршрутизації

| № | Назва                                                | Зміст                                                                                                                                                                                          | Наслідки                                                                                       |
|---|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| 1 | "Викрадення" префіксів / маршрутів (route hijacking) | Оператор або зловмисник видає себе за іншу мережу, імітуючи, що сервер або мережа – це їх клієнт                                                                                               | Пакети направляються за хибною адресою, що може спричинити DDoS-ефект або перехоплення трафіку |
| 2 | Витік маршрутів (route leaks)                        | Оператор через кілька апстрімів (часто через випадкову неправильну конфігурацію) анонсує одному апстрім-провайдеру, що в нього є маршрут до пункту призначення через іншого апстрім-провайдера | Може використовуватися для відслідковування та перехоплення трафіку                            |
| 3 | Підrobка IP адрес (IP address spoofing)              | Зловмисник створює пакети з підrobною IP адресою джерела, щоб унеможливити ідентифікацію відправника або видати себе за іншу автономну систему (AS)                                            | Передумова створення DDoS атак                                                                 |

При аналізі ризиків, пов'язаних із загрозами системі глобальної маршрутизації приймаються до уваги умови (сценарії) і ймовірності виникнення загроз та можливі наслідки реалізації загроз (табл..2), тяжкість яких залежить від параметрів автономної системи-жертви.

Таблиця 2 – Умови, ймовірності і наслідки атак

| Атака                      | Ймовірність | Умови                                                                                                                                                                                                                                                                              | Наслідки                                                                                                                                                                                                                                                                  |
|----------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Відмова в обслуговуванні   | Дуже висока | Зловмисник має можливість:<br>1) перехопити маршрути;<br>2) створити чорну діру;<br>3) спрямувати увесь трафік, який адресований жертві, або його частину у чорну діру.<br>Не потребує отримання та аналізу трафіку                                                                | Порушення доступності.                                                                                                                                                                                                                                                    |
| Підміна мережевих об'єктів | Висока      | Зловмисник має можливість реалізувати наступний алгоритм:<br>1) IP-адреси мережі жертви присвоюються іншим мережевим пристроям, якими керує зловмисник;<br>2) зловмисник анонсує IP-адреси жертви так, щоб новий хибний маршрут мав вищий пріоритет порівняно з істинним маршрутом | Зловмисник набуває можливості скоювати певні дії в мережі з власних мережевих пристроїв, маскуючи їх під пристрої жертви (у граничному випадку – ініціювати та приймати повноцінні сесії клієнт-сервер). Реалізація цієї атаки створює умови для виникнення інших загроз. |

| Атака                   | Ймовірність | Умови                                                                                                                                                                                                                                                                     | Наслідки                                                                                                                                                             |
|-------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Розголошення інформації | Висока      | Зловмисник має можливість:<br>1) перехопити трафік;<br>2) провести аналіз трафіку і визначити особливості побудови мережних протоколів рівня застосувань;<br>3) повернути трафік в мережу з метою маскування                                                              | Порушення конфіденційності                                                                                                                                           |
| Модифікація даних       | Середня     | Зловмисник має можливість:<br>1) створити хибний анонс;<br>2) перехопити трафік;<br>3) модифікувати трафік;<br>4) повернути модифікований трафік в Інтернет з метою доставки істинному адресату.<br>Така атака може відбуватись з підміною мережних об'єктів або без неї. | Порушення цілісності даних. Якщо зловмисник має можливість модифікувати дані, то він також може прослуховувати трафік, аналізувати його, впроваджувати шкідливий код |
| Відмова від авторства   |             | Зловмисник має можливість реалізувати підміну мережних об'єктів                                                                                                                                                                                                           | Відмова від авторства, маскування                                                                                                                                    |

Порушення безпеки глобальної маршрутизації можливе завдяки наявності вразливостей протоколів маршрутизації. Відповідно, загрози глобальної маршрутизації можуть бути класифіковані за протоко-

лами, типами протоколів, вразливості яких спричинили появу загрози, і за самими протоколами, BGP, BGPsec тощо.

Прикладом уразливостей безпеки BGP є фальшиві оновлення маршрутизації, що призводять до викрадення та перехоплення трафіку [4], яке може бути реалізоване різними методами, що також є критерієм класифікації атак:

- захоплення префіксу: вузол анонсує чужий префікс, тобто у якості джерела вказує адресний простір, який йому не належить. Якщо фіктивний маршрут буде кротким, то BGP при виборі маршруту віддасть перевагу самк йому. Така атака може бути досить швидко виявлена за наявністю двох джерел з однаковим префіксом, що є помилкою у глобальній маршрутизації;

- захоплення маршруту: вузол легально отримує анонс чужого адресного простору і ретранслює його, пропонуючи транзит через себе. В цьому випадку хибний маршрут також конкурує з істинним, однак виявити захоплення маршруту важчк, ніж захоплення префіксу, бо джерело є істинним і не дублюється;

- захоплення підмереж: вузол ділить чужий адресний простір на дрібніші підмережі і анонсує їх специфічні префікси. Якщо конкуруючі префікси такого ж розміру відсутні, то аносування більш специфічних префіксів має глобальний ефект, оскільки BGP при виборі маршруту віддає їм перевагу. Таким чином зловмисник, незважаючи на реальну топологічну віддаленість стає вузлом маршруту, який помилково вважається оптимальним;

- захоплення нерозподіленого або невикористаного адресного простору: зловмисник анонсує префікси нерозподіленого або невикористаного адресного простору, які не співпадають з іншими префіксами і тому не фільтруються, тобто мають змогу поширитися по всій мережі Інтернет. Захоплення нерозподіленого або невикористаного адресного простору може бути використане для короткострокової генерації довільного трафіку, в тому числі – для доставки шкідливого контенту, наприклад спаму. За більш складним сценарієм атаки перехоплений трафік спочатку використовується зловмисником для виконання певних дій (прослуховування, аналіз, модифікації даних), а потім повертається назад у мережу. При поверненні у мережу прослуханий, проаналізований чи содифікований трафік може просуватись далі легітимним маршрутом.

Перехоплення IP-адреси може статися випадково або може бути скоєне навмисно одним з перелічених вище способів, спільним для яких є отримуваний результат – пересилання процесів у невірну або тупикову частину мережі та порушення нормального процесу маршрутизації в мережі. Пакети, що потрапляють у неправильну частину мережі, потім або потрапляють у нескінченний цикл (і відкидаються), або опиняються у власності зловмисника. За фактом порушення доступності така атака може бути ідентифікована.

Зазвичай інтернет-провайдери фільтрують трафік BGP, дозволяючи оголошенням BGP зі своїх мереж містити тільки дійсний простір IP-адрес, однак на практиці можливі виключення.

Ризики глобальної маршрутизації мають ряд особливостей:

- загрози, з якими вони асоціюються, зазвичай виникають як результат навмисної діяльності або випадкових помилок суб'єктів глобальної маршрутизації (загрози типів A і D за ДСТУ ISO/IEC 27005:2023 [7]). Тобто, загрози природного походження (тип E) практично не аналізуються [2-6];

- вразливості, експлуатація яких дозволяє цим загрозам бути успішно реалізованими, є недоліками протоколів маршрутизації і/або недоліками налаштувань роутерів;

- наслідки реалізації цих загроз утворюють ієрархічну систему: на першому рівні – зміни в глобальній таблиці маршрутизації або її хибна інтерпретація, на другому рівні – несанкціонована зміна напрямку проходження мережевого трафіку, на третьому рівні – можливі дії зловмисника, який отримав доступ до трафіку (блокування трафіку чи його частини, модифікація даних тощо), на четвертому рівні результати певних дій зловмисника над трафіком (DDoS, спрямування на фальсифікований сайт, розсилання спаму тощо), на п'ятому рівні – наслідки для AS, на шостому рівні – наслідки для бізнес-процесів.

### **Висновки**

В даній роботі проведено аналіз відкритих літературних джерел і визначені загрози та ризики глобальної маршрутизації, їх особливості та взаємозв'язки, розроблена класифікація загроз глобальній маршрутизації, показано, що порушення безпеки глобальної ма-

ршрутизації становить глобальну загрозу в сучасному кіберпросторі, з якою пов'язані ризики, що мають тенденцію до зростання.

Ризики глобальної маршрутизації можуть мати негативний вплив на бізнес- процеси і спілкування в мережі, особливо, якщо постачальники мережевих послуг (постачальники підключень, хмари та мережі доставки контенту) не приділяють достатньо уваги захисту процесів маршрутизації, не впроваджують новітні методи безпеки маршрутизації. Оскільки нормативні документи наявні тільки для протоколів маршрутизації, то єдиним способом запобігти ризикам глобальної маршрутизації на даний час є приєднання до спільноти MANRS [1], дотримання і популяризація її рекомендацій, застосування новітніх способів маршрутизації [6, 8].

#### **Список літератури:**

1. MANRS: Protect the Internet URL: <https://www.manrs.org/>
2. 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>
3. 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](https://ipme.kiev.ua/wp-content/uploads/2022/07/Zubok_Mokhor_Kiberbezpeka_Topologii_Internet.pdf)
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. Чакрян В.Х. Моделі та методи маршрутизації трафіку в телекомунікаційних мережах з урахуванням вимог інформаційної безпеки. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.12.02 «Телекомунікаційні системи та мережі» (172 – Телекомунікації та радіотехніка). – Харківський національний університет радіоелектроніки, Харків, 2017. URL: [https://nure.ua/wp-content/uploads/2018/Dissertation/diss\\_Chakryan.pdf](https://nure.ua/wp-content/uploads/2018/Dissertation/diss_Chakryan.pdf)

7. 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](https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400)

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

**УДК 004.056.52:53**

## **РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ РЕЖИМНО-СЕКРЕТНОГО ВІДДІЛУ МОРСЬКОГО ПОРТУ**

***Автор:** Харченко М.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**

Забезпечення інформаційної безпеки держави стоїть на одному рівні із захистом територіальної цілісності України та захистом суверенітету, як найважливішими функціями держави. Державна політика забезпечення інформаційної безпеки України є невіддільною частиною державної політики у сфері національної безпеки і оборони України. Інформаційна безпека полягає в аналізі загроз, які можуть виникнути в інформаційній сфері, і створенні умов для запобігання їхньому виникненню.

Аналіз, оцінка та використання позитивних здобутків країн ЄС та НАТО мають важливе значення при розбудові системи забезпечення інформаційної безпеки України, адже нині наша країна стикається з новими викликами та загрозами в інформаційній сфері та перебуває на

стадії становлення інформаційного суспільства, яка супроводжується стрімким розвитком інформаційної інфраструктури. Вивчення практики країн ЄС та НАТО у побудові власних моделей правового забезпечення інформаційної безпеки, протидії кіберзагрозам, а також аналіз ряду міжнародних правових документів дає змогу нам резюмувати відсутність єдиної унікальної моделі національної системи правового забезпечення інформаційної безпеки.

### **Вступ**

Водно-транспортний комплекс (ВТК) України є важливою складовою національної економіки. Порушення безпеки портів може не тільки спричинити значні економічні збитки, але й негативно вплинути на міжнародний імідж країни. Тому розробка та реалізація цілеспрямованої та системної політики захисту інформації від зовнішніх та внутрішніх інформаційних загроз є актуальним питанням для підприємств портової галузі (ПГ), вирішення якого безпосередньо пов'язане з розробкою та затвердженням процедур підготовки КСЗІ. Різні аспекти цього питання розглядалися низкою науковців.

При проектуванні та будівництві нових портових телекомунікацій необхідно впроваджувати заходи захисту інформації за перевіреними, єдиними процедурами, але також необхідно передбачити можливість розробки КСЗІ в процесі розвитку та вдосконалення портової інфраструктури, ІКС, виробничих потужностей та нормативно-правової бази, але наразі такі єдині процедури не передбачені.

**Метою роботи** є розробка шаблону КСЗІ для режимно-секретного органу з урахуванням міжнародного досвіду та галузевих особливостей інформаційної безпеки.

Для досягнення цієї мети були визначені наступні завдання:

- Аналіз нормативно-правової та законодавчої бази України по створенню КСЗІ на об'єктах інформаційної діяльності критичної інфраструктури;
- Аналіз досвіду побудови систем інформаційної безпеки для об'єктів ВТК в ЄС та США;
- Аналіз методи та принципи побудови КСЗІ на об'єкті інформаційної діяльності критичної інфраструктури;
- Розробка шаблону КСЗІ в РСО морського порту.

## **1. Нормативно-правової та законодавчої бази України по створенню КСЗІ**

Нормативно-правовою базою щодо захисту інформації та створення КСЗІ АС 1 класу є Закони України «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах» та інші, державні стандарти «3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення» та нормативні документи системи ТЗІ в Україні, а також застосування нормативних документів, що відносяться до об'єктів критичної інфраструктури такий як Наказ Адміністрації Держспецзв'язку «Про затвердження форми Плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент» від 04 жовтня 2023 року №877»

## **2. Досвід побудови систем інформаційної безпеки для об'єктів ВТК в ЄС та США**

У 1991 році був розроблений «Європейський стандарт з безпеки інформаційних технологій», в якому конкретно розглядалося питання забезпечення інформаційної безпеки шляхом:

- захисту інформаційних ресурсів від несанкціонованого доступу та забезпечення їх конфіденційності;
- забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої зміни або знищення;
- забезпечення доступності системи від загроз відмови в обслуговуванні.

Важливу роль у правовому регулюванні ІБ США відіграє Закон про інформаційну безпеку. Його метою є «здійснення мінімальних дій, достатніх, без обмеження всіх можливих дій, для забезпечення безпеки інформації в комп'ютерних системах федерального уряду». Закон передбачає, що Національний інститут стандартів і технологій відповідає за видання стандартів і керівних принципів, спрямованих на захист інформації від знищення і несанкціонованого доступу.

### **3. Методи та принципи побудови КСЗІ на об'єкті інформаційної діяльності критичної інфраструктури**

Реалізація функцій захисту досягається шляхом використання об'єднаних в єдину систему вбудованих послуг безпеки операційних систем робочих станцій, сертифікованих криптографічних засобів захисту, можливостей спеціалізованого і антивірусного програмного забезпечення, а також шляхом виконання спеціальних організаційних, інженерних та технологічних заходів із захисту інформації. Компоненти комплексу програмно-апаратних засобів ІТС, що беруть участь в реалізації політики безпеки інформації є складовими КСЗІ ІТС.

Захист інформації в розподілених інформаційно-телекомунікаційних системах є складною системною задачею, яка вимагає застосування комплексу інженерно-технічних, криптографічних, апаратно-програмних та організаційних заходів захисту.

### **4. Особливості формування шаблону КСЗІ в РСО морського порту**

Для організації робіт зі створення КСЗІ в ІКС створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000.

Організаційні заходи є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності.

У разі необхідності, в рамках проведення організаційних заходів може бути створена служба ІБ, проведена реорганізація системи діловодства та зберігання документів. Інженерно-технічні заходи – сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити.

### **Висновки**

Загроза національній безпеці держави в інформаційній сфері – будь-яка сукупність умов і факторів, що створюють загрозу життєво важливим інтересам держави, суспільства та інших осіб у зв'язку з можливістю негативного інформаційного впливу на свідомість і поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру.

В даній роботі було проведено:

- аналіз нормативно-правової та законодавчої бази України по створенню КСЗІ на об'єктах інформаційної діяльності критичної інфраструктури;

- аналіз досвіду побудови систем інформаційної безпеки для об'єктів ВТК в ЄС та США;
- аналіз методи та принципи побудови КСЗІ на об'єкті інформаційної діяльності критичної інфраструктури;
- розробка шаблону КСЗІ в РСО морського порту.

#### **Список літератури:**

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 №80/94-ВР. [Ел. ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text>
2. Про захист персональних даних: Закон України від 01.06.2010 №2297-VI. [Ел. ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>.
3. Почепцов Г. Г. Інформаційна політика / Г. Г. Почепцов, С. А. Чукут // Навчальний посібник. 2-ге вид., стер. – К.: Знання, 2008. – 663 с. – (Вища освіта ХХІ століття).
4. Конституція України: Верховна Рада України; Конституція України, Конституція, Закон від 28.06.1996 № 254к/96-ВР [Ел. ресурс]. – URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>
5. Про національну безпеку України: Закон України від 21.06.2018 №2496-VIII. [Ел. ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>.

**УДК 004.056.52:53**

### **РОЗРОБКА РЕКОМЕНДАЦІЙ ПО ВДОСКОНАЛЕННЮ ЄДИНОГО ЕЛЕКТРОННОГО РЕЄСТРУ «ОБЕРІГ»**

***Автор:** Харченко С.М., 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**

Документообіг та система реєстрації військовозобов'язаних мають важливе значення для забезпечення національної безпеки та оборони. Використання єдиного державного реєстру призовників, війсь-

ковозобов'язаних та резервів є ключовим елементом організації та управління цими процесами.

### **Вступ**

Вже другий рік в Україні проводиться мобілізація. Вона показала ряд проблем і недоліків при роботі ведення та обліку особистих даних. Основна задача, яка стає перед державою питання призову, яким займається ТЦК та СП. Під час повномасштабного вторгнення показали негативні факти перед суспільством – це корупційні прояви та зловживання при призові з боку посадових осіб в окремих регіонах, зменшення кількості бажаючих захищати Вітчизну через відтік за кордон т.д

Для вирішення цих проблем розроблено та запроваджено реєстр "ОБЕРІГ", який дозволить підвищити прозорість та ефективність призову, уникнути зловживань та порушень прав призовників.

Проте в структурі та функціонуванні реєстру залишаються певні недоліки, зокрема щодо захисту персональних даних, неузгодженості з іншими базами даних, складнощів доступу для військоматів тощо. З основних проблем, які замічені під час роботи операторами були – це постійна недоступність серверів, неможливість внесення певних особистих даних до реєстру. До неосновних проблем можна віднести грама-тичні помилки та використання російської мови при появі помилки.

### **Мета та задачі**

Метою цієї роботи є розробка рекомендацій щодо подальшого вдосконалення системи «ОБЕРІГ» шляхом підвищення точності, релевантності та зручності системи для користувачів.

Для досягнення вищезазначеної мети вирішувались наступні завдання:

1. Проведення аналізу поточний стан системи «ОБЕРІГ».
2. Виявлення основних проблем та недоліків системи.
3. Розроблення пропозиції щодо вдосконалення системи та визначення шляхів подальшого розвитку і вдосконалення системи.

### **1. Аналіз поточного стану системи «ОБЕРІГ»**

Єдиний державний реєстр військовозобов'язаних (далі Реєстр ) – автоматизована інформаційно-телекомунікаційна система, призначена для збирання, зберігання, обробки та використання даних про військо-вобов'язаних (призовників), створена для забезпечення військового обліку громадян України [1] .

Основні завдання Реєстру :

- Ведення військового обліку громадян України – військовозобов'язаних (призовників);
- Планування та виконання заходів з мобілізації, призову на строкову військову службу за контрактом
- Інформаційне забезпечення осіб, звільнених з військової служби, які мають право на пенсію, та членів сімей загиблих військовослужбовців відомостями щодо військового обліку.

Метою реформи військкоматів є насамперед переформатування «військових комісаріатів» на «територіальні центри комплектування та соціальної підтримки». Основною метою таких центрів є створення прозорої системи надання сервісних адміністративних послуг щодо соціального і правового захисту військовозобов'язаним, резервістам, ветеранам війни та військової служби, пенсіонерам з числа військовослужбовців Збройних сил України та членам їхніх сімей, яка здійснюватиметься за системою «єдиного вікна».

Для реалізації поставленої мети був створений Єдиний державний реєстр призовників, військовозобов'язаних і резервістів є автоматизованою інформаційно-комунікаційною системою, яка призначена для збирання, зберігання, обробки та використання даних про військовозобов'язаних (призовників), створена для забезпечення військового обліку громадян.

## **2. Аналіз основних проблем та недоліків системи**

Автоматизована система обробки інформації «ОБЕРІГ» є АС 1 класу. Система «ОБЕРІГ» вирізняється своєю комплексністю та високою ефективністю в області забезпечення безпеки об'єктів. З її чіткою структурою, що складається з функціональних модулів, система забезпечує ефективне взаємодію та функціонування. Ця система має велике значення цифровізації в галузі військового реєстру. Її функціонал дозволяє вчасно виявляти потенційні загрози та приймати необхідні заходи для їх усунення, що робить її ефективним інструментом для збереження майна та інформації [2].

Переваги системи включають можливість ефективного контролю за військовозобов'язаними, облік їх особистих даних та забезпечення єдиної інформації для прийняття важливих рішень. Також важливою є

можливість інтеграції з іншими системами, що підсилює цілісність та доступність даних.

У загальному, функціонування системи «ОБЕРІГ» є не лише необхідним, а й ефективним інструментом для держави у забезпеченні військової готовності та національної безпеки.

Проблеми, які потрібно вирішити першим ділом для зручності користувачів системи – це:

а) Відсутність можливості редагування поля 23 «призовною комісією призваний на строкову службу (зарахований в запас)».

б) У разі виключення з військового обліку за станом здоров'я не передбачено розбіжність між дати виключення та датою медичного огляду.

в) У розділі «Освіта» не вистачає деяких варіантів застарілих або новітніх ступенів освіти (фахова передвища, неповна вища, базова вища, Молодший бакалавр, кандидат/ доктора наук).

г) У розділі медогляд пункт «Наказ МОУ від\*» не вистачає деяких застарілих наказів про затвердження Положення про ВЛК в ЗС України (за 1997 р. тощо ).

### **3. Пропозиції щодо вдосконалення системи.**

Вирішення вищезазначених проблем буде доповнення додаткових полів наприклад проблема б) має рішення передбачення доповнення додаткового поля «Дата виключення з військового обліку» у відповідному розділі «Виключення з обліку» – «визнані ВЛК не придатними до військової служби з виключенням з військового обліку (ВО)» та інші.

### **4. Шляхи подальшого розвитку і вдосконалення системи.**

Вдосконалення Безпеки та Конфіденційності:

- вдосконалення заходів безпеки та захисту даних для уникнення можливого несанкціонованого доступу або витоку конфіденційної інформації;
- розширення функціональності;
- розгляд можливості розширення функціональності реєстру для включення додаткової інформації, яка може бути корисною для ефективного використання даних;
- використання технологій штучного інтелекту (ШІ);
- впровадження технологій ШІ для аналізу та обробки великої кількості даних, що може полегшити прийняття рішень та покращити ефективність системи;
- міжсекторальна співпраця;

- розгляд можливостей співпраці з іншими галузями та агентствами для обміну інформацією та вдосконалення координації;
- регулярне оновлення та підтримка;
- забезпечення регулярного оновлення системи, включаючи програмне та апаратне забезпечення, для забезпечення актуальності та функціональності;
- залучення громадськості;
- залучення громадськості у процес розвитку та вдосконалення реєстру, сприяючи більшій відкритості та взаєморозумінню;
- тестування та захист від атак;
- проведення систематичних тестів безпеки для виявлення потенційних слабких місць та застосування заходів для захисту від можливих кібератак;
- регулярні аудити та оцінки;
- проведення регулярних аудитів та оцінок для перевірки ефективності та відповідності реєстру стандартам безпеки та законодавству.

Ці заходи можуть сприяти подальшому вдосконаленню та розвитку реєстру військовозобов'язаних «ОБЕРІГ» і покращенню його функціональності та ефективності.

### **Висновки**

Під час проведення аналізу поточний стан системи «ОБЕРІГ» було встановлено, що система має велике значення для цифровізації в галузі військового реєстру. Та визначили, що її функціонал дозволяє вчасно виявляти потенційні загрози та приймати необхідні заходи для їх усунення, що робить її ефективним інструментом для збереження майна та інформації.

Під час роботи пункту було встановлено, що система має певні проблеми, які заважають виконувати функцію обробки та захист даних – це використання російського коду під час розробки реєстру та недоступність серверів.

Є певна упевненість у тому, що запропоновані зміни та вдосконалення внесуть позитивний внесок у роботу «ОБЕРІГ», сприяючи вдосконаленню обліку та управління військовозобов'язаними.

**Список літератури:**

1. Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів Відомості Верховної Ради (ВВР), 2017, № 18, ст.217 – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1951-19#Text>
2. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-99 [Електронний ресурс]. – Режим доступу: <https://www.tzi.ua/assets/files/НД-ТЗІ-2.5-005-99.pdf>

## СЕКЦІЯ 4. МОДЕЛЮВАННЯ ОБ'ЄКТІВ І ПРОЦЕСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.53: 534.8/78

### ФАКТОРИ, ЩО ВПЛИВАЮТЬ НА РОЗБІРЛИВІСТЬ МОВИ

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

*Науковий керівник: Касьянов Ю.І., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

**Вступ.** В епоху технологічних зрушень та глобалізації, де весь світ стає взаємопов'язаним, роль комунікації стає не тільки важливою, але й критичною для успіху та розвитку різних аспектів життя. Комунікація перетворилася з простого інструменту передачі інформації в суттєву основу для розвитку суспільства, бізнесу, науки та міжнародних відносин. Внаслідок чого захист мовної інформації також має велику значимість.

Наразі існує велика кількість засобів захисту інформації від витoku акустичним каналом, так само як і засобів перехоплення мовлених повідомлень, однак не слід забувати, що за технікою вперш за все стоїть людина. Отже у питанні захисту інформації також слід враховувати ті фактори, що впливають на розбірливість мови, які залежать від слухача.

**Мета** роботи полягає в дослідженні факторів, що впливають на розбірливість мови, для подальшого включення їх впливу у методику оцінювання захищеності мовної інформації формантним методом.

**Основна частина.** Спершу слід зазначити, що мається на увазі під фразою «розбірливість мови». Згідно з міжнародними стандартами, зокрема ISO/TR 4870 [1], під розбірливістю мови розуміється «ступінь, з якою мова може бути зрозуміла (розшифрована) слухачами». Попередні дослідження, які проводилися з цього питання, виявили, що на розбірливість мови впливає багато факторів. Рисунок 1 узагальнює деякі найбільш популярні фактори, які було виявлено [2].

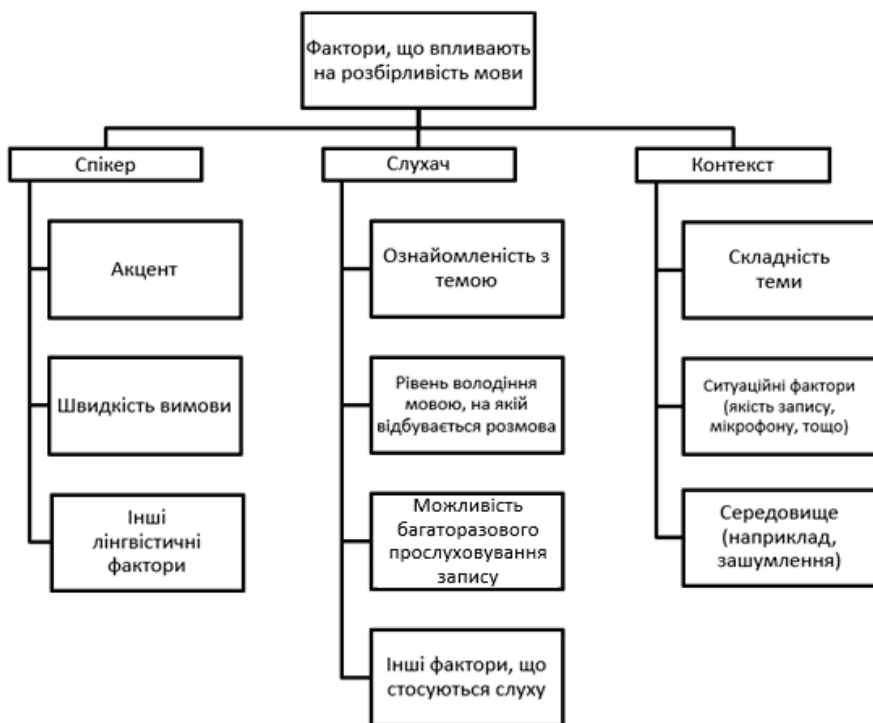


Рисунок 1 – Фактори, що впливають на розбірливість мови

В контексті подальших досліджень нас буде цікавити вплив на розбірливість мови професійно-лінгвістичної підготовки слухача та можливості багаторазового прослуховування записаної розмови. Отже докладніше розглянемо саме ці фактори.

Ознайомленість з темою може суттєво впливати на розуміння почутого через ряд ключових аспектів [2]:

- Розпізнавання термінів та специфічної лексики. Коли слухач ознайомлений з темою, йому легше розпізнати та розуміти специфічні терміни та лексику, які використовуються у розмові. Це допомагає легше вловлювати ключові ідеї.

- Відсутність порушень у розумінні. Ознайомленість з темою дозволяє уникати непорозуміння, оскільки слухач в тій чи іншій мірі

розпізнає загальні принципи та концепції, які можуть бути висловлені у розмові.

– Здатність сприймати деталі. Знання теми робить слухача більш здатним сприймати деталі та конкретику, що обговорюється. Він легше розрізняє важливе від другорядного та можливо краще сприймає контекст ситуації.

– Аналіз мовлення в контексті. Ознайомленість з темою допомагає аналізувати мовлення в конкретному контексті. Слухач можете розуміти, як конкретні висловлювання взаємодіють зі знаннями та інформацією, яку він вже має, а також завдяки контексту вгадати те, що було не почуто.

Ця теорія підтверджується у [3], де описано методику та результати експерименту. Згідно з методикою в якості аудиторів виступали дипломники-бакалаври напряму "Системи технічного захисту інформації", яким було представлено мовні повідомлення (зв'язні тексти і набори слів) з області ТЗІ та з області медицини. По результатам зв'язних текстів – словесна розбірливість фахово відомих текстів більша ніж невідомих на 2,9%. По результатам наборів слів – розбірливість фахово відомих слів більша ніж невідомих на 9,5%.

Багаторазове прослуховування так само має вплив на розуміння почутого в кількох аспектах:

– Уточнення деталей. Повторне прослуховування може допомогти уточнити та виокремити деталі, які можливо було пропущені під час першого прослуховування.

– Зростання розуміння контексту. При повторному прослуховуванні слухач можете краще зрозуміти контекст, в якому подана інформація.

– Зменшення помилок. Під час повторного прослуховування слухач може уникнути частково неправильних чи неправильних інтерпретацій, які можуть виникнути під час першого прослуховування.

