



**НАУКОВО-ТЕХНІЧНІ
КОНФЕРЕНЦІЇ**

Національний університет кораблебудування
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

МАТЕРІАЛИ

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

27-28 листопада 2025 р.

**У двох частинах
Частина 2**



Миколаїв ■ НУК ■ 2025

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова**

**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**

**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**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

**СУЧАСНІ ПРОБЛЕМИ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
НА ТРАНСПОРТІ**

СПІБТ–2025

МАТЕРІАЛИ

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

27–28 листопада 2025 року

**У двох частинах
Частина 2**

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



МИКОЛАЇВ • НУК • 2025

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 XIII Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2025. – Ч. 2. – 100 с.

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

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

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

УДК 004

© Національний університет кораблебудування
імені адмірала Макарова, 2025

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТРАНСПОРТНИХ ЗАСОБІВ І СИСТЕМ

ПОБУДОВА РЕЛЯЦІЙНОЇ МОДЕЛІ ВЗАЄМОВПЛИВУ ФАКТОРІВ ВРАЗЛИВОСТЕЙ НА ЗАХИЩЕНІСТЬ ОБ'ЄКТУ ВОДНОГО ТРАНСПОРТУ

Автор: Бондаренко І.Ю., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

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

На сучасному етапі розвитку транспортної галузі одним із ключових напрямів є забезпечення стійкості та захищеності об'єктів водного транспорту, які функціонують у умовах дії техногенних, організаційних, природних, кібернетичних та соціально-криміногенних загроз. Висока динамічність змін середовища, складність технічних систем та багатоаспектність факторів ризику зумовлюють необхідність використання формалізованих математичних підходів, серед яких реляційні моделі займають провідне місце.

Реляційна модель дозволяє описати об'єкт водного транспорту як систему взаємопов'язаних сутностей: факторів вразливостей, загроз, умов середовища, контрзаходів та можливих інцидентів. На відміну від традиційних логічних чи експертних методів, вона забезпечує структурований опис даних, встановлює формальні зв'язки між параметрами та дозволяє виконувати багатофакторний аналіз ризиків.

На основі аналізу факторів, що впливають на безпеку об'єктів водного транспорту, визначено такі ключові групи вразливостей:

- **технічні** (несправність навігаційних і енергетичних систем, зношеність конструкцій);
- **організаційні** (недоліки регламентів, порушення процедур);
- **людський фактор** (кваліфікація та стан оператора);
- **інформаційно-кібернетичні** (атаки на навігаційні дані, уразливості мереж, вплив хибної інформації);
- **природні та екологічні** (погодні умови, течії, туман);
- **соціально-криміногенні** (нелегальні дії, диверсії).

Особливістю зазначених факторів вразливостей є неможливість їх прямого вимірювання, оскільки вони мають ймовірнісну природу та часто характеризуються невизначеністю. Для розв'язання цієї проблеми реляційна модель може бути інтегрована з імовірнісними методами, зокрема Байєсовими мережами, які дозволяють оцінювати рівень ризику на основі умовних залежностей та неповних даних. Такий підхід уже довів свою ефективність для оцінки стійкості систем критичного призначення, де зовнішні впливи та вразливості важко оцінити традиційними методами.

Усі зазначені фактори мають здатність взаємодіяти між собою, формуючи каскадні та комбіновані сценарії розвитку небезпечних ситуацій. Наприклад, технічна відмова у поєднанні з недостатньою видимістю та помилкою особи що приймає рішення (ОПР) значно підвищує ризик навігаційного інциденту. Таким чином, класичний однофакторний підхід є недостатнім, тому доцільним є моделювання саме системи взаємовпливу нечітких факторів загроз.

Виходячи з цього на рисунку 1 наведена структура реляційної моделі.

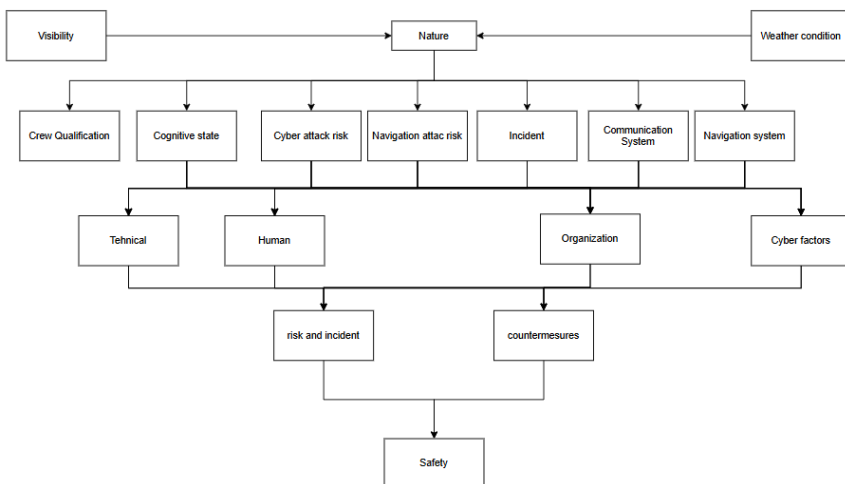


Рис. 1 – Структура реляційної моделі.

Побудована реляційна модель включає сутності **Asset**, **VulnerabilityFactor**, **Threat**, **Control**, **Environment**, **Incident** та відповідні зв'язки типу «багато-до-багатьох». Це дає змогу визначати, які фактори вразливостей характерні для конкретного об'єкта, які загрози їх експлуатують, що посилює чи знижує ризики, та яким чином контрзаходи впливають на загальний рівень захищеності.

Для оцінки стійкості та захищеності об'єктів водного транспорту розроблена Байєсова мережа довіри (БМД), яка представляє імовірнісну графічну модель, що є набором випадкових величин та їх умовних ймовірностей за допомогою ациклічного орієнтованого графа (рис. 2).

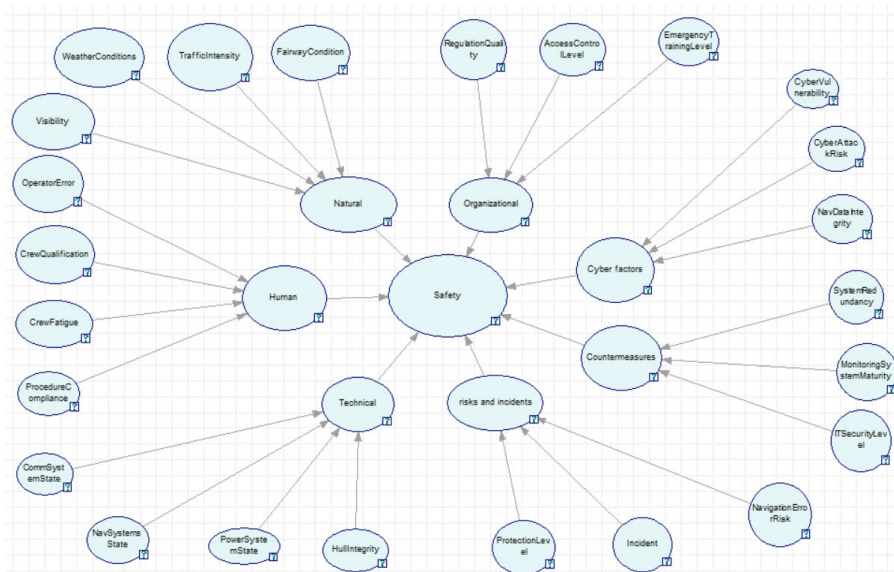


Рис. 2 – Байєсова мережа довіри оцінки стійкості та захищеності об'єкту водного транспорту.

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

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

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

У відповідності до БМР (рис.2) проведено експерименти з оцінювання захищеності об'єкту водного транспорту у середовищі GeNIe 4. Результати наведено на рисунку 3.

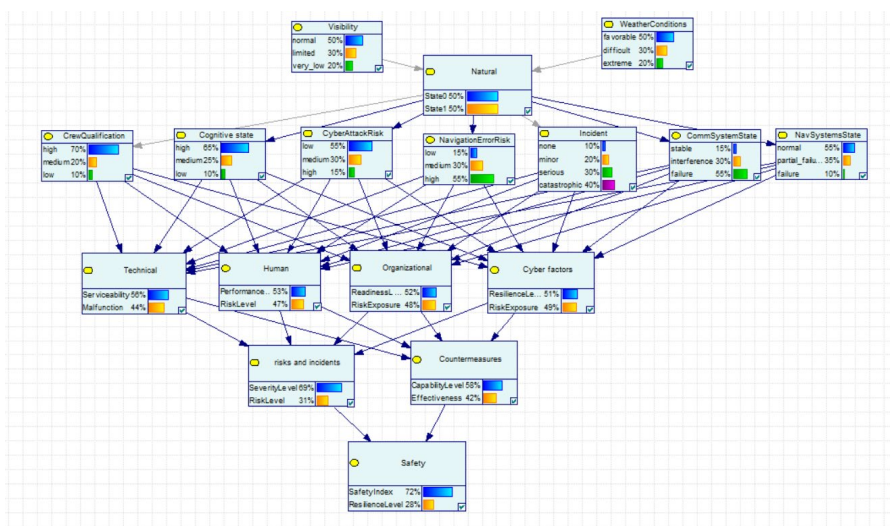


Рис.3 – Результати оцінювання захищеності об'єкту водного транспорту на основі БМД.

Висновки.

Отже, побудова реляційної моделі взаємовпливу факторів вразливостей може бути одним із необхідним етапом формування комплексної системи безпеки об'єктів водного транспорту, що забезпечить:

- формалізацію факторів ризику;
- структурований опис їх взаємодій;
- можливість автоматизованої оцінки загроз;

- інтеграцію з імовірнісними методами;
- обґрунтоване прийняття управлінських рішень щодо підвищення рівня захищеності.

Запропонований підхід є актуальним та перспективним у зв'язку з ускладненням умов функціонування водного транспорту і зростанням значення інформаційної, технічної та кібербезпеки у забезпеченні стабільності його роботи.

Список літератури:

1. Terje Aven. Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*. 2016. V. 253. № 1. P. 1–13.

2. 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.

3. Perederyi, V., Borchik, E., Zosimov, V., Bulgakova, O. (2024). Assessment and Support of Critical Multilevel Infrastructure Security Using Information and Cognitive Technologies. In: Hu, Z., Zhang, Q., He, M. (eds) *Advances in Artificial Systems for Logistics Engineering IV. ICAILE 2024. Lecture Notes on Data Engineering and Communications Technologies*, vol 223. Springer, Cham. https://doi.org/10.1007/978-3-031-72017-8_8)

4. В. І. Передерій, Є. Ю. Борчик. Оцінка та підтримка функціональної стійкості засобів водного транспорту. *Науковий вісник Херсонської державної морської академії: науковий журнал*. –Херсон: Херсонська державна морська академія, 2025. No 2(31). С. 64-76

УДК 004.056.5

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ РОЗПІЗНАВАННЯ ОЗНАК В БІОМЕТРИЧНИХ СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ

Автор: Гальченко О.Л., 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

Біометричні системи контролю доступу (БСКД) швидко розповсюджуються в завдяки зручності та потенційно високій надійності реалізованої в них багатофакторної автентифікації. Розробці БСКД присвячені роботи багатьох вітчизняних та іноземних фахівців [1-12].