Це підтверджено попередніми дослідженнями, які було описано у [4], а також [5]. Згідно з методикою цих досліджень у прослуховуванні приймали участь 5 аудиторів, які прослуховували 4 рази аудіозапис таблиць слів, взятих з [6], записуючи при кожному прослуховуванні зрозумілі слова, доповнюючи чи коригуючи записаний при попередніх прослуховуваннях набір слів. В результаті цих досліджень було

отримано наступні дані: збільшення розбірливості за рахунок багаторазового прослуховування становить 5...20%.

**Висновки. 1.** Наявність професійно-лінгвістичної підготовки порушника може збільшити розбірливість перехопленого повідомлення до 2,9% для зв'язних текстів та до 9,5% для окремих слів. **2.** Багаторазове прослуховування перехопленого повідомлення може збільшити розбірливість до 20%. **3.** Отримувані в результаті експериментів залежності дозволять скоригувати методики оцінки захищеності мовної інформації за критерієм розбірливості мови.

**Список літератури:**

1. Acoustics – The construction and calibration of Speech intelligibility tests. ISO/TR 4870 [Електронний ресурс]. Режим доступу до ресурсу: <https://cdn.standards.iteh.ai/samples/10853/6eebba263b3d4351be1bf92d0bcb1a30/ISO-TR-4870-1991.pdf>

2. Venus Chan. Factors Influencing Intelligibility and Comprehensibility / Venus Chan. [Електронний ресурс] – 2021. Режим доступу до ресурсу: <https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=1024&context=jele>

3. Касьянов Ю.І. Методика оцінювання залежності розбірливості мови від професійно-сленгової підготовленості слухача / Ю.І. Касьянов, О.Є. Феоктистова // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали V всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2015.

4. Касьянов Ю.І. Дослідження впливу багаторазового прослуховування на словесну розбірливість мови / Ю.І. Касьянов, А.В. Сафіулліна // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали VI всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2016. – С. 28 – 34.

5. Касьянов Ю.І. Врахування підвищення залишкової розбірливості мови в каналі витоку при багаторазовому прослуховуванні / Ю.І. Касьянов, А.В. Іванова // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали X всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2022. – С. 74–79.

6. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений: ГОСТ 16600-72. – М.: ИПК Издательство стандартов, 1973. – 90 с.

УДК 004.056.5: 534.[784: 835]: 621.391.883

## ОТРИМАННЯ АНАЛІТИЧНИХ ЗАЛЕЖНОСТЕЙ ЕФЕКТИВНОГО РІВНЯ ВІДЧУТТЯ ФОРМАНТ ВІД КОЕФІЦІЄНТА ЇХ СПРИЙНЯТТЯ

*Автори: Касьянов Ю.І., ст. викладач; Золотченко В.В., магістрантка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

**Вступ.** Захист виділених приміщень від витоку мовної інформації акустичним каналом будується на використанні пасивних і активних засобів. Основним пасивним засобом виступає звукоізоляція огорожувальних конструкцій, а активним – застосування генераторів акустичних завад. Пасивні та активні засоби захисту, як правило використовуються в комплексі і доповнюють один одного, для забезпечення заданого ступеня захищеності.

Відома інструментально-розрахункова методика оцінювання захищеності мовної інформації від витоку акустичним каналом, розроблена під керівництвом А.А. Хорева [1], яка базується на результатах досліджень М.Б. Покровського [2]. На основі цієї методики було розроблено методики оцінювання за критерієм розбірливості мови ефективності звукоізоляційних огорожувальних конструкцій [3, 4] та генераторів реальних мовоподібних завад [5, 6]. Ці методики розв'язують задачу аналізу (оцінювання) ефективності засобів захисту мовної інформації від витоку акустичними каналами і в них при розрахунках залишкової розбірливості мови в контрольних точках використовується залежність коефіцієнта сприйняття формант від ефективного рівня відчуття формант  $P(E')$ , представлена графічно [2] чи аналітично [1].

Однак, не менш важливою є зворотна задача (синтезу), коли за нормативними вимогами до захищеності мовної інформації, які виражаються залишковою словесною розбірливістю мови, потрібно визначити характеристики звукоізоляції та шумової завади, для чого потрібно мати зворотну залежність рівня відчуття формант від коефіцієнта сприйняття  $E'(P)$ .

**Метою роботи** є отримання аналітичних залежностей ефективного рівня відчуття формант від коефіцієнта їх сприйняття.

**Основна частина.** Розроблено методику розрахунку необхідних характеристик звукоізоляції та шумової завади за октавними рівнями бажаної формантної розбірливості мови для заданого ступеня захищеності мовної інформації [7].

Розроблена методика дозволяє вирішувати дві взаємозалежні задачі.

Перша задача – при відомому рівні мовного сигналу у виділеному приміщенні і відомому рівні шуму та його спектру (октавних рівнів) в контрольній точці (з урахуванням активної шумової завади) визначається частотна характеристика звукоізоляційної конструкції, яка разом з даним шумом забезпечить необхідний ступінь захисту мовної інформації (необхідні октавні рівні формантної розбірливості і загальні значення формантної та словесної розбірливості в контрольній точці).

Друга задача – при відомому рівні мовного сигналу у ВП і відомій частотній характеристиці звукоізоляції визначаються октавні рівні шумової завади (рівень та спектр завади), яка разом з даною звукоізоляційною конструкцією забезпечить необхідний ступінь захисту мовної інформації.

На одному з етапів цієї методики визначається ефективний рівні відчуття формант  $E'$  в октавних смугах за відомим коефіцієнтом сприйняття формант  $P$ , який відображає ймовірність проходження формант до слухача.

Для отримання такої залежності було виконано наступне.

За графіком залежності  $P(E')$  (рис.1), взятим з [2], було отримано зворотну залежність в табличній формі (табл. 1).

Таблиця 1

|            |       |       |       |       |       |       |       |     |
|------------|-------|-------|-------|-------|-------|-------|-------|-----|
| $E$ , дБ   | -35   | -30   | -25   | -20   | -15   | -10   | -5    | 0   |
| $P$ , в.о. | 0,001 | 0,01  | 0,025 | 0,057 | 0,12  | 0,225 | 0,35  | 0,5 |
| $E$ , дБ   | 5     | 10    | 15    | 20    | 25    | 30    | 35    |     |
| $P$ , в.о. | 0,65  | 0,775 | 0,88  | 0,943 | 0,975 | 0,99  | 0,999 |     |

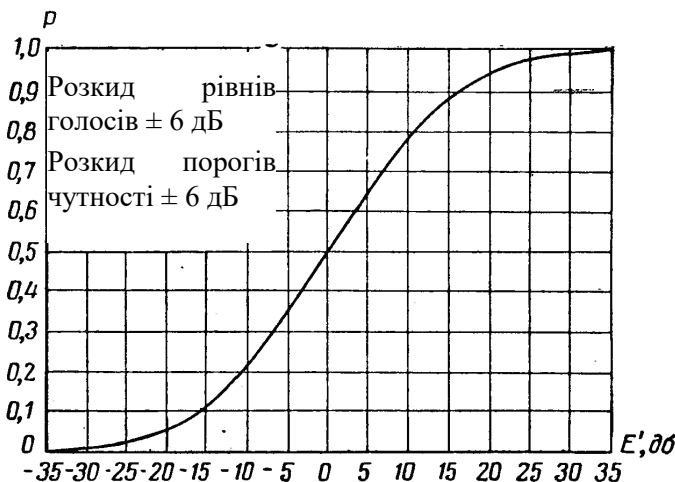


Рисунок 1 – Залежність коефіцієнта сприйняття від ефективного рівня відчуття формант

За даними табл.1 в програмі Advanced Grapher побудовано графік (суцільна лінія) залежності  $E'(P)$  (рис.2). Використовуючи можливості регресійного аналізу даної програми, отримано аналітичні вирази цієї залежності при апроксимації многочленом 9-го порядку

$$E'_i = 105134.5 \cdot P_i^9 - 473105 \cdot P_i^8 + 898968 \cdot P_i^7 - 938564.5 \cdot P_i^6 + 587075 \cdot P_i^5 - 225187 \cdot P_i^4 + 52197.5 \cdot P_i^3 - 6988 \cdot P_i^2 + 540.5 \cdot P_i - 35.2 \quad (1)$$

та при її апроксимації логарифмічною залежністю

$$E'_i = \begin{cases} -5.63 \cdot \ln(1-P_i) + 18.5 \cdot P_i - 13.2, & \text{якщо } P_i \geq 0.5 \\ 5.63 \cdot \ln(P_i) + 18.5 \cdot P_i - 5.5, & \text{якщо } P_i < 0.5 \end{cases} \quad (2)$$

Похибка апроксимації в обох випадках не перевищувала 1%.

На рис.2, окрім графіка, побудованого за даними табл.2, наведено результат логарифмічної апроксимації верхньої та нижньої віток графіка.

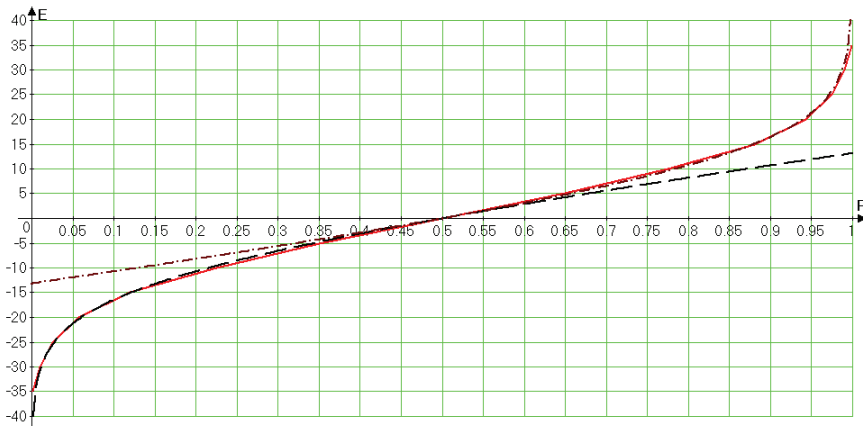


Рисунок 2 – Апроксимація верхньої та нижньої вітки залежності  $E(P)$  логарифмічною залежністю

Отримані аналітичні залежності дозволяють автоматизувати розрахунок при розв'язанні задач проектування системи технічного захисту мовної інформації у виділеному приміщенні.

**Висновок:** Отримано аналітичні залежності ефективного рівня відчуття формант від коефіцієнта їх сприйняття, необхідні для проектування системи технічного захисту виділеного приміщення за нормами захищеності мовної інформації.

#### Список літератури:

1. Хорев А.А. Методы защиты речевой информации и оценки их эффективности / А.А.Хорев, Ю.К. Макаров // Защита информации. Конфидент. – 2001. – № 4. – С. 22 – 33.
2. Покровский Н. Б. Расчет и измерение разборчивости речи / Н. Б. Покровский. – М.: Гос. изд-во литературы по вопросам связи и радио, 1962. – 392 с.
3. Касьянов Ю.І. Визначення впливу шумової завади та звукоізоляції на розбірливість мови формантним методом / Ю.І. Касьянов // Комп'ютерні технології друкарства. – 2014. – №31. – С.85 – 93.
4. Касьянов Ю.І. Визначення можливостей матеріалів звукоізоляційних конструкцій щодо зниження розбірливості мови / Ю.І. Касьянов

янов, А.І. Кривда // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали VI всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2016. – С. 17 – 21.

5. Касьянов Ю.І. Оцінювання ефективності генератора реальної мовоподібної завади за критерієм розбірливості мови / Ю.І. Касьянов, С.М. Нужний // Вісник НУ "Львівська політехніка": Автоматика вимірювання та керування. – 2016. – №.852 – С. 105 – 110.

6. Касьянов Ю.І. Методологія оцінювання генераторів реальних мовоподібних завад в захисті мовної інформації / Ю.І. Касьянов, Ю.П. Кисельова. // Інформаційні системи та технології ICT-2018: Матеріали 7-ї міжнародної науково-технічної конференції. – Харків: ХНУРЕ, 2018. – С. 333 – 336.

7. Касьянов Ю.І. Розрахунок бажаних характеристик звукоізоляції та шумової завади за октавними рівнями формантної розбірливості мови / Ю.І. Касьянов, В.В. Золотченко // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали X всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2022. – С. 80 – 84.

**УДК 004.056.53: 534.781**

### **УЗАГАЛЬНЕННЯ СПЕКТРІВ ДОВГОТРИВАЛИХ МОВЛЕННЄВИХ СИГНАЛІВ З ВИКОРИСТАННЯМ ПРОЦЕДУР ОБРОБКИ ЗОБРАЖЕНЬ**

***Автори:** Касьянов Ю.І., ст. викладач; Щербаков М.С., магістрант; Троценко С.С., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

**Вступ.** Наразі в області інформаційної безпеки відбувається зміна критерію нормування і оцінювання захищеності захисту мовної інформації від витoku акустичними каналами. Замість загальноприйнятого раніше критерію відношення сигнал/шум, який був прив'язаний до завади «білого шуму» впроваджується критерій словесної розбірливості мови в точках можливого знімання інформації (контрольних точках). Це пояснюється

тим, що критерій відношення сигнал/шум є неінваріантним до виду шумової завади, тобто при одних видах завад нормоване значення може бути надлишковим, а при інших – недостатнім [1-4]. Критерій же розбірливості мови є первинним чисельним показником зрозумілості мовного повідомлення і норма залишкової словесної розбірливості в контрольній точці не залежить від виду завади.

Сертифіковані методики оцінювання захищеності мовної інформації базуються на формантному методі та його модифікаціях, в яких для визначення словесної розбірливості мови використовуються спектральні характеристики мови – узагальнений спектр довготривалої мови та розподіл формант у мовному діапазоні частот [1, 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 українськомовними, потрібно отримати такі спектральні характеристики для української мови, зокрема узагальнений спектр 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 процедур обробки зображень для узагальнення спектрів довготривалих українських мовленнєвих сигналів, отриманих спектроаналізаторами програм обробки звуку.

**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:

- 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 середньгеометричних частотах октавних смуг 125, 250, 500, 1000, 2000, 4000, 8000 Гц. Узагальнений спектр визначався як обвідна середньоарифметичних значень рівнів звукового тиску на цих частотах.

Проведення аналізу спектрів довготривалих мовленнєвих сигналів з використанням швидкого перетворення Фур'є в програмних математичних середовищах обмежується великими розмірами масивів даних. Верхня межа мовного діапазону складає 11200 Гц. Відповідно до теореми Котельникова частота дискретизації повинна бути більшою за 22400 Гц, з урахуванням 10% запасу – приблизно 25 кГц. Це значить, що для 15 с мовного сигналу матимемо масив у 375000 відліків.

Щодо вирішення задачі узагальнення спектрів довготривалих мовленнєвих сигналів при аналізі за допомогою спеціальних програмних засобів обробки звуку було проаналізовано наступні варіанти:

- 1) Коли функція узагальнення (усереднення) є в самій програмі;
- 2) Коли такої функції у програмі нема, але є можливість виводу чи експорту спектрів у вигляді файлів даних з можливістю подальшої математичної обробки в інших програмах (наприклад, Mathcad, MatLab тощо);
- 3) Коли спектри отримані у вигляді зображень (рисуноків), цифровою обробкою яких в інших програмах (наприклад, Mathcad) спектри формуються у відповідні масиви даних і виконується їх усереднення.

Проведений аналіз програм обробки звуку Sound Forge, SpectraLab, SpeechAnalyzer, Right Mark Audio Analyzer, Praat, GoldWave показав, що функції усереднення (узагальнення) спектрів вони не ма-

ють, як не мають і можливості виводу чи експорту спектрів у вигляді файлів (масивів) даних. Тому було прийнято рішення реалізувати 3-й варіант, для чого було розроблено спеціальні процедури обробки зображень в середовищі Mathcad.

Спектроаналізатором програми Sound Forge було отримано спектри фонограм, записаних для досліджень в [7]. На одному зображенні розміщувалось 5 спектрів різних дикторів.

Процес обробки відбувався наступним чином:

1. Зображення графіку спектрів сканованого з вікна спектроаналізатора програми Sound Forge програмою Paint перетворювалось в монохромний рисунок формату .bmp.

2. Зображення з файлу зчитувалось у робочу область програми Mathcad.

3. За допомогою функції READBMP отримувалась матриця, елементи якої задають яскравість пікселів зображення від 0 до 255, що представляє відтінки (градації) сірого від чорного до білого. Оскільки зображення є чорно-білим, то матриця містить лише елементи 0 і 255. Елементи зі значенням 0 відповідають точкам сітки і ліній спектрів.

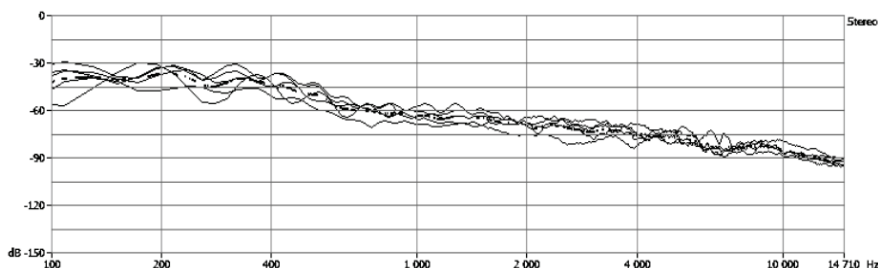
4. Для того, щоб точки сітки не сприймалися як точки спектрів і не впливали на математичну операцію усереднення, виконувалось їх висвітлення спеціально розробленою програмною процедурою.

5. За координатами точок спектрів спеціально розробленою процедурою усереднення розраховувались координати точок узагальненого спектру і відповідним елементам матриці зображення присвоювалось значення 0 (чорне).

Результат обробки наведено на рис.1. Жирна лінія відповідає узагальненому спектру.

Уривчастість лінії узагальненого спектру обумовлена пропуском цих точок при невідповідності кількості нульових елементів у стовпці матриці зображення і кількості спектрів, яка виникає при пересіканні кількох спектрів або швидкій зміні якогось спектру.

Цей недолік можна ліквідувати, якщо обробкою зображень кожного спектру окремо сформувати масиви значень, а потім виконати усереднення.



Д

Рисунок 1 – Спектри дикторів та узагальнений спектр

**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. Для узагальнення спектрів в цьому випадку можуть бути використані процедури обробки зображень.

#### **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.И., 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., Nuzhnyi, 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.

**УДК 004.056.53 : 004.891.2**

**ГЕНЕТИЧНИЙ АЛГОРИТМ ОЦІНЮВАННЯ РІВНЯ  
ЗАХИЩЕНОСТІ СКЛАДНОЗАШУМЛЕНОЇ МОВНОЇ  
ІНФОРМАЦІЇ ЗА КРИТЕРІЄМ ЗАЛИШКОВОЇ  
РОЗБІРЛИВОСТІ МОВИ**

***Автори:** Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна; Передерій В.І., д.т.н., професор кафедри Інформаційних технологій, Миколаївський національний університет імені В.О. Сухомлинського, м. Миколаїв, Україна*

**Анотація**

Визначення рівня захищеності мовної інформації, що озвучується в контрольованій зоні (КЗ), відноситься до однієї з головних задач при проведенні інструментального контролю та атестації виділеного приміщення (ВП). Важливість цієї задачі значно зросла в умовах повномасштабного вторгнення російського загарбника в Україну. Безпечне обговорення питань будь-якого рівня конфіденційності є безумовним

завданням для систем комплексного захисту інформації (КСЗІ) / комплекту технічних засобів захисту інформації (КТЗЗІ).

### Вступ

Побудова КСЗІ об'єкту критичної інформаційної інфраструктури (ОКІІ), його задачі та структура визначається нормативно-правовими документами [1-3], нормативними документами (НД) з технічного захисту інформації (ТЗІ) [4-6], наказами Адміністрації Держспецзв'язку [7-9] та ін.

До переліку обов'язкових робіт, що повинні підтвердити стан та якість роботи КСЗІ, є проведення інструментально контролю [10]. По відношенню до вібраційного та акустичного технічних каналів витоку інформації (ТКВІ) критерієм захищеності є коефіцієнт, який визначається як відношення рівня небезпечного сигналу до рівня завади в точці можливого встановлення технічного засобу розвідки (ТЗР) за межами КЗ. В ЄС, США та інших англослов'янських країнах, цей коефіцієнт отримав назву *SNR (signal-to-noise ratio)*. В Канаді використовують одну з його модифікацій – коефіцієнт приватності розмови *SPC (speech privacy class)*

Головним недоліком такого відходу є не врахування впливу спектрального складу мовного сигналу, «особливих» частотних смуг в тембрі голосу конкретного диктора, які можуть «з'явитись» і мати значну амплітуду. Їх виникнення пов'язане з «особливими» резонансами в голосовому тракті диктора і залежить від багатьох випадкових факторів. Також можлива поява таких частотних слуг, однак в набагато меншій мірі, і в наслідок впливу зовнішніх факторів. Так, наприклад, в результаті взаємодії таких фізичних явищ як реверберація, резонанс звуків на конструкційних елементах (в тому числі інтер'єр приміщення, меблі та інше), нелінійна модуляція і т.д.

Для виправлення вказаного недоліку, США та ЄС ввели нормативний коефіцієнт, який дозволяє розрахувати рівень захищеності мовної інформації (РЗМІ) з врахуванням спектрального складу мовного сигналу та вагомості октав в передачі інформації – коефіцієнт (індекс) розбірливості мови *SII (speech intelligibility index)*. Однак, як показано в [11,12], його використання при застосуванні процедур цифрової обробки (фільтрації, очистки), наприклад таких як вейвлет-

перетворення, може дати негативний ефект. Так при досягненні досить високої якості очистки досліджуваного сигналу від завади на низьких та середніх частотах (до 4,5...5 кГц), на високих та надвисоких частотах спостерігається суттєве погіршення (зашумлення) досліджуваного сигналу [11,12]. Це призводить до визначення коефіцієнту  $SII$ , значення якого є некоректним і, відповідно, призводить до невірної оцінки рівня захищеності мовної інформації.

#### **Мета та задачі дослідження**

Метою роботи є розробка методу оцінки рівня захищеності складнозашумленої мовної інформації (РЗСЗМІ) на критерієм залишкової розбірливості мови диктора на основі генетичного алгоритму

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

1) Аналіз сучасного стану проблем оцінки РЗМІ методами цифрової обробки та очищення (фільтрації) зашумлених мовних сигналів.

2) Розробка генетичного алгоритму системи визначення та оцінки РЗСЗМІ на критерієм залишкової розбірливості мови диктора.

#### **Методи оцінки рівня захищеності мовної інформації**

Захист мовної/акустичної інформації є однією з пріоритетних задач забезпечення безпеки держави, її військової, політичної, економічної, наукової та ін. складових. Аналогічні задачі стоять і перед організаціями та фірмами. Проріхи в захисті призводять як до локальних так і до стратегічних збитків. Недостатній рівень захисту мовної інформації це не тільки неповага до себе та інтересів своєї фірми/організації, а до партнерів (співвиконавців, контрагентів та ін.).

Тому перед відповідними «структурами» (підрозділами) завжди стояла задача визначення рівня захищеності мовної інформації на конкретному об'єкті (кімнаті, наметі, споруді і т.д.) та підтриманні його на необхідному рівні.

Історично так склалось, що люди в першу чергу покладалися на можливості людського організму – можливості слухового апарату та здатність вирізняти окремі звуки (мову) з загального акустичного потоку. Це призвело до формування, так званих, суб'єктивних методів оцінки РЗМІ (рис.1).



Рисунок 1 – Методи оцінки рівня захищеності мовної інформації

Один з найпоширеніших показників – коефіцієнт розбірливості мови  $W$ . Він заснований на проведенні експертизи [13], до якої залучаються диктор (або фонограма надиктованого ним тестового повідомлення) та група із 3-5 експертів-слухачів. Основною перевагою цього методу є розрахунок РЗМІ на основі обробки експертних оцінок і, відповідно, визначення реальної можливості розпізнавання порушником в перехопленому сигналі мовної інформації. Однак це й є основним недоліком методу. Він суттєво залежить від кваліфікації експертів-слухачів, їх настрою, стану здоров'я та ін. – тобто є суб'єктивним. З цього пункту випиває ще декілька особливостей – він потребує значних витрат робочого часу експертів і виведення з технологічного процесу досліджуваного приміщення та приміщень що його оточують з усіх сторін, а також зверху і знизу. У зв'язку з цим, цей метод, наразі, використовується майже тільки в лабораторних дослідженнях особливо відповідальних конструкційних елементів (приладів, систем, комплексів та ін.).

Розробка систем, які б забезпечували об'єктивне розпізнавання мовної інформації є надто складною задачею. Одні з перших науково обґрунтованих спроб відносяться до 17-о початку 19-о століть. Різними авторами були розроблені пристрої, що отримали назву «механічна

голова» («*talking head*») або «розмовний пристрій» («*talking device*», наприклад розмовний пристрій *Euphonia*). Деякі з них могли прослухати питання і відповісти на нього.

З розвитком ЕВМ, експертних систем (інформаційно-аналітичні системи, системи контролю доступу за голосовими сповіщеннями та багато інших), нейронних мереж і штучного інтелекту, питання розробки «електронного вуха» набули нового поштовху [14,15].

Втім ці методи мають ряд значних недоліків і основним з них є суттєва залежність від якості мовного сигналу і коефіцієнту  $SNR$  – вони не працюють з зашумленими сигналами (ЗС) ( $SNR \geq 0$  дБ). Це призвело, на даний момент, до відсутності об'єктивних методів оцінки РЗМІ здатних працювати в умовах з від'ємними  $SNR$  ( $SNR \leq -5$  дБ).

Вирішенням проблеми, на даний час, стало використання об'єктизованих методів оцінки РЗМІ – тобто методів заснованих на інструментальному вимірюванні параметрів, які на пряму не пов'язані з РЗМІ та розрахунок, за певними аналітичними виразами, коефіцієнту, який і використовується для оцінки РЗМІ. До таких коефіцієнтів відносяться: (згадані вище)  $SNR$ ,  $SPC$ ,  $SII$  та індекс артикуляції  $AI$  (*articulation index*) і коефіцієнт залишкової розбірливості мови  $RII$  (*residual intelligibility index*) [11,12].

#### **Типи сигналів завади та методи їх синтезу**

Методи формування сигналу завади, в першу чергу, діляться в залежності від сигналу, що потребує захисту (рівень амплітуди сигналу завади до уваги не береться):

- сигналозалежні – створені/синтезовані на основі сигналу, що захищається;
- сигналонезалежні – створені без використання сигналу що захищається (автономні пристрої).

Всі типи завад, що використовуються в системах захисту інформації, поділяються на чотири групи:

- 1) білий шум та спеціально сформовані на його основі сигнали (наприклад, його «кольорові» клони та «мовоподібний» сигнал);
- 2) комбінаційні шум (використовується декілька незалежних джерел акустичного сигналу – отримали назву «мовний хор» або вечірка («party»));

3) ревербераційний шум (використовується частотна або тимчасова реверберація);

4) комбінований шум (використовується декілька з вказаних вище методів синтезу сигналу завади).

Доцільним є вказати, що 1) та 2) типи завад відносяться до сигналонезалежних методів формування сигналу завади, 3) тип завад є сигналозалежним, а 4) залежить від застосованих при його синтезі типів завад.

Ефективність використання того чи іншого типу завади визначається шляхом проведення інструментальних досліджень на об'єкті захисту або в лабораторії і розрахунком коефіцієнту РЗМІ.

Слід зауважити, що в Україні, США, ЄС та ін., в якості сигналу завади для захисту інформації, що містить конфіденційну інформацію та/або державну таємницю, дозволено використовувати тільки сигнали першої групи – білий шум та спеціально сформовані на його основі сигнали [11,12]. Інші групи можна використовувати виключно для захисту комерційної інформації.

Що ж до типів тест-сигналів, які використовуються при проведенні інструментальних досліджень, то на даний час використовуються:

1) білий шум;

2) моно- чи мультитоновий сигнал (наприклад, з розрахунку один чи декілька тонів на кожну  $\frac{1}{3}$ -октавну смугу);

3) мовоподібний сигнал (використовується нормована фонограма надиктованого диктором тестового повідомлення).

Тип тест-сигналу залежить від коефіцієнту який використовується для оцінки РЗМІ при проведенні досліджень. Так для *SNR* використовується білий шум, для *AI*, *SII* та *RII* – мовоподібний сигнал (фонограма мови диктора), а для та *SPC* можна використовувати як білий шум так і мовоподібний.

### **Попередня обробка зашумлених сигналів**

Додатково, на можливість розпізнавання тест-сигналу на фоні сигналу завади при оцінці РЗМІ, за умови що  $SNR \leq -7 \dots -5$ дБ, суттєвий вплив має метод та процедура попередньої обробки сигналу (фільтрації) [11,12]. Так, при визначенні РЗМІ за коефіцієнтами *SNR* та *SPC* (за

умови використання в якості тест-сигналу білого шуму) проведення попередньої обробки сигналу не допускається (див. рис.2). При застосуванні мовоподібного тест-сигналу (фонограми мови диктора) для визначенні РЗМІ за коефіцієнтами  $SPC$ ,  $AI$  та  $SII$  проведення попередньої обробки, навіть для ЗС, в офіційних методиках не розглядається. Більше того, передбачено проведення розрахунків коефіцієнтів  $SPC$ ,  $AI$  та  $SII$  виключно для попередньо не оброблених сигналів. Для коефіцієнту  $RII$  проведення попередньої обробки є доцільним, необхідність проведення визначається рівнем впливу сигналу завади на СЗ.

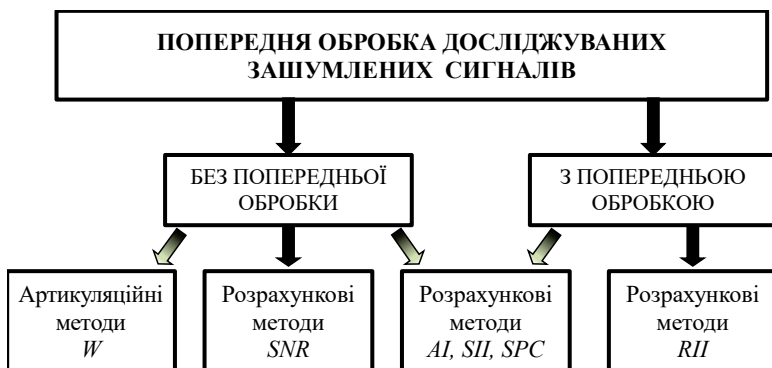


Рисунок 2 – Розподіл коефіцієнтів оцінки РЗАІ за попередньою обробкою досліджуваних СЗ

Намагання покращити якість фонограми отриманого/перехопленого сигналу, за умови впливу на його шумової завади, завжди було одним із необхідних технологічних процесів. Однак, при використанні аналогових методів попередньої обробки, це можливо тільки в лабораторних умовах. При цьому перелік методів, які можуть дати позитивний ефект, є суттєво обмеженою (див. рис. 3). До них відносяться смугові та кореляційні методи.

При використанні цифрових методів обробки сигналів, перелік можливих до застосування методів є набагато різноманітним, як з точки зору рівня фільтрації так і вибіркості спектру. З врахуванням особливостей мовної інформації – її семантики, фонетики, умов формування в звуковому тракті людини та ін., виділяється декілька особливих ме-

тодів попередньої обробки для ЗС, що пов'язані з частотно-часовим розподілом енергії в сигналі.

Найбільшого розповсюдження отримали вейвлет-перетворення, адаптивна фільтрація та кореляційний аналіз. Це зумовлюється тим, що, навіть при відносно не великих значеннях частотного спектру звукового сигналу (умовно, від 20 Гц до 20кГц) та його випадковості, зміну форми дотичної можна вважати квазістаціонарною (для часових періодів близьких до 0,1...0,2 типової протяжності фонем, тобто від 10 мс до 50 мс). Враховуючи (при рівномірному розподілу частот в спектрі сигналу завади типу білий шум) амплітуди окремих тонів сигналу завади в часовому і частотному вимірах є випадковими величинами, а отже і відповідні дотичні до такого сигналу на вказаних відтинках часу не можуть вважатись квазістаціонарними. Такий підхід на даний час став основою теоретичного апарату в обробці ЗС.

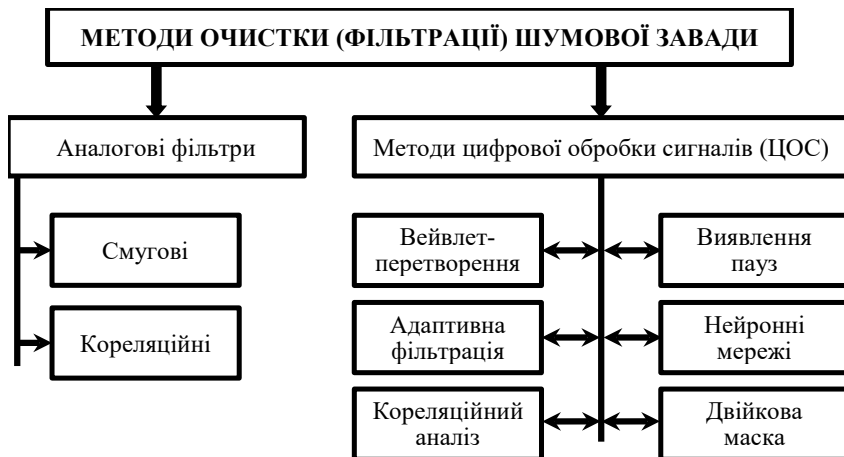


Рисунок 3 – Методи очистки (фільтрації) ЗС від шумової завади

Наступним елементом в підході до попередньої обробки ЗС стали методи виявлення пауз у мові диктора між словами. Це зумовлено тим, що в паузах відсутні квазістаціонарні сигнали, що відповідають елементам (енергії) спектру людської мови, а шуми, що пов'язані з

навколишнім середовищем, мають більшу за часом і частотою стабільність (скрипи дверей, стільців та інших предметів, шерхїт вітру і т.д.). В більшості методів попередньої обробки виявлені паузи використовують для сегментації мови на окремі блоки (ансамблі) і далі виконують попередню обробку до кожного з них окремо (див. рис. 4).

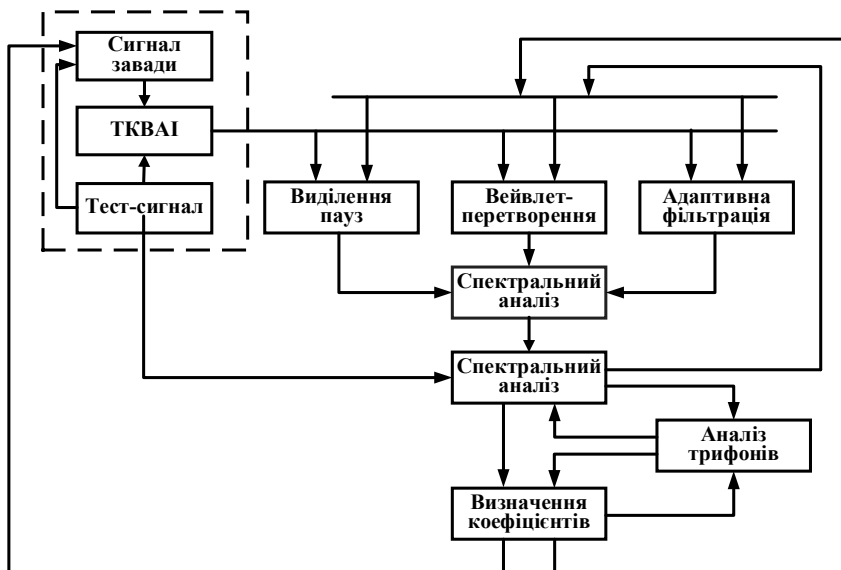


Рисунок 4 – Структурна модель системи оцінки рівня захищеності ЗС мовної інформації за критерієм залишкової розбірливості мови диктора

Такий підхід дозволяє перейти до паралельної обробки сигналу, що суттєво підвищує якість та продуктивність роботи системи, однак потребує значно більших розрахункових потужностей (цей недолік виправляється, наприклад, використанням «майнінгових» станцій). Одночасно з цим, виявлення пауз додатково дає можливість збільшити якість основної обробки за рахунок застосування методу трифонів [11,12] і перейти до оцінки рівня захищеності ЗС мовної інформації за критерієм залишкової розбірливості мови диктора.

При такому підході є доцільним поєднати попередню обробку з використанням, наприклад, вейвлет-перетворення та виявлення пауз, з аналізом трифонів, в якості основної обробки. Найбільш доцільним при цьому є використання нейронної мережі, що дозволить створити цілісну структуру.

### **Висновки**

В роботі розглянуто нормативно-правову базу, методи та технології захисту мовної інформації на об'єкті інформаційної діяльності критичної інфраструктури, що дозволили запропоновано метод оцінки рівня захищеності мовної інформації за критерієм залишкової розбірливості мови диктора та аргументувати використання нейронної мережі.

### **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. 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>
5. НД ТЗІ 3.6-003-2016
6. НД ТЗІ 3.5-001-2017
7. Наказ Адміністрації Держспецзв'язку від 19.06.2015 № 023 (зі змінами від 23.01.2023 № 01т)
8. 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, кібе-

рзахисту, 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>

9. 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>

10. 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>

11. 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>

12. 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>

13. 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>

14. Gornostal, Alexandr & Dorogyy, Yaroslav. (2017). Development of audio-visual speech recognition system. *Science Rise*. 12. 42-47. <https://doi.org/10.15587/2313-8416.2017.118212>. URL: <https://journals.uran.ua/sciencerise/article/view/118212>

15. Ткаченко, М & Федоренко, Р & Кондратенко, Ю & Зотова, І. (2019). Методи автоматичної ідентифікації диктора за голосом. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняхівського. 131-135. <https://doi.org/10.33099/2304-2745/2018-3-64/131-135> – URL: <http://znp-cvsvd.nuou.org.ua/article/view/178061>

УДК 004.2

## ОЦІНКА СТАНУ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

*Автори: Передерій В.І., д.т.н., професор кафедри Інформаційних технологій, Миколаївський національний університет імені В.О. Сухомлинського, м. Миколаїв, Україна; Федорчук Є.Ю., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Згідно Закону України “Про основні засади забезпечення кібербезпеки України” [1]; Стратегії кібербезпеки України [2], кібербезпеку об'єктів критичної інформаційної інфраструктури (ОКІІ) визначено як пріоритетний напрямок наукових досліджень. Але на разі відсутнє нормативно-правове врегулювання питання щодо типових вимог до системи захисту інформації і кібербезпеки ОКІІ. Відсутність зазначених елементів призводить до унеможливлення оцінювання ефективності функціонування ОКІІ.

Разом з тим, останнім часом кібератаки на людино-машинні системи (ЛМС) критичного призначення по всьому світу, показали значний розрив між можливостями захисту і відновлення традиційних систем і новими вимогами безпеки, особливо в контексті застосування інтелектуальних та інформаційно – когнітивних технологій.

Таким чином, актуальною науковою проблемою є підвищення функціональної безпеки ОКІІ за рахунок розробки та впровадження нових методів і способів з використанням інтелектуальних та інформаційно – когнітивних технологій.

У наукових роботах [3,4] запропоновані методи які дають можливість визначати сумарний ризик кібербезпеки ОКІІ, сумарні збитки в результаті дії множини кіберзагроз, сумарну величину збитків за певний період часу та ймовірність виникнення максимальних втрат. Зазначено також, що процес визначення та оцінки ризику від помилкових прийнять рішень особою, що приймає рішення (ОПР), під впли-

вом кіберзагроз, є основою та підґрунтям для наукових досліджень в області аналізу та удосконалення наявних, а також винаходу нових методів оцінки ризику, підвищення точності його оцінки, здійснення над ризиками математичних операцій.

Враховуючи результати наукових досліджень для оцінки і підтримки захисту інформації і кібербезпеки ОКП пропонується наступна інформаційна модель (рис.1).

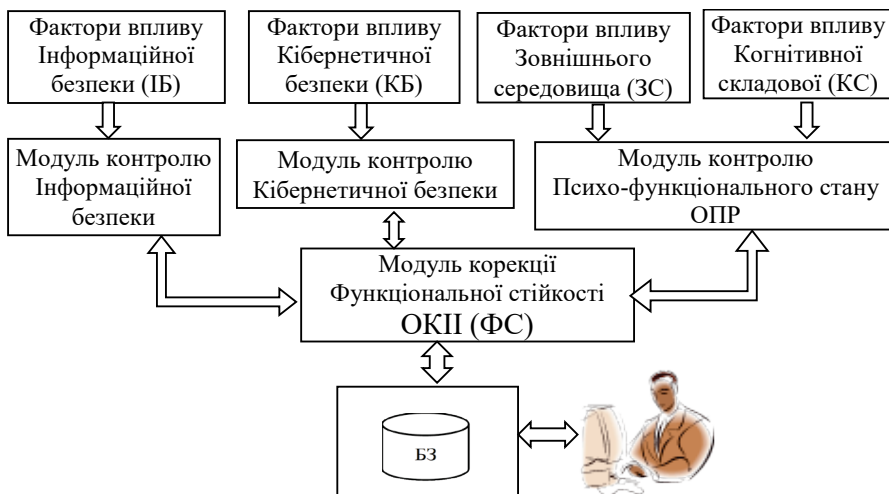


Рисунок1 – Інформаційна модель оцінки та корекції оперативного стану захисту інформації і кібербезпеки ОКП

Згідно інформаційної моделі для оцінки та корекції оперативного стану захисту інформації і кібербезпеки ОКП розроблена Байєсівська мережа довіри (БМД), спрощена структура якої наведена на рисунку 2.

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

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:

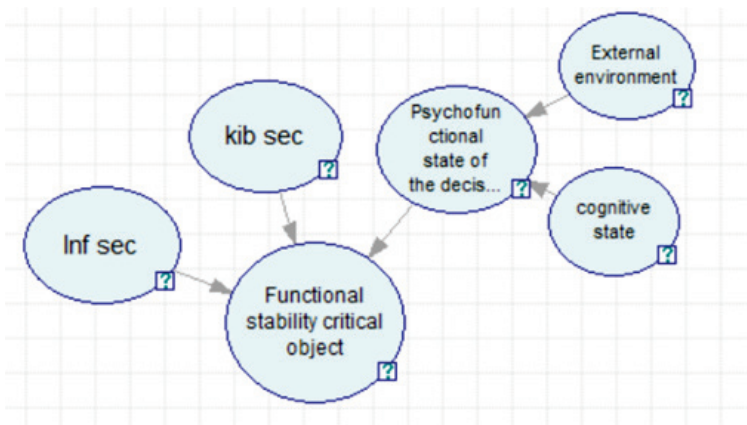


Рисунок 2 – Спрощена структура БМД

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

де  $\text{Parents}(A_i)$  – 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:

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

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

При функціонуванні ОКП найбільш нестабільним звіном є ОПР, на якого впливають, в основному, чотири фактори: зовнішнє середовище, інформаційне навантаження та його психологічний і когнітивний стан, що вимагає окремого розгляду оцінки.

На підставі запропонованої БМД розроблено алгоритм оцінки ймовірності захисту інформації і кібербезпеки ОКП.

1. За результатами сканування модулів контролю захисту інформації і кібербезпеки ОКП оцінюються ймовірності  $P_i$  безпечної роботи цих модулів.

2. На першому етапі вимірюються значення факторів, що впливають на інформаційне навантаження ОПР, факторів впливу зовнішнього середовища на ОПР; проводяться тести для оцінки психологічного і когнітивного станів ОПР.

3. На підставі даних, отриманих на першому етапі по формулах (1,2), обчислюються ймовірності того, що вершини "Інформаційна безпека" і "Кібернетична безпека" перебувають у стані "захищено".

4. За результатами тестування ОПР обчислюються ймовірності станів вершин "Психо-функціональний стан ОПР".

5. За допомогою побудованої Байесовської мережі обчислюється повна ймовірність захисту інформації і кібербезпеки ОКП.

Якщо ця ймовірність більше або рівна деякої критичної величини (значення даної величини залежить від ступеня важливості ОКП), то ОКП можна вважати захищеним. Якщо на ОКП виявилась вразливість, то усуваються і корегуються відповідні загрози, на які вказують результати сканування секторів контролю.

**Висновки.** Запропоновано рішення актуальної наукової проблеми з підвищення функціональної безпеки ОКП за рахунок розробки методу оцінки та корекції захисту інформації і кібербезпеки з використанням інтелектуальних та інформаційно – когнітивних технологій.

#### **Список літератури:**

1. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2021) (Україна). <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", Указ Президента України № 96/2016 (2021) (Україна). <https://zakon.rada.gov.ua/laws/show/96/2016#Text>.

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. 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.

**УДК 004.056.5: 534.843**

## **РОЗРОБКА СТРУКТУРИ МОДЕЛІ СИСТЕМИ АВТОМАТИЧНОГО ВИЗНАЧЕННЯ РОЗБІРЛИВОСТІ МОВНОЇ ІНФОРМАЦІЇ**

***Автор:** Трізно С.О., магістрантка, 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.** Захист мовної інформації від витoku акустичними каналами є одним з важливою задачею на будь-якому об'єкті інформаційної діяльності. Умови для захисту такої інформації можуть бути закладені ще на рівні проектування проектуванні будівлі, при проведенні ремонтних робіт тощо. Здебільшого при проектуванні приміщень проводять заміри звукоізоляції приміщення але при цьому не враховують особливості проходження саме мовного сигналу.

При проектуванні або модернізації приміщення де можуть бути озвучені конфіденційні повідомлення (такі як усні розпорядження, що не можуть бути довірені іншим засобам передачі інформації) слід приділити увагу саме процесу звукоізоляції на окремих діапазонах частот, що притаманні людській мові.

Для визначення якості захищеності мовної інформації в приміщенні пропонується використання тонального методу визначення розбірливості мови. Використання даного методу дасть змогу перевірити захист інформації на стадії проектування системи захисту та вибору

звукоізолюючих матеріалів. Спрощення даних розрахунків пропонується створення спеціалізованої моделі визначення розбірливості мовної інформації при проходженні через перешкоди.

**Метою роботи** є розробка структури системи дослідження захисту інформації від витoku акустичними шляхами з використанням точального методу визначення розбірливості мови.

#### **Основна частина.**

Структура моделі системи автоматичного визначення розбірливості мови (рис. 1) базується на лабораторній установці, що була описана в [1]. Ця структура представляє собою послідовний потік обробки сигналу в системі Simulink. Блоки виконують наступні функції:

– джерело сигналу – подає вхідний цифровий аудіосигнал в відносних одиницях від максимального значення. В якості джерела сигналу використовується аудіофайл або вхід мікрофона. Потім даний сигнал приводиться до режиму відтворення звуку моно. На виході ми отримуємо масив даних інтенсивності різних частот в діапазоні від 0 до 1.



Рисунок 1 – Структура моделі визначення розбірливості мови

– приведення до фізичної величини – на цьому етапі сигнал від 0 до 1 конвертується у фізичну величину – інтенсивність звуку в Вт/м<sup>2</sup>, за формулою:

$$I_1 = s \cdot 10^{(M/20)},$$

де  $s$  – рівень сигналу;  $M$  – максимальний рівень потужності в дБ.

– генератор шуму – генерує та додає шум білий шум до сигналу. Складається з двох частин сам генератор випадкових чисел, що буде рівень шуму на матриці частот сигналу та системи приведення шуму до фізичної величини, що працює аналогічним чином з попереднім блоком. Може бути корисно для моделювання реальних умов або для тестування стійкості системи до шумових впливів.

– моделювання перешкод – враховує затухання проходження звукового сигналу через перешкоду, дані про ослаблення відповідних частот беруться з довідників про звукоізоляційні матеріали.

– спектральний аналізатор – модуль, що показує рівень частот в дБ на всьому проміжку звукового сигналу в режимі реального часу та створює діаграму запам'ятовування даного сигналу в невеликих проміжках часу з в графічному вигляді (рис. 2).

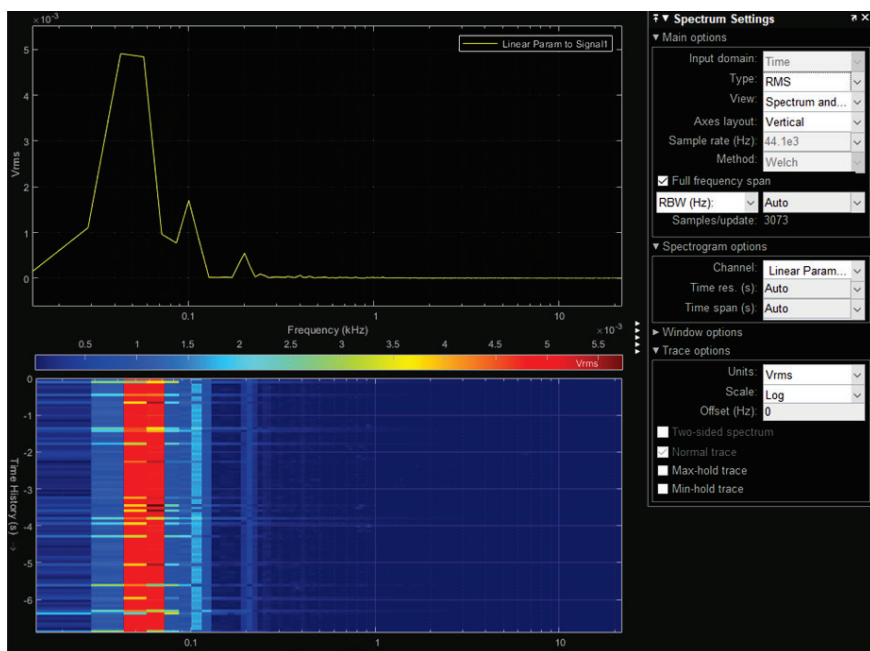


Рисунок 2 – Спектральний аналізатор системи Matlab Simulink

– аудіовихід – призначений для виходу звуку на пристрої виведення, такі як динаміки, навушники, бузери тощо, для того щоб оператор міг контролювати правильність викладених даних.

– розрахунковий метод – модуль що виділяє основні частоти, що лежать в основі розрахунку розбірливості мови тональним методом. Відповідно до математичної моделі, що представлена в [2,3] проводить розрахунки та на виході отримуємо параметр розбірливості мови в даний момент часу.

– система запам'ятовування – зберігає отриманні результати в файл для їх подальшого аналізу, а також будує графік мовної розбірливості в конкретний момент часу Це може бути важливим для збереження інформації про попередні етапи обробки.

#### **Висновок:**

Дана структура є першим етапом для створення моделі автоматичного визначення розбірливості мови, що в подальшому може використовуватись для попередніх розрахунків захищеності інформації на стадіях проектування захищених об'єктів.

#### **Список літератури:**

1. Трізно С.О., Кучер В.С (2021) Задача об'єктивізації тонального методу визначення розбірливості мови. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали ІХ всеукраїнської науково-практичної конференції з міжнародною участю. Миколаїв, НУК, С. 211-215.

2. Касьянов Ю.І., Дума С.В. (2015) Використання тонального методу визначення розбірливості мови для задачі оцінки захищеності мовної інформації. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали V всеукраїнської науково-практичної конференції з міжнародною участю. Миколаїв, НУК, С. 32 – 38.

3. Касьянов Ю.І., Стаканов Д.К. (2018) Об'єктивізація тонального методу для оцінювання захищеності мовної інформації за критерієм розбірливості мови. Сучасні проблеми автоматики та електротехніки: Матеріали всеукраїнської наук.-техн. конференції. Миколаїв, НУК, С. 78 – 80.

УДК 621.318; 004.056

## ЕЛЕКТРОМАГНІТНА СУМІСНІСТЬ ЯК ВПЛИВОВИЙ ФАКТОР РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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

На перших етапах розвитку теорії електромагнітної сумісності (ЕМС) більшість наукових робіт була пов'язана із ЕМС радіообладнання. Зокрема, науковці і практики намагалися вирішити питання шумів, завад і заземлення для забезпечення якісного радіозв'язку.

На даний час проблема ЕМС розглядається у глобальному масштабі, і її вирішенню присвячена діяльність:

- міжнародних, регіональних і національних організацій із стандартизації, що має на меті гарантувати якість товарів і послуг на міжнародному ринку [1-4];

- науковців, виробників товарів і постачальників послуг, спрямована на вирішення питань ЕМС на теоретичному і практичному рівнях для певних пристроїв, установок, технологій і галузей, які характеризуються різними діапазонами робочих частот і потужностей, працюють в різних електромагнітній обстановці (ЕМО), мають різний рівень імунітету (несприйнятливості) до відхилень ЕМО від нормованих значень і є джерелами емісії в різних діапазонах частот і потужностей [5-10].

Збої, викликані порушенням ЕМС, можуть впливати на порушення штатних режимів роботи засобів обробки інформації і засобів захисту інформації.

Метою даної роботи є визначення впливу порушення ЕМС на ризики інформаційної безпеки.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- визначити фактори, що негативно впливають на ЕМС комп'ютерних систем (КС);

- визначити наслідки порушення ЕМС з точки зору ризиків інформаційної безпеки.

Широке впровадження інформаційних технологій у всі сфери людської діяльності і побуту, поширення автоматизованих систем у технологіях виробництва різноманітних товарів, розповсюдження побутових електричних приладів суттєво ускладнюють електромагнітну обстановку для будь-якого сучасного електрообладнання.

Крім того, проблема ЕМС загострюється внаслідок наявних трендів у галузі електроніки [9], що є елементною базою пристроїв обробки та захисту інформації:

- наявна тенденція до зниження рівнів порогових напруг елементної бази. Перехід від технологій реалізації перетворювальних пристроїв і засобів обробки сигналів на електронних вентилях, порогові напруги для яких могли сягати до кількох сотень вольт, до сучасної цифрової логіки і мікросхем техніки, порогові напруги яких складають кілька вольт, підвищує чутливість сучасної елементної бази електронних пристроїв до впливу сторонніх електромагнітних полів (ЕМП), тобто знижує імунітет обладнання;

- наявна тенденція до пришвидшення процесів обробки та передавання сигналів, зумовлена необхідністю обробляти постійно зростаючі в інформаційному суспільстві обсяги інформації, ускладненням автоматизованих систем (АС) та систем керування ними. Для досягнення високих швидкостей обробки сигналів в електронних блоках обладнання застосовують схеми технічні рішення, які забезпечують коротші імпульси з крутими фронтами наростання і спадання. Зменшення часу наростання імпульсу призводить до того, що зростає доля енергії, яка перетворюється на високих частотах внаслідок появи високочастотних гармонік. Електромагнітні випромінювання високої частоти здатні поширюватися на великі відстані і, відповідно, негативно впливати на ЕМО як на місці експлуатації електрообладнання, так і на віддалених територіях;

- наявна тенденція до використання при виробництві електрообладнання не провідникових матеріалів для корпусів обладнання і/або його окремих блоків, наприклад, пластмаси. Такі матеріали є більш дешевими, однак вони не мають таких екрануючих властивостей як металевий корпус, внаслідок чого погіршується ЕМО на місці експлуатації обладнання. ЕМО на віддалених територіях також може погір-

шуватися, що залежить не тільки від наявних екранів, а й від частот електромагнітних випромінювань певного обладнання;

– наявна тенденція до мініатюризації напівпровідникових приладів і мікросхем, застосування планарних конструкцій також негативно впливає на ЕМО для цих компонентів електрообладнання, внаслідок зменшення відстаней, на які вони рознесені, підвищення щільності локальних енергетичних впливів і погіршення умов охолодження приладів, що викликає появу додаткових теплових шумів і гармонік, значимих струмів витоку.

Негативний вплив на ЕМС обладнання також має тенденція до викривлення напруги його живлення, яка зумовлена:

– сезонними і добовими коливаннями споживаної потужності в електричній мережі, вмиканням та вимиканням потужних споживачів, які спричиняють зниження, провали, відключення і підвищення напруги і, як наслідок, відключення, перевантаження та вихід з ладу обладнання, що змінює ЕМО;

– атмосферними явищами (грозовими розрядами), які можуть викликати появу високовольтних імпульсів і супроводжуються генерацією високочастотних коливань;

– взаємним впливом електрообладнання, розташованого на одній території, що викликає появу електричних шумів;

– процесами в установках і обладнанні споживачів, пов'язаними з генерацією в мережу гармонік, що викривлюють форму кривої споживаної потужності, і реактивної потужності, що змінює енергетичний баланс;

– застосуванням імпульсних джерел вторинного електроживлення в комп'ютерних мережах і системах, автоматизованих системах тощо. Джерела вторинного електроживлення ключового типу на даний час є одними з найбільш розповсюджених джерел електромагнітних завад, і спричиняють зростання рівнів і розширення спектрів завад, тобто змінюють гармонійний склад напруги живлення та ЕМО як на місці експлуатації джерел вторинного електроживлення і систем, для яких вони призначені, так і на територіях, віддалених на відносно невелику відстань, що зумовлено процесами згасанням;

– застосуванням електричної мережі як середовища передачі сигналів.

Перелічені вище впливові фактори призводять до зростання рівнів і розширення спектрів завад у системах електроживлення обладнання і ускладнення електромагнітної обстановки.

Порушення ЕМС може викликати збої в роботі в пристроїв обробки та захисту інформації, тобто є джерелом загроз інформаційної безпеки (ІБ). Загрози ІБ можуть бути класифіковані за різними критеріями, зокрема, згідно НД ТЗІ 2.5-004-99 [11] комплекс засобів захисту повинен надавати послуги:

– із захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Порушення ЕМС апаратних і апаратно-програмних засобів розмежування доступу може привести до тимчасової або остаточної втрати працездатності таких засобів і, відповідно, до порушення конфіденційності інформації;

– із захисту оброблюваної інформації від несанкціонованої модифікації. Порушення ЕМС апаратно-програмних складових обробки інформації в процесі запису і видалення інформації може привести до порушення цілісності інформації;

– із забезпечення доступності інформаційних ресурсів та послуг на певному проміжку часу і спроможності КС відновлюватися і функціонувати в разі відмови її компонентів. Порушення ЕМС безпосередньо впливає на стійкість до відмов і відновлення обладнання після збоїв;

– із забезпечення спостереженості як засобу підтримки спроможності КЗЗ виконувати свої функції. Порушення ЕМС може вплинути на індикатори процесів і результати само тестування.

Крім того, згідно НД ТЗІ 2.5-004-99 [11] для гарантування коректності реалізації КЗЗ для рівнів гарантій вище третього мають бути наявні методики забезпечення фізичної і технічної безпеки, в яких за змістом потрібно враховувати ЕМО, побічні випромінювання і наведення тощо, тобто приймати до уваги параметри ЕМС обладнання.

Таким чином, порушення ЕМС може бути джерелом загроз і, відповідно, ризиків порушення конфіденційності, цілісності і доступності інформації.

При керуванні ризиками інформаційної безпеки [12] загрози за ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) [13] класифікуються за іншими критеріями: за природою виникнення, за типом наслідків загроз і за типами зловмисників.

За природою виникнення порушення ЕМС може бути класифіковане як:

- навмисна загроза (категорія *D*), граничним випадком якої є застосування зловмисником електромагнітної зброї або засобів радіоелектронної боротьби;

- випадкова загроза (категорія *A*), якщо внаслідок випадкових, ненавмисних дій людини порушення ЕМС негативно впливає на інформаційні активи;

- природна (екологічна) загроза (категорія *E*), якщо порушення ЕМС відбувається внаслідок природних причин, які не пов'язані із цілеспрямованими або випадковими діями людини, наприклад, внаслідок деградаційних процесів в обладнанні, внаслідок грозових розрядів тощо.

За типом наслідків загроз порушення ЕМС може бути класифіковане як:

- а) фізичні пошкодження категорій *A*, *D*, *E*, якщо відхилення параметрів ЕМС є суттєвим і спричиняє вихід обладнання з ладу;

- б) природна подія (категорія *E*), якщо порушення ЕМС є наслідком грозових розрядів;

- в) втрата необхідних сервісів, якщо порушення ЕМС спричиняє: відмову телекомунікаційного обладнання або сервісних систем АС, наприклад, системи охолодження, (категорії *A*, *D*) або втрату електроживлення (категорії *A*, *D*, *E*);

- г) несправність внаслідок негативного впливу випромінювання різної природи: теплового, електромагнітного, радіаційного випромінювання, електромагнітних імпульсів (категорії *A*, *D*, *E*);

- д) компрометація інформації категорії *D*, якщо порушення ЕМС пов'язане з перехопленням і відправленням скомпрометованого сигналу, дистанційним шпигуванням, виявленням місця розташування або втручанням в роботу апаратних і програмних засобів;

е) технічна відмова категорії *A*, якщо наслідком порушення ЕМС є відмови і збої в роботі апаратно-програмних засобів, або категорій *A*, *D*, якщо наслідком є втрата ремонтпридатності АС;

ж) несанкціонована дія категорії *D*, якщо порушення ЕМС пов'язане з несанкціонованим використанням обладнання, викривленням даних, несанкціонованою обробкою даних;

з) компрометація функцій категорії *A*, якщо порушення ЕМС спричиняє помилки у використанні, або категорій *A*, *D*, *E*, якщо наслідком порушення ЕМС є порушення працездатності персоналу. В останньому випадку мають прийматися до уваги Державні санітарні норми і правила [14].