Водночас різні методи розпізнавання біометричних ознак (feature-based, шаблонні, статистичні, нейромережеві, зокрема, глибинного навчання – deep learning) передбачають використання різних математичних апаратів та алгоритмів і мають принципово різні показники якості (точність, що характеризується багатьма показниками, стійкість до завад і атак, вимоги до обчислювальних ресурсів і приватності тощо). Стрімкий розвиток обчислювальної техніки, інформаційних технологій і датчиків біометричних ознак зумовлюють лавиноподібний розвиток підходів, методів і методик виявлення біометричних ознак і розпізнавання осіб в БСКД.

Метою даної роботи є порівняльний аналіз основних сучасних підходів до виділення та розпізнавання біометричних ознак у БСКД.

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

- провести комплексний аналіз сучасних БСКД і визначити множину методів, для яких буде проводитися порівняння;
- визначити критерії порівняння реалізованих у відібраних методах підходів до виділення та розпізнавання біометричних ознак;
- провести порівняльний аналіз визначених підходів до виділення та розпізнавання біометричних ознак у БСКД за визначеними критеріями.

Для аналізу були обрані БСКД, що працюють на різних біометричних ознаках (ознаки обличчя особи, відбитків пальців, райдужної оболонки ока) та мультимодальні системи. До уваги були прийняті огляди нейромереж глибокого навчання в біометрії, класичні дослідження з локальних бінарних шаблонів (англ. Local Binary Patterns, LBP) та звіти NIST щодо продуктивності систем розпізнавання облич [1-12]. Як показав комплексний аналіз сучасних БСКД, на поточний час найбільш популярними для розпізнавання осіб за біометричними ознаками є:

- класичні дескриптори й алгоритми (характеристики для відбитків, фільтри Delaunay/Gabor, детектори SIFT (англ. scale-invariant feature transform) та ORB (англ. (Oriented FAST and Rotated BRIEF) для зображень);
- текстурно-локальні методи, такі як LBPi дескриптори особливих точок, (Histogram of Oriented Gradients, HOG);
- статистичні підходи, зокрема, метод головних компонент (principal component analysis, PCA) і лінійний дискримінантний аналіз (англ. Linear Discriminant Analysis, LDA) як методи зменшення розмірності/побудови шаблонів;
- підходи на основі загорткових нейромереж (англ. convolutional neural network, CNN) і поглибленого навчання з врахуванням спеціалізованих архітектур для облич, відбитків пальців, райдужки ока);
- мультибіометричні та мультимодальні підходи з рівнями злиття (англ. fusion).

Для порівняння підходів до виділення та розпізнавання біометричних ознак у БСКД обрано наступні критерії:

- точність та стабільність результатів;
- стійкість до спуфінгу та підробок ознак;
- вимоги до обчислювальних ресурсів;
- масштабованість і обслуговування бази зразків;
- приватність та законодавчі обмеження.

Порівняння підходів, реалізованих в сучасних БСКД для виділення та розпізнавання біометричних ознак, за визначеними критеріями дозволяє зробити наступні висновки/

CNN забезпечують значне підвищення точності в задачах розпізнавання облич і райдужної оболонки порівняно з класичними дескрипторами [4, 5, 8-11], що підтверджується оглядовими роботами про

застосування глибинного навчання (англ. deep learning) у біометрії. Проте в умовах обмежених даних або сильних викривлень прості локальні дескриптори (наприклад, LBP) можуть давати конкурентні результати завдяки інваріантності до локальних змін освітлення і простоті реалізації [5].

Шаблонні методи, що використовують лише однорідні дані (наприклад, 2D-зображення обличчя), є вразливими до високоякісних підробок фото і відео зображень [2, 3, 12]. Методи глибокого навчання дозволяють додавати модулі детекції фальсифікацій (anti-spoofing), але загальна стійкість зростає суттєво при мультибіометричному підході (поєднання декількох модальностей) — саме злиття дає найкращий баланс безпеки й точності, хоч і підвищує складність системи [1, 2, 5, 7].

Класичні алгоритми (LBP, PCA, продуктивні алгоритми за шаблоном) зазвичай мають низькі вимоги до обчислювальних ресурсів і при певних умовах здатні працювати в реальному часі, що робить їх придатними для вбудованих пристроїв доступу. Натомість глибинні моделі потребують значних ресурсів при навчанні та, в багатьох випадках, при виконанні їх алгоритмів (хоча мобільні оптимізації й квантування помітно зменшують ці вимоги). Практично перевірено [5], що з точки зору мінімізації вимог до обчислювальних ресурсів і швидкодії ефективним є використання гібридних архітектур, в яких локальні швидкі дескриптори використовуються на точках збирання ознак, а серверні нейромережі – для остаточної верифікації.

Для великих баз (на підприємствах чи в державних реєстрах) критичним є час пошуку образу в пам'яті, масштабованість БСКД, забезпечення зручності і коректності введення і видалення даних з бази образів. Звіти NIST [6, 7] демонструють, що реалізації сучасних алгоритмів різняться за масштабованістю та ймовірністю хибно-позитивного знаходження; вибір алгоритму має враховувати компроміс між точністю і швидкістю пошуку.

Зберігання біометричних шаблонів викликає серйозні ризики приватності. Методики, що зберігають відновлювані шаблони (англ. plaintext templates), потребують додаткового шифрування або використання приватних багатосторонніх протоколів / гомоморфного

порівняння. Технічно сприятливі підходи — збереження хешованих/бінаризованих неповторних шаблонів або застосування федеративного навчання при БСКД в розподілених системах [3].

Для критичних застосувань контролю доступу в статті [8] рекомендовано мультимодальний підхід з поєднанням принаймні двох різних сенсорних модальностей (наприклад, відбиток + обличчя або райдужка + обличчя) і злиттям на рівні ознак/рішень; це підвищує стійкість до атак і зменшує помилки.

У сценаріях з обмеженими ресурсами доцільно застосовувати локальні дескриптори (LBP, HOG) в комбінації з легкими класифікаторами, а при наявності серверної інфраструктури — слід інтегрувати CNN для остаточної ідентифікації [4].

Згідно з фреймворками NIST [6, 7] необхідно впроваджувати механізми захисту шаблонів (шифрування, біометричні ключі) та проводити регулярні тестування продуктивності й упередженості алгоритмів.

Висновки. В даній роботі на основі інформації з відкритих джерел проведено комплексний аналіз сучасних БСКД, визначена множина методів, доцільних для порівняння, критерії порівняння реалізованих у відібраних методах підходів до виділення та розпізнавання біометричних ознак, проведено порівняльний аналіз підходів визначених підходів за обраними критеріями.

Отримані результати є обґрунтованими теоретично і в конкретних умовах експлуатації БСКД мають бути перевірені на реальних наборах даних із тестуванням проти спуфінгу.

Список літератури:

1. Abdo A.A., Lawgali A.O., Abdalla M.A.E. A Review of the Iris Recognition Methods Used for the Individual Authentication. Transactions on Machine Learning and Artificial Intelligence. 2021. Vol.8. No.6. P.16-26. DOI: 10.14738/tmlai.86.9687. URL: <http://dx.doi.org/10.14738/tmlai.86.9687>
2. Face Recognition Technology Evaluation (FRTE) 1:1 Verification. URL: <https://pages.nist.gov/frvt/html/frvt11.html>
3. Guo Y., Mu H., Liu X., Ren H., Han C. Federated learning for biometric recognition: a survey. The Artificial Intelligence Review. 2024. Vol.57. Issue 8. DOI:10.1007/s10462-024-10847-7. URL: https://link.springer.com/article/10.1007/s10462-024-10847-7?utm_source=chatgpt.com

4. Huang D., Shan C., Ardabilian M., Wang Y., Chen L. Local Binary Patterns and Its Application to Facial Image Analysis: A Survey. IEEE Transactions on Systems, Man, and Cybernetics, Part C. 2011. Vol.41. P.765-781. URL: <https://liris.cnrs.fr/Documents/Liris-5004.pdf> liris.cnrs.fr
5. Minaee S., Abdolrashidi A., Su H., Benamoun M., Zhang D. — Biometrics Recognition Using Deep Learning: A Survey. arXiv. 2021. P.1-32. URL: <https://arxiv.org/abs/1912.00271>
6. NIST – Face Recognition Vendor Test (FRVT). URL: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt> NIST
7. NISTIR 8381 Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel and Immigration. URL: <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8381.pdf>
8. Purohit H., Pawan K Ajmera P.K. Multimodal Biometric Systems: A Brief Study. // International Journal of Innovative Technology and Exploring Engineering (IJITEE). 2019. Vol.8. Issue 7. P.108-111. URL: <https://www.ijitee.org/wp-content/uploads/papers/v8i7/F3796048619.pdf>
9. Дадиверін В.В., Фещенко І.О., Потапова К.Р., Тарасенко-Кляченко О.В., Івасенко Д.В. Система розпізнавання обличчя з використанням поєднання методів HAAR та SVM. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2022. Том 33 (72). №6. С.86-91. DOI <https://doi.org/10.32782/2663-5941/2022.6/15>. URL: https://www.tech.vernadskyjournals.in.ua/journals/2022/6_2022/15.pdf
10. Максименко Д., Шкурят О., Дичка, А. Методи глибинного навчання для розпізнавання облич, візуалізованих в умовах недостатнього освітлення на основі моделі MOBILENETV2. Вісник Хмельницького національного університету. Серія: Технічні науки. 2025. Том.355. №4. С.335-341. URL: <https://doi.org/10.31891/307-5732-2025-355-48>
11. Стасєв Ю.В., Гончаренко К.Г., Мороз В.І. Аналіз методу багатofакторної аутентифікації користувачів інформаційних систем на основі райдужної оболонки ока. Системи обробки інформації. 2023. Вип. (174). С.63-69. DOI: 10.30748/soi.2023.174.09. URL: <https://journal-hnups.com.ua/index.php/soi/article/download/1482/1350/>
12. Хенк Е. Прості методи розпізнавання облич. URL: <https://gijn.org/ua/resurs-ua/prosti-metodi-rozpiznavanna-oblic/>

УДК 004.056.5

ІНФОРМАЦІЙНА МОДЕЛЬ ВИБОРУ БАЗОВОГО ПРОФІЛЮ БЕЗПЕКИ

Автор: Ломова О.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

Метою проектування систем захисту інформації є формування придатного для впровадження на конкретному об'єкті інформаційної діяльності (ОІД) набору заходів захисту, який відповідає вимогам чинної нормативно-правової бази і ефективно вирішує питання управління ризиками інформаційної безпеки (ІБ).