За типами зловмисників порушення ЕМС може бути класифіковане як:

- загроза, викликана діяльністю комп'ютерних злочинців, якщо для реалізації порушення ЕМС АС використовувалася комп'ютерна техніка;
- промислове шпигунство, якщо порушення ЕМС було здійснене в інтересах конкурентів або в інтересах певних урядових груп (в тому числі іноземних);
- загроза створена інсайдерами (співробітниками недостатньої кваліфікації; невдоволеними, зловмисними або недбалими співробітниками).

### **Висновки**

В даній роботі проведено аналіз проблеми ЕМС і визначені фактори, що негативно впливають на ЕМС комп'ютерних систем, та наслідки порушення ЕМС з точки зору ризиків інформаційної безпеки. Показано, що порушення ЕМС може бути класифіковане як загроза інформаційної безпеки і може непрямым чином викликати порушення конфіденційності, цілісності і спостереженості інформації та безпосередньо впливати на доступність інформації. Наявні тренди в динаміці факторів, які негативно впливають на ЕМС КС, дозволяють стверджувати, що ризики інформаційної безпеки внаслідок порушення ЕМС надалі зростатимуть.

### **Список літератури:**

1. Committed to connecting the world. About International Telecommunication Union (ITU). URL: <https://www.itu.int/en/about/Pages/default.aspx>

2. Committed to connecting the world. TIES Services. URL: <https://www.itu.int/en/ties-services/Pages/default.aspx>
3. ITU-R SM.329-10. Unwanted emissions in the spurious domain. URL: [https://www.itu.int/dms\\_pubrec/itu-r/rec/sm/R-REC-SM.329-10-200302-S!!PDF-E.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.329-10-200302-S!!PDF-E.pdf)
4. Перелік національних стандартів для цілей застосування Технічного регламенту з електромагнітної сумісності обладнання, затвердженого постановою Кабінету Міністрів України від 16.12.2015 № 1077, затверджений Наказом Міністерства розвитку економіки, торгівлі та сільського господарства України 08 грудня 2020 року № 2569. URL: <https://zakon.rada.gov.ua/rada/show/v2569915-20#n11>
5. Keller R.B Design for Electromagnetic Compatibility–In a Nutshell Theory and Practice (eBook). Open access publication. – Switzerland, Cham: Springer, 2023. – 423 p. URL: <https://library.oapen.org/bitstream/id/46a00bdeb59-42f6-a21f-072289004fa3/978-3-031-14186-7.pdf>
6. Даки О.А., Іваненко В.М., Федунів В.М., Бажак О.В. Електромагнітна сумісність систем зв'язку та оповіщення у надзвичайних ситуаціях на морі // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2021. – №2(68). – С.38-44. URL: <https://journal-hnups.com.ua/index.php/zhups/article/view/593/506>
7. Електромагнітна зброя: Від потенціалу до реалізації – ключ до підвищення обороноздатності України. URL: <https://zovu.org/elektromagnitnoye-oruzhiye-ot-potentsial/>
8. Король Е.Г., Пантелят М.Г. Требования по электромагнитной совместимости технических средств на объектах электроэнергетики и промышленности // Вісник НТУ "ХПІ". – 2013. – №15 (988). – С.35-60. URL: <http://pema.khpi.edu.ua/article/view/13170/11060/>
9. Лазебний В.С., Пілінський В.В., Швайченко В.Б. Електромагнітна сумісність електронних засобів: Навчальний посібник. Електронне мережне навчальне видання. – К.: КПІ ім. Ігоря Сікорського, 2023. – 343 с.
10. Розорінов Г.М., Платоненко А.В. Захист інформаційних систем від потужних електромагнітних випромінювань //Сучасний захист

інформації. – 2014. – №3. – С.16-20. URL: <http://journals.dut.edu.ua/index.php/dataprotect/article/view/180/178>

11. 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>

12. Корченко О.Г., Гнатюк С.О, Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. – К.: Центр навчально.-наукових. та науково-практичних видань НА СБ України, 2014. – 190 с.

13. 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](https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400)

14. ДСанПіН № 3.3.6.096-2002 Державні санітарні норми і правила при роботі з джерелами електромагнітних полів, затверджені наказом Міністерства охорони здоров'я України від 18 грудня 2002 року № 476, зареєстрованих в Міністерстві юстиції України 13 березня 2003 року за № 203/7524. URL: <https://zakon.rada.gov.ua/laws/show/z0203-03>

## **СЕКЦІЯ 5. СТВОРЕННЯ ПІДВОДНО-ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ ЗАХИСТУ МОРСЬКИХ ОБ'ЄКТІВ ТА АКВАТОРІЙ**

**УДК 629**

### **ВИБІР ОПТИМАЛЬНОЇ СИСТЕМИ КЕРУВАННЯ ЕЛЕКТРОПРИВОДОМ СТРІЧКОВОГО КОНВЕЄРА**

***Автор:** Аннич С.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*

До групи механізмів безперервного транспорту відносяться всілякі конвеєри (стрічкові, роликові, ланцюгові й ін.), канатні дороги, ескалатори, багаокабінні ліфти, трубопровідний транспорт і т.д. Ці механізми використовуються для переміщення вантажів або пасажирів у строго визначеному напрямку і на обмежену відстань. Їхні робочі органи приводяться в рух від електродвигунів безпосередньо або через механічні передачі, а в трубопровідному транспорті для створення підвищеного тиску використовуються компресори.

Стрічковий конвеєр (рис. 1) має станину 6, на кінцях якої встановлені два барабани: передній 7 – приводний і задній 1 – натяжний. Вертикально замкнута стрічка 5 обгинає ці кінцеві барабани і по всій довжині підтримується опорними роликами, які називаються роликкоопорами, – верхніми 4 і нижніми 10, укріпленими на станині 6. Іноді замість роликів застосовують настил. Приводний барабан 7 одержує обертання від привода 11 і надає рух стрічці уздовж траси конвеєра.

Стрічка завантажувється через одну або кілька завантажувальних лійок 2, розміщених на конвеєрі. Вантаж, що транспортується, переміщується на верхній (вантажонесучій, робочій) стороні стрічки, а нижня сторона є поворотною (зворотною). Можливо також транспортування вантажів одночасно на верхній і нижній сторонах стрічки в різних напрямках.

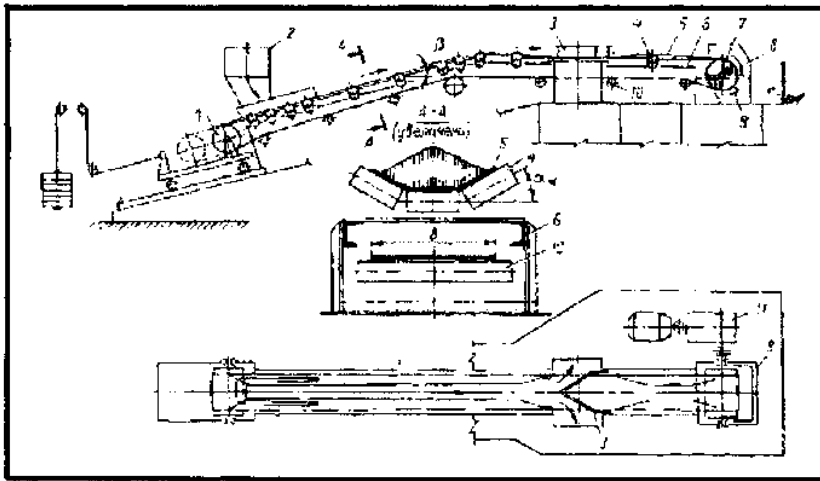


Рис.1 – Загальний вид стрічкового конвеєра

Вантаж вивантажується на передньому барабані 7 через розвантажувальну лійку 8 або в проміжних пунктах конвеєра за допомогою розвантажувальних пристроїв: плужкових 3 або барабанних розвантажувачів. Зовнішня поверхня стрічки очищається від прилиплих до неї часток вантажу очисним пристроєм 9, встановленим біля переднього барабана 7.

Стрічкові конвеєри застосовують для переміщення в горизонтальному і пологонахлонному напрямках різноманітних насипних і штучних вантажів, а також для міжопераційного транспортування виробів при поточковому виробництві. Вони одержали широке поширення у всіх галузях промисловості і є основними агрегатами механізації транспорту в ливарних цехах (подача і розподіл землі і збирання відходів), на топливоподачах електростанцій, підземного і наземного транспорту вугілля і породи у вуглевидобувній промисловості, руди, коксу і флюсів у металургії, будівельних матеріалів і корисних копалин у кар'єрах, зерна в зерносховищах, піску і каменю на будівництві каналів і гідроелектростанцій і ін.

Стрічкові конвеєри служать складовими частинами таких складних машин, як роторні екскаватори, перевантажувальні й відвальні мости, вантажно-розвантажувальні машини і т.п. Велике поширення

стрічкові конвеєри одержали завдяки можливості одержання високої продуктивності, великій довжині транспортування (до 3 – 4 км в одному конвеєрі і до 100 км у системі з декількох конвеєрів), простоти конструкції й експлуатації і високій надійності роботи.

По розташуванню на місцевості стрічкові конвеєри розділяють на стаціонарні і рухливі, пересувні і переносні, переставні (для кар'єрів відкритих розробок) і надводні, що плавають на понтонах.

По конструкції і призначенню розрізняють стрічкові конвеєри загального призначення і спеціальні: підземні, для харчової, мукомельно-круп'яної і комбікормової промисловості і потокового виробництва в приладобудівній, радіотехнічній і легкій промисловості.

По типу стрічки конвеєри бувають із прогумованою, сталевую цільнопрокатною і дровою стрічкою. Найбільше поширення одержали конвеєри з прогумованою стрічкою. По конструкції прогумованої стрічки, опорних ходових пристроїв і передачі стискального зусилля розрізняють стрічкові конвеєри, у яких стрічка є вантажонесучим і тяговим елементом (основний тип), стрічково-канатна і стрічково-ланцюгові, у яких стрічка служить тільки вантажонесучим елементом, а тяговим елементом є два канати або один ланцюг.

По профілю траси стрічкові конвеєри розділяються на горизонтальні, похилі і комбіновані: похило-горизонтальні і горизонтально-похилі з одним або декількома перегинами і зі складною трасою. При проектуванні конвеєра прагнуть по можливості приймати найбільш просту прямолінійну трасу. Складну трасу мають магістральні конвеєри відповідно до профілю місцевості.

Конвеєри з різними видами стрічок можуть мати по типу однакові траси, однак радіуси поворотів  $K_i$  і  $K_g$  і кути нахилу ( $\beta$  для кожного виду стрічок будуть різними. Кут нахилу конвеєра до обрію (залежить від коефіцієнта тертя вантажу, що транспортується, об стрічку при русі, а отже, від матеріалу і характеру поверхні стрічки), форми профілю стрічки (плоского або жолобчаста), кута природного укосу насипного вантажу, способу завантаження і швидкості руху стрічки.

Для забезпечення стійкого нерухомого положення вантажу на стрічці без його подовжнього сповзання вниз кут нахилу конвеєра по-

винний бути приблизно на 10—15° менше кута тертя вантажу об стрічку в спокої. Такий запас необхідний тому що через прогин стрічки кут її підйому в роликоопор виходить більшим, ніж загальний геометричний кут нахилу конвеєра. Крім того, стрічка на роликоопорах струшується через неминуче биття роликів, що сприяє сповзанню вантажу вниз. Струшування буде тим інтенсивніше, чим більше швидкість стрічки і грубіше виготовлені опорні ролики. Безперервне рівномірне завантаження забезпечує більший кут нахилу, чим періодичне завантаження з перервами потоку вантажу.

Прогумована стрічка в загальному виді має тяговий каркас, покритий з усіх боків еластичним захисним заповнювачем. Тяговий каркас сприймає подовжні розтяжні зусилля в стрічці і забезпечує її необхідну поперечну твердість, а заповнювач охороняє каркас від впливу вологи, механічних ушкоджень і стирання переміщуванням вантажем і поєднує його в єдине ціле.

Обкладки служать для захисту тягового каркаса від ушкодження і зношування, ударів вантажів, що транспортуються, при завантаженні і вологи навколишнього середовища.

По всій структурі конвеєрні лінії поділяються на розгалужені і нерозгалужені. Нерозгалуженою конвеєрною лінією називається однопотокова лінія, у якій на кожен конвеєр вантаж надходить тільки з одного попереднього конвеєра. Розгалуженої називається лінія, що складається з конвеєрів головного напрямку і конвеєрів, розташованих на його відгалуженнях і транспортуючих вантаж на конвеєри головного напрямку.

Розгалужена конвеєрна лінія вимагає два і більш маршрути, що утворюються конвеєрними відгалуженнями і тими конвеєрами головного напрямку, по яких вантаж транспортується від відгалуження до навантажувального пункту.

По технологічному призначенню конвеєрні лінії поділяються на стаціонарні, напівстаціонарні і пересувні.

Стаціонарні конвеєрні лінії складаються з конвеєрів, розташованих у капітальних виробленнях, термін служби яких визначається часом відпрацьовування шахтного получи (крила). Напівстаціонарні конвеєрні лінії складаються з конвеєрів, розташовуваних у дільничних виробленнях,

термін служби яких відповідає часу обробки ділянки. Пересувні конвеєрні лінії складаються з конвеєрів, розташовуваних в очисному вибої, просіки і печі, пересувка і перенос яких виробляється після кожного циклу роботи очисної машини і відпрацьовування просіка.

Стаціонарні конвеєрні лінії відрізняються великою продуктивністю, довжиною, значним терміном служби і часто бувають розгалуженими, що обумовлює необхідність окремого запуску декількох різних маршрутів. На противагу їм переносні конвеєрні лінії мають, як правило, один маршрут, відносно невисоку продуктивність і невеликі терміни служби. Напівстаціонарні конвеєрні лінії займають як би проміжне положення між стаціонарними і переносними. В одних випадках у них переважають властивості стаціонарних, в інші – переносних ліній.

**УДК 629.58**

## **ВИКОРИСТАННЯ ВІМ ТЕХНОЛОГІЇ ДЛЯ СТВОРЕННЯ ЗАСОБІВ МОРСЬКОЇ РОБОТОТЕХНІКИ**

***Автор:** Бабкін Г.В., к.т.н., доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Зростаючі воєнні і терористичні загрози з морських акваторій вимагають створення адекватних технічних засобів оборонного призначення. Доступ до морських комунікаційних шляхів, будь якої країни, що веде активну торговельну діяльність, має важливе значення для розвитку національної економіки і безпеки в цілому.

У відповідності до нової Військової Доктрини України, на ВМС ЗС України покладається завдання щодо захисту країни від можливої агресії, забезпечення контролю морської обстановки в прибережних водах і забезпечення національних інтересів в межах виключної економічної зони [1].

Серійне виробництво засобів морської робототехніки (ЗМР) вимагає виконання комплексу заходів з проведення проектно-конструкторських робіт для створення конкурентоздатних нових видів підводної робототехніки та формування команд для їх ефективного застосування.

Створення засобів морської робототехніки є наукоємний процес, якій включає в себе значну розрахункову складову, що пов'язана з значним об'ємом робіт пов'язаних з математичним моделюванням складових ЗМР. При цьому основне навантаження розрахункових робіт приходить на початкові етапи проектних робіт, та на передпроектні етап.

Скорочення термінів виконання цих етапів та витрат на їх проведення можливо за умов поширеного використання ВІМ технології [2].

Використання ВІМ технології передбачає повний перехід від фізичного та «гібридного» моделювання до математичного, об'єднання розрізнених математичних моделей елементів ЗМР в єдину комплексну модель з використанням: віртуальних прототипів, чисельного моделювання та результатів натурних випробувань, комплексні бази даних елементів ЗМР зі всіма відомими характеристиками елементів, поєднаних загальним програмним забезпеченням з елементами штучного інтелекту. Тобто створити інформаційно-моделюючий програмний комплекс (ІМПК).

Для створення ефективного ІМПК який вирішує проектні завдання необхідно сформулювати систему критеріїв, за допомогою яких ІМПК буде приймати рішення по формуванню складу ЗМР, а головний конструктор оцінювати результат його роботи.

Застосування сучасних інформаційних технологій під час проектування ЗМР робить процес більш ефективним та скорочує час проектно-конструкторських робіт порівняно з традиційними способами проектування. Досягається це за рахунок того, що такий спосіб передбачає не роботу з документацією в її класичному розумінні, а з комплексами програм, які генерують модель і всі необхідні для виробництва на верстатах з ЧПК файли, а потім самі ними розпоряджаються. Завдяки чому на першому етапі проектування є можливість отримати орієнтовну, не оптимізовану конструкцію майбутнього ЗМР і заощадити час та інші ресурси проекту.

Це дає змогу ставити на порядок денний питання щодо започаткування галузевої програми розробки і створення ЗМР в інтересах організацій України та інших міністерств України, які проводять активну виробничу діяльність на морі.

Крім того, такий вид науково ємної продукції може мати успіх на зовнішньому ринку і бути джерелом валютних надходжень для бюджету України.

**Список літератури:**

1. Воєнна доктрина України. Затверджено Указом Президент України від 24 вересня 2015 року № 555/2015.
2. Талапов, В. В. Основы ВІМ: введение в информационное моделирование зданий : учебное пособие. – Москва : ДМК Пресс, 2011. – 392 с.

**УДК 629**

**БУКСИРНА ЛЕБІДКА МАЛОГАБАРИТНОГО ПІДВОДНОГО  
АПАРАТУ**

*Автор: Гаринкін Д.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*

Людству завжди було цікаво – а що там, під водою. Іноді цей інтерес приносив пряму вигоду – тут можна говорити про ловців перлин. Цікаво відмітити, що з давніх давен до нас дійшли так звані міфи про пірнальників (птиця, черепаха..), що дістають землю з морського дна та створюють сушу -- варіант створення світу.

Останні десятиріччя людство звернуло пильну увагу на ресурси дна мирового океану. Я вважаю, що це обумовлено трьома головними чинниками. По-перше це вичерпання легкодоступних мінеральних ресурсів суші, або прогнози про неминучість такого розвитку подій (Римський клуб, наприклад), по-друге органічно присутня риса капіталізму – експансія (це подібно велосипеду — зупинка неминуче приведе до падіння) и по-третє, наявність к середині 20-го сторіччя досить досконалих технічних засобів (водолазні костюми, водолазні дзвони, технологія будівництва населених підводних апаратів, що була відпрацьована на сотнях бойових підводних човнів). Сюди ж можна відне-

сти винахід аквалангу (англ. SCUBA, Self-contained underwater breathing apparatus, автономний апарат для дихання під водою), та створення титанової промисловості у найбільш могутніх індустріальних державах того часу (США та СРСР). Як говорив Карл Макс, -- необхідність штовхає науку сильніше за десяток університетів. Маю відмітити, що технічний прогрес у освоєнні глибин був вельми довгим (десятиріччя аж з середини 19-го століття, та багатім на жертви). Перші водолази гинули від отруєння киснем та азотом під великим тиском, або від декомпресійної хвороби («кесонка»). Жюль Верн написав «20 тисяч льє під водою» ще у 1870р, де описав вже існуючий на тій час апарат для дихання під водою, створений Бенуа Рокейролем та Огюстом Денейрузом.

На початку великої епохи освоєння глибин малими населеними апаратами (після Другої світової війни), йшлося, наприклад, про майбутню добичу залізно-марганцевих конкрецій з великих глибин, та використання глибоководних родовищ газогідратів для потреб енергетики. Поки це фантастика, навіть не з технологічних причин, а скоріше з економічних. Але добича нафти та природного газу з шельфу та більших глибин за допомогою великих бурових платформ – це вже кілька десятиріч звичне явище для людства. Для контролю та обслуговування існуючого підводного техногенного середовища (підводні кабелі зв'язку, електрики, Інтернету, трубопроводів, опор мостів та ін.) вже давно використовуються малі підводні апарати. Населені малі підводні човни гарно послужили людству (з відомих широкої спільноті фактів я наведу два, це – кінозйомки знаменитого затонулого пароплаву «Титанік», та підняття втраченої американської ядерної зброї зі дна океану біля іспанського сільця Паломарес). Але я вважаю, що майбутнє як під водою, так і у космічному просторі виключно за безпілотними апаратами.

Ми знаємо поверхню місяця краще, ніж дно мирового океану. Підводне середовище є набагато смертоносним, ніж космос. Якщо аварія населеного апарату стається на глибині, то допомогти з поверхні практично неможливо навіть у наші часи (підводні човни «Курськ», «Скорпіон», «Трешер»), і зовсім вчора батискаф «Титан». Як правило, такі катастрофи розвиваються дуже швидко внаслідок колосальної

різниці в тиску в апараті, та ззовні. Намагання виключити таку тенденцію істоту як людина із процесу, здешевити підводні апарати за рахунок відмови від герметичного міцного корпусу та систем життєзабезпечення екіпажу, та розвиток техніки (матеріалознавство, системи управління, емки та відносно легкі акумулятори), дозволили у наш час (точніше, цей процес тривав останні років 20), таки створити безпilotні підводні апарати. Вони поділяються на два великих класу – автономні роботи та буксировані або телекеровані апарати. Важливою частиною комплексу «судно забезпечення – телекерований апарат» є буксирна лебідка. Вона повинна «відпрацьовувати» коливання судноносія апарату від хвиль та забезпечити відсутність коливань підводного апарату, його безпечний спуск та підйом на борт.

## УДК 629

### **ДОСЛІДЖЕННЯ ТА АНАЛІЗ МЕТОДІВ ВЕКТОРНОГО КЕРУВАННЯ ДВИГУНОМ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО КЕРУВАННЯ СУДНОВИМИ ЕЛЕКТРОПРИВОДАМИ**

***Автор:** Жигадло О.М., 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*

За минулі роки асинхронні двигуни знайшли дуже широке застосування у різних галузях промисловості та на транспорті. Це основний споживач електричної енергії на судні. В останні два десятиліття регульований асинхронний електропривод зазнав настільки суттєвих змін у своєму розвитку, що повністю витіснив із багатьох областей синхронний привід та привід постійного струму. Це пов'язано, перш за все, з досягненнями в галузі силової електроніки та мікропроцесорної техніки, на основі яких були розроблені перетворювачі частоти, що забезпечують керування асинхронними короткозамкнутими двигуна-

ми з енергетичними та динамічними показниками, порівнянними або перевершуваними показниками інших приводів.

Висока швидкість обробки інформації сучасними процесорами дала поштовх розвитку старих та розробці нових алгоритмів управління системою «перетворювач-двигун». Сьогодні частотне управління для асинхронного приводу свого роду є технічним стандартом. У той же час не використовуються в сучасних розробках такі способи управління та пристрої як управління напругою, управління введенням додаткових опорів у ланцюги статора та ротора, управління змінною числа пар полюсів та ін. Практично у всіх сучасних системах управління інформація про електромагнітні процеси в двигуні представлена до векторної форми.

**Основною метою даного проекту є:**

- дослідження та аналіз методів та способів векторного управління сучасних типів удосконалених електродвигунів та обґрунтування їх використання для заміни застарілих типів електроприводів;

- произвести анализ систем управления электродвигателем и осуществить выбор способа векторного управления для повышения эффективности работы устройства с преобразователем частоты(ПЧ);

- произведены расчеты величины индуктивности для методики выбора дополнительного оборудования для схемы ПЧ — АД при модернизации судов. Результаты расчетов и технические характеристики параметров оборудования сведены в таблицы;

- наведено приклад використання методики вибору перетворювачів частоти, вхідних дроселів, згладжуючих та моторних дроселів, для сучасного ефективного електроприводу, що відповідає всім технічним умовам та вимогам з енергозбереження, надійності та довговічності.

УДК 629

## ЕЛЕКТРОПРИВОД РУШІЙНО-РУЛЬОВОГО ПРИСТРОЮ ПІДВОДНОГО АПАРАТА

*Автор: Лебедік В.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*

Діяльність людини на морі сьогодні все більш характеризується виконанням робіт під водою. До таких робіт відносяться, пошукові, дослідницькі, аварійно-рятувальні, а також роботи по будівництву гідротехнічних споруджень. У зв'язку з освоєнням ресурсів Світового океану значно зріс обсяг робіт з дослідження донної поверхні.

На глибинах, що перевищують водолазні, дослідницькі і розшукові роботи виконують буксируємі чи самохідні підводні апарати, які на сьогоднішній день досить розвинені та класифікуються за різними ознаками. За способом переміщуватися під водою ПА розділяють на самохідні та несамохідні. Переміщення у просторі та керування самохідними ПА здійснюється за допомогою рушійно-кермового комплексу. При русі ПА переміщується в тривимірному просторі, для чого йому необхідні шість ступенів свободи — поступальний рух рівнобіжно осям координат  $x$ ,  $y$ ,  $z$  і обертальний рух навколо цих осей. Рушійно-рульові комплекси сучасних апаратів дозволяють здійснювати поступальний рух по осі  $x$  (передній і задній хід) і по осі  $y$  (занурення і виринання), обертання навколо осі  $y$  (поворот) і навколо осі  $z$  (диферент), переміщення уздовж осі  $z$  (рух лагом) і обертання навколо осі  $x$  (крен).

РКК — комплекс спеціально орієнтованих приводів, що забезпечують прокольний рух, маневрування у просторі та стабілізацію ПА у водному середовищі під час виконання робочих операцій.

Звичайно РКК складається з маршових рушіїв, які забезпечують повздовжній рух та одного або декількох маневрових кермових при-

водів – для маневрування у просторі. Найбільш поширеними типами рушіїв є гребні гвинти в направляючій насадці. Як електропривод для РКК ПА можуть використовуватися електродвигуни постійного і змінного струму як в герметичному, так і заглибному виконання.

Рушійно–рульовий комплекс у загальному випадку повинний забезпечувати гарні ходові і маневрені якості при мінімальній витраті енергії для виконання наступних операцій:

- занурення під воду і виринання ПА на поверхню;
- рух у будь-якому напрямку з можливістю реверса і зміни швидкості в широкому діапазоні;
- зависання в заданій крапці товщі води в горизонтальному положенні чи з визначеним кутом диференту;
- маневрування в обмеженому просторі і на складному рельєфі поблизу дна;
- безпечна посадка і виринання з ґрунту.

До складу рушійно–рульових комплексів можуть входити маршові, підрулюючі пристрої і рушії різного типу, розміщення яких на підвідному апараті залежить від його призначення і визначається в процесі проектування. Більшість підвідних апаратів, особливо дослідницьких, звичайно мають відносно малу швидкість, тому для маневрування сучасних підводних апаратів виконують рушії на поворотних колонках, а також підрулюючі пристрої, що представляють собою гребні гвинти, встановлені усередині горизонтальних чи вертикальних каналів (гвинти в насадках). При цьому необхідний ступінь стійкості руху ПА забезпечується або визначеною формою апарата, або стабілізаторами, закріпленими на апараті в необхідній площині.

Електродвигун, розміщений в герметичному міцному корпусі, що захищає його від дії навколишнього середовища. Істотним недоліком при цьому є великі втрати на тертя в сальникових ущільненнях місця виходу валу електродвигуна з міцного корпусу, значні аксіальні сили, що виникають під дією зовнішнього гідростатичного тиску на вал, а так само обмеження електромагнітних навантажень і щільності струму в обмотках зважаючи на небезпеку перегріву елементів машини в повітряному замкнутому просторі корпусу. Тому частіше використовують заглибні електродвигуни, заповнені рідким діелектриком, який

знаходиться під тиском навколишнього середовища і відділяється від неї корпусом з компенсатором у вигляді сифона або діафрагми. Тому хоча сам електродвигун працює при високому гідростатичному тиску, сальникове ущільнення валу випробовує малий перепад тиску завдяки внутрішній протидії рідкого діелектрика. Перевагами заглибних електродвигунів є також можливість підвищення електромагнітних навантажень унаслідок хорошої теплопровідності рідкого діелектрика, забезпечення механічної і електричної міцності ізоляції обмоток, захисту активного заліза від корозії, мастила підшипників.

Існує велика кількість різновидів електричних двигунів. Кожний тип з яких має свої особливості, переваги та недоліки. Аналіз характеристик різних типів двигунів та досвід роботи ПА показав, що найбільш раціональним варіантом є використання серійних асинхронних двигунів змінного струму. Це зумовлено наступними чинниками:

- простота конструкцій АД;
- заглибне виконання технічно простіше реалізувати для двигунів змінного струму, особливо для АД;
- використання серійних двигунів значно спрощує процес проектування та дозволяє використовувати серійні системи курування. Все це значно здешевлює конструкцію ПА;
- можливість вибору електродвигуна з невеликою синхронною частотою обертання, що дає змогу відмовитись від редукторів. Це полегшує конструкцію рушія, здешевлює виріб, зменшує розміри заглибного корпусу, при цьому можливо використовувати меншу кількість рідкого діелектрика;
- можливість вибору оптимальної частоти обертання. Для ПА найбільш оптимальна швидкість обертання гребного гвинта 1200-1500 об/хв. При цьому чим більше швидкість – тим менші розміри гвинта та навпаки;
- однофазний серійний двигун досить просто модернізувати у трьохфазний.

Єдиним суттєвим недоліком таких двигунів є масо габаритні показники.

### Список літератури:

1. Ястребов В. С., Горлов А. А., Симинський В. В. Електроенергетичні установки підводних апаратів – Л. Судостроение, 1986. – 184 с.
2. Блінцов В.С., Магула В.Е. Проектування самохідних прив'язних підводних систем. – Київ: Наукова думка, 1997. – 140 с.
3. Блінцов В.С. Прив'язні підводні системи. – Київ: Наукова думка, 1998. – 232 с.
4. Філатов Л.С., Гімейн С.М. Довідник по техніці безпеки (у питаннях і відповідях). – 2-е вид., перероб. і доп. – М.: Россільгосвид, 1983. – 303 с.

### УДК 629

## ОПТИМІЗАЦІЯ ХАРАКТЕРИСТИК ЕЛЕКТРООБЛАДНАННЯ БУКСИРУВАНОЇ ПІДВОДНОЇ СИСТЕМИ

*Автор:* Мімра В.Я., 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

Енергетична забезпеченість підводного апарату є найважливішим показником, який визначає його можливості і ефективність використання. Система енергозабезпечення підводного апарату виконує дві функції: по-перше, забезпечує його достатнім рівнем електроенергії, по-друге, забезпечує режими мінімізації споживання електроенергії. Однак ефективність системи енергозабезпечення підводного апарату в більшій мірі залежить від складу його бортового обладнання та оптимальності характеристик енергоспоживання кожного елемента.

Комплекси на базі підводних апаратів вирішують цілий спектр важливих і актуальних завдань цивільних і військових відомств:

- екологічний моніторинг водного середовища, в тому числі спостереження за зміною флори і фауни в заданій акваторії;
- донна геологорозвідка в важкодоступних районах світового океану і в арктичному регіоні;
- пошукові роботи і обстеження затонулих об'єктів;

- фото та відеозйомка в науково-дослідних, промислових і військових цілях;
- патрулювання водних рубежів і об'єктів;
- супровід військових цілей;
- обслуговування комунікацій портів;
- ведення інформаційної боротьби шляхом створення помилкових цілей і перешкод;
- проведення розвідки пунктів базування ймовірного противника;
- установка, виявлення або знищення мінних полів;
- підводне обстеження корпусів суден, платформ, трубопроводів та ін.

Кожен з існуючих типів підводних апаратів, автономні і прив'язні, по-своєму залежать від енергетичного забезпечення. Автономні – від енергоємності енергоносіїв, прив'язні – від досконалості передачі і перетворення енергії, здатності енергосистеми забезпечувати пікові навантаження.

Для прив'язних підводних апаратів, найважливіше значення набуває система перетворення і передачі електроенергії по кабелю, часто значної протяжності. Оптимальний вибір обладнання істотно визначає масогабаритні характеристики не тільки самого підводного апарату, а й кабелю, спускопод'ємного пристрої і в кінцевому підсумку – судна забезпечення.

Найважливіше значення має вибір способу передачі електроенергії по кабелю. Тут центральним стає питання зазнавати перешкод яку створює енергетичний канал, на надзвичайно чутливі канали передачі інформації, управління і телеметрії.

**Мета дослідження** – розробка та дослідження основ побудови енергетичних систем підводних апаратів.

Для досягнення поставленої мети в під час досліджень вирішені наступні основні завдання:

- аналіз основних факторів, що впливають на вибір характеристик енергетичної системи буксированих підводних апаратів.

– аналіз і оцінка ступеня впливу систем буксированого підводного апарату на параметри енергетичної системи.

– дослідження впливу структури і ступеня надмірності рушійно-кормового комплексу, типу і структури системи передачі енергії на структуру енергетичної системи буксированого підводного апарату.

**Об'єкт дослідження** – система енергозабезпечення буксированих підводних апаратів.

**Методи дослідження.** Науково-прикладна задача оптимізації характеристик електрообладнання буксированого підводного апарату вирішувалася в рамках новітніх концепцій і сучасних технологій створення засобів морської робототехніки. При виконанні досліджень застосовувалися методи моделювання елементів системи в середовищі Matlab – Simulink.

Наукова новизна отриманих результатів полягає в подальшому розвитку науково-методологічних основ створення засобів морської робототехніки

Отримала подальший розвиток основи побудови систем енергозабезпечення буксированих підводних апаратів, що забезпечують мінімальне енергоспоживання, шляхом оптимізації характеристик енергоспоживання базових споживачів енергії.

#### **Список літератури:**

1. Кувшинов Г.Е., Чупина К.В. Спуско-подъемное устройство. Патент на изобретение № 2114756С1 кл. 6В63 В27/ОВ. БИ № 19, 1998.
2. Тимошенко С.П. Колебания в инженерном деле. М.: Машиностроение, 1985. – 472 с.
3. Иванченко Ф.К. Конструкция и расчет грузоподъемных машин. – Киев: Высш. шк., 1988. – 422с.
4. Бугаенко Б.А., Магула В.Э. Специальные судовые устройства. – Л.: Судостроение, 1985. – 392 с.
5. Судовые спуско-подъемные устройства. Бугаенко Б.А., Резчик Ю.И., Сорокин Б.И., Хононов А.З. – Л.: Судостроение, 1980. – 173 с.

УДК 629

## **АЛЬТЕРНАТИВНЕ ДЖЕРЕЛО ЖИВЛЕННЯ БЕРЕГОВОГО ПОСТУ МОНІТОРИНГУ ПІДВОДНОЇ ОБСТАНОВКИ**

***Автор:** Решетило О.Є., 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*

З самого початку повномасштабної військової агресії з боку РФ щодо України об'єкти енергетичної інфраструктури нашої країни були і залишаються одними з головних цілей для ворожої армії. Спочатку це були нафтопереробні заводи, сховища нафтопродуктів, електростанції та підстанції, що живлять залізницю, а зараз – об'єкти критичної енергетики. Регулярне та цілеспрямоване руйнування енергетичної інфраструктури України спричинило аварійні та стабілізаційні відключення електроенергії, відключення вуличного освітлення, обмеження руху метро та тролейбусів і споживання енергії промисловими підприємствами.

Війна в Україні також сильно вплинула і на світові енергетичні ринки, призвівши до нестабільності цін, дефіциту поставок, проблем з безпекою та економічної невизначеності – усього того, що Міжнародне енергетичне агентство (МЕА) вже називало «першою справді глобальною енергетичною кризою».

Усі ці події змусили ряд країн зосередитися на питаннях енергетичної безпеки і формуванні надійного та різноманітного енергетичного балансу, невід'ємною частиною якого є також відновлювальна енергетика.

Відновлювана енергія – це енергія, отримана з природних джерел, що поповнюється з більшою швидкістю, ніж споживається. Така енергія не може вичерпатися на відміну від викопних видів палива (вугілля, нафти і газу), що є невідновлюваними ресурсами, на формування яких витрачаються сотні мільйонів років, а при їх спалюванні утворюються шкідливі викиди парникових газів.

Виробництво відновлюваної енергії створює набагато менше викидів, тому перехід від викопного палива до відновлюваних джерел енергії вважається ключем до подолання кліматичної кризи.

Крім того застосування відновлювальної енергії може допомогти знизити вартість електроенергії, зробити внесок у відмовистійку електричну мережу, створити робочі місця та стимулювати економічне зростання, генерувати резервну енергію на час відключення у поєднанні з її зберіганням, а також працювати з однаковою ефективністю як у малих, так і великих масштабах.

Відновлювані джерела енергії численні та оточують нас усюди. В даний час найбільш популярними серед них є:

- сонячна енергія;
- енергія вітру;
- гідроенергетика;
- енергія припливів;
- геотермальна енергія;
- енергія біомаси.

## УДК 629

### ЕЛЕКТРООБЛАДНАННЯ КАБЕЛЬНОЇ ЛЕБІДКИ ДИСТАНЦІЙНО КЕРОВАНОГО ПІДВОДНОГО АПАРАТА

*Автор: Стрельцов С.А., 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*

Впровадження на морських судах засобів автоматизації дозволяє підвищити експлуатаційну надійність і безпеку плавання, підвищити продуктивність і поліпшити умови праці, сприяє вдосконаленню форм технічного обслуговування. Останнім часом морський транспортний флот поповнюється великим числом судів, обладнаних засобами автоматизації, яка стала одним з головних напрямів технічного прогресу у всіх галузях промисловості. Основною особливістю автоматизації морських судів на даному етапі є комплексна автоматизація роботи

енергетичної установки, палубних механізмів, вантажних операцій і процесів навігації. Впровадження комплексної автоматизації зв'язане із застосуванням електронних обчислювальних машин (ЕОМ).

Досвід експлуатації світового транспортного флоту показує доцільність застосування ЕОМ для управління машинним відділенням, процесами навігації і вантажними операціями. Наприклад, на великотоннажних танкерах водотоннажністю 150 тис. т. для цієї мети встановлено дві ЕОМ. Перспективним напрямом розвитку комп'ютеризованих систем управління є їх децентралізація. Поява на ринку достатньо багатofункціональних і відносно дешевих мікроконтролерів дозволяє створювати окремі підсистеми для управління різним устаткуванням на судні.

Не є виключенням і підємне устаткування судна. Цифровий управляючий комплекс складається з мікроконтролера і пристрою сполучення з пультом управління верхнього рівня, а також з вихідними і вхідними пристроями. Вихідними є погоджуючі та виконавчі пристрої. Вхідними є пристрої для збору аналогової і дискретної інформації про стан об'єкту, в даній роботі — кабельної лебідки.

Джерелами інформації системи є аналогові і цифрові датчики енкадер, які характеризують параметри кабельної лебідки, як об'єкту, що контролюється та управляється.

Інформація управляючого цифрового комплексу поступає на пульт управління, мнемосхему, блоки узагальненої сигналізації, апаратуру управління системи і в енергетичну установку.

Система передбачає також наявність засобів надання інформації операторові. По виклику оператора на пульті виникає необхідна в даний момент інформація, а при виникненні відповідної ситуації автоматично включається діагностична програма і на екрані пристрою висвічується потрібний кадр і рекомендації по усуненню несправностей.

**Актуальність роботи.** Тема роботи є актуальною, тому що пропонується використовувати більш надійний одношвидкісний асинхронний двигун з короткозамкненим ротором та застосувати сучасні методи керування за допомогою мікропроцесорної техніки.

**Мета роботи.** Мета даної роботи — провести розрахунки та визначити пропозиції для модернізації електропривода кабельної лебідки судна.

**Об'єкт дослідження** – електропривод кабельної лебідки судна. Впровадження на судах систем автоматизації та керування системами за допомогою мікроконтролерів дозволяє підвищити надійність роботи електрообладнання на судні, підвищити продуктивність і поліпшити умови праці, сприяє більш якісному технічного обслуговування.

**Предмет дослідження** – характеристики електропривода кабельної лебідки на судні при застосуванні сучасних перетворювачів частоти.

**Практичне значення отриманих результатів.** Впровадження електро- приводів з сучасними перетворювачами частоти дозволяє: спрощувати керування електроприводами, зменшити фізичне навантаження на людину, що керує електроприводом, підвищити надійність роботи вантажопідйомних механізмів, використати більш дешевий та більш надійний одношвидкісний асинхронний електродвигун.

## СЕКЦІЯ 7. ШКОЛА МОЛОДИХ НАУКОВЦІВ

УДК 621.318; 004.056

### НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ ЗАСОБІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

*Автор:* Баранов А.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

Актуальність проблеми забезпечення електромагнітної сумісності (ЕМС) зумовлена широким впровадженням автоматизованих систем різного технологічного призначення і телекомунікаційних систем, в яких здійснюється формування, збереження, перетворення, обробка, передавання та приймання електромагнітних сигналів в різних діапазонах частот і потужностей. Ця проблема має глобальний характер, оскільки ЕМС є умовою стабільної масової технологічної діяльності в єдиному середовищі функціонування різноманітного обладнання.

Вирішенню задач забезпечення електромагнітної сумісності в різноманітних сферах технологічної діяльності присвячено багато робіт вітчизняних [1-4] і зарубіжних [5-6] науковців та практиків, а також низку нормативно правових актів [7-14], розроблених як міжнародними організаціями [7, 8, 10], так і українськими організаціями, які відповідають за якість товарів та послуг [9, 11-14]. Однак, на даний час питання забезпечення ЕМС технічних засобів захисту інформації, які застосовуються в автоматизованих системах управління технологічними процесами, із технологічним обладнанням, а також ЕМС телекомунікацій та певних технологічних засобів не може вважатися вирішеним.

Метою даної роботи є визначення нормативно-правової бази забезпечення електромагнітної сумісності засобів технічного захисту інформації і технологічного обладнання.

Для досягнення поставленої мети необхідно провести аналіз відкритих нормативно-правових актів і визначити базові нормативні документи та їх вимоги щодо забезпечення ЕМС засобів технічного захисту інформації і технологічного обладнання.

Нормативно-правові акти в сфері ЕМС, які діють в Україні, можуть бути поділені на наступні групи:

- закони України;
- постанови Кабінету міністрів України;
- накази і постанови окремих міністерств України, в тому числі накази адміністрації Держспецзв'язку України;
- державні стандарти України (ДСТУ) і діючі міждержавні стандарти (ГОСТ);
- галузеві нормативні документи, в тому числі документи із зони відповідальності Генерального штабу Збройних сил України;
- угоди щодо розподілу частот.
- Державні санітарні норми і правила, які встановлюють вимоги щодо гранично припустимих рівнів напруженостей постійних і змінних електромагнітних полів на робочих місцях.

Нормативні документи з ЕМС можуть бути класифіковані за різними критеріями:

1) Тип документу:

- стандарти;
- технічні звіти;
- публікації;
- норми.

2) Сфера дії:

а) діапазони частот;

б) територія:

- міжнародні нормативні документи;
- регіональні нормативні документи;
- національні нормативні документи;
- галузеві нормативні документи;
- стандарти підприємств та організацій;
- в) розташування в ієрархії стандартів:

– базові публікації, які містять загальні умови і/або правила забезпечення ЕМС і безпосередньо не використовуються для оцінювання ЕМС окремих виробів і груп виробів, однак на їх основі розробляються родові стандарти, і на них мають бути посилення в стандартах, що розробляються тематичними комітетами за видами виробів. За формою базові нормативні документи з ЕМС можуть бути технічними звітами або стандартами, а за змістом класифікуватися відповідно 4);

– родові (загальні) стандарти, які призначені для виробів, що функціонують у певній ЕМО і містять основні вимоги з ЕМС, опис випробувальних процедур і узагальнені критерії оцінювання робочих характеристик виробів з точки зору ЕМС. Родові стандарти застосовуються для виробів або систем у певній ЕМО, та якщо для них відсутні стандарти з ЕМС на групу однотипних виробів чи на конкретний вид виробу;

– стандарти на групи однотипних виробів, які визначають вимоги з точки зору ЕМС до електромагнітних параметрів на групи однотипних виробів, робочі режими устаткування, процедури проведення випробувань і вимоги до точності вимірювань. Ці стандарти посиляються на базові стандарти і виходять з вимог родових стандартів. Для груп виробів існує спеціальна класифікація ІЕС, яка, зокрема, містить такі групи як промислове устаткування; телекомунікаційне устаткування; технічні засоби інформаційних технологій тощо;

з) стандарти на конкретні види виробів, для яких потрібно визначати певні вимоги, відмінні від вимог групи. Серед стандартів на певні види виробів можна виділити: стандарти на компоненти (елементи); стандарти на пристрої (апаратуру); стандарти на обладнання; стандарти на системи; стандарти на установки.

3) Обов'язковість для виконання:

а) обов'язкові:

– національні стандарти, які мають силу закону, більшість з яких гармонізована з регіональними (EN) та міжнародними (ISO, IEC, CENELEC) стандартами і базується на регіональних договорах (договори ЄС, Директиви Ради ЄС, CENELEC, CISPR), міжнародних договорах (ООН, IEC) та рекомендаціях ISO, IEC;

б) рекомендовані, які можуть бути гармонізовані з регіональними та міжнародними стандартами і базуються на міжнародних рекомендаціях ISO, IEC, CENELEC, CISPR;

4) Зміст:

а) документи з визначень понять і класифікацій:

- стандарти з термінології;
- стандарти з опису електромагнітних явищ;
- стандарти з опису і класифікації електромагнітної обстановки;

б) документи з нормування вимог щодо:

- рівнів сумісності;
- емісії завод: стандарти щодо кондуктивних завод і стандарти щодо завод у навколишньому просторі;
- несприйнятливості (імунітету) устаткування: стандарти щодо імунітету до кондуктивних завод і стандарти щодо імунітету до завод у навколишньому просторі;

- високочастотних характеристик приймачів;

- небажаних сигналів передавачів;

в) методики проведення випробувань та вимірювань параметрів ЕМС.

5) Відомства, з якими необхідно узгоджувати стандарти.

6) Серія. Наприклад: IEC 61000-X-Y (міжнародний документ), EN 550ZZ (регіональний документ для ЄС). Серія являє собою – це комплект документів, зокрема, в серії IEC 61000-X-Y: 1 – загальні положення; 2 – ЕМО; 3 – норми; 4 – методики випробувань та вимірювань; 5 – настанови щодо встановлення обладнання та придушення завод; 6 – загальні стандарти; 7 – інше.

В Україні діють:

- «Технічний регламент з електромагнітної сумісності обладнання» [22], розроблений на основі Директиви 2014/30/ЄС [20] про гармонізацію законодавства держав-членів ЄС стосовно ЕМС і затверджений Постановою Кабінету міністрів України у 2015 році.

- «Перелік національних стандартів для цілей застосування Технічного регламенту з електромагнітної сумісності обладнання» [23], сформований на основі переліку гармонізованих європейських стандартів 2018 року і затверджений наказом Мінекономіки у 2020 році. На даний час для цього переліку входять 136 національних стандартів.

## **Висновки**

В даній роботі проведено аналіз відкритих нормативно-правових актів і визначені базові нормативні документи та їх вимоги щодо забезпечення ЕМС засобів технічного захисту інформації і технологічного обладнання ТО.

## **Список літератури:**

1. Король Е.Г., Пантелят М.Г. Требования по электромагнитной совместимости технических средств на объектах электроэнергетики и промышленности // Вісник НТУ "ХПІ". – 2013. – №15 (988). – С.35-60. URL: <http://pema.khpi.edu.ua/article/view/13170/11060/>
2. Лазебний В.С., Пілінський В.В., Швайченко В.Б. Електромагнітна сумісність електронних засобів: Навчальний посібник. Електронне мережне навчальне видання. – К.: КПІ ім. Ігоря Сікорського, 2023. – 343 с.
3. Мушаров А.А. Методика исследования функционирования систем электроснабжения военного назначения в условиях силовых деструктивных воздействий //Збірник наукових праць Харківського ун-ту Повітряних Сил. – 2013. – Вип. 2(35) – С.157-160.
4. Розорінов Г.М., Платоненко А.В. Захист інформаційних систем від потужних електромагнітних випромінювань //Сучасний захист інформації. – 2014. – №3. – С.16-20. URL: <http://journals.dut.edu.ua/index.php/dataprotect/article/view/180/178>
5. Keller R.B Design for Electromagnetic Compatibility–In a Nutshell Theory and Practice (eBook). Open access publication. – Switzerland, Cham: Springer, 2023. – 423 p. URL: <https://library.oapen.org/bitstream/id/46a00bde-bd59-42f6-a21f-072289004fa3/978-3-031-14186-7.pdf>
6. Kimihiro Tajima, Yoshiharu Akiyama, Tetsuya Tominaga, Tadahito Aoki Activities for Information Security Against Electromagnetic Radiation from Telecommunication Facilities // URL: <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200810sf1.html>
7. Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0030>

8. ITU-R SM.329-10. Unwanted emissions in the spurious domain. URL: [https://www.itu.int/dms\\_pubrec/itu-r/rec/sm/R-REC-SM.329-10-200302-S!!PDF-E.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.329-10-200302-S!!PDF-E.pdf)

9. ГОСТ 13109-97 Электрична энергия. Сумисність технiчних засобiв електромагнiтна. Норми якостi електричної енергiї в системах електропостачання загального призначення. URL: [https://dnaop.com/html/42313/doc-%D0%93%D0%9E%D0%A1%D0%A2\\_13109-97](https://dnaop.com/html/42313/doc-%D0%93%D0%9E%D0%A1%D0%A2_13109-97)

10. Директива № 2004/108/ЄС Європейського Парламенту та Ради ЄС щодо зближення законодавств держав-членiв ЄС щодо електромагнiтної сумисностi та про скасування Директиви 89/336/ЄЕС. URL: [https://zakononline.com.ua/documents/show/245590\\_\\_245655](https://zakononline.com.ua/documents/show/245590__245655)

11. Закон України «Про електронні комунікації». URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

12. Перелік національних стандартів для цілей застосування Технічного регламенту з електромагнiтної сумисностi обладнання, затвердженого постановою Кабінету Міністрів України від 16.12.2015 № 1077, затверджений Наказом Міністерства розвитку економіки, торгівлі та сільського господарства України 08 грудня 2020 року № 2569. URL: <https://zakon.rada.gov.ua/rada/show/v2569915-20#n11>

13. Про затвердження Переліку національних стандартів для цілей застосування Технічного регламенту з електромагнiтної сумисностi обладнання, сформованого на основі Рішення з імплементації Комісії (ЄС) 2019/1326 від 05.08.2019. Наказ № 74 від 15.01.2021 Міністерства розвитку економіки, торгівлі та сільського господарства України. URL: <https://zakon.rada.gov.ua/rada/show/v0074915-21#Text>

14. Технічний регламент з електромагнiтної сумисностi обладнання, затверджений постановою Кабінету Міністрів України від 16 грудня 2015 р. №1077. URL: <https://zakon.rada.gov.ua/rada/show/1077-2015-%D0%BF#n13>.

УДК 004.056:627

## ПРИНЦИПИ ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ КОРПОРАТИВНОЇ МЕРЕЖІ ПОРТУ

*Автор:* Грищенко С.Л., 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

Україна є морською державою з розвинуеною інфраструктурою портової галузі (рис.1) і серед країн Азово-Чорноморського басейну має найбільшу довжину морського узбережжя (2759,2 км). Крім того, територією України проходить частина водних шляхів країн Балто Чорноморського басейну. За висновками експертів Світового банку портова галузь України системне значення для світової торгівлі.

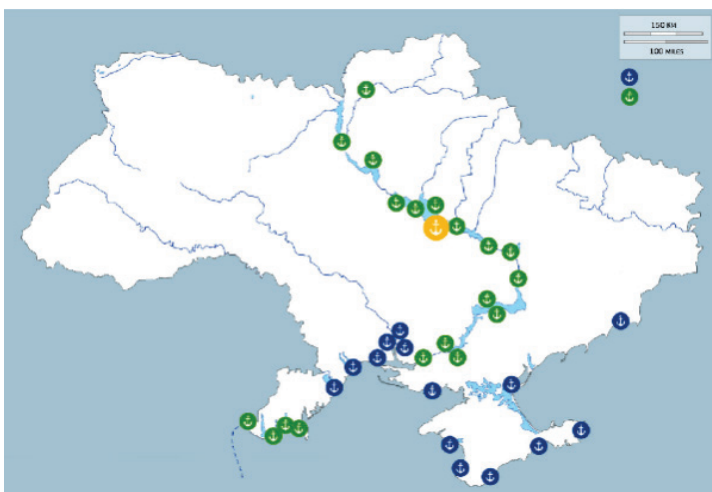


Рисунок 1 – Річкові (зелений колір) та морські (синій колір) порти України [1]

На даний час наявна тенденція до підвищення кількості кібератак об'єкти на портові інфраструктури як з метою вимагання грошей, так і з політичними цілями. Так у середині 2023 року була здійснена атака на web-сайти портів Нідерландів. За даними нідерландського інформаційного агентства RTL DDoS-атака була здійснена з російських та сербських IP-адрес проросійською хакерською групою під назвою «NoName057(16)» у відповідь на оприлюднені плани Нідерландів щодо закупки швейцарських танків для України. Під вплив атаки потрапили порти Роттердама, Амстердама та Гронінгена. Раніше спецслужби попередили про високу ймовірність загроз морській інфраструктурі Нідерландів з боку Росії. В результаті атаки web-сайт порту Амстердама 6 червня не працював більше години, а порти Гронінгена дві доби мали перебої у роботі мережі. Однак, за інформацією [2] жодних даних не було викрадено, і порти не сплачували зловмисникам жодних викупів.

Атаки на портові інфраструктури відбуваються на фоні загального зростання кіберзлочинів. За даними [3] у 2022 році у Нідерландах зареєстровано втричі більше кіберзлочинів ніж у 2018 році, однак одночасно знизилася кількість звичайних крадіжок зі зломом та пограбувань. На думку експертів розвиток кібершахрайства пов'язаний з пандемією COVID-19, яка обмежила можливості здійснення традиційних злочинів.

У січні 2022 року в Осло була атакована вірусом-вимагачем компанія Det Norske Veritas (DNV), яка спеціалізується на сертифікації обладнання, призначеного для використання в морському та прибережному середовищах, і є однією з найбільших у світі морських організацій. В результаті атаки DNV була змушена вимкнути підключені до системи ShipManager IT-сервери, внаслідок чого постраждало 70 клієнтів, які керували приблизно тисячею суден. Це становить близько 13% від загальної кількості суден (понад 13 175 суден), які обслуговує DNV.

Аналітики компанії Cisco [3] прогнозують, що послаблення процесів глобалізації, зумовлене COVID-19 і зростанням напруженості у відносинах між державами, формує глобальну кібербезпекову тенденцію до зростання активності спонсорованих державами хакерів та збільшення ризиків для різних секторів критичної інфраструктури.

Забезпечення інформаційної і кібербезпеки портів як об'єктів критичної інфраструктури має пріоритетне значення і повинне здійснюватися на основі новітніх технологій з дотриманням актуальних

нормативно-правових актів і врахуванням перспектив розвитку галузі і трендів в інформаційній безпеці.

За даними експерименту, проведеного коаліцією НАТО [3], зміцнити кібербезпеку об'єктів критичної інфраструктури можуть системи штучного інтелекту (СШ). Під час експерименту шість команд з країн-членів НАТО перевіряли ефективність СШ для захисту від кібератак уявної комп'ютерної системи в уявній інформаційно-комунікаційній мережі на уявній військовій базі. Результати експерименту показали ефективність СШ при організації реагування на кібератаки, спрямовані на критично важливі системи і сервіси, зокрема довели успішність виконання СШ наступних функцій:

- збирання даних і визначення шаблонів кібератак на критичну інфраструктуру;
- виявлення кібератак на основі аналізу мережевої активності;
- виявлення шкідливого програмного забезпечення.

Метою даної роботи є визначення особливостей побудови інтелектуальних систем управління інформаційною безпекою порту.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- визначити переваги інтелектуальних систем управління інформаційною безпекою;
- визначити особливості корпоративних мереж портів;
- визначити принципи побудови інтелектуальних систем управління інформаційною безпекою портів.

Система управління інформаційною безпекою (СУІБ) порту є частиною загальної системи управління, і спрямована на мінімізацію ризиків (бізнес-ризиків, репутаційних ризиків, екологічних ризиків тощо), які асоціюються із загрозами інформаційної безпеки. СУІБ порту функціонує за моделлю PCDA:

P – Plan (плануй: ідентифікація ризиків, їх оцінювання і вибір відповідних заходів для зниження критичності наслідків реалізації загроз);

D – Do (дій: реалізація обраних під час обробки ризиків заходів);

C – Check (перевіряй: моніторинг та аудит стану інформаційної безпеки з метою визначення ефективності СУІБ);

А – Акт (дій: виявлення недоліків СУІБ і прийняття рішення щодо коригування окремих процедур захисту інформації або модернізації СУІБ в цілому).

Інтелектуальними називаються системи управління, в яких для вирішення задач управління використовуються експертні системи, нечіткі системи, нейронні мережі, генетичні алгоритми та системи динамічного структурного моделювання. Загальною рисою таких систем є імітація природних процесів розпізнавання певних ознак стану об'єкта управління і процесів прийняття рішень людиною.

Застосування штучного інтелекту у системі управління підприємством [4], частиною якої є СУІБ, в загальному випадку дозволяє отримати ряд переваг:

- здатність зберігати без спотворень, властивих людській пам'яті, великі обсяги даних і виконувати процедури аналізу даних зі стабільними показниками якості на відміну від людини, яка може не тільки забувати якусь інформацію, а й порушувати задані алгоритми обробки інформації чи неправильно обирати ці алгоритми внаслідок поганого самопочуття, поганого настрою чи відволікання уваги на сторонні події;
- дружній до користувача інтерфейс, здатний забезпечити постановку задачі користувачем за допомогою обмеженого словника природної мови і отримання пояснень щодо ланцюга послідовних висновків СШІ (характерно для експертних систем);
- адаптованість до нових задач і нових умов експлуатації за рахунок здатності до навчання і самонавчання, що підвищує конкурентоспроможність підприємств (характерно для нейронних мереж);
- підвищення наочності і обґрунтованості висновків, отриманих в тому числі на основі нечітких даних;
- збільшення долі операцій, які виконуються автоматично, що дозволяє, з одного боку, підвищити швидкість процесів управління, зменшити кількість випадкових помилок персоналу та звужити поле діяльності інсайдерів, але з іншого боку – створює додаткові ризики внаслідок потенційної можливості втручання в автоматичні процеси зловмисників.

Оскільки порт виконує логістичні операції, то інтелектуальна система управління портом має виконувати ряд типових процедур [5], наведених на рис.2.

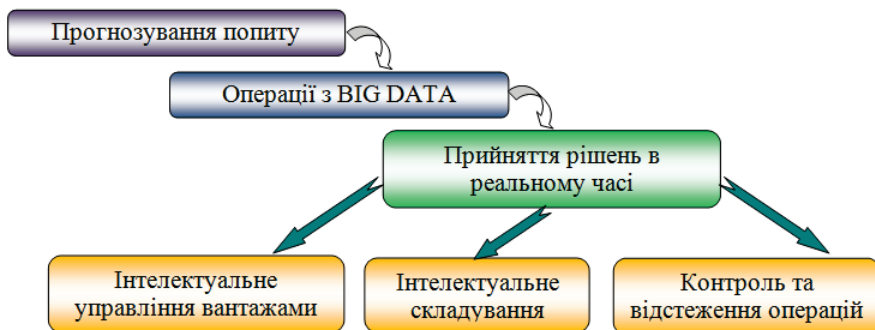


Рисунок 2 – Застосування штучного інтелекту в логістичних операціях

Корпоративні мережі призначені для підтримки функціонування організації-власника мережі. Ці мережі зазвичай не надають послуг стороннім організаціям або користувачам, і до груп користувачів корпоративної мережі входять тільки співробітники організації-власника (в даному випадку – порту або портової галузі).