Мінімально необхідний набір заходів захисту (ЗЗ) для інформаційної системи (ІС) певної категорії критичності (КК) визначено в НД ТЗІ 3.6-004-21 [1] як базовий профіль безпеки (БПБ). БПБ є основою для побудови інших профілів безпеки – галузевого профіля безпеки (ГПБ), а в разі відсутності специфічних галузевих вимог – цільового профілю безпеки (ЦПБ).

Розробка профілів безпеки є необхідною за вимогами низки міжнародних і вітчизняних нормативно-правових актів і потрапляє у сферу діяльності таких організацій як Кабінет міністрів України, Державна служба спеціального зв'язку та захисту інформації (ДССЗІ) України [1-3], Міністерство оборони України [4], Мінцифри України [5], Національний банк України та інших організацій, які розробляють ГПБ.

На даний час у відкритому доступі наявні базові профілі безпеки, затверджені наказами Адміністрації ДССЗІ у 2025 році для ІС, де обробляється відкрита або конфіденційна інформація (Наказ Адміністрації Держспецзв'язку від 30.06.2025 №409 [2]), і для ІС, де обробляється службова інформація (Наказ Адміністрації Держспецзв'язку від 02.07.2025 № 419 [3]). Для низки галузей на основі БПБ вже розроблені галузеві профілі безпеки [4] чи їх проекти [5]. Швидкість і відсутність помилок при виборі БПБ є запорукою успішного створення ефективної системи безпеки інформації (СБІ) і можуть досягатися впровадженням засобів автоматизації цього процесу.

Метою даної роботи є розробка інформаційної моделі вибору базового профілю безпеки згідно з нормативними вимогами за параметрами інформаційної системи і об'єкта інформаційної діяльності, що задаються користувачем.

Для досягнення даної мети необхідно провести аналіз актуальних базових і галузевих профілів безпеки і визначити критерії і алгоритми їх вибору, вхідні та вихідні дані розроблюваної інформаційної моделі.

Критерії вибору БПБ/ГПБ (рис.1) визначаємо з моделі впровадження СБІ, наведеної в НД ТЗІ 3.6-004-21 [1]. Ці критерії одночасно визначають нормативно-правові акти, які мають враховуватися при проектуванні СБІ.

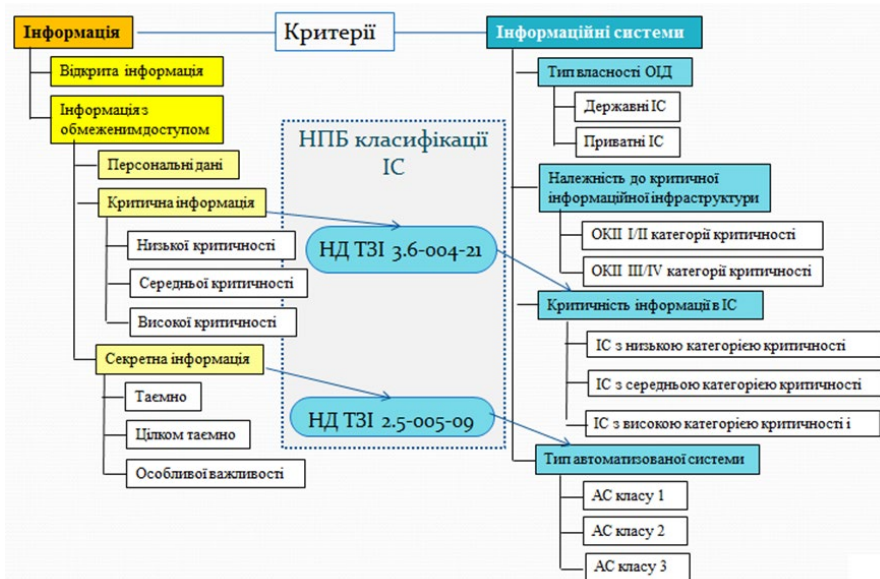


Рисунок 1 – Критерії вибору БПБ/ГПБ

Вхідні дані для розроблюваної інформаційної моделі можна умовно поділити на дві великі групи:

– вбудовані вхідні дані, що є відносно статичними, оскільки є відомостями щодо нормативно-правових актів, «защитих» у бібліотеку системи, і відомостями з цих актів, які використовуються в процесі розроблення СБІ. Ці відомості підлягають зміні тільки в разі зміни цих актів;

– вхідні дані, що вводяться користувачем, і описують інформацію та ІС, для якої створюється СБІ.

Статичними (вбудованими) вхідними даними розроблюваної інформаційної моделі є:

а) нормативно-правові акти, призначені для розміщення у бібліотеці. Склад нормативно-правової бази вибору базових профілів безпеки наведено у п.1.2 даної кваліфікаційної роботи;

б) каталог базових профілів безпеки;

в) каталог галузевих профілів безпеки;

г) каталог заходів захисту з НД ТЗІ 3.6-006-24 [6];

Вбудовані дані повинні коригуватися адміністратором бази даних в разі зміни нормативних документів і правових актів.

До вхідних даних, які вводяться користувачем для вибору БПБ, відносяться:

а) характеристики інформації, яка обробляється в ІС: відкрита інформація, персональні дані, критична інформація із визначеною категорією критичності, секретна інформація із визначеним грифом секретності, службовою інформацією;

б) характеристики ІС: тип власності, галузь діяльності організації, в якій діє ІС, що захищається СБІ, належність ІС до ОКП із визначеною категорією критичності; категорія критичності самої ІС.

Вихідними даними інформаційної моделі є:

– базовий або галузевий профіль безпеки, який містить перелік заходів захисту з номером дії з безпеки із визначеними вимогами до налаштувань параметрів заходів захисту;

– пояснення щодо вибору БПБ або ГПБ.

Узагальнений алгоритм вибору БПБ/ГПБ наведено на рис.2, а структуру інформаційної моделі – на рис.3.

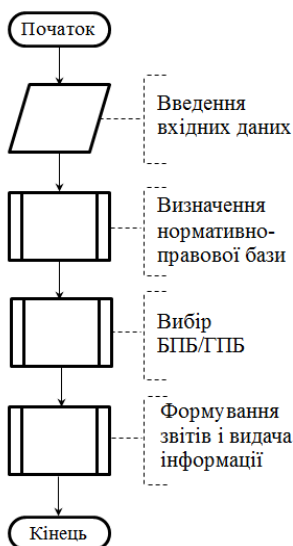


Рисунок 2 – Узагальнений алгоритм вибору БПБ і ГПБ

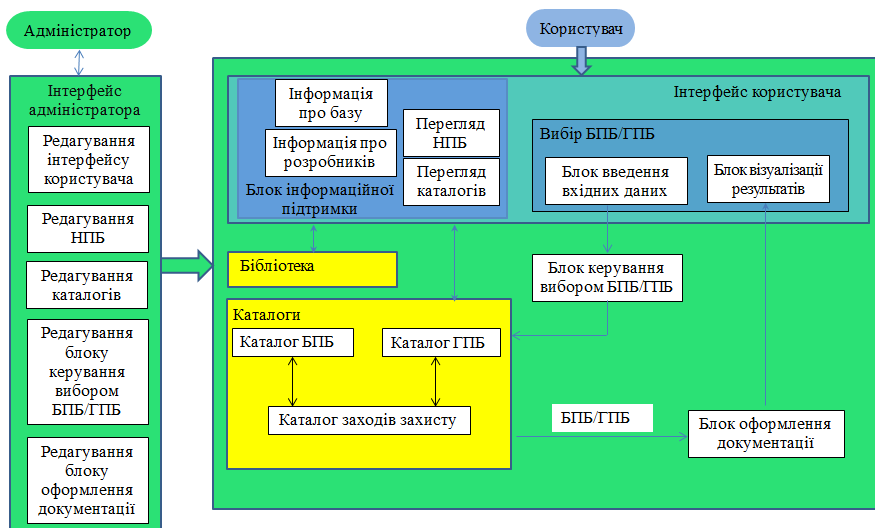


Рисунок 3 – Інформаційна модель вибору БПБ

Апробація розробленої моделі була здійснена в MS Access (рис.4).

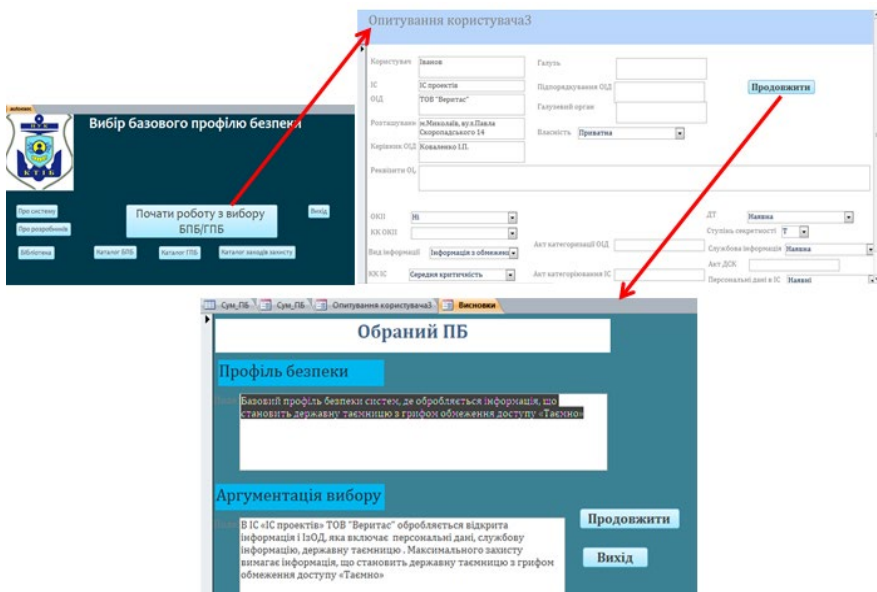


Рисунок 4 – Апробація розробленої моделі

Висновки. В даній роботі на основі інформації з відкритих джерел проведено комплексний аналіз актуальних базових і галузевих профілів безпеки і визначено критерії і алгоритми їх вибору, розроблено інформаційну модель вибору базового профілю безпеки за параметрами інформаційної системи і об'єкта інформаційної діяльності, що задаються користувачем.