Особливістю корпоративних мереж порту є тісна взаємодія інфраструктури порту і інфраструктури судна (рис.3), необхідність обміну даними і узгодження рішень з іншими портами, авіаперевізниками, автотранспортними підприємствами, залізницею, лоцманськими і прикордонними службами тощо, причому цей обмін даними і узгодження рішень потрібно здійснювати не тільки з українськими компаніями і службами. Тобто інтелектуальна система управління повинна базуватися як на українських, так і на міжнародних нормативно-правових актах, і надавати можливість враховувати особливі вимоги країн експорту та імпорту товарів. Порушення функціонування порту внаслідок кібератак може не тільки порушити логістичні ланцюги, а й негативно вплинути на стан кібербезпеки інших критичних інфраструктур.

При розробці інтелектуальних СУІБ для корпоративних мереж портів доцільно дотримуватися наступних принципів:

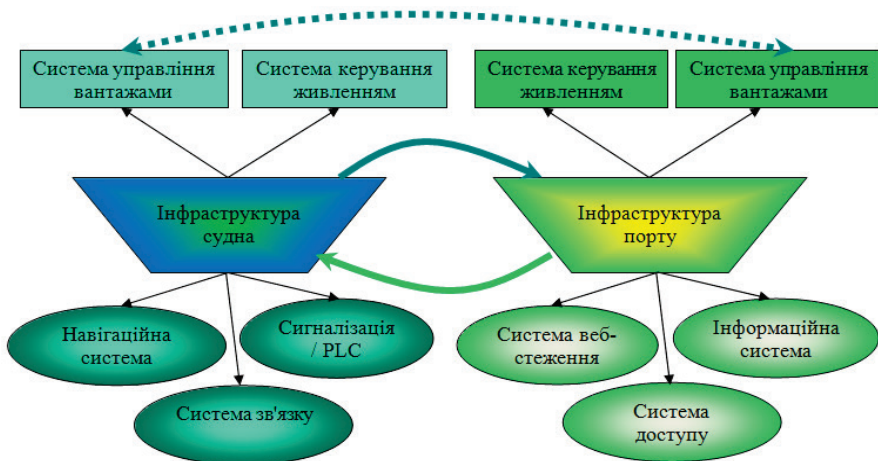


Рисунок 3 – Взаємозв'язок інфраструктур судна і порту

1) математичні основи обробки даних в СУІБ мають враховувати необхідність обробки нечітких даних і BigData;

2) архітектура СУІБ має містити:

а) блоки оперативного і організаційно-технічного управління, в яких формується керуюча інформація на основі інтелектуальних технологій;

б) підсистему узгодження інтересів зацікавлених сторін, яка є системою підтримки прийняття рішень для менеджерів порту;

в) підсистему прогнозування, яка складається з блоків:

- прогнозування сценаріїв подій в логістичній системі;

- прогнозування подій в корпоративній мережі;

- прогнозування наслідків впливу подій інформаційної безпеки в корпоративній мережі порту на стан інформаційної безпеки кооперованих з нею критичних інфраструктур;

- прогнозування наслідків впливу подій інформаційної безпеки в корпоративній мережі порту на бізнес-процеси;

3) моделі загроз порушення інформаційної безпеки мають бути представлені в формі, що дозволяє врахувати їх об'єктивну невизначеність, взаємозв'язки з активами, бізнес-процесами і вразливостями системи та будувати дерева загроз і подій в корпоративній мережі порту, в інфраструктурі порту і кооперованих з ним інфраструктурах;

4) оцінювання ризиків інформаційної безпеки проводиться методами, що дозволяють врахувати синергізм наслідків загроз;

5) обробка ризиків інформаційної безпеки в сегменті корпоративної мережі порту має виходити із раціонального варіанту реагування, який є узгодженим із зацікавленими сторонами і здійснюватися методом прийняття рішень на основі даних із об'єктивною і суб'єктивною невизначеністю в умовах обмежених витрат на реалізацію системи СУІБ і системи захисту і обмежених знизу показниках захищеності активів, бізнес-процесів і порту в цілому;

6) при розробці СУІБ слід враховувати рекомендації провідних компаній галузі [6, 7].

### **Висновки**

В даній роботі проведено аналіз відкритих літературних джерел і визначені переваги інтелектуальних систем управління, особливості корпоративних мереж портів і принципи побудови інтелектуальних систем управління інформаційною безпекою портів.

### **Список літератури:**

1. Коли в Україні річковий транспорт складе конкуренцію наземному. URL: <https://dzvin.media/news/koli-v-ukrayini-richkoviy-transport-sklade-konkurentsiyu-nazemnomu/>

2. Проросійські хакери атакували сайт найбільшого в Європі порту Роттердама. URL: <https://www.ukrinform.ua/rubric-technology/3722731-prorosijski-hakeri-atakuvali-sajt-najbilsogo-v-evropi-portu-rotterdam.html>

3. Cyber Digest. Огляд подій в сфері кібербезпеки, січень 2023. Національний координаційний центр з кібербезпеки. URL: [https://www.mbo.gov.ua/files/2023/NKCK/Cyber%20digest\\_january\\_2023\\_fin.pdf](https://www.mbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_2023_fin.pdf)

4. Ковтуненко Ю.В. Застосування штучного інтелекту у системі управління підприємством: проблеми та переваги // Економічний журнал Одеського політехнічного університету. – 2019. – №2(8). – С.92-99. URL: <https://economics.net.ua/ejopu/2019/No2/93.pdf>

5. Кирлик Н.Ю. «Штучний інтелект» та його використання в логістичних процесах // Актуальні проблеми економіки. 2021 – №9-

10(243-244). – С.59-66. URL: [https://eco-science.net/wp-content/uploads/2021/12/9-10.21.\\_topik\\_Kyrlyk-N.Yu\\_.59-66.pdf](https://eco-science.net/wp-content/uploads/2021/12/9-10.21._topik_Kyrlyk-N.Yu_.59-66.pdf)

6. MSC-FAL.1/Circ.3/Rev.2. Guidelines on maritime cyber risk management. URL: [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSF-FAL.1-Circ.3-Rev.2 %20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSF-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf)

7. Port Cybersecurity – Good practices for cybersecurity in the maritime sector. URL: <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector>

**УДК 004.056.5;057.2**

## **ПЕРСПЕКТИВИ ВИКОРИСТАННЯ КЛАСТЕРНОГО АНАЛІЗУ ДЛЯ ОЦІНЮВАННЯ ІНВЕСТИЦІЙ В ІНФОРМАЦІЙНУ БЕЗПЕКУ**

***Автор:** Задорожний 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*

Відповідно до Конституції України, одним із пріоритетів захисту суверенітету і територіальної цілісності нашої країни є забезпечення інформаційної безпеки. І це є однією з найважливіших функцій держави та справою всього Українського народу. Отже інформаційна безпека, ефективна протидія інформаційним загрозам – це питання об'єднання зусиль усіх сфер і напрямів: як органів державної влади, так і громадських об'єднань, наукових установ, медіа тощо.

Із зростанням науково-технічного прогресу зростатиме й важливість питання інформаційної безпеки громадянина, суспільства, держави. Тобто інформація стала чинником, який може призвести до значних технологічних аварій, військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, і чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав все більше здійснюється.

ся за допомогою інформатизації. Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися кругозір та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план постає аналіз сутності та форм проявів сучасних методів скритого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямках [7].

Актуальність теми дослідження визначається і загостренням проблем інформаційної безпеки в умовах інтенсивного вдосконалення технологій та інструментів захисту даних. Про це свідчать зростання порушень інформаційної безпеки і посилюється тяжкість їх наслідків. Так, загальне число порушень у світі щорічно збільшується більш ніж на 100%.

Таким чином, існують чинники, що визначають необхідність зваженого підходу до зазначеної проблеми. До них, насамперед, необхідно віднести постійно зростаючу кількість інформаційних загроз і ризиків, а також недостатній рівень забезпечення інформаційної безпеки існуючих інформаційних систем. Інформаційні ризики реалізуються через уразливості сучасних інформаційних систем, що підтримують різні види господарської діяльності промислових підприємств. У даній ситуації виникає необхідність забезпечення інформаційної безпеки соціально-економічної системи в цілому.

Сьогодні можна з упевненістю стверджувати, що інвестувати в інформаційну безпеку необхідно, так як інформація є важливим важелем впливу, а від якості забезпечення її безпеки може залежати навіть майбутнє країни. На даний час існує низка методів оцінювання ефективності інвестицій в інформаційну безпеку [3, 5], кожен з яких має свої переваги та недоліки.

**Метою даної роботи** є визначення доцільності використання кластерного аналізу для оцінювання інвестицій в інформаційну безпеку.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- визначити особливості процедур кластерного аналізу та алгоритмів оцінювання інвестицій на його основі;

– оцінити перспективи використання кластерного аналізу для визначення ефективності інвестицій в інформаційну безпеку.

Сутність кластерного аналізу полягає у здійсненні класифікації об'єктів дослідження не за однією ознакою, а за декількома одночасно. У результаті цього утворюються «кластери» – групи елементів, які характеризуються загальною властивістю або групи дуже схожих об'єктів. Для цього вводяться відповідні показники, що характеризують певну міру близькості за всіма класифікаційними параметрами.[5]

Мета кластерного аналізу полягає в пошуку наявних структур, що виражається в утворенні груп схожих між собою об'єктів. Водночас його дія полягає й у привнесенні структури в досліджувані об'єкти. Це означає, що методи кластеризації необхідні для виявлення структури в даних, яку нелегко знайти при візуальному обстеженні або за допомогою експертів [6].

Кластерний аналіз потребує здійснення таких послідовних кроків [6]:

- 1) визначення множини ознак, за якими будуть оцінюватися об'єкти класифікації;
- 2) оцінка міри подібності об'єктів;
- 3) застосування кластерного аналізу для створення груп подібних об'єктів;
- 4) перевірка достовірності результатів кластерного рішення.

Кожен із цих кроків відіграє значну роль у практичному здійсненні аналізу.

Визначення множини ознак, які покладаються в основу оцінки об'єктів ( $x_1, x_2, x_3, \dots, x_n$ ), у кластерному аналізі є одним із найважливіших завдань дослідження. Мета цього кроку повинна полягати у визначенні сукупності змінних ознак, яка найкраще відображає поняття подібності. Ці ознаки мають вибиратися з урахуванням теоретичних положень, покладених в основу класифікації, а також мети дослідження.

Інвестиційна стратегія держави, регіону – це стратегія стимулювання інвестиційної активності внутрішніх і зовнішніх інвесторів через важелі монетарної, фінансової політики, створення привабливого інвестиційного клімату з метою збільшення інвестиційних потоків в економіку держави (регіону), в пріоритетні сектори економіки, в розвиток інфраструктури, в розвиток людського капіталу, в підвищення рівня і якості людського життя. [9]

Для оцінки поточного стану складових інтегрального показника інформаційної безпеки національної економіки та визначення резервів для його підвищення проведено аналіз ефективності системи забезпечення інформаційної безпеки національної економіки та надати рекомендації щодо напрямів її покращення. [13]

В залежності від мети аналізу у науковій літературі та на практиці застосовують різні підходи. Традиційним вважається класична модель Дюпона «Рентабельність капіталу», яка передбачає використання двох груп показників: перша – для порівняння результатів діяльності з витратами; друга – для визначення ефективності використання окремих видів ресурсів [11, с. 454]. Для розрізнення рентабельних процесів від нерентабельних використовується процесно-орієнтований аналіз рентабельності (Activity – Based Profitability Analysis, ABPA), який було запропоновано М. Мейером та В. Маршалом [8]. Для комплексної оцінки суб'єктів господарювання, як правило, використовуються фінансові та нефінансові показники, які дозволяють збалансовано підійти до визначення ефективності діяльності. Такий підхід має назву «Управління результатами» (Performance Management) та був розроблений Р. Капланом та Д. Нортонем [10]. Для оцінки об'єктів з позиції потенційної можливості здійснення інвестицій традиційно застосовують методику аналізу, засновану на аналізі грошових потоків, яка передбачає розрахунок чистогрошового потоку (NCF -net cash flow), внутрішньої норми прибутковості (IRR – Internal Rate Of Return), модифікованої внутрішньої норми прибутковості (MIRR – Modified Internal Rate Of Return), індексу рентабельності (PI – profitability index), методу повернення на вкладені інвестиції (ROI – Return On Investment), чистої поточної вартості (NPV – Net Present Value) [4].

Основними недоліками перелічених методів є те, що їх використання доцільно для аналізу ефективності господарської діяльності та передбачає розрахунок різних коефіцієнтів, за результатами яких робиться висновок. У випадку оцінювання ефективності системи забезпечення інформаційної безпеки національної економіки доцільно використання саме математичних методів, які дозволяють проводити оцінювання параметрів відносно значень, які є найкращими у групі аналізованих об'єктів. Саме

тому для проведення дослідження було використано DEA-метод (Data Envelopment Analysis), який було запропоновано А. Чарнсом, В. Купером та Е. Родесом у 1978 році [1]. Цей інструмент не залежить від мети аналізу та використовується у багатьох галузях для оцінки ефективності складних систем, що відбувається шляхом рішення оптимізаційної задачі лінійного програмування.

Оскільки DEA-метод є ефективним для даних, які мають близькі характеристики, то доцільно додатково провести кластерний аналіз, який дозволить сформувати кластери країн з урахуванням не тільки кінцевого інтегрального значення, а й з урахуванням всіх його складових. З цією метою використаємо аналітичну платформу «Deductor Academic» [12], яка є потужним програмним інструментом для здійснення математичного моделювання та просунутої аналітики, а саме реалізації інструментів Data Mining. [13]

Перед початком здійснення кластерного аналізу необхідно здійснити перевірку вхідних даних на якість, виявлення викидів, дублікатів та протиріч. В результаті аналізу якості даних було виявлено викиди за індикатором оцінки політичної стабільності і відсутності насилля / тероризму, що свідчить про необхідність коректування даних за цим показником. В цілому отриманий показник якості для всіх змінних знаходиться у межах від 0,8299 до 0,9771, що говорить о високій якості початкового набору даних. Перевірка даних на наявність дублікатів та протиріч виявила, що вони відсутні у наборі даних. В результаті проведених перевірок було здійснено коректування тільки даних індикатора політична стабільність і відсутність насилля / тероризму, для чого було обрано метод обмеження для критичних значень викидів. [3].

Важливим напрямком у розвитку інформаційної безпеки країни є використання сучасних методів та інструментів, які спрямовані на підвищення її ефективності. Так, Коліні Ф. та Янчевський Л. [3] досліджують можливості використання математичних методів для підвищення ефективності формування стратегій захисту інформації, а саме вони виділяють кластерний аналіз та тематичне моделювання. Н. Фентон та М. Фейл [2] вивчають напрямки використання байєсівських причинно-наслідкових моделей ризику в процесі його оцінки для забезпечення більш ефективного управління та процесу прийняття рішень щодо кіберзахисту. [13]

## Висновки

В даній роботі визначені особливості процедур кластерного аналізу та алгоритмів оцінювання інвестицій на його основі і оцінені перспективи використання кластерного аналізу для визначення ефективності інвестицій в інформаційну безпеку. Показано, що кластерний метод для оцінки ефективності інвестицій в інформаційну безпеку бачимо, що кластерний метод є доволі інформативним та ефективним, і тому має перспективи для застосування, особливо у поєднанні DEA-методом.

## Список літератури:

1. Charnes A., Cooper W.W., Rhodes E. Measuring the efficiency of decision making units. *European Journal of Operational Research*. 1978. № 2. P. 429-444.
2. Fenton N., Neil M. Risk assessment and decision analysis with bayesian networks. In *Risk Assessment and Decision Analysis with Bayesian Networks*. CRC Press, 2012. P. 1-494. DOI: <https://doi.org/10.1201/b21982>.
3. Kolini F., Janczewski L. Clustering and topic modelling: A new approach for analysis of national cybersecurity strategies. In *Pacific Asia Conference on Information Systems (PACIS)*. Association For Information Systems. 2017.
4. Бланк И.А. Инвестиционный менеджмент. К. : Эльга-Н, Ника – Центр, 2001. 448 с.
5. Верескун М. В. Ефективність інвестицій в інформаційну безпеку: проблеми і рішення / М. В. Верескун // Вісник Приазовського державного технічного університету. Серія : Економічні науки. – 2015. – Вип. 30. – С. 220-227. – Режим доступу: [http://nbuv.gov.ua/UJRN/VPDTU\\_ek\\_2015\\_30\\_30](http://nbuv.gov.ua/UJRN/VPDTU_ek_2015_30_30).
6. Єріна А.М. Статистичне моделювання та прогнозування: Навч. посіб. / А.М. Єріна. – К.: КНЕУ, 2001. – 170 с.
7. Лужецький В. А. Інформаційна безпека: навч. посіб. / В. А. Лужецький, О. П. Войнович, А. В. Дудатьєв. – Вінниця : УНІВЕРСУМ-Вінниця, 2009. – 240 с.

8. Мейер М.В., Маршал В. Оценка эффективности бизнеса. М. : ООО «Вершина», 2004. 272 с.

9. Момот В. Є. Кластерний аналіз інвестиційного клімату у різних регіонах України / В. Є. Момот // Ефективна економіка № 9, 2013 – Режим доступу: <http://www.economy.nauka.com.ua/?op=1&z=2316>

10. Нортон Д., Каплан Р. Сбалансированная система показателей. От стратегии к действию. М. : ОлимпБизнес, 2010. 320 с.

11. Пилипенко С.М. Теоретичні засади оцінки ефективності діяльності підприємства. *Глобальні та національні проблеми економіки*. 2016. № 10. С. 452-456. URL: <http://global-national.in.ua/archive/10-2016/94.pdf>.

12. Платформа Loginom. Скачать Deductor. *BaseGroup Labs* : веб-сайт. URL: <https://basegroup.ru/deductor/download>.

13. Яровенко Г. М. Дисертація на тему «Інформаційна безпека як драйвер розвитку національної економіки» / Г. М. Яровенко // Суми. 2021. – Режим доступу : [https://essuir.sumdu.edu.ua/bitstream/123456789/83664/6/diss\\_Yarovenko.pdf](https://essuir.sumdu.edu.ua/bitstream/123456789/83664/6/diss_Yarovenko.pdf)

**УДК 004.056:629.12**

## **КРИТЕРІЙ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ОБРОБКИ РИЗИКІВ ОБ'ЄКТІВ МОРСЬКОЇ ІНФРАСТРУКТУРИ**

***Автор:** Зубков А.П., 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*

Морська інфраструктура згідно [1] є підсектором критичної інфраструктури (КІ) України. Захисту об'єктів критичної інфраструктури (ОКІ) і об'єктів критичної інформаційної інфраструктури (ОКІІ) в останні роки приділяється велика увага як на міжнародному [2], так і на національному рівні [1, 3-8]. Вимоги до організації захисту таких об'єктів сформульовані в низці нормативно-правових актів [1-8], однак процедури обробки ризиків є індивідуальними для кожного об'єкта і на даний час мають характер наукових досліджень [9, 10] або узагальнених рекомендацій [11-13].

**Метою даної роботи** є визначення критеріїв прийняття рішень щодо обробки ризиків об'єктів морської інфраструктури.

Для досягнення даної мети необхідно вирішити наступні задачі:

- провести аналіз методів обробки ризиків;
- визначити особливості прийняття рішень щодо обробки ризиків морської інфраструктури України (МІУ);
- визначити базові критерії щодо прийняття рішень щодо ризиків МІУ.

Згідно [14] обробка ризиків є етапом менеджменту ризиків інформаційної безпеки і здійснюється на основі оцінок ризиків, отриманих на етапі оцінювання ризиків, та критеріїв обробки ризиків, визначених на етапі визначення контексту. При цьому можуть задаватися окремі критерії прийняття рішень щодо ризиків, асоційованих з певними активами, певними загрозами, певними бізнес-процесами тощо.

МІУ підпорядковується Мінінфраструктури України, а тісно пов'язана з нею галузь промисловості «суднобудування» – Мінстратегпрому України [3].

МІУ надаються послуги з:

- контролю і управління судноплавством;
- операцій на пасажирському та вантажному транспорті, які проводяться на внутрішніх і морських водних шляхах або у прибережній зоні;
- організації функціонування керуючих органів портів;
- організації роботи суб'єктів, які експлуатують портове обладнання;
- експлуатації та обслуговування інфраструктури (каналів, дамб, фарватерів тощо).

Відповідно, ризики інформаційної безпеки можуть оброблятися з врахуванням потенційної небезпеки реалізації загроз на надання перелічених вище послуг, що віддзеркалює особливості МІУ як специфічну галузь господарської діяльності.

ДСТУ ISO/IEC 27005:2023 [14] передбачає, що оцінювання і обробка ризиків може проводитися у 2 етапи, на кожному з яких застосовуються окремі критерії оцінювання.

Перший етап передбачає проведення узагальненого аналізу без технічної деталізації і зі звуженим спектром загроз. Метою першого етапу є виявлення загроз для бізнесу, які підлягають детальному аналізу на другому етапі. Критеріями прийняття рішень на цьому етапі є величини прийнятних ризиків для бізнес-процесів. Обробка ризиків на цьому етапі полягає у визначенні множини загроз, які підлягають детальному аналізу, визначення організаційних засад захисту інформації та контролю ефективності засобів та заходів захисту.

На другому етапі після проведення детального аналізу ризиків, асоційованих із загрозами, визначеними на першому етапі, на основі уточнених оцінок ризиків проводиться вибір методів обробки ризиків із переліку і за критеріями, які були сформовані на етапі визначення контексту відповідно до політики безпеки організації. Серед доступних для застосування методів обробки ризиків можуть бути:

- усунування джерела ризику;
- зміна можливості виникнення ризику шляхом усунування вразливостей або шляхом впровадження більш якісних засобів і заходів захисту, що зменшує ймовірності виникнення і успішної реалізації загрози;
- зміна наслідків реалізації загроз шляхом розробки і впровадження заходів реагування на інциденти, застосування засобів захисту, що забезпечують менш критичні наслідки;
- розподіл ризику з іншою стороною шляхом страхування ризиків, фінансування ризиків, включення положень щодо розподілу ризиків у договори, перекладання ризиків на іншу сторону де-факто (наприклад, перекладання ризиків на споживачів послуг);
- прийняття ризику. Цей метод може застосовуватися для відносно малих ризиків, які не становлять суттєвої небезпеки для організації, або для значних ризиків, якщо витрати на усунування джерела ризику, зміну можливостей виникнення і наслідків ризиків, розподіл ризиків з іншою стороною є занадто великими для організації, а також якщо цей значний ризик є усвідомленим ризиком і приймається для досягнення певної мети;
- уникання ризику шляхом прийняття рішення щодо припинення діяльності, внаслідок якої виникає ризик.

Обробка певного ризику може змінювати інші наявні ризики або створювати нові.

Порядок обробки ризиків визначається за їх положенням у ранжованому списку ризиків, який розбивається на групи за пріоритетами обробки. Кількість таких груп і і правила віднесення ризику до певної групи визначаються на етапі опису контенту і можуть бути уточнені на наступних етапах.

Критеріями віднесення ризиків до групи з певним пріоритетом обробки можуть бути:

- якісні або кількісні оцінки ризиків;
- ступені невизначеності (ймовірності або міри впевненості) вхідних даних для оцінювання ризиків;
- відповідність певному зовнішньому і внутрішньому контексту менеджменту ризиків інформаційної безпеки;
- відповідність меті організації;
- відповідність інтересам зацікавлених сторін;
- відповідність нормативно-правовим вимогам в галузі діяльності організації.

МІУ належить як КІ має оцінюватися за рівнем критичності згідно «Методичних рекомендацій щодо категоризації об'єктів КІ» [6]. Категорія присвоюється ОКІ на підставі оцінок, отриманих за секторальними і міжсекторальними критеріями, які враховують:

- значимість ОКІ для соціуму, екології, економіки, національної безпеки, обороноздатності країни;
- наявність взаємозв'язків і з іншими ОКІ, в тому числі з об'єктами інших КІ країни та інфраструктур, визнаних критичними на міжнародному рівні [2];
- ступінь негативного впливу на надання основних послуг у разі порушення функціонування ОКІ.

За [12] морський кіберризик асоціюється із технологічними активами, пошкодження, втрата або компрометація яких можуть призвести до пов'язаних із судноплаством операційних збоїв, збоїв у безпеці судноплавства, негативних екологічних наслідків тощо.

Розробка та впровадження конкретних процесів управління ризиками МІБ, повинна проводитися не тільки з врахуванням вимог ак-

туальних міжнародних і галузевих стандартів і передової практики менеджменту ризиків інформаційної безпеки, а й з врахуванням вимог зацікавлених урядів і адміністрацій прапорів.

При цьому підлягають аналізу вразливості і загрози для всіх систем, порушення функціонування яких може мати негативні соціальні, екологічні, економічні, репутаційні, політичні, оборонні наслідки для МІБ в цілому, зокрема:

- навігаційні системи;
- системи зв'язку, зокрема Глобальна морська система зв'язку під час лиха і для забезпечення безпеки мореплавства;
- системи обробки та управління вантажами;
- системи управління маяками;
- системи обслуговування та управління пасажирями;
- системи контролю і моніторингу доступу;
- системи адміністрування діяльності
- системи життєзабезпечення екіпажів суден, пасажирів та персоналу портів;
- системи керування силовими установками і механізмами та системи керування потужністю, що застосовуються на суднах і в портах;
- мережі загального користування, звернені до пасажирів;
- системи мостів, шлюзів тощо.

Для деталізації критеріїв прийняття рішень щодо обробки ризиків об'єктів МІУ можуть використовуватися рекомендації провідних організацій і фірм в галузі:

- в галузі кібербезпеки. Наприклад, Фреймворк NIST – концепція Національного інституту стандартів і технологій США з удосконалення системи кібербезпеки критичної інфраструктури; Rec 166 – консолідована рекомендація IACS щодо кібервідмовостійкості);
- у галузі морського транспорту. Наприклад, Керівництво щодо кібербезпеки на борту суден, створене та підтримуване Міжнародною палатою судноплавства (ICS), Міжнародний союз морського страхування (IUMI), Балтійською і міжнародною морською радою (BIMCO), Міжнародним морським форумом нафтових компаній (OCIMF), Міжнародною асоціацією незалежних власників танкерів (INTERTANKO), Міжнародною асоціацією власників суховантажних суден

(INTERCARGO), Міжнародною асоціацією суднових менеджерів (InterManager), Всесвітньою радою судноплавства (WSC) та Асоціацією будівельників суперяхт (SYBAss); рекомендації Міжнародної асоціації портів і гаваней (IAPH) і Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) щодо кібербезпеки для суден, портів і портових засобів [13, 15].

### **Висновки**

В даній роботі проведено аналіз методів обробки ризиків, визначені особливості прийняття рішень щодо обробки ризиків МІУ і базові критерії для проведення цієї процедури менеджменту ризиків інформаційної безпеки.

### **Список літератури:**

1. Деякі питання 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-%D0%BF#n16>
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](https://zakon.rada.gov.ua/rada/show/984_002-08#n4)
3. Деякі питання об'єктів критичної інформаційної інфраструктури. Постанова Кабінету міністрів України від 9 жовтня 2020 р. №1109. URL: <https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#Text>
4. 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>
5. План реалізації Стратегії кібербезпеки України. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>
6. Про затвердження Методичних рекомендацій щодо категоризації об'єктів КІ. Наказ №23 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021. URL: <https://zakon.rada.gov.ua/rada/show/v0023519-21#Text>
7. Про критичну інфраструктуру. Закон України. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

8. Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури, затверджений Постановою Кабінету Міністрів України від 22 липня 2022 р. № 821. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-poriadku-prove-a821>

9. Бірюков Д. С. Захист КІ в Україні: від наукового осмислення до розробки засад політики / Д. С. Бірюков // Науково-інформаційний вісник Академії національної безпеки. – 2015. – № 3-4. – С. 155-170. – URL: [http://nbuv.gov.ua/UJRN/nivanb\\_2015\\_3-4\\_14](http://nbuv.gov.ua/UJRN/nivanb_2015_3-4_14).

10. 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://znp-cvsvd.nuou.org.ua/article/view/12552>

11. 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](https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf)

12. MSC-FAL.1/Circ.3/Rev.2. Guidelines on maritime cyber risk management. URL: [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSF-FAL.1-Circ.3-Rev.2 %20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSF-FAL.1-Circ.3-Rev.2%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf)

13. Port Cybersecurity – Good practices for cybersecurity in the maritime sector. URL: <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector>

14. 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](https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400)

15. The Cyber Security Policy Framework: NIS Directive and Cyber Security in Maritime. URL: [https://static1.squarespace.com/static/57a8878837c58153c1897c2c/t/5b9a72db4ae23743\\_aef\\_2c2f8/1536848627336/5AthanasiosDrougkas\\_SMM18.pdf](https://static1.squarespace.com/static/57a8878837c58153c1897c2c/t/5b9a72db4ae23743_aef_2c2f8/1536848627336/5AthanasiosDrougkas_SMM18.pdf)

УДК 004.056.5:057.2

## ДОСЛІДЖЕННЯ ДЕМАСКУЮЧИХ ФАКТОРІВ СИСТЕМИ STARLINK

*Автор: Каплюк О.П., 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*

Інтернет в сучасному світі відіграє значущу роль.

Завдяки Інтернету ми можемо зв'язатися з людьми в будь-якому куточку світу, можемо в чужому місті дістатися до необхідної локації всього лиш проклавши маршрут у телефоні з Інтернетом, можемо віддалено керувати пристроями у власному будинку з технологією «розумний дім», наприклад вимикати розетки по Wi-Fi і не думати чи вимкнув праску.

З початком повномасштабного вторгнення росії на територію України, дуже важливим став Інтернет-зв'язок, завдяки якому військові змогли б у найкоротші терміни отримувати та передавати стратегічно важливу інформацію навіть у епіцентрі бойових дій. Справжнім порятунком тоді для українських військових стала супутникова система Starlink, бо на початку повномасштабного вторгнення росії Ілон Маск відгукнувся на прохання України та надав доступ до супутникового зв'язку Starlink. Перші термінали були активовані 26 лютого, а зараз їх уже понад 30 тисяч, що робить Україну однією з держав із найбільшою їх кількістю.