Список літератури:

1. НД ТЗІ 3.6-004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=53375>

2. Наказ Адміністрації Держспецв'язку від 30.06.2025 № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація». URL:

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

<https://cip.gov.ua/ua/docs/nakaz-pro-zatverdzhennya-bazovogo-profilu-bezpeki-sistemi-de-obroblyayetsya-vidkrita-abo-konfidentiina-informaciya>

3. Наказ Адміністрації Держспецзв'язку від 02.07.2025 № 419 «Про затвердження базового профілю безпеки системи, де обробляється службова інформація». URL: <https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-02-07-2025-419-pro-zatverdzhennya-bazovogo-profilu-bezpeki-sistemi-de-obroblyayetsya-sluzhbova-informaciya>

4. Міноборони затвердило нові стандарти кіберзахисту інформаційних систем. URL: <https://mod.gov.ua/news/minoboroni-zatverdilo-novi-standarti-kiberzahistu-informacijnih-sistem>

5. Повідомлення про оприлюднення проекту наказу Міністерства цифрової трансформації України «Про затвердження галузевого профілю безпеки систем, що використовуються для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або критично важливим об'єктам інфраструктури». URL: [https://thedigital.gov.ua/documents/legislation/povidomlennia-pro-opryliudnennia-proektu-nakazu-ministerstva-tsyfrovoyi-transfor matsiyi-ukrayiny-pro-zatverdzenia-haluzevoho-profilu-bezpeky-system-shcho-vykor ystovuiutsia-dlia-nadannia-khmarnykh-posluh-taabo-posluh-tsentru-obrobky-danykh-publichnym-korystuvacham-taabo-krytychno-vazlyvym-obyektam-infrastruktury](https://thedigital.gov.ua/documents/legislation/povidomlennia-pro-opryliudnennia-proektu-nakazu-ministerstva-tsyfrovoyi-transfor-matsiyi-ukrayiny-pro-zatverdzenia-haluzevoho-profilu-bezpeky-system-shcho-vykor-ystovuiutsia-dlia-nadannia-khmarnykh-posluh-taabo-posluh-tsentru-obrobky-danykh-publichnym-korystuvacham-taabo-krytychno-vazlyvym-obyektam-infrastruktury)

6. НД ТЗІ 3.6-006-24. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=64620>

УДК 004.056.5

ІНФОРМАЦІЙНА МОДЕЛЬ ВИБОРУ АЛЬТЕРНАТИВНИХ ЗАХОДІВ ЗАХИСТУ ПРИ СТВОРЕННІ СИСТЕМИ БЕЗПЕКИ ІНФОРМАЦІЇ

***Автор:** Ткаченко Д.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*

При проектуванні систем захисту інформації головним завданням є формування набору заходів захисту, який би відповідав вимогам чинних для конкретного об'єкта інформаційної діяльності (ОІД) нормативно-правових актів, забезпечував необхідний рівень захищеності інформації і міг бути реалізований на конкретному ОІД в умовах обмежених ресурсів. При цьому впроваджувані заходи захисту (ЗЗ) мають бути адекватними наявним ризикам інформаційної безпеки як з технічної, так і з економічної точки зору і не мати критичного негативного впливу на бізнес-процеси організації.

Для інформаційної системи (ІС) мають застосовуватися ЗЗ, визначені профілем безпеки згідно НД ТЗІ 3.6-004-21 [1]. Процедура впровадження ЗЗ передбачає, що мінімально необхідний набір ЗЗ для ІС певної категорії критичності (КК) визначається базовим профілем безпеки (БПБ), а бажаний склад системи безпеки інформації (СБІ) – цільовим профілем безпеки (ЦПБ).

В процесі розробки і впровадження ЦПБ можлива ситуація, коли деякі ЗЗ не можуть бути впроваджені внаслідок їх неприйнятної для організації вартості або внаслідок їх неприйнятного негативного впливу на операційні і бізнес-процеси організації. В цьому випадку мають застосовуватися компенсаційні ЗЗ, а в разі їх відсутності – ЗЗ можуть бути аргументовано виключені з СБІ, в результаті чого утворюється адаптований профіль безпеки (АПБ). Цей процес документується і згідно моделі Плануй – Виконуй – Перевірай – Дій циклічно повторюється.

Велика кількість ЗЗ, наведених в НД ТЗІ 3.6-006-24 [2] уповільнює процес розробки СБІ і затримує процес обробки ризиків інформаційної безпеки. Крім того, повторюваність операцій і великий обсяг

оброблюваної інформації зумовлюють велику ймовірність виникнення помилок. Для усунення цих недоліків найбільш застосовуваним засобом є автоматизація процесів роботи з АПБ.

Метою даної роботи є розробка системи інформаційної моделі вибору альтернативних заходів захисту для адаптованих профілів безпеки.

Для досягнення поставленої мети необхідно розв'язати наступні **задачі**:

- провести аналіз відкритих літературних джерел і визначити актуальну нормативно-правову базу (НПБ) розробки адаптованих профілів безпеки;
- провести аналіз нормативно-правової бази розробки адаптованих профілів безпеки і визначити алгоритми їх створення та документаційного супроводу, вхідні та вихідні дані для розроблюваної інформаційної моделі;
- розробити інформаційну модель вибору альтернативних заходів захисту для адаптованих профілів безпеки.

Нормативно-правову базу дослідження складають:

1) нормативно-правові акти стосовно захисту критичної інфраструктури, персональних даних, організації захисту інформації в Україні, управління ризиками інформаційної безпеки, серед яких Закони України, Укази Президента України, Рішення Ради національної безпеки і оборони України, Постанови Кабінету Міністрів України, державні стандарти України, нормативні документи з технічного захисту інформації (НД ТЗІ), Накази Адміністрації ДССЗІ, міжнародні стандарти ISO, IEC, ISO/IEC (більшість прийняті в Україні як ДСТУ) та інші, міжнародні конвенції і Директиви Ради Європи;

2) нормативно-правові акти, які безпосередньо стосуються роботи з профілями безпеки в Україні, серед яких Постанови Кабінету Міністрів України, НД ТЗІ, Накази Адміністрації ДССЗІ і галузевих органів, які відповідають за розробку галузевих профілів безпеки (ГПБ);

3) нормативно-правові акти, які визначають принципи і процедури роботи з альтернативними ЗЗ:

а) Постанови Кабінету міністрів України:

- від 18 червня 2025 р. №712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» [3];
- від 29 листопада 2025 р. №1531 «Про внесення змін до постанови Кабінету Міністрів України від 29 березня 2006 р. № 373» [4];
- б) накази Адміністрації Держспецзв'язку:
 - від 29.05.23 №463 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами» [5], який визначає вимоги до цільових профілів безпеки автоматизованих систем управління технологічними процесами;
 - від 10.07.2024 №354 «Про затвердження Рекомендацій з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації» [6];
 - від 8.12.2025 №810 «Про затвердження Рекомендацій з оцінювання дотримання вимог цільового профілю безпеки системи» [7];
 - від 8.12.2025 №811 «Про затвердження Рекомендацій з розроблення цільового профілю безпеки системи» [8];
 - к) нормативні документи (НД) з технічного захисту інформації (ТЗІ):
 - НД ТЗІ 2.3-025-21 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [9];
 - НД ТЗІ 2.6-004-21 «Порядок авторизації безпеки інформаційних систем» [10];
 - НД ТЗІ 3.6-004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці» [1];
 - НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [2];
 - НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [11];

– НД ТЗІ 3.6-008-21 «Порядок моніторингу безпеки інформаційних систем» [12].

Вибір заходів захисту здійснюється згідно НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [2].

Аналіз нормативно-правової бази показав, що після вибору БПБ/ГПБ організації мають можливість реалізувати будь-який захід захисту з обраного профілю будь-яким способом, який забезпечить виконання вимоги безпеки та приватності і відповідає законодавству, цілям і потребам організації, концепції безпеки та політиці безпеки організації. Особливості СБІ конкретної організації віддзеркалюються в ЦПБ.

Узагальнений алгоритм створення і документування цільового профілю безпеки на основі налаштованого базового або галузевого профілю безпеки наведено на рис.1.

Вхідними даними для алгоритму рис.1 є:

- а) тип профілю безпеки (БПБ або ГПБ);
- б) зміст профілю безпеки: перелік заходів захисту, згрупований по класах і по групах в класі, із визначеними вимогами до налаштувань параметрів заходів захисту.

Вихідними даними для алгоритму рис.1 є ЦПБ і його зміст:

– перелік заходів захисту з номером дії з безпеки відповідно до БПБ із визначеними вимогами до налаштувань параметрів заходів захисту, не меншими, ніж в БПБ

– перелік дій з безпеки, які додані та/або посилені в рамках розроблення ЦПБ з окремою нумерацією

В організації призначаються відповідальні особи, які відповідають за вибір, обґрунтування та призначення параметрів для кожного ЗЗ, тобто за ці процедури відповідають організації. При цьому мають враховуватися конкретні умови діяльності організації, структура і функції ІС, результатів аналізу ризиків безпеки, вимоги політики безпеки та конфіденційності конкретних зацікавлених сторін. З цих міркувань бажані заходи захисту для організації можуть мати більш жорсткі параметри порівняно з БПБ, чи бути посиленими, а також до ЦПБ можуть бути додані ЗЗ, що відсутні в БПБ.

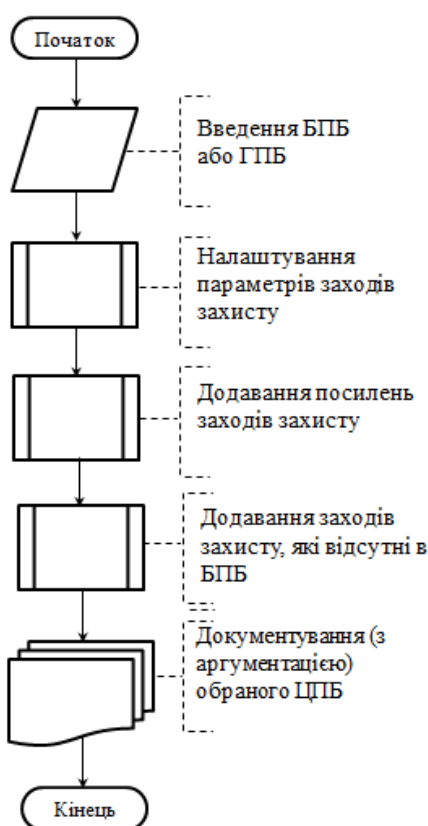


Рисунок 1 – Узагальнений алгоритм вибору і документування ЦПБ

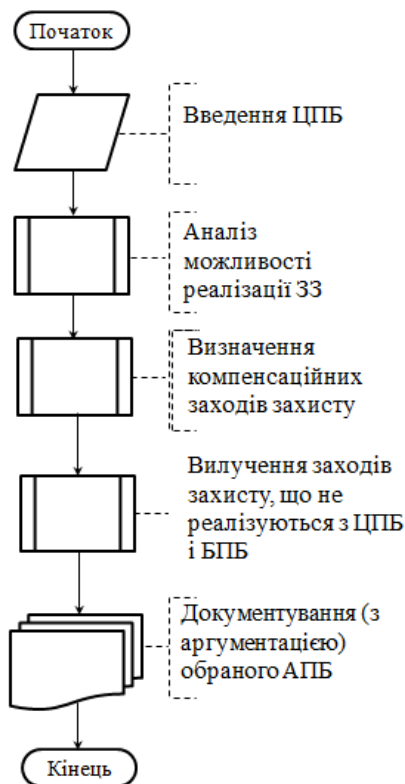


Рисунок 2 – Узагальнений алгоритм вибору і документування АПБ

В процесі розробки ЦПБ можуть виникати ситуації, коли окремі ЗЗ формально не відповідають архітектурі конкретної ІС. Наприклад, ІС функціонує у відокремленому середовищі. Тоді підключення до інших мереж відсутні і вимоги до організації мережових з'єднань не мають сенсу. Тоді для таких заходів захисту оформляється примітка, в якій зазначається технічне чи організаційне рішення, яке визначає відсутність необхідності у виконанні певної вимоги, і посилання на документ, яким це рішення закріплене (технічне завдання, політика, наказ, регламент

тощо). Всі зміни ЗЗ, які вносяться в ЦПБ відносно БПБ або ГПБ мають бути аргументовані і задокументовані.

Формування АПБ здійснюється з ЦПБ за алгоритмом, наведеним на рис.2.

Вхідними даними для алгоритму рис.2 є результати моніторингу, результати впровадження ЗЗ і поточний цільовий профіль безпеки, який містить:

- перелік заходів захисту з номером дії з безпеки відповідно до БПБ із визначеними вимогами до налаштувань параметрів заходів захисту, не меншими, ніж в БПБ;

- перелік дій з безпеки, які додані та/або посилені в рамках розроблення ЦПБ з окремою нумерацією.

На виході отримуємо:

- перелік заходів захисту з номером дії з безпеки відповідно до БПБ із визначеними вимогами до налаштувань параметрів заходів захисту, не меншими, ніж в БПБ;

- перелік дій з безпеки, які додані та/або посилені в рамках розроблення ЦПБ з окремою нумерацією;

- перелік заходів захисту, аргументовано вилучених з ЦПБ, а в разі необхідності – з БПБ. Всі виключення мають бути аргументовані і задокументовані.

Розроблена інформаційна модель наведена на рис.3.

Висновки. В даній роботі проведено аналіз відкритих літературних джерел і визначена актуальна НПБ розробки АПБ; проведено аналіз НПБ розробки АПБ і визначені алгоритми їх створення та документаційного супроводу, вхідні та вихідні дані для розроблюваної інформаційної моделі; розроблена інформаційна модель вибору альтернативних ЗЗ для АПБ.

Список літератури:

1. НД ТЗІ 3.6-004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=53375>

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

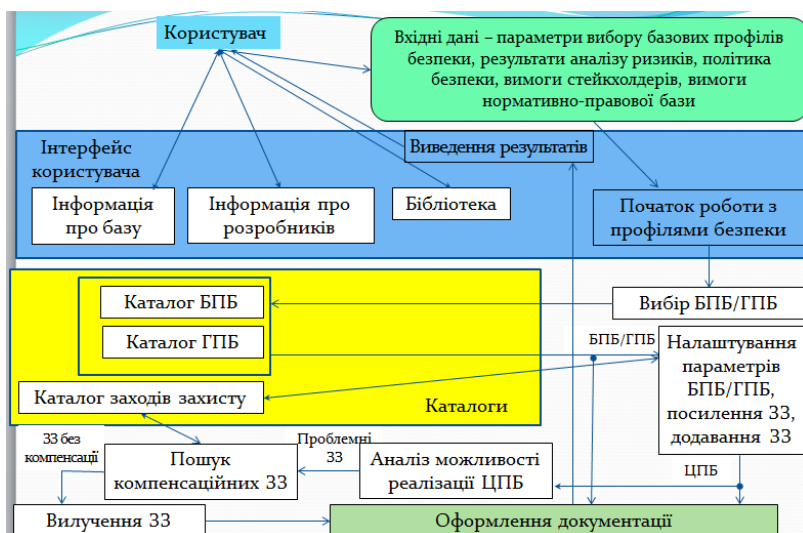


Рисунок 3 – Інформаційна модель вибору альтернативних засобів захисту

2. НД ТЗІ 3.6-006-24. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=64620>

3. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем : Постанова Кабінету Міністрів України №712 від 18.06.2025. URL: <https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text>

4. Про внесення змін до постанови Кабінету Міністрів України від 29 березня 2006 р. № 373 : Постанова Кабінету міністрів України №1531 від 29.11.2025 р. URL: <https://www.kmu.gov.ua/npas/pro-vnesennia-zmin-do-postanovy-kabinetu-ministriv-ukrainy-vid-29-bereznia-2006-r-t261125>

5. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.05.2023 №463. URL: https://zakon.rada.gov.ua/rada/show/v0463519-23?find=1&text=%D0%BF%D1%80%D0%BE%D1%84%D1%96%D0%BB#w1_2

6. Про затвердження Рекомендацій з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації: Наказ Адміністрації Держспецзв'язку №354 від 10.07.2024. URL: <https://zakon.rada.gov.ua/rada/show/v0354519-24#Text>

7. Про затвердження Рекомендацій з оцінювання дотримання вимог цільового профілю безпеки системи : Наказ Адміністрації Держспецзв'язку від 08.12.2025 № 810. URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-08-12-2025-810-pro-zatverdzhennya-rekomendacii-z-ocinyuvannya-dotrimannya-vimog-cilovogo-profilyu-bezpeki-sistemi>

8. Про затвердження Рекомендацій з розроблення цільового профілю безпеки системи : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 8.12.2025 №811. URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-08-12-2025-811-pro-zatverdzhennya-rekomendacii-z-rozroblennya-cilovogo-profilyu-bezpeki-sistemi>

9. НД ТЗІ 2.3-025-21. Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. URL: <https://cip.gov.ua/ua/news/normativni-dokumenty-sistemi-tzi2024>

10. НД ТЗІ 2.6-004-21. Порядок авторизації безпеки інформаційних систем. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=65411>

11. НД ТЗІ 3.6-007-21. Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=53387>

12. НД ТЗІ 3.6-008-21. Порядок моніторингу безпеки інформаційних систем. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=53390>

УДК 004.056.5

ІНФОРМАЦІЙНА МОДЕЛЬ ВИБОРУ ЗАХОДІВ ЗАХИСТУ ЗА НД ТЗІ 3.6-006-24

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

Україна є морською державою з активно працюючою інфраструктурою морської галузі. Безпека річкового і морського транспорту є складовою національної економічної безпеки. Водний транспорт є важливою складовою сучасних логістичних систем і належить до критичної інфраструктури (КІ). На даний час спостерігається тенденція до підвищення кількості кібератак на об'єкти критичної інфраструктури (ОКІ) фактично у всіх секторах – в енергетиці, банківській сфері, на різних видах транспорту тощо. Функціонування водного транспорту суттєво залежить від здатності критичної морської інформаційної інфраструктури, яка включає в себе берегові і суднові компоненти, протистояти кіберзагрозам.

Кібербезпека в галузі річкового і морського транспорту регламентується нормативно-правовими актами [1-11], що видаються організаціями різного підпорядкування і з різними повноваженнями, кількість цих актів і кількість організацій, задіяних у їх розробці, постійно зростає. Крім того, дослідженням проблем захисту інформації в галузі водного транспорту, теоретичним обґрунтуванням ефективних методів вирішення цих займаються вітчизняні і зарубіжні науковці [12-16]. Однак, на даний час в Україні відсутні галузеві профілі безпеки і затверджені методики управління ризиками інформаційної безпеки у галузі водного транспорту.

Метою даної роботи є визначення особливостей проектування суден з врахуванням уніфікованих вимог Міжнародної асоціації класифікаційних товариств (англ. International Association of Classification Societies, IACS) до забезпечення кібербезпеки судових комп'ютеризованих систем (англ. Computer-Based Systems, CBS).

Для досягнення поставленої мети необхідно розв'язати наступні задачі: провести аналіз нормативно-правової бази забезпечення кібербезпеки у галузі водного транспорту і визначити вимоги IACS до CBS та їх узгодженість з вітчизняною нормативно-правовою базою.

Нормативно-правова бази забезпечення кібербезпеки у галузі водного транспорту може бути умовно поділена на два блоки:

- загальні нормативно-правові акти, які стосуються управління якістю товарів і послуг; захисту критичної інфраструктури; організаційного, технічного і криптографічного захисту інформації, розробки комплексних систем захисту інформації / систем безпеки інформації; менеджменту інформаційної безпеки;

- спеціалізовані нормативно-правові акти, які стосуються організації діяльності морського та внутрішнього водного транспорту; безпеки навігації, екіпажу, пасажирів, вантажів, кібербезпеки морської галузі, портів і портових споруд, суден, бортових комп'ютеризованих систем, зокрема кіберстійкості [2, 3, 6].

До нормативно-правової бази забезпечення кібербезпеки у галузі водного транспорту відносяться [16]:

- міжнародні стандарти;
- директиви та регламенти Європейського Союзу захисту критичних інфраструктур, мережевих та інформаційних систем, загального рівня кібербезпеки на території Союзу;
- базові законодавчі акти України і постанови Кабінету Міністрів у галузі кібербезпеки, державні стандарти України, нормативна документація з технічного захисту інформації;
- документи, видані провідними міжнародними організаціями і групами організацій у галузі водного транспорту, одна частина з яких має рекомендаційний характер, а інша є обов'язковою для виконання.

З 1 червня 2024 року для проектів суден є обов'язковими уніфіковані вимоги Міжнародної асоціації класифікаційних товариств до судових комп'ютеризованих систем – IACS UR E22 «Computer-based systems» [1].

IACS UR E22 поширюється на весь життєвий цикл всіх судових CBS, що використовують програмне забезпечення і мають відповідати класифікаційним вимогам, за виключенням тих систем, вимоги до яких регулюються іншими нормативними актами. Наприклад, вимоги до радіо-комунікаційних і навігаційних систем визначені у IV і V главах

Міжнародної конвенції з охорони людського життя на морі (англ. International Convention for the Safety of Life at Sea, SOLAS) [9].

В IACS UR E22 судно розглядається як сукупність систем, підсистем і окремих програмованих приладів з власним програмним забезпеченням. Вимоги IACS UR E22 до CBS є диференційованими залежно від категорії критичності CBS, яка визначається згідно з [1] ймовірною тяжкістю наслідків виходу CBS з ладу для безпеки людини, судна та/або навколишнього середовища, і оцінюються в контексті (категорії однакових CBS на різних судах можуть бути різними):

- категорія I: небезпечні ситуації не виникнуть. CBS цієї категорії не перевіряються IACS, однак у проекті має бути передбачене можливе надходження запиту щодо підтвердження категорії або щодо надання гарантій відсутності прямого і опосередкованого впливу CBS цієї категорії критичності на роботу інших CBS II і III категорій критичності;

- категорія II: небезпечні ситуації можуть виникнути;

- категорія III: небезпечні ситуації негайно виникнуть і можуть бути катастрофічними.