### Що таке Starlink?

Система Starlink, якою володіє компанія Маска SpaceX, забезпечує доступ до ширококутового інтернету в будь-якій точці планети. [4] Супутники перебувають на низькій навколоземній орбіті, приблизно за 550 кілометрів над поверхнею Землі, тому затримка сигналу майже непомітна – до 20 мілісекунд, на відміну від найближчих конкурентів, у яких сигнал може затримуватися на секунди. [1]

SpaceX хочуть до 2027 року розмістити на орбіті понад 42 тис. супутників. Для розуміння масштабів: станом на початок літа 2022

року в космосі всього було трохи більше 13 тис. супутників, запущених за всю історію освоєння позаземного простору.

Технологія старлінк використовує радіосигнали від наземних станцій-шлюзів до супутників, які направляють його назад, у користувацькі термінали старлінк на Землі. Термінал підключається до Wi-Fi-роутера старлінк (він входить у набір) та забезпечує користувача інтернетом. [5]

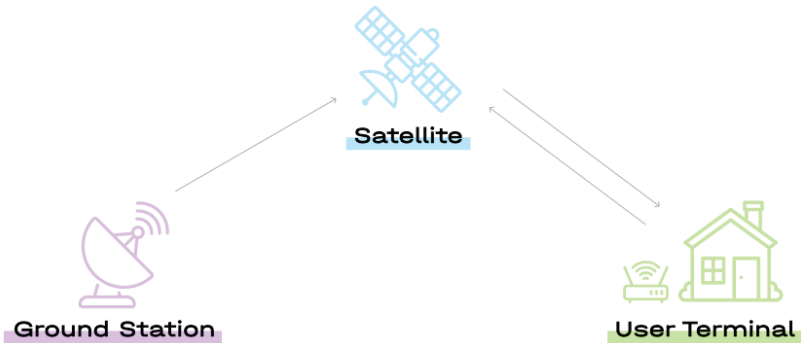


Рисунок 1 – Принцип роботи Starlink

Основна мета проекту – створення високошвидкісного інтернету в космосі з мінімальною затримкою відповіді. Крім того, за допомогою старлінк можна швидко відновлювати зв'язок та інтернет-покриття у критичних ситуаціях. Наприклад, ще навесні за допомогою цієї технології Vodafone відновив зв'язок у деокупованих населених пунктах. Схема використання Starlink як ключового розподільчого терміналу для екстреного чи тимчасового відновлення мережі застосовується мобільними операторами і зараз.

Офіційно швидкість Starlink сягає близько 150 мегабіт на секунду (Мбіт/с), але компанія планує подвоїти показник найближчим часом. І це схоже на правду: за даними проведеного в червні 2022 року Speedtest від Ookla, максимальна швидкість завантаження Starlink уже трохи вища – 160 Мбіт/с. [5]

### **Starlink можна зламати? Він безпечний?**

Одразу після повідомлень про початок роботи Starlink в Україні експерти почали сперечатися, чи може використання платформи бути небезпечним. Наприклад, Джон Скотт-Рейлтон, старший науковий

співробітник проекту Citizen Lab Університету Торонто, написав цілу серію твітів, у яких попереджав, що термінали можуть стати російськими цілями. «Росія десятиріччями вражає людей, націлюючись на їхній супутній зв'язок», – написав він.

Також у коментарі EuroNews Тім Фаррар, експерт із супутникового зв'язку, зазначив, що однією з проблем встановлення терміналів для кінцевих користувачів є місця встановлення – це зазвичай звичайні багатоповерхівки, які мають найкращий огляд неба без перешкод. І таким чином можуть стати цілями для російської зброї.

При цьому інші експерти вважають такий сценарій малоімовірним і кажуть, що Starlink хоча й не зможуть повноцінно замінити звичайних інтернет-провайдерів, але можуть бути вкрай важливими для журналістів, волонтерів, військових та держави. Про це в коментарі Бі-бі-сі розповів керівник ІТ-компанії NetBlocks Альп Токер. «Starlink може забезпечити зв'язок, створити особисту точку доступу для людей поблизу терміналу. Це дуже корисно для журналістів, груп спротиву, уряду, аби донести важливу інформацію про Україну світу. Навіть якщо це невелика група людей – це краще, ніж повна відсутність зв'язку», – розповів Токер.

При цьому, вважають експерти, такий зв'язок фактично неможливо ані зламати, ані відключити: це можливо лише за умови, якщо пошкодити самі наземні станції, причому одночасно в декількох країнах, що вкрай малоімовірно. «Starlink – це супутниковий зв'язок, який включає телефон, телебачення та інтернет. І заблокувати його неможливо. Також неможливо перехопити канал та зняти інформацію. Ворог нічого не зробить і нічого не перехопить. Це нереально, таких технологій взагалі немає», – розповів «КП в Україні» виконавчий директор Лабораторії комп'ютерної криміналістики Сергій Денисенко. І додав, що навіть частково заблокувати сигнал не вдасться: оскільки платформа використовує не один, а ціле сузір'я супутників, які майже миттєво передають сигнал один одному й далі до користувача. Тому фактично Starlink – найстабільніша та найменш вразлива інтернет-мережа.[2]

Налаштування Starlink виконується дуже просто, за принципом plug-n-play. На початку потрібно встановити термінал, під'єднати його

до живлення та Wi-Fi-роутера, після чого приєднатися з телефону до нової Wi-Fi-мережі, запустити фірмовий додаток та почекати приблизно 15 хвилин.

За цей час Starlink проаналізує місце розташування терміналу, підкоригує його позицію – кут нахилу та розворот тарілки, – під'єднається до супутника та завершить налаштування. Усе відбувається автоматично, на обладнанні взагалі немає кнопок чи регуляторів. [5]

Аналізуючи принцип роботи супутникової системи Starlink дослідимо її можливі демаскуючі признаки.

Так як термінал зв'язується із супутником в певному діапазоні, то його головним демаскуючим признаком будуть саме робочі частоти. Знаючи ці частоти та скануючи простір спеціальними виявлювачами, можливе розпізнавання активності таких терміналів.

Ризик візуального виявлення Starlink ворогом через тепловізори має місце під час війни. Тому SpaceX як додатковий, але обов'язковий захід, пропонує накривати термінал оптично прозорою плівкою із захистом від інфрачервоного випромінювання – це може знизити візуальну, радіолокаційну та інфрачервону видимість Starlink на відкритих майданчиках.

Інфрачервоне випромінювання (від лат. *infra* – нижче, скорочено ІЧ) – електромагнітне випромінювання, що охоплює спектральну область між червоною межею видимого світла з довжиною хвилі  $\lambda = 700$  нм (частота близько 430 ТГц) та мікрохвильовим випромінюванням з довжиною хвилі  $\lambda \sim 1$  мм (частота близько 300 ГГц) [6]. Плівка з ІЧ захистом знижує ризик радіопеленгації на 53%. [7]

Задля максимального забезпечення користувацької частини системи супутникового зв'язку Starlink, термінал також можна помістити у яму, але при тому забезпечити достатній доступ до неба (віртуальний конус мінімум  $100^\circ$ , оптимум  $140^\circ$ ). [7]

Виявити положення терміналу супутникового зв'язку Starlink з поверхні землі практично не можливо з дистанції понад 1 км.

Але неприхований «під землю» Wi-Fi роутер, котрий працює зазвичай в комплекті з терміналом, виявити можна й на дистанції 10 км спеціально обладнаним БПЛА та на ситуаційно меншій відстані з поверхні землі.

Це, до речі, одна з причин, чому більшість фахівців надає перевагу круглим терміналам V1 – є можливість працювати без Wi-Fi.[3]

Підбиваючи підсумки, можна сказати, що головними з демаскуючих факторів системи Starlink є його робочі частоти, Wi-Fi роутери, які підключаються до терміналів, та інфрачервоне випромінювання терміналу. Також важливим є маскування не лише терміналу, а й кабелю і мобільність самої установки.

### **Список літератури:**

1. Starlink: чому інтернет від Ілона Маска такий важливий для України. Режим доступу : <https://www.bbc.com/ukrainian/features-63306893>.
2. Starlink: що це таке, як працює та хто зможе ним користуватися в Україні. Режим доступу: <https://ms.detector.media/it-kompanii/post/29166/2022-03-13-starlink-shcho-tse-take-yak-pratsyuie-ta-khto-zmozhe-nym-korystuvatysya-v-ukraini/>.
3. Бойова гігієна. Чим небезпечний Wi-Fi на передовій, та чому інколи прилітає по Starlink: пояснює айтишник. Режим доступу : <https://dev.ua/news/chym-nebezpechnyi-wi-fi-peredovii-ta-chomu-inkoly-prylitaie-po-starlink-poiasnuiue-aitishnyk-1656419615>.
4. Все, що ви хотіли знати про Starlink, і не знали, як спитати. Режим доступу : <https://cip.gov.ua/ua/news/vse-sho-vi-khotili-znati-pro-starlink-i-ne-znali-yak-spitati>.
5. Усе, що потрібно знати про Starlink. Режим доступу : <https://laba.ua/blog/3317-vse-chto-vam-nuzhno-znat-pro-starlink>.
6. Інфрачервоне випромінювання (назва з екрану). Режим доступу : [https://uk.wikipedia.org/wiki/Інфрачервоне\\_випромінювання](https://uk.wikipedia.org/wiki/Інфрачервоне_випромінювання)
7. Як встановити та замаскувати Starlink у польових умовах: інструкція. Режим доступу : <https://dev.ua/news/starlink-1665298597>.

УДК 004.056.52:53

## ДОСЛІДЖЕННЯ СТІЙКОСТІ СИСТЕМИ STARLINK ДО ЗОВНІШНІХ ЗАВАД

*Автор: Ковальський Д.А., 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*

**Вступ.** Під час вторгнення рф на територію суверенної, незалежної України, головним з напрямків взаємодії збройних формувань України це зв'язок. Одним з ефективніших типів зв'язку є супутниковий. Він має високу якість та надійність каналів зв'язку, велику пропускну здатність, необмежені площини покриття та конфіденційність зв'язку. Супутниковий зв'язок нині є одним з основних видів військового зв'язку на великі та середні відстані для виконання завдань під час протистояння сил оборони України агресії рф.

Перші користувацькі термінали супутникової системи Starlink з'явилися в Україні у лютому 2022 року.

Завдяки цій мережі космічних супутників, які роздають високошвидкісний бездротовий інтернет у місцях де він недоступний, українська армія може завдати точні удари по російських військах та керувати безпілотниками, а мирні жителі мають можливість підтримувати зв'язок із рідними та близькими, й отримувати життєво важливу інформацію.

Наявність зв'язку – вкрай важлива ланка у сучасній війні, і одна з цілей противника – позбавити вас цього. Із самого початку війни росія намагалася порушити роботу каналів зв'язку.

Дослідження стійкості системи Starlink до зовнішніх завад буде проведено шляхом аналізу робочих характеристик системи та наявних засобів радіоелектронної боротьби рф, а також характеристик терміналів та глобальної супутникової системи Starlink.

### **Засоби радіоелектронного придушення та розвідки рф**

**Станція РЕБ Р-330Ж «Житель».** Автоматизована станція перешкод Р-330Ж «Житель» входить до складу комплексу РЕБ Р-330М1П «Діабазол» (див. рис. 1). Комплекс забезпечує: автоматизоване виявлен-

ня, синхронне пеленгування джерел випромінювання у діапазоні частот від 100 до 2000 МГц; визначення координат виявлених джерел випромінювання; автоматизоване радіоелектронне придушення ліній УКХ радіозв'язку, приймальних пристроїв базових станцій стільникового зв'язку, терміналів супутникового зв'язку «Inmarsat», «Iridium» та абонентських станцій навігаційної системи GPS.

Станція здатна перешкоджати супутниковому зв'язку «Inmarsat» та «Iridium», мобільному зв'язку GSM900 та GSM1800, а також навігаційним системам. Постановка перешкод здійснюється у радіусі 30 км.

**Комплекс «Дзюдоїст».** Комплекс «Дзюдоїст» (див. рис. 2) призначений для ведення радіо-, радіотехнічного і спеціального контролю ефективності захисту інформації та оцінювання радіоелектронної обстановки.



Рисунок 1 – РЕБ Р-330М1П  
«Діабазол»



Рисунок 2 – Комплекс «Дзюдоїст».

Комплекс забезпечує: виявлення, вимірювання параметрів і визначення місць знаходження радіоелектронних засобів; оцінювання радіоелектронної обстановки; виявлення та закриття технічних каналів витоку інформації на об'єктах. Комплекс забезпечує виявлення та контроль переговорів і передачі даних по каналах КХ, УКХ, стільникового та супутникового радіозв'язку, пеленгування будь-яких сто-

ронніх джерел радіовипромінювання (у тому числі – радіомаркерів, датчиків систем наведення, радіомаяків), закриття технічних каналів витоку інформації на військових об’єктах і в місцях постійної або тимчасової дислокації підрозділів. Склад комплексу: автоматизоване робоче місце (далі – АРМ) радіо-, радіотехнічного контролю (АРМ-РРТК); АРМ технічного аналізу та оцінювання (АРМ ТАО); АРМ спеціального контролю (АРМ-СК) з комплектом виносної апаратури; апаратура зв’язку, електроживлення, життєзабезпечення. Результати роботи комплексу можуть бут використані для оперативної оцінки та управління засобами постановки радіоперешкод або для комплексної оцінки стану безпеки і рівня маскування об’єктів.

### Основні технічні характеристики комплексу «Дзюдоїст»

|                                                                                                                   |              |
|-------------------------------------------------------------------------------------------------------------------|--------------|
| Діапазон частот радіо-, радіотехнічного контролю, МГц                                                             | 0,1 – 18000  |
| Точність пеленгування, град.                                                                                      | 2-3          |
| Діапазон частот контролю електромагнітних випромінювань, МГц                                                      | 0,01 – 20000 |
| Діапазон частот акустичного та віброакустичного контролю, Гц                                                      | 10 – 20000   |
| Діапазон частот виявлення спеціальних електронних пристроїв перехоплення інформації за сигналами радіоканала, МГц | 0,1 – 10000  |
| Дальність радіозв’язку, не більше, км:                                                                            |              |
| з використанням возимої радіостанції                                                                              | 20           |
| з використанням носимої радіостанції                                                                              | 5            |
| Час розгортання / згортання, хв.                                                                                  | 30           |
| Потужність, яка споживається, кВт                                                                                 | 3,5          |

**Комплекс РЭБ 14Ц227 «Тобол».** Комплекс 14Ц227 «Тобол» (див. рис.3) відноситься до найбільш засекречених – про неї, у відкритому доступі, вкрай мало даних. Частково про комплекс, його структуру, призначення та принцип дії можна лише за [6]. Стаття вийшла ще в листопаді 2020 року і нової інформації про характеристики та можливості комплексу в відкритому доступі немає.

Згідно з [6] принцип дії комплексу оснований на використанні спеціальної наземної станції, що контролює часткове відбиття (розсі-

ювання) від тропосфери сигналу системи супутникового зв'язку/інтернету (див. рис. 4). Сигнал аналізується і передається на спеціальний блок, який формує сигнал перешкод та надсилає його на супутник зв'язку.



Рисунок 3 – Комплекс РЕБ  
14Ц227 «Тобол»

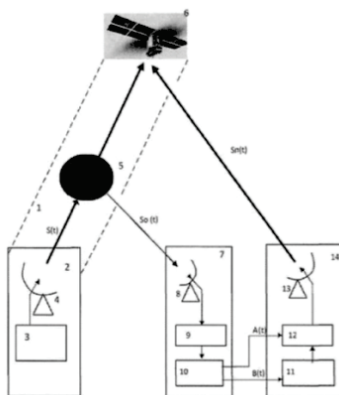


Рисунок 4 – Схема принципу роботи комплексу РЭБ «Тобол»

Основним завданням комплексу 14Ц227 «Тобол» в Україні є створення атак на систему Starlink, яка широко використовується в Україні та безпосередньо ЗСУ.

В SpaceX коротко розповів про спроби кремля «глушити і зламувати» Starlink, але технологія продемонструвала свою стійкість до таких спроб. Однак, росіяни почала шукати нові схеми блокування роботи Starlink.

Як зазначають ЗМІ, в компанії SpaceX відмовилася коментувати нові атаки на Starlink. Пентагон також не відповів на запитання журналістів щодо цієї ситуації. Представник міністерства оборони, лише зазначив, що Starlink складає важливий шар у мережі зв'язку України і додав, що увага відомства «як і раніше зосереджена на тому, щоб надати українцям необхідні їм супутникові можливості».

Однак, незважаючи на це, у жовтні українські військові почали повідомляти про перебої у роботі Starlink. На той час офіційні особи України припустили, що SpaceX обмежила доступ до Інтернету в цих районах, щоб росіяни не могли користуватися цією послугою.

Недавно в The Washington Post повідомили, що проблеми з роботою Starlink могли бути результатом російських експериментів на Тоболі.

Комплекс розташований під Москвою, один – поблизу Криму та ще один – у Калінінграді. Центром, де росіяни намагались глушили Starlink, був район Бахмута та східна частина Донецької області.

За даними американського Фонду безпечного світу, який займається космічною безпекою, супутникові перешкоди можуть виникати у двох місцях: у космосі, коли вони націлюються безпосередньо на супутники, і землі, де можуть націлюватися на приймачі. Перешкоди, що виникають у космосі, відомі як глушіння висхідної лінії зв'язку, змішують сигнал з вихідною трансляцією, що спотворює інформацію, яку отримують усі користувачі супутника. За словами дослідника Барта Хендрікса, Тобол, напевно, працює таким чином.

### **Особливості супутникового зв'язку**

Супутники у космосі спілкуються між собою на частоті понад 10 ГГц за допомогою лазерного променя. Із наземними станціями та терміналами користувачів зв'язок здійснюється у радіодіапазонах (Ku- та Ka-) на частоті 12 ГГц. Ku-антени більш надійні у роботі навіть у хмарну та дощову погоду, а Ka-антени забезпечують значно більшу пропускну здатність. Зазвичай зв'язок із геостаціонарним супутником має мінімальну кругову затримку сигналу (туди-назад) у 239 мс, але іноді вона може сягати і 600 мс. Супутники Starlink обертаються на висоті в 1/30 цієї відстані, тому затримка сигналу становитиме лише 25-30 мс, що еквівалентно з кабельним або оптоволоконним зв'язком.

В Україні широко застосовуються два типи терміналів Starlink (див. рис.5) – UT-1 та UT-2.



а)



б)

Рисунок 5 – Загальний вигляд терміналів Starlink: а) UT-1; б) UT-2

### Основні характеристики терміналів Starlink

|                          | UT-1                    | UT-2      |
|--------------------------|-------------------------|-----------|
| Діапазон частот, ГГц:    |                         |           |
| - прийом                 | 10,7-12,7               | 10,7-12,7 |
| - передача               | 14-14,5                 | 14-14,5   |
| Довжина хвилі, м         | 0,02                    | 0,02      |
| Ширина смуги частот, МГц |                         |           |
| - прийом                 | 2000                    | 2000      |
| - передача               | 500                     | 500       |
| Робоча температура       | від -30 ° С до +50 ° С; |           |
| Ступінь захисту:         | IP54.                   |           |

### Характеристики роутера терміналу Starlink

|                         |                                              |
|-------------------------|----------------------------------------------|
| Стандарти:              | IEEE 802.11a/b/g/n/ac                        |
| Подвійний діапазон, ГГц | 2,4 та 5;                                    |
| Безпека                 | WPA2 та WPA3                                 |
| Робоча температура, ° С | від -30 до +50;                              |
| Ступінь захисту         | IP54 (для використання всередині приміщень). |

### **Висновки:**

1. При використанні терміналів Starlink бажано не користуватись роутером, щоб уникнути виявлення засобами РЕБ рф та подальшого глушіння сигналу чи фізичного знищення терміналу.

2. Зв'язок терміналу з супутниками придушити практично неможливо, враховуючи його велику пропускну здатність та велику кількість супутників в мережі глобальної системи Starlink.

3. В цілому, не враховуючи вразливість роутерів терміналів Starlink, можливо стверджувати про стійкість системи Starlink до зовнішніх завад.

### **Список літератури:**

1. Закон України від 16.11.2021 № 1882-IX «Про критичну інфраструктуру» (Із змінами, внесеними згідно із Законом України від 18.10.2022 р). URL: <https://zakon.rada.gov.ua/laws/main/1882-20#Text> (<https://zakon.rada.gov.ua/laws/show/2684-20#Text>)

2. Постанова Кабінету Міністрів України від 09.10.2020 № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» (Із змінами та доповненнями). URL: <https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text>

3. Засоби радіоелектронної боротьби ворога (Назва з екрану) – URL: <https://sprotyvg7.com.ua/lesson/zasobi-radioelektronnoi-borotbi-voroga>

4. Секретна зброя. Як РФ глушить Starlink в Україні (назва з екрану). Режим доступу: <https://ua.korrespondent.net/world/worldabus/4582569-sekretna-zbroia-yak-rf-hlushyt-Starlink-v-ukraini>

5. S. V. Pehterev, S. I. Makarenko, A. A. Kovalsky (2022) Descriptive Model of Starlink Satellite Communication System. Systems of Control, Communication and Security, (4). 190-255. DOI: 10.24412/2410-9916-2022-4-190-255. URL: <http://sccs.intelgr.com/archive/2022-04/07-Pehterev.pdf>

6. Russia gears up for electronic warfare in space (part 2). URL: <https://www.thespacereview.com/article/4060/1>

УДК 004.056.5; 004.89; 514.743.4

## ОСОБЛИВОСТІ ВИКОРИСТАННЯ RASPBERRY PI ДЛЯ ПЕНТЕСТИНГУ

*Автор: Литвиненко О.-Н., студент, 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*

В умовах сучасного існування людства, де майже кожна сфера діяльності потребує використання комп'ютерних технологій та засобів для комунікації, вагомий вклад у функціонування систем несуть фахівці з кібербезпеки та захисту інформації. Стандартні принципи моделі інформаційної безпеки (CIA Triad) поєднують в собі: *конфіденційність, цілісність, доступність інформації (КЦД)*, але завжди варто пам'ятати про зворотні до них – *розкриття, зміна та знищення інформації (РЗЗ)*. За даними авторитетного американського журналу Security Magazine [1] було встановлено, що за 2023 рік через мережу Інтернет відбувається близько 2200 атак на користувацькі комп'ютери за день, а це, в середньому, кожні 39 секунди. Саме тому в останній час багато організацій та державних структур звертаються за послугами сертифікованих етичних хакерів (відомих як «пентестери» або «white hat»). Їхньою основною метою є виявлення потенційних загроз, що можуть бути використані зловмисниками в ході протиправних дій та, відповідно, усунення недоліків в системах. Проведенню тестуванню на проникнення в комп'ютерних системах було присвячено велику кількість робіт вітчизняних та зарубіжних вчених [2-3]. Особливо цікавою ця процедура постає у випадку, коли такий комплекс захищеності відбувається з використанням маловартісного комп'ютера розміром з банківську картку. Відповідно, актуальною задачею є визначення особливостей використання Raspberry Pi при вирішенні конкретних прикладних задач інформаційної безпеки.

Метою цієї роботи є ознайомлення із функціональними можливостями та технічними характеристиками Raspberry Pi 4 Model B в дис-

трибутиві Linux на основі Debian – Kali Linux, а також проведення порівнянь продуктивності з портативним ПК під час простих тестувань.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- ознайомитись із технічними характеристиками RPi 4 Model B;
- описати передовий дистрибутив Kali Linux, що використовується спеціалістами з кібербезпеки при вирішенні прикладних задач;
- провести порівняльний аналіз продуктивності роботи одноплатного комп'ютера RPi та портативного ПК (ноутбуку) в Kali.

**Raspberry Pi 4 Model B** – це одноплатний комп'ютер серії Raspberry, розроблений у Великобританії та представлений світу у червні 2019 року. На рис. 1 наведено загальний вигляд цього пристрою, під'єднаного до джерела живлення.



Рисунок 1 – Загальний вигляд Raspberry Pi 4 Model B

Авжеж, такий компактний розмір дуже приваблює користувачів та ентузіастів, але окрему увагу треба приділити технічним характеристикам. В табл. 1 продемонстровано апаратну частину, з якої складається Raspberry Pi 4 Model B.

Таблиця 1 – Апаратна частина Raspberry PI 4 Model B

| № | Складова                                              | Опис                                                                                                                           |
|---|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 1 | Центральний процесор                                  | 4-ри ядерний Quad core 64-bit ARM-Cortex A72, тактова частота якого сягає 1.5GHz                                               |
| 2 | Оперативна пам'ять                                    | Можливість конфігурації з 1, 2, 4 або 8GB в залежності від моделі LPDDR4 (тип оперативної пам'яті для смартфонів та планшетів) |
| 3 | Мультимедіа                                           | H.265 (HEVC) апаратне прискорення (до 4Kp60); H.264 апаратне прискорення (до 1080p60), OpenGL ES, 3.0 graphics.                |
| 4 | Графічний процесор                                    | VideoCore VI 3D Graphics                                                                                                       |
| 5 | Інтерфейси вводу/виводу загального призначення (GPIO) | Стандартний 40-контактний роз'єм GPIO                                                                                          |
| 6 | Живлення                                              | 5В постійного струму через USB-C (мін. 3A);<br>5В постійного струму через GPIO (мін. 3A);<br>Живлення через Ethernet (PoE).    |

**Kali Linux** відноситься до сімейства Linux (Unix-подібних систем) та є дистрибутивом із відкритим вихідним кодом, що дозволяє користуватися ним в повному об'ємі безкоштовно. Його широкому поширенню та пізнаваності певною мірою сприяв телесеріал «Містер Робот», де молодий та талановитий інженер кібербезпеки користується можливостями системи для знищення найкрупнішого в світі конгломерату. Варто зазначити, що цей дистрибутив підтримує ARM-образи, тому його досить легко було завантажено на Raspberry PI 4 Model B з офіційного сайту розробника. На рис. 2 було продемонстровано запуск Kali Linux на раніше згаданому комп'ютері.

В арсеналі тестувальника на проникнення комп'ютер може стати відмінним помічником, наприклад, під час неможливості тут і зараз скористатися основною робочою станцією. Було складено табл. 2, в якій продемонстровано порівняльні дані щодо швидкості відпрацю-

вання деяких утиліт для виконання пентестингу на Raspberry та ноутбуку Acer Nitro AN517-51.



Рисунок 2 – Запуск Kali Linux

Таблиця 2 – Порівняльні дані швидкості роботи пристроїв

| Утиліта     | Швидкість відпрацювання, с |                        |
|-------------|----------------------------|------------------------|
|             | Acer Nitro AN517-51        | Raspberry PI 4 Model B |
| 1. nmap     | 19.88                      | 27.13                  |
| 2. nikto    | 104                        | 171                    |
| 3. curl     | 2.03                       | 9.3                    |
| 4. hashdeep | 8.3                        | 25.09                  |

Можна дійти висновку, що RPi, враховуючи його досить низьку вартість, не суттєво поступається ноутбуку в продуктивності під час використання стандартних можливостей Kali.Linux. Не можна стверджувати, що в більш вимогливих умовах (таких як брутфорс паролів за словником, виконання аналізу вразливостей бездротових мереж чи серверів) цей пристрій проявить себе аналогічним чином – потрібно більше тестувань та вихідної інформації.

Головним недоліком RaspPi є те, що в будь-якому випадку для його використання необхідно мати монітор, а також активну систему охолодження для максимальної працездатності. До переваг можна ві-

днести: відносно низьку вартість у порівнянні із ПК та можливість імплементації в проектних рішеннях (наприклад, використання як VPN серверу, планшету, FM радіо станції або навіть в якості центрального/ периферійного пристрою розумного дому).

**Висновки.** В роботі розглянуто основні можливості одноплатного комп'ютера Raspberry PI 4 Model B в дистрибутиві Kali Linux. Було ознайомлено із основними технічними характеристиками пристрою та визначена роль пентестингу в сучасних умовах цифровізації.

З правильним конфігуруванням та оптимізацією, RasPi може стати незамінним помічником при розв'язанні прикладних завдань, хоч з певними недоліками. Це робить пристрій привабливим вибором для тих, хто цінує ефективність та гнучкість у проведенні тестування на проникнення з обмеженими ресурсами.

#### **Список літератури:**

1. Security Magazine. URL: <https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds>
2. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.
3. Aamir Lakhani, Joseph Muniz. Penetration Testing with Raspberry Pi, ISBN 978-1-78439-643-5, Birmingham, UK, 2015. – 208 с.
4. Технічні характеристики Raspberry PI 4 Model B. URL: <https://www.raspberrypi.com/products/raspberry-pi-4-model-b/specifications/>
5. Офіційна сторінка kali.org. URL: <https://www.kali.org/get-kali/#kali-arm>

УДК 004.056

## СУЧАСНІ МОДЕЛІ ДОСТУПНОСТІ ІНФОРМАЦІЇ

***Автор:** Машикін О.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*

Інтенсивний розвиток інформаційних технологій зумовлює необхідність забезпечення адекватності методів і засобів захисту інформаційних ресурсів обмеженого доступу актуальним стратегіям, методам і засобам, що застосовуються злоумисниками. При проектуванні і модернізації комплексних систем захисту інформації об'єкт інформаційної діяльності має бути всебічно обстежений, а рішення, що підлягає реалізації має бути оптимальним для даного об'єкту. Одним із способів оцінювання якості рішень в галузі інформаційної безпеки є їх дослідження на моделях безпеки.

На даний час існують моделі безпеки [1-4], які різняться за контрольованими параметрами, наборами суб'єктів і об'єктів, способами взаємодії суб'єктів і об'єктів, правилами опису станів системи і сценаріїв переходів між станами системи. Серед цих моделей можна виокремити моделі політик безпеки і пов'язані з ними моделі забезпечення конфіденційності, цілісності і доступності інформації, кожна з яких має власні переваги і недоліки.

**Метою даної роботи** є визначення переваг і недоліків сучасних моделей забезпечення доступності інформації.

Для досягнення даної мети необхідно вирішити наступні задачі:

- провести аналіз методів порушення доступності інформації сучасними злоумисниками;
- визначити особливості, переваги і недоліки сучасних моделей забезпечення доступності інформації;
- визначити критерії оцінювання якості моделей забезпечення доступності інформації.

Згідно НД ТЗІ 1.1-002-99 [5] інформація зберігає доступність, якщо за легітимним користувачем упродовж будь-якого певного (малого) проміжку часу зберігається можливість виконання дій відповідно

до встановлених правил, таких як: ознайомлення з інформацією, її модифікація чи видалення, створення нових інформаційних ресурсів.

Доступність інформації може бути порушена внаслідок подій як:

- примусова зупинка зловмисником роботи певного програмного і /або апаратного забезпечення;
- вичерпування ресурсів часу і пам'яті внаслідок спрямування всіх ресурсів комп'ютерної системи на виконання задач, заданих зловмисником;
- порушення працездатності комунікаційних каналів внаслідок вичерпування пропускної здатності каналів або порушення системи глобальної маршрутизації і спрямовування повідомлень у «чорні діри» мережі або до зловмисника замість ліgitимного адресату.

Порушення доступності інформації відбувається під час успішних DoS і DDoS атак, атак на систему глобальної маршрутизації та в разі втрати електроживлення. При цьому кожен тип атаки може бути здійснений за різними технологіями, наприклад, DDoS-атака може бути організована зловмисником одноосібно або із використанням слеш-дот-ефекту, флешмобів або ботнетів. Порушення доступності може бути здійснене за допомогою експлоїтів і спеціального програмного забезпечення, які наявні у вільному доступі.

Дослідження забезпеченості доступності інформації може бути проведено на формалізованих моделях, на математичних моделях функціонування системи, наприклад, побудованих на основі теорії масового обслуговування, на моделях інформаційно-комунікаційних систем, побудованих у спеціальних програмних засобах, що дозволяють проводити віртуальні експерименти і збирати статистичні дані, які підлягають наступному аналізу, або на спеціальних моделях забезпечення доступності інформації.

Порушенням доступності ресурсів і послуг вважається факт перевищення часом очікування легітимним користувачем відповіді на його запит щодо доступу до ресурсів та послуг так званого часу максимального очікування.

Відповідно до однієї з перших моделей інформаційної безпеки – моделі Біба [1, 3] всіх суб'єктів і об'єкти попередньо розподіляють по кільком наперед визначеним рівням доступу, а процеси їх взаємодії накладаються обмеження за двома правилами:

- «не має читання вниз» (англ. *no reading down*, NRD): суб'єкт не може викликати на виконання (прочитати) суб'єктів, рівень доступу яких нижчий за його власний;
- «не має запису вгору» (англ. *no write up*, NWU): суб'єкт не може модифікувати (виконати запис) об'єкти, рівень доступу яких вищий за його власний.

В моделях мандатної політики безпеки для забезпечення доступності використовуються нотації моделей Белла-ЛаПадули і Бібі: суб'єктам присвоюються пріоритети, а об'єктам – рівні критичності, а далі задіюють правила NRD та NWU. Вважається, що суб'єкт, який надіслав запит на надання послуг, отримує відмову в обслуговуванні, якщо відповідь на його запит не надходить протягом часу максимального очікування. Перевагою правил NRD та NWU є використання простого механізму пріоритетів, які (хоча б частково) вже наявні в автоматизованій системі, наприклад, пріоритети процесів операційних систем. Недоліками в даному випадку є:

- можливість використання моделі тільки при умові можливості встановлення декількох рівнів пріоритетів і критичності;
- правила NRD та NWU не враховують розподіл ресурсів надання послуг у часі і просторі;
- теоретичне і практичне доведення факту, що можна побудувати систему захисту відповідно до правил NRD та NWU, однак доступність не буде забезпечена, тобто відповідність цим правилам є необхідною, але не достатньою умовою забезпечення доступності.

Модель відмови в обслуговуванні Ю-Глігора [1] дозволяє врахувати обмеженість наявних ресурсів і складається з двох частин: угоди користувача і політики скінченного часу очікування

Угода користувача визначає властивості, які мають бути наявними у користувачів сервера, з метою запобігання небажаних послідовностей викликів і відмові в обслуговуванні. Угода користувача не є частиною специфікації послуги, оскільки передбачає дії, які не стосуються конкретної послуги, а, наприклад, визначають умови взаємодії користувача з кількома службами. Для уникнення тупикових ситуацій необхідний механізм примусового виконання, оскільки користувачі можуть не виконувати угоду та навіть не знати про неї. Угода користувача містить:

- набори послідовностей усіх можливих викликів служби;
- набори послідовностей усіх можливих викликів користувача;
- набори операцій для кожної послуги, які виконує користувач;
- набір операцій, які створюють ресурси, що споживаються користувачем, і мають бути виконані до того, як користувач почне виконувати операцію.

В результаті формується множина операцій, що є доступною для користувача за умов обмежених ресурсів.

Політика обмеженого часу очікування призначена для реалізації прав всіх користувачів на користування ресурсом і складається з трьох частин:

- політика справедливості, яка визначає такі умови конкурування процесів за ресурси, що жоден процес не може отримати і звільнити ресурси так, щоб інший процес позбувся шансів отримати ці ресурси, тобто гарантує, що процес, якому потрібен відсутній на поточний момент ресурс, не буде заблокованим назавжди;

- політика одночасності забезпечує прогрес, надаючи можливості, що необхідні процесу для використання ресурсу, і доповнює політику справедливості, надаючи всім процесам можливості для прогресу;

- політика виконання угод користувачів, яка передбачає, що вимоги цих угод можна задовольнити або застосуванням обмежень виклику служби, або шляхом виконання індивідуальних угод користувачів, які гарантують, що послідовності викликів користувачів є контролюється до того, як відбудуться фактичні виклики.

Якщо всі три частини зберігаються, то жоден процес не чекатиме нескінченний час перед доступом до ресурсу. Однак, якщо принаймні одна з цих частин не виконується, кінцевий час очікування не гарантується, і процес може чекати нескінченно.

Визначення частин політики кінцевого часу очікування є частиною специфікації послуги.

Специфікація служби складається з операцій інтерфейсу, приватних операцій, недоступних за межами служби, ресурсів і обмежень паралелізму, а також політики кінцевого часу очікування. Таким чином, зміст специфікації служби залежить від параметрів певної служби і визначених процедур її виклику.

Перевагою моделі Ю- Глігора є те, що політики специфікації послуг і угоди користувача запобігають відмові в обслуговуванні, якщо їх дотримуються. Однак, час очікування послуги ними не обмежується, він тільки є гарантовано скінченним.

Модель Міллена [3] дозволяє врахувати нерівномірність розподілу ресурсів надання послуг користувачам при визначенні стратегій відмов за рахунок правил, що враховують не тільки часу максимального очікування, а й скінченний час очікування, наявні в системі ресурси та кількість ресурсів, виділених кожному процесу:

- сума всіх виділених ресурсів для множини активних процесів не може перевищувати кількість наявних ресурсів (процеси, що порушують це правило називають неправдоподібними);
- поточні процеси повинні мати нульові просторові вимоги, тобто вони можуть початися і тривати тільки за умови наявності всіх потрібних ресурсів. В іншому випадку процес зависає доти, поки вимоги до ресурсів не будуть виконані;
- для поточних процесів розподіл ресурсів не змінюється, тобто вони не вивантажуються;
- тривалість процесу визначається розподілом ресурсів центрального процесорного пристрою і може тільки зростати;
- для застиглих процесів встановлюються просторові вимоги (якщо з'являються потрібні ресурси, то процес активується і переходить у стан поточних процесів) і не встановлюються просторові вимоги;
- якщо процес зупиняється, то здійснюється перерозподіл тільки ресурсів центрального процесорного пристрою, а інші ресурси залишаються в резерві для відновлення процесу, але після відновлення процесу можуть перерозподілятися.

Перевагою моделі Міллена є можливість врахування розподілу ресурсів у часі і просторі та гарантування скінченного часу очікування послуги користувачем. Недоліком моделі Міллена є її відносна складність порівняно з іншими моделями.

Для моделювання доступності інформації систем критичного застосування в статті [4] запропоновано прикладну модель доступності з врахуванням архітектурних особливостей інформаційно-комунікаційної системи на мултисерверній платформі, за якою виділення ресурсів інформаційного середовища авторизованому суб'єкту відбува-

ється у межах віртуальної машини. Обмеження доступності сервісних операцій з вивільнення системних ресурсів в [4] зумовлюється відсутністю вільних ресурсів для створення нових віртуальних машин за запитами легітимних суб'єктів. При цьому зв'язок множини сервісних операцій і множини відповідей системи на запити легітимних суб'єктів формалізовано у вигляді керованого напівмарковського процесу з резервуванням ресурсів для самозабезпечення. Правила реагування на вхідні запити легітимних суб'єктів враховують завантаженість системи і виконувані в ній сервісні операції. Перевірка побудованої на основі методів математичного програмування імітаційної моделі у середовищі Matlab показала, що такий підхід:

- дозволяє визначити правила реагування, які гарантують належність імовірності відхилення вхідних запитів легітимних суб'єктів до заданого інтервалу, при мінімальних витратах на функціонування системи;
- на етапі проектування вимагає закладання 20% резерву системних ресурсів, оскільки в разі стрімкого зростання інтенсивності запитів, особливо від легітимних суб'єктів з високим показником критичності, кількість відмов зростає за квадратичною залежністю.

Згідно проведеного аналізу якості моделей забезпечення доступності інформації може бути визначена за наступними критеріями:

- здатність описувати суб'єкти і об'єкти системи, їх взаємозв'язки;
- здатність описувати доступні операції в системі;
- здатність описувати ресурси системи;
- здатність описувати розподіл ресурсів системи у часі і просторі;
- здатність гарантувати права користувачів на використання ресурсів;
- здатність формувати множини операцій, що забезпечені ресурсами;
- здатність формувати множини операцій, які доступні конкретним користувачам у поточний момент часу;
- здатність гарантувати скінченний час очікування послуги;
- здатність гарантувати певний довірчий інтервал відхилень вхідних запитів легітимних суб'єктів.

### **Висновки**

Таким чином, в даній роботі проведено аналіз методів порушення доступності інформації сучасними зловмисниками; визначені особливості, переваги і недоліки сучасних моделей забезпечення доступності інформації і критерії оцінювання їх якості.

### **Список літератури:**

1. Bishop, M. Computer security: art and science / M. Bishop. 2nd ed. – Addison-Wesley Professional, 2018. – 2865 p. URL: <https://dokumen.pub/qdownload/computer-security-art-and-science-2nbped-0321712331-9780321712332-0134097173-9780134097176.html>
2. Khazanch D., Martin A. P. Information Availability //Handbook of Research on Information Security and Assurance. Editors: Jatinder Gupta, Sushil Sharma. – USA, PA, Hershey: IGI Global Inc, 2009. – P.230-239. URL: [https://www.researchgate.net/publication/281277243\\_Information\\_Availability](https://www.researchgate.net/publication/281277243_Information_Availability)
3. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій.. – К.: ДУІКТ, 2009. – 292 с. URL: <https://studfile.net/preview/5367403>
4. Ковтун В. В. Моделювання доступності інформаційної системи критичного застосування //Вісник Вінницького політехнічного інституту. – 2019. – № 1. – С.41-55. URL: <https://ir.lib.vntu.edu.ua/handle/123456789/25366>
5. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: <https://tzi.com.ua/downloads/1.1-002-99.pdf>

УДК 004.056

## АНАЛІЗ ОСОБЛИВОСТЕЙ АТАК ТИПУ CLICKJACKING

*Автор: Потоцький О.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*

Розвиток комп'ютерних технологій нерозривно пов'язаний з розвитком інструментарію зловмисників. Постійна поява нових типів атак, удосконалення методів атак і поява у відкритому доступі спеціальних програмних засобів з рекомендаціями до застосування при організації атак зумовлюють необхідність побудови систем захисту інформації з врахуванням особливостей відомих методів і засобів організації та результатів прогнозування щодо появи нових видів і засобів порушення інформаційної безпеки. Багато сайтів, таких як Twitter, Facebook та інші, були зламані внаслідок атаки clickjacking [1].

**Метою даної роботи** є визначення особливостей атаки clickjacking і перспективних методів протидії цій атаці.

Для досягнення даної мети необхідно вирішити наступні задачі:

- визначити принципи організації атаки clickjacking;
- провести аналіз сучасних методів запобігання атаці clickjacking і визначити їх ефективність.

Сутність атаки типу clickjacking, що перекладається з англійської як "захоплення кліка", полягає в тому, зловмисник отримує можливість виконати під чужим іменем певні дії – клікнути по сайту-жертві.

Атака clickjacking здійснюється за наступним алгоритмом.

1. Зловмисник створює сторінку, яка містить шкідливий код з посиланням на сайт-жертву. Це посилання надається у формі, що має зацікавити користувача (наприклад, «Отримай скидку», «Смішні котики» тощо) і на перший погляд видається абсолютно безпечним.
2. Поверх цього ніби безпечного посилання на шкідливий сторінці розміщується прозорий <iframe> з src із сайту-жертви так, щоб прозо-

ра кнопка, наприклад, «like», знаходилася точно над посиланням. Для цього зазвичай використовують z-index CSS.

3. Відвідувача будь-яким способом заманюють на шкідливу сторінку.

4. Якщо відвідувач натискає на привабливе і ніби безпечне посилання, то насправді він натискає на кнопку. В результаті відвідувач може, наприклад, додати «лайк», якщо він авторизований на сайті-жертві, і не здогадуватися про це.

Зловмисник також може [2-4]:

- створити кадр розміром 1×1 піксель, який переміщається разом з курсором миші і є невидимим для користувача внаслідок малого розміру. Тоді користувач, клацаючи у будь-якому місці, натискає на все, що завантажено та розташоване в цьому кадрі 1×1.

- обрізати фрагменти та вставити їх на шкідливій сторінці. Так можна вставити iFrame кнопки «Надіслати» і надати їй органічний вигляд на шкідливій сторінці;

- здійснити прокруточні атаки – приховати частину довіреного діалогу, прокручуючи сторінку доти, доки більшість діалогу не перестане відображатися на екрані, і залишаться лише кнопки «ОК» та «Отмена». Це змушує кінцевого користувача повірити, що кнопки відповідають питанню, розташованому зліва;

- здійснити швидку заміну контенту з метою обійти захист від очищення екрана під час подвійного клацання мишею користувачем: перше клацання видалить шкідливе накладення, а друге клацання буде відправлено в довірений діалог під ним. Процес займає мілісекунди і не помічається користувачем;

- створювати і застосовувати фантомні курсори миші;

- здійснити перетягування цікавого для зловмисника контенту на шкідливий сайт за допомогою хибної смуги прокрутки тощо.

Теоретично можна переспрямовувати не тільки кліки миші, а й клавіатурне введення, однак такий метод практично не застосовується внаслідок наступних причин:

- по-перше, потрібно створити умови, щоб відвідувач сайту почав вводити конфіденційну інформацію, в якій зацікавлений зловмисник, на прозорому текстовому полі, накладеному на інше текстове поле;

- по-друге, символи, які вводить відвідувач, будуть невидимими, бо верхнє текстове поле є прозорим;

– по-третє, відвідувач зазвичай припиняє друк, коли не бачить результатів.

Для запобігання clickjacking можуть застосовуватися різні методи:

– framebusting – використання коду JavaScript, який фактично забороняє відкривання сторінки у фреймі: як тільки виявляється, що вікно відкрите у фреймі, воно розміщується поверх нього. Це старий спосіб захисту, для обходу якого зловмисник може блокувати тор-навігацію в обробнику подій beforeunload або зняти обмеження на використання скриптів і форм за допомогою атрибутів sandbox;

– заголовок X-Frame-Options з боку сервера, який може мати різні значення, в залежності від яких сторінка у фреймі ніколи не буде відкриватися, або буде відкриватися, тільки якщо батьківський документ має те ж саме джерело чи розташовується на вказаному у заголовку домені;

– блок <div>, розташований поверх всієї сторінки (блок зі стилями height: 100%; width: 100%;), який дозволяє перехоплювати всі кліки і прибирається за умови window == top або тоді, коли ми впевнені, що захист не потрібен;

– атрибут samesite файлів cookie дозволяє відправляти ці файли на сайт тільки тоді, коли вони відкриті тільки напряму, а не через фрейм чи якимось іншим чином. Цей метод не дозволяє захиститися від clickjacking, якщо файли cookie не використовуються.

### **Висновки**

В даній роботі визначені принципи організації атаки clickjacking, проведено аналіз сучасних методів запобігання атаці clickjacking і визначено їх ефективність.

Атака clickjacking дозволяє хакеру перехопити лише один клік, однак:

– вразливості можуть бути наявні в будь-яких блоках сторінки, де відвідувач може здійснити клік;

– при проектуванні інтерфейсів зазвичай не передбачається, що хакер може здійснити клік від імені легітимного авторизованого користувача;

– якщо після перехопленого кліку з'являються інші елементи управління, то хакер отримує додаткові можливості для скоєння злочинних дій.

Для захисту від атаки clickjacking рекомендується використовувати:

- на сторінках, які не призначені для перегляду у кадрі – X-Frame-Options: SAMEORIGIN;
- на сторінках, які призначені для перегляду у кадрі – перекриваючий блок <div>.

**Список літератури:**

1. Атака типа clickjacking. URL: <https://learn.javascript.ru/clickjacking>
2. CAPEC-103: Clickjacking. URL: <https://capec.mitre.org/data/definitions/103.html>
3. Testing for Clickjacking. URL: [https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/11-Client-side\\_Testing/09-Testing\\_for\\_Clickjacking.html](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking.html)
4. Clickjacking Threats. URL: [https://www.w3.org/Security/wiki/Clickjacking\\_Threats](https://www.w3.org/Security/wiki/Clickjacking_Threats)

**УДК 004.056:629.12**

## **НАСЛІДКИ DDOS-АТАК НА ВОДНИЙ ТРАНСПОРТ**

***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 інформаційних технологій 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, 2]. Розробці засобів виявлення і запобігання DoS і DDoS-атакам, присвячено багато наукових робіт [3-7], а на ринку наявні як ряд засобів організації атак цього типу [8], так і ряд різноманітних за принципами дії, за функціональними та експлуатаційними властивостями засобів захисту від DoS і DDoS атак, але методика їх оптимального вибору для галузі водного транспорту на даний момент відсутня.

Вибір засобів захисту має бути адекватним наявним ризикам, які визначаються за процедурами [9] з врахуванням потенційних наслідків реалізації загроз.

**Метою даної роботи** є визначення наслідків DoS і DDoS-атак на водний транспорт.

Для досягнення поставленої мети необхідно провести аналіз можливих наслідків DDoS-атак і визначити їх вплив на складові морської інфраструктури і бізнес процеси.

Як показав проведений аналіз, DoS і DDoS-атаки на водний транспорт можуть викликати наступні проблеми для цієї критичної інфраструктури:

1. Перебої у роботі електронних систем: DOS-атаки можуть спричинити відмову електронних систем на судах та в інфраструктурі, призводячи до значних перебоїв у їх нормальній роботі.

2. Навігаційні проблеми та загрози безпеці плавання: Відмова систем навігації може створити серйозні ризики для безпеки плавання, загрожуючи як пасажиром, так і екіпажам.

3. Економічні втрати для компаній та організацій: Затримки та проблеми, викликані DDOS-атаками, можуть призвести до значних економічних втрат для компаній, які управляють водним транспортом.

4. Можливість аварій та безпеки плавання: Відмова систем безпеки може створити потенційно небезпечні умови для плавання та збільшити ризик аварій.

5. Порушення логістичних ланцюгів та господарської діяльності: DDOS-атаки можуть вплинути на логістичні ланцюги, обмежуючи рух суден та порушуючи господарську діяльність, пов'язану з водним транспортом.

6. Міжнародні наслідки: Атаки можуть мати міжнародні наслідки, оскільки вони можуть впливати на транскордонний рух суден та міжнародний транспорт.

7. Зниження довіри до безпеки водного транспорту: Подібні інциденти можуть призвести до зниження довіри громадськості та пасажирів до безпеки водного транспорту.

8. Необхідність вдосконалення кібербезпеки: Висока ймовірність підвищення уваги до потреби вдосконалення заходів кібербезпеки для запобігання подібним атакам у майбутньому.

9. Відновлення та усунення наслідків: Після атаки необхідно витратити час і ресурси на відновлення та усунення наслідків, що може вимагати значних зусиль та коштів.

10. Зміцнення кібербезпекових стандартів: Атаки на водний транспорт підкреслюють важливість розробки та дотримання високих кібербезпечних стандартів в даній галузі для забезпечення стійкості та надійності систем.

11. Зниження ефективності транспортної системи: DDOS-атаки можуть призвести до зниження ефективності та продуктивності водного транспорту, що впливає на розклади та обслуговування.

### **Висновки**

В даній роботі проведено аналіз можливих наслідків DDoS-атак і визначено їх вплив на складові морської інфраструктури та бізнес процеси. При обробці ризиків за методикою [9] критичність наслідків повинна оцінюватися відповідно до «Морської доктрини України» [10] з врахуванням рекомендацій Міжнародної морської організації [11] і Агентства Європейського Союзу з кібербезпеки (ENISA) [12].

### **Список літератури:**

1. Дайджест событий в мире кибербезопасности за первый квартал 2023 года. URL: <https://ddos-guard.net/ru/blog/daidzhest-kiberbezopasnosti-2023-Q1>
2. Обзор первого квартала 2023 года: отчет StormWall о DDoS-атаках. URL: <https://stormwall.pro/otchet-o-ddos-atakah-stormwall-pervyj-kvarta-l-2023>
3. Anthony D. Wood and John A. Stankovic A Taxonomy for Denial-of-Servi ce Attacks in Wireless Sensor Networks. URL: <https://www.cs.virginia.edu/~stankovic/psfiles/computer02-dos.pdf>
4. 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>
5. Raymond D. R., Midkiff S. F. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. – IEEE Pervasive Computing. – January-March 2008. – P. 74-81. URL: <http://irep.iium.edu.my/576/1/Pathan-P.pdf>

6. Александер 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. Луцкий М.Г., Гавриленко А.В., Корченко А.А., Охрименко А.А. Модели эталонов лингвистических переменных для систем выявления атак //Захист інформації. – 2012. – №12. – С.5-12. URL: <https://jrn1.nau.edu.ua/index.php/ZI/article/view/2188/13231>

8. 15 найкращих безкоштовних інструментів DDoS-атаки в Інтернеті. URL:<https://techukraine.net/15-%D0%BD%D0%B0%D0%B9%D0%BA%D1>

9. 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](https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400)

10. Морська доктрина України на період до 2035 року, затверджена постановою Кабінету Міністрів України від 7 жовтня 2009 р. №1307. URL: <https://zakon.rada.gov.ua/laws/show/1307-2009-%D0%BF#Text>

11. MSC-FAL.1/Circ.3/Rev.2. Guidelines on maritime cyber risk management. URL: [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSF-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSF-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf)

12. Port Cybersecurity – Good practices for cybersecurity in the maritime sector. URL: <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector>

## ЗМІСТ

### **Секція 1. Інформаційна безпека транспортних засобів і систем..... 3**

|                                                                                                                                       |    |
|---------------------------------------------------------------------------------------------------------------------------------------|----|
| Розробка системи віддаленого керування камерою на базі месенджера «Телеграм» <i>Байдиков А.О.; Білець О.О.; Вовк Є.Р.</i> .....       | 3  |
| Сучасні завдання забезпечення національної системи стійкості на водному транспорті <i>Блінцов В.С.; Буруніна Ж.Ю.</i> .....           | 5  |
| OSINT-методологія розвідки у кіберпросторі <i>Божаткін С.М.; Пасюк Б.Б.</i> .....                                                     | 12 |
| Класифікація систем Інтернет речей <i>Бондар О.О.</i> .....                                                                           | 19 |
| Роль CTF-змагань в кібербезпеці <i>Іванов В.І.</i> .....                                                                              | 21 |
| Проблеми інформаційної безпеки при віддаленому керуванні лабораторним обладнанням стенду «Цифровий автомат» <i>Клеошин С.К.</i> ..... | 25 |
| Сучасні виклики інформаційній безпеці в галузі морських перевезень <i>Кучер В.С.</i> .....                                            | 30 |
| Оптимізація та контроль процесів виявлення та реагування на кібератаки SOC-центру <i>Михайличенко А.В.</i> .....                      | 35 |
| Класифікація систем Інтернет речей <i>Рукинов В.А.</i> .....                                                                          | 40 |
| Системи виявлення вторгнень для водного транспорту, як основний метод захисту <i>Тотх М.</i> .....                                    | 43 |

### **Секція 2. Захист інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах ..... 47**

|                                                                                                                                                    |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Методи і засоби захисту інформації у технічних каналах об'єкта інформаційної діяльності Національної гвардії України <i>Болтовський А.В.</i> ..... | 47 |
| Аналіз задач та структури системи захищеного електронного документообігу для об'єктів інформатизації <i>Дзюбас Д.С.</i> .....                      | 52 |
| Порушення блокуючих інструкцій в асинхронних методах Java <i>Самойленко Д.М.</i> .....                                                             | 59 |
| Вдосконалення захищеності бездротових точок доступу в мережі WI-FI <i>Соболев В.В.</i> .....                                                       | 63 |
| Система аналізу захищеності точок доступу Wi-Fi <i>Соболев В.В.; Козирев С.С.</i> .....                                                            | 66 |

|                                                                                                                                                                          |            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| Аналіз ринку та основних рекомендацій щодо безпеки пристроїв IoT <i>Стефанюк Ю.О.</i> .....                                                                              | 69         |
| Захист програмних продуктів під час розробки <i>Тихонов О.Ю.</i> .....                                                                                                   | 74         |
| Інформаційна безпека віддаленого доступу до корпоративних мереж <i>Трибулькевич С.Л.; Трибулькевич В.В.</i> .....                                                        | 78         |
| Загрози глобальній маршрутизації в сучасному кіберпросторі <i>Турти М.В.</i> .....                                                                                       | 83         |
| Розробка комплексної системи захисту інформації режимно-секретного відділу морського порту <i>Харченко М.С.</i> .....                                                    | 92         |
| Розробка рекомендацій по вдосконаленню єдиного електронного реєстру «ОБЕРІГ» <i>Харченко С.М.</i> .....                                                                  | 96         |
| <b>Секція 4. МОДЕЛЮВАННЯ ОБ'ЄКТІВ І ПРОЦЕСІВ<br/>ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ</b> .....                                                                                 | <b>102</b> |
| Фактори, що впливають на розбірливість мови <i>Іванова А.В.</i> .....                                                                                                    | 102        |
| Отримання аналітичних залежностей ефективного рівня відчуття формант від коефіцієнта їх сприйняття <i>Касьянов Ю.І.; Золотченко В.В.</i> .....                           | 106        |
| Узагальнення спектрів довготривалих мовленнєвих сигналів з використанням процедур обробки зображень <i>Касьянов Ю.І.; Щербаков М.С.; Троценко С.С.</i> .....             | 110        |
| Генетичний алгоритм оцінювання рівня захищеності складнозашумленої мовної інформації за критерієм залишкової розбірливості мови <i>Нужний С.М.; Передерій В.І.</i> ..... | 115        |
| Оцінка стану інформаційної та кібернетичної безпеки об'єктів критичної інформаційної інфраструктури <i>Передерій В.І.; Федорчук Є.Ю.</i> .....                           | 126        |
| Розробка структури моделі системи автоматичного визначення розбірливості мовної інформації <i>Трізно С.О.</i> .....                                                      | 130        |
| Електромагнітна сумісність як впливовий фактор ризиків інформаційної безпеки <i>Турти М.В.</i> .....                                                                     | 134        |

**Секція 5. СТВОРЕННЯ ПІДВОДНО-ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ  
ЗАХИСТУ МОРСЬКИХ ОБ'ЄКТІВ ТА АКВАТОРІЙ..... 142**

|                                                                                                                                                         |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Вибір оптимальної системи керування електроприводом стрічкового конвеєра <i>Аннич С.В.</i> .....                                                        | 142 |
| Використання ВІМ технології для створення засобів морської робототехніки <i>Бабкін Г.В.</i> .....                                                       | 146 |
| Буксирна лебідка малогабаритного підводного апарату <i>Гаринкін Д.Ю.</i> .....                                                                          | 148 |
| Дослідження та аналіз методів векторного керування двигуном для забезпечення ефективного керування судновими електроприводами <i>Жигadlo О.М.</i> ..... | 150 |
| Електропривод рушійно-рульового пристрою підводного апарата <i>Лебедік В.І.</i> .....                                                                   | 152 |
| Оптимізація характеристик електрообладнання буксируваної підводної системи <i>Мібра В.Я.</i> .....                                                      | 155 |
| Альтернативне джерело живлення берегового посту моніторингу підводної обстановки <i>Решетило О.Є.</i> .....                                             | 158 |
| Електрообладнання кабельної лебідки дистанційно керованого підводного апарата <i>Стрельцов С.А.</i> .....                                               | 159 |

**Секція 7. ШКОЛА МОЛОДИХ НАУКОВЦІВ ..... 162**

|                                                                                                                                    |     |
|------------------------------------------------------------------------------------------------------------------------------------|-----|
| Нормативно-правові засади забезпечення електромагнітної сумісності засобів технічного захисту інформації <i>Баранов А.В.</i> ..... | 162 |
| Принципи інтелектуального управління інформаційною безпекою корпоративної мережі порту <i>Грищенко С.Л.</i> .....                  | 168 |
| Перспективи використання кластерного аналізу для оцінювання інвестицій в інформаційну безпеку <i>Задорожний А.О.</i> .....         | 175 |
| Критерії прийняття рішень щодо обробки ризиків об'єктів морської інфраструктури <i>Зубков А.П.</i> .....                           | 181 |
| Дослідження демаскуючих факторів системи Starlink <i>Каплюк О.П.</i> .....                                                         | 188 |
| Дослідження стійкості системи Starlink до зовнішніх завад <i>Ковальський Д.А.</i> .....                                            | 193 |

|                                                                                        |     |
|----------------------------------------------------------------------------------------|-----|
| Особливості використання Raspberry PI для пентестингу<br><i>Литвиненко О.-Н.</i> ..... | 200 |
| Сучасні моделі доступності інформації <i>Машикін О.О.</i> .....                        | 205 |
| Аналіз особливостей атак типу clickjacking <i>Потоцький О.О.</i> .....                 | 212 |
| Наслідки DDoS-атак на водний транспорт <i>Садалюк Є.О.</i> .....                       | 215 |

*Наукове видання*

**СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ  
БЕЗПЕКИ НА ТРАНСПОРТІ**

**СПІБТ–2023**

**XI Всеукраїнська науково-технічна конференція  
з міжнародною участю**

**23–24 листопада 2023 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

---