Уніфіковані вимоги до CBS, поділяються на наступні групи:

- загальні вимоги;

- вимоги до складових системи;

- вимоги до системного інтегратора, яким зазвичай є верф;

- вимоги до обслуговування CBS, що окремо визначені для власника, системного інтегратора і постачальників;

- вимоги до управління змінами;

- технічні вимоги до CBS, які включають вимоги щодо звітності і журналювання інцидентів, підвищені вимоги до систем II і III категорії критичності, вимоги до застосування бездротових мереж (заборонені для CBS III категорії критичності, а для інших – можуть застосовуватися за ряду умов) і вимоги щодо перевірки відповідності технічним вимогам Класифікаційного товариства.

Вимоги IACS UR E22 щодо програмного забезпечення операційного технологічного обладнання та інтегрованих систем в цілому відповідають вимогам ISO 24060:2021 «Ships and marine technology — Ship software logging system for operational technology» [4], згідно з яким воно має бути зареєстроване, і має бути доступною інформація про його поточний робочий стан.

Вимоги IACS щодо кіберстійкості бортових систем і обладнання визначені в окремому документі [3] і згруповані за підцілями досягнення кіберстійкості – ідентифікація (SG1), захист (SG2), виявлення (SG3), реагування (SG4), відновлення (SG5). За змістом ці вимоги поділяються на функціональні вимоги, технічні аспекти і вимоги щодо верифікації і тестування.

Настанови щодо менеджменту морських кіберризиків Міжнародної ідентифікація, захист, виявлення, реагування, відновлення морської організації MSC-FAL.1/Circ.3/Rev.2 [5], як і вимоги IACS щодо кіберстійкості [3], також згруповані по розділах ідентифікація, захист, виявлення, реагування, відновлення.

Мінімальні функціональні вимоги і критерії продуктивності, щоб судно можна було визнати кіберстійким, визначені в IACS UR E26 «Cyber resilience of ships» [2] за цільовим підходом, при якому функціональні/технічні вимоги наведені для досягнення кожної субцілі. Вимоги [2] призначені для того, щоб забезпечити однакову реалізацію всіма зацікавленими сторонами у певних умовах однакових рішень і забезпечити за рахунок цього прийнятний рівень стійкості для всіх класифікованих суден/блоків незалежно від експлуатаційних ризиків і складності систем операційних технологій (ОТ-систем).

Аналогічним чином в уніфікованих вимогах IACS UR E27 [3] представлені вимоги щодо кіберстійкості бортових систем і обладнання.

Слід зауважити, що вимоги [1-3] є узгодженими і уніфікованими, а порівняно з вітчизняною нормативно-правовою базою, не дивлячись на спорідненість підходів до забезпечення кібербезпеки, спостерігається ряд суттєвих відмінностей, які необхідно нівелювати:

- категорії критичності об'єктів критичної інформаційної інфраструктури визначаються інакше [15];
- при розробці систем безпеки інформації за НД ТЗІ використовується інша класифікація заходів захисту.

Висновки

В даній роботі проведено аналіз нормативно-правової і визначені вимоги до CBS. Обґрунтовано необхідність узгодження нормативних документів, виданих різними відповідальними органами у морській галузі.

Список літератури:

1. IACS E22. Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e22_rev.3_june_2023_ul.pdf
2. IACS UR E26 Cyber resilience of ships. URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf
3. IACS UR E27 Cyber resilience of on-board systems and equipment. URL: <https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103854/UR-E27-Rev.1-Sep-2023-UL.pdf>
4. ISO 24060:2021 Ships and marine technology – Ship software logging system for operational technology. URL: <https://www.iso.org/ru/standard/77678.html>
5. MSC-FAL.1/Circ.3/Rev.2 Guidelines on maritime cyber risk management. URL: [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MS-C-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\)%20\(1\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MS-C-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf)
6. Recommendation on Cyber Resilience No. 166. URL: <https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/24150438/rec-166-corr2-apr-2022-ul.pdf>
7. Rules for the survey and construction of steel ships. Part X. Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/rules/465_part_x_e_202406.pdf
8. The Guidelines on Cyber Security Onboard Ships. Version 5 (2024). URL: https://www.maritimeworldsecurity.org/media/g3qlxdaw/2024-11-14-guidelines_on_cyber_security-v5-final.pdf
9. Treaties and international agreements registered on 30 June 1980 No. 18961. International Convention for the Safety of Life at Sea, 1974 (with annex and final act of the International Conference on Safety of Life at Sea, 1974). Concluded at London on 1 November 1974. URL: <https://treaties.un.org/doc/Publication/UNTS/Volume%201184/volume-1184-I-18961-English.pdf>
10. 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

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

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

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

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

15. Турти М.В. Зважене оцінювання критичності об'єктів морського та річкового транспорту //Матеріали XII Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». – Миколаїв: НУК, 2024. – С.22-28.

16. Хван Ю.В. Норматино-правова база кібербезпеки галузі водного транспорту //Матеріали XII Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». Миколаїв: НУК, 2024. С156-162

УДК 004.056.5

ІНФОРМАЦІЙНА МОДЕЛЬ ВИБОРУ ЗАХОДІВ ЗАХИСТУ ЗА НД ТЗІ 3.6-006-24

Автор: Шаповалова О.П., 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

Вибір заходів захисту (ЗЗ) є окремим етапом впровадження систем безпеки інформації (СБІ) і, в разі відсутності в інформаційній системі (ІС) інформації, що є державною таємницею, і наявності іншої інформації, вимога щодо захисту якої встановлена законом, має проводитися у порядку, визначеному НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [1].

Комплекс ЗЗ має відповідати вимогам нормативних документів і бути ефективним з точки зору управління ризиками інформаційної безпеки на конкретному об'єкті інформаційної діяльності (ОІД), який, зокрема, може належати до критичної інфраструктури певного рівня критичності, і повинен будуватися з врахуванням особливостей конкретної ІС на ОІД, що визначаються характеристиками і технологіями обробки інформації, категорією критичності ІС, наявними ризиками, обраним цільовим профілем безпеки (ЦПБ) [2].

Вибір ЗЗ спочатку здійснюється на основі базового профілю безпеки (БПБ) або, в разі наявності, галузевого профілю безпеки (ГПБ). БПБ визначає мінімально необхідний набір ЗЗ, на основі якого формується цільовий профіль безпеки, що після аналізу можливостей його реалізації перетворюється в адаптований профіль безпеки (АПБ). Тобто, в процесі створення СБІ набір заходів захисту неодноразово переглядається. Враховуючи, що перелік ЗЗ, наведений в НД ТЗІ 3.6-006-24 [1], має великий обсяг, можна стверджувати, що з метою пришвидшення процесу проектування СБІ і уникання помилок є доцільним впровадження засобів автоматизації процесів роботи із набором ЗЗ.

Метою даної роботи є розробка інформаційної моделі вибору заходів захисту за НД ТЗІ 3.6-006-24 згідно з обраним користувачем профілем безпеки.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- провести аналіз каталогу заходів захисту, наведеного в НД ТЗІ 3.6-006-24 і визначити структуру ЗЗ, критерії і алгоритми їх вибору, вхідні і вихідні дані інформаційної моделі;
- розробити і апробувати інформаційну модель вибору ЗЗ за НД ТЗІ 3.6-006-24.

В каталозі ЗЗ згруповані по класам, кожен з яких має свій ідентифікатор (*ID* класу) і назву. В каталозі НД ТЗІ 3.6-006-24 [1] наведено перелік заходів захисту, в якому наявні гіперпосилання для зручності доступу до класів і груп заходів захисту, що входять у класи. Всього в НД ТЗІ 3.6-006-24 наявні 20 класів заходів захисту, які стосуються певних аспектів забезпечення безпеки інформації. Кожний клас містить певний набір груп заходів захисту (всього 294 групи). Кількість груп у кожному класі різна. Максимальну кількість груп містить клас *SC* «Системний і комунікаційний захист» – 51 група, а мінімальну кількість – клас *AT* «Обізнаність і навчання» – 6 груп.

Таким чином, згідно каталогу НД ТЗІ 3.6-006-24 класи заходів захисту описуються наступним набором параметрів:

- номер класу – числа в інтервалі 1...20;
- *ID* класу – текст, дволітерна аббревіатура;
- назва класу – текст до 124 символів;
- кількість груп заходів захисту в класі – числа в інтервалі 6...51.

Кожна група заходів захисту характеризується наступними параметрами:

- клас, до якого належить група, – текст, дволітерна аббревіатура;
- назва групи заходів захисту – текст до 124 ;символів
- номер групи в класі – числа в інтервалі 6...51;
- *ID* групи заходів захисту, який складається із *ID* класу і номеру групи заходів захисту, розділених дефісом;
- кількість класів захисту в групі – числа в інтервалі 1... 50.

Заходи захисту для автоматизованої обробки мають представлятися наступним набором параметрів:

- ID групи класу заходів захисту – дві великі літери англійської абетки і через дефіс – число в інтервалі від 1 до 51;
- ID підсилення – число в круглих дужках;
- код заходу захисту в групі – маленька англійська літера;
- назва заходу захисту – текст обсягом декілька сотень символів;
- кількість дій – число в діапазоні 1...20;
- рекомендації з реалізації заходу захисту – текст обсягом декілька тисяч символів;
- рекомендації з реалізації посилення заходу захисту – текст обсягом декілька тисяч символів (максимум);
- кількість пов'язаних заходів захисту – число в діапазоні 0...15;
- список пов'язаних заходів захисту, які в свою чергу можуть бути пов'язані з іншими заходами захисту – текст обсягом декілька сотень символів;
- кількість посилань – число в діапазоні 0...20;
- список посилань – текст обсягом до декількох сотень символів;
- кількість налаштовуваних параметрів, які стосуються всього 33.

Код заходу захисту при автоматизованій обробці має представлятися у вигляді $XX-N(M) Y$, де $XX-N(M)$ – код групи заходів захисту (XX – клас 33, N – номер групи 33, M – номер посилення 33), Y – літера, що відповідає заходу захисту в групі.

Кожна дія для певного 33 характеризується наступним набором параметрів:

- код дії, який при автоматизованій обробці має представлятися у вигляді $XX-N(M) Y.K$, де K – номер дії заходу захисту;
- зміст дії – текст обсягом до декількох сотень символів;
- кількість налаштовуваних параметрів для даної дії – число в інтервалі 0...15;
- список налаштовуваних параметрів для даної дії – текст обсягом до декількох сотень символів.

Налаштовувані параметри для кожної дії певного 33 характеризуються наступним набором параметрів:

- код налаштовуваного параметру, який при автоматизованій обробці має представлятися у вигляді $XX-N(M) Y.K.L$, де L – номер налаштовуваного параметру дії K заходу захисту $XX-N(M) Y$;

- назва налаштовуваного параметру;
- значення налаштовуваного параметру.

Як показав аналіз нормативних документів [1-8], критерії вибору ЗЗ різняться в залежності від профілю безпеки, згідно з яким їх обирають (рис.1). Базовий і галузевий профілі є нормативно визначеними, тобто вибір може стосуватися будь-якого засобу захисту в них. Відмінність полягає в тому, що в галузевому профілі порівняно з базовим заходи захисту відповідають не тільки параметрам інформаційної системи та інформації в ній, а й специфічним галузевим вимогам.

Для цільового профілю додається відповідність вимогам організації – політиці безпеки, результатам аналізу ризиків безпеки, призначенню інформаційної системи, її структурно-функціональним характеристикам та особливостям функціонування ІС.

Для адаптованого профілю до цих критеріїв вибору додається вимога щодо можливості реалізації з фінансових і технологічних міркувань.

Для БПБ:

- Наявність в базовому профілі безпеки, що відповідає параметрам ІС та інформації в ній

Для ГПБ:

- Наявність в галузевому профілі безпеки, що відповідає параметрам ІС та інформації в ній, а також специфічним галузевим вимогам

Для ЦПБ:

- Ступінь посилення не менша за наявну в базовому чи галузевому (при наявності) профілі безпеки
- Відповідність параметрам ІС та інформації в ній, а також специфічним галузевим вимогам (впливає з БПБ чи ГПБ, на основі яких будується ЦПБ)
- Відповідність політиці безпеки організації, призначенню ІС, структурно-функціональним характеристикам ІС, результатам аналізу ризиків безпеки та особливостям функціонування ІС

Для АПБ:

- Ступінь посилення не менша за наявну в базовому чи галузевому (при наявності) профілі безпеки
- Відповідність параметрам ІС та інформації в ній, а також специфічним галузевим вимогам (впливає з БПБ чи ГПБ, на основі яких будується ЦПБ)
- Відповідність політиці безпеки організації, призначенню ІС, структурно-функціональним характеристикам ІС, результатам аналізу ризиків безпеки та особливостей функціонування ІС
- Можливість реалізації з фінансових і технологічних міркувань

Рисунок 1 – Критерії вибору заходів захисту

При виконанні операцій із заходами захисту слід враховувати, що для базового і цільового профілів можливо тільки виконати вибірку засобів захисту з цих профілів за заданим параметром (наприклад, вибрати заходи захисту, пов'язані один з одним, підсилених засобів захисту тощо).

Доступними (незабороненими) операціями із засобами захисту з цільового і адаптованого профілів безпеки додатково є оцінювання відповідності вимогам організації, ризикам, особливостям функціонування інформаційної системи, додавання заходів захисту, зміна їх налаштувань, вибір компенсаційних заходів захисту або виключення заходів захисту з профілю, аргументація і документування цих процедур.

На рис.2 наведено визначений для цих операцій узагальнений алгоритм.

Розроблена інформаційна модель вибору заходів захисту наведена на рис.3.

Вхідними даним моделі є параметри профілів безпеки, заходів захисту – каталогів, обрані користувачем операції і їх параметри. Вихідними даними є результати виконання операцій.

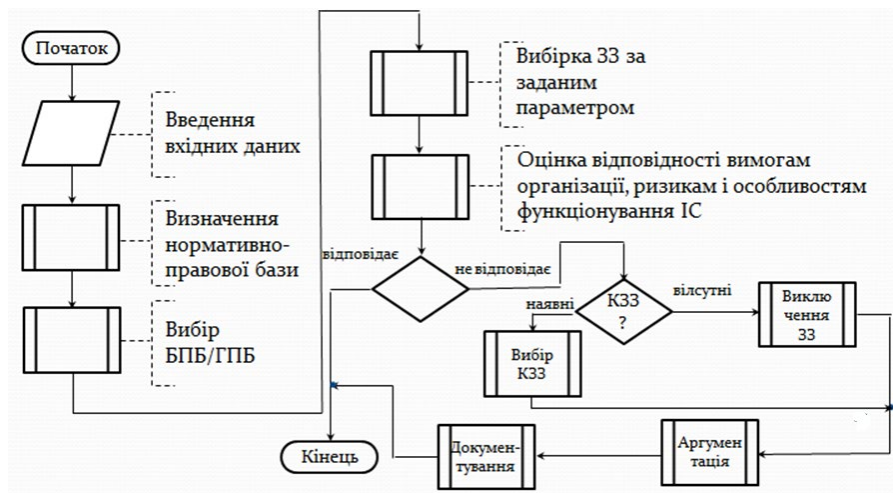


Рисунок 2 – Узагальнений алгоритм вибору заходів захисту

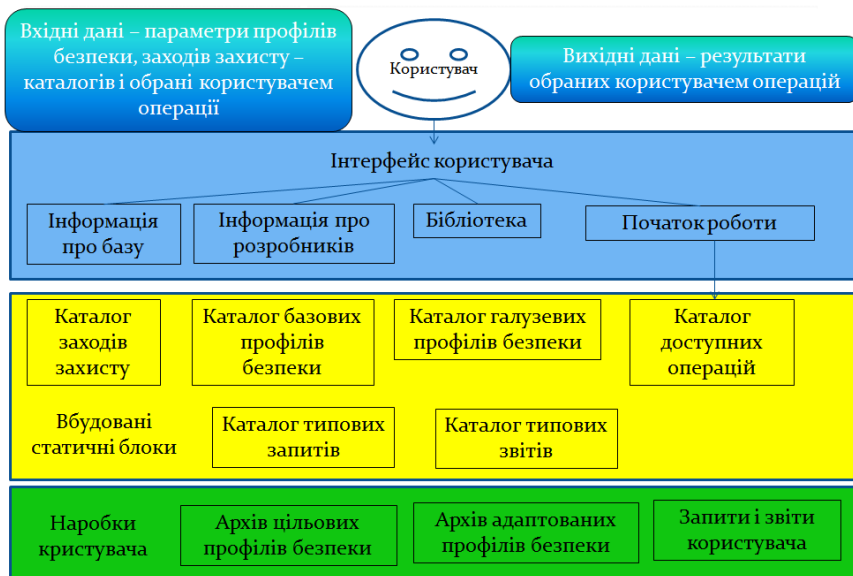


Рисунок 3 – Інформаційна модель вибору заходів захисту

Апробація розробленої моделі була здійснена в MS Access (рис.4) у вигляді бази даних, що містить низку взаємопов'язаних таблиць, форми, запити і звіти. В таблиці «Класи захисту» описані всі класи заходів захисту з НД ТЗІ 3.6-006-24. В таблицю «Заходи захисту» внесено частину інформації з каталогу структуровану відповідно НД ТЗІ 3.6-006-24. При цьому клас заходу захисту обирається із списку, створеного з поля таблиці «Класи захисту» за допомогою майстра підстановок. Посилення заходів захисту і зв'язки між заходами захисту винесені в окремі таблиці.

Для зручності введення даних у великі таблиці створено форми, поля яких в разі відсутності даних, наприклад, при відсутності пов'язаних заходів залишаються порожніми. При відсутності посилень у відповідній таблиці і формі залишається визначене за замовчуванням значення «не має». В базі даних наявна також система запитів, наприклад, на рис.5 наведено структури пов'язаних таблиць і результати спрацьовування запиту до них, який визначає вимоги безпеки, що відповідають кожному заходу захисту.

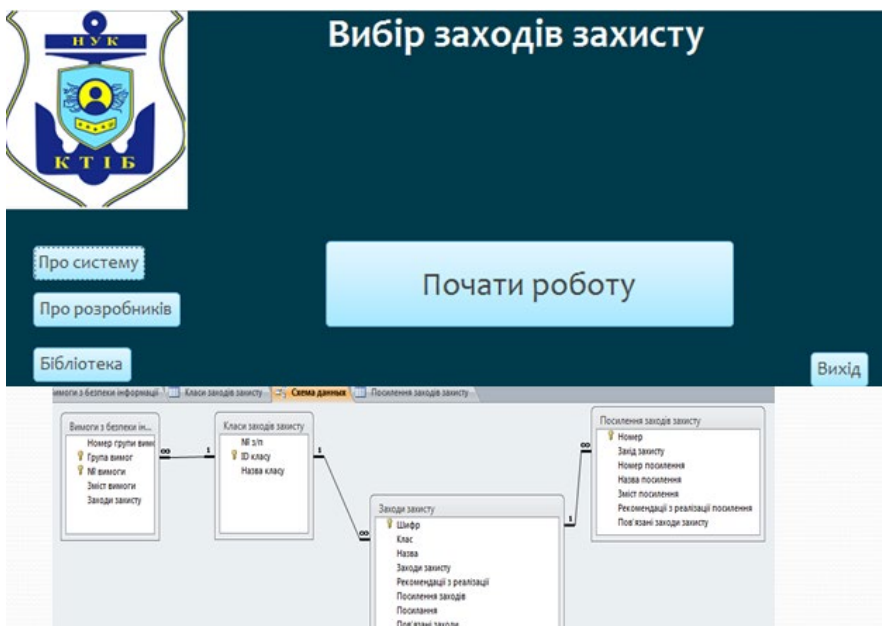


Рисунок 4 – Апробація розробленої моделі

Висновки. В даній роботі проведено аналіз каталогу заходів захисту, наведеного в НД ТЗІ 3.6-006-24, визначена структура ЗЗ, критерії і алгоритм їх вибору, вхідні і вихідні дані інформаційної моделі; розроблено і апробовано інформаційну модель вибору заходів захисту за НД ТЗІ 3.6-006-24.

Список літератури:

1. НД ТЗІ 3.6-006-24. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=64620>
2. НД ТЗІ 3.6-004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=53375>

Структура таблиці «Класи
заходів захисту»

Имя поля	Тип
№ з/п	Числове
ID класу	Текстовий
Назва класу	Текстовий

Структура таблиці «Вимоги
з безпеки інформації»

Имя поля	Тип
Номер групи вимог	Числове
Група вимог	Текстовий
№ вимоги	Текстовий
Назва вимоги	Текстовий
Зміст вимоги	Поле МЕІ
Заходи захисту	Текстовий

Структура таблиці «Заходи
захисту»

Имя поля	Тип
Шифр	Текстовий
Клас	Текстовий
Назва	Текстовий
Заходи захисту	Поле МЕІ
Рекомендації з реалізації	Поле МЕІ
Посилення заходів	Поле МЕІ
Посилання	Текстовий
Пов'язані заходи	Текстовий

Шифр	Клас	№ вимоги	Зміст вимоги
АС-2	АС	1.1	1) визначити дозволені та заборонені облікових записів у системі; 2) створювати, активувати, деактивувати та видаляти облікові записи системи відповідно до політики передумов і критеріїв організації; 3) визначити авторизованих користувачів системи, належність до груп; також повноваження доступу (тобто права); 4) авторизувати доступ до системи на основі чинного дозволу на доступ до системи; 5) контролювати використання облікових записів у системі; 6) оповістити персонал або користувачів, коли: - облікові записи більше не використовуються; - користувачі звільняються з роботи.
АС-1	АС	1.2	Застосовувати затверджені процедури для логічного доступу до конфіденційної інформації та ресурсів у системі.

Рисунок 5 – Джерела даних і результати запиту
«Заходи захисту – вимоги безпеки»

3. Наказ Адміністрації Держспецзв'язку від 10.07.2024 №354 «Про затвердження Рекомендацій з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації». URL: <https://zakon.rada.gov.ua/rada/show/v0354519-24#Text>

4. Наказ Адміністрації Держспецзв'язку від 08.12.2025 № 810 «Про затвердження Рекомендацій з оцінювання дотримання вимог цільового

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

профілю безпеки системи». URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-08-12-2025-810-pro-zatverdzhennya-rekomendacii-z-ocinyuvannya-dotrimannya-vimog-cilovogo-profilu-bezpeki-sistemi>

5. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 8.12.2025 №811 «Про затвердження Рекомендацій з розроблення цільового профілю безпеки системи». URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-08-12-2025-811-pro-zatverdzhennya-rekomendacii-z-rozroblennya-cilovogo-profilu-bezpeki-sistemi>

6. НД ТЗІ 2.3-025-21. Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. URL: <https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024>

7. НД ТЗІ 2.6-004-21. Порядок авторизації безпеки інформаційних систем. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=65411>

8. НД ТЗІ 3.6-007-21. Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=53387>

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

УДК 004.9

**ОБҐРУНТУВАННЯ МЕТОДИКИ ОЦІНКИ ЧАСОВОЇ
СКЛАДНОСТІ АЛГОРИТМІВ НА БАЗІ КОРЕЛЯЦІЙНОГО
АНАЛІЗУ**

***Автори:** Бабенко Н.В., викладач кафедри ІТ та ФП; Пантєлєєв В.В., к.т.н., доцент кафедри ІТ та ФП; Самойленко Д.М., к.ф.-м.н., доцент, завідувач кафедри ІТ та ФП; Суліма М.М., к.т.н., доцент кафедри ІТ та ФП; Туманов О.А., викладач кафедри ІТ та ФП, Одеський технологічний університет «ШАГ», м. Одеса, Україна*

При визначенні чи порівнянні складності алгоритмів, зазвичай, головну роль відіграє асимптотична оцінка функції їх працемісткості. У межах даної роботи обмежимося поліноміальними функціями, для яких такою оцінкою є максимальний ступінь аргументу, що входить до їх складу. Зробимо акцент на питанні практичного визначення максимального ступеня функції працемісткості за результатами прямих вимірювань часу виконання програмної реалізації алгоритму для різних значень розмірності вхідних даних.

Вплив на цей час різних факторів призводить до відхилення експериментально одержаних даних від теоретичних оцінок. Передбачається, що такі фактори спричиняють більш тривалий час роботи коду у порівнянні з теоретично обчисленим. Причому затримки спричиняються складовими лінійного або постійного характеру, пов'язаними як з особливостями роботи програм у багатозадачних операційних системах, так і нехтуванням у теоретичних оцінках реальними операціями організації циклів, умов, викликів функцій тощо. У результаті внесок головного ступеня зменшується, а зроблена оцінка наближає цей ступінь до одиниці. Причому як для функцій з головним ступенем більшим за 1 (гіперлінійних), так для тих, в яких цей ступінь менший за 1 (сублінійних).

У роботі [1] розвинена методика, що базується на диференціально-регресійному аналізі часу виконання програмного коду. Методика дозволила виявити та обґрунтувати загальний характер явища «step effect», що полягає в екстремальному збільшенні часу роботи коду при певних розмірах даних, що оброблюються. Виявлений ефект можна додатково вважати обґрунтуванням ненадійності теоретичних оцінок на практиці.

Акцент на практичне визначення часу роботи алгоритмів зазначений у роботі [2]. Авторами наведено спосіб визначення найбільш швидкого виконавця поставлених задач в залежності від характеру самих задач. Але результати наведеного дослідження є вельми локалізованими та обмежуються як розглянутим переліком виконавців, так і типами програмних задач. Також не проводилось асимптотичного аналізу працездатності, що ускладнює екстраполяцію проведених досліджень на задачі зі збільшеним розміром вхідних даних.

Найпоширенішими представниками поліноміально-працездатних алгоритмів є алгоритми матричної алгебри. Актуальність дослідження їх часових показників наведено у роботі [2]. Незважаючи на тривалий історичний розвиток даної галузі показано необхідність пошуку та дослідження нових обчислювальних алгоритмів.

Підсумовуючи зазначаємо, що дослідження реального, фізичного часу роботи програмних алгоритмів залишаються актуальними, а в якості прикладів для дослідження актуальними залишаються алгоритми матричної алгебри.

Основу методу кореляційного аналізу даних є коефіцієнт лінійної кореляції двох серій: практично одержаних даних η та теоретично розрахованих ξ (1).

$$k(\xi, \eta) = \frac{\text{cov}(\xi, \eta)}{\sigma_{\xi} \cdot \sigma_{\eta}}. \quad (1)$$

Припустимо, що експериментальні дані складаються з двох частин: основної ступеневої, що походить від самого алгоритму, та додаткової постійної складової (2)

$$\eta = ax^n + b. \quad (2)$$

Розрахункова серія формується як результат обчислення ступенева функція (3)

$$\xi = x^\alpha, \quad (3)$$

де α – параметр, що змінюється в рамках застосування методики.

Для спрощення перетворень вважатимемо, що послідовності задані на діапазоні $x \in [0, 1]$, що завжди може бути досягнуто на практиці шляхом масштабування змінної x . Більш того, на загальні висновки область визначення змінної впливу не чинить. Також обмежимося практичним випадком $\alpha > 0$, що відповідає зростанню часу роботи програми зі зростанням розмірів вхідних даних. Зворотна поведінка для реальних алгоритмів не очікується.

Оскільки вирази задані як неперервні величини, використаємо інтегральні означення для коваріації (4), середнього значення (5) та стандартного відхилення (6) та підставимо до них вирази (2) та (3):

$$\begin{aligned} \text{cov}(\xi, \eta) &= \int_0^1 x^\alpha (ax^n + b) dx - \int_0^1 x^\alpha dx \cdot \int_0^1 (ax^n + b) dx = \\ &= \frac{a}{\alpha + n + 1} + \frac{b}{\alpha + 1} - \frac{1}{\alpha + 1} \cdot \left(\frac{a}{n + 1} + b \right), \\ \text{cov}(\xi, \eta) &= \frac{an}{n + 1} \cdot \frac{\alpha}{(\alpha + 1)(\alpha + n + 1)}, \end{aligned} \quad (4)$$

$$\mu_\xi = \int_0^1 \xi(x) dx = \int_0^1 x^\alpha dx = \frac{1}{\alpha + 1}, \quad (5)$$

$$\begin{aligned}\sigma_{\xi} &= \sqrt{\int_0^1 (x^{\alpha} - \mu_{\xi})^2 dx} = \sqrt{\int_0^1 \left(x^{\alpha} - \frac{1}{\alpha+1}\right)^2 dx} = \\ &= \sqrt{\frac{\alpha^2}{(\alpha+1)^2 (2\alpha+1)}} = \frac{\alpha}{(\alpha+1)\sqrt{(2\alpha+1)}}.\end{aligned}\quad (6)$$

Стандартне відхилення для серії η не залежить від параметра α , тому залишимо його як константу у виразі, одержимо

$$k(\xi, \eta) = \frac{\text{cov}(\xi, \eta)}{\sigma_{\xi} \cdot \sigma_{\eta}} = \frac{an}{(n+1)\sigma_{\eta}} \cdot \frac{\sqrt{2\alpha+1}}{\alpha+n+1} \quad (7)$$

Одержаний вираз закладає основу подальших досліджень через аналіз характеру залежності коефіцієнта кореляції від показника ступеня серії ξ , який грає роль параметра α у (7).

Дослідимо вираз (7) як залежність від параметра α . Обчислимо похідну за цим параметром:

$$\begin{aligned}\frac{d}{d\alpha} k(\xi, \eta) &= \frac{an}{(n+1)\sigma_{\eta}} \cdot \frac{\frac{\alpha+n+1}{\sqrt{2\alpha+1}} - \sqrt{2\alpha+1}}{(\alpha+n+1)^2} = \\ &= \frac{an}{(n+1)\sigma_{\eta}} \cdot \frac{n-\alpha}{(\alpha+n+1)^2 \sqrt{2\alpha+1}}.\end{aligned}\quad (8)$$

Як видно з (8) єдиний знакозмінний множник у виразі $(n-\alpha)$ задає єдине значення параметра α , за якого похідна дорівнює нулю: $n=\alpha$. Відповідно, при цьому значенні коефіцієнт кореляції (7) набуває екстремального значення. Детальне дослідження характеру екстремуму опустимо, зазначивши висновки проведеного аналізу: він є максимумом при позитивному коефіцієнті $a > 0$ та мінімумом для від'ємних

значень. Від'ємні значення коефіцієнту не відповідають дійсності, оскільки за (2) означають негативну величину часу виконання програми. Тому цей випадок було вилучено з подальшого розгляду, через що підсумковим висновком було прийняте те, що коефіцієнт кореляції завжди матиме максимум при зазначеній величині параметра α .

Визначене положення максимуму та його незалежність від інших параметрів, окрім ступені n залежності (2) надає математичне обґрунтування методики: коефіцієнт кореляції (1) набуває максимального значення коли ступені практичної та розрахункової послідовностей рівні між собою ($n = \alpha$). Причому ця величина є єдиним екстремумом функції, що, по-перше, вилучає з аналізу інші точки та, по-друге, дозволяє вживати методику в умовах дії похибок вимірювання часу. За таких умов абсолютна величина коефіцієнту кореляції зменшується, проте, положення екстремуму не змінюється. Окремо підкреслимо незалежність висновків від величини додатку b у (2), що також є позитивною характеристикою методики.

Список літератури:

1. Danylets, Y., Korchevskyi, D., Novak, S., Samoilenko, D., & Sulima, M. (2025). Estimation of software structures dimension influence on data processing time increasing. *Eastern-European Journal of Enterprise Technologies*, 1(9 (133), 24–34. <https://doi.org/10.15587/1729-4061.2025.322989>
2. Jeffry Chavarría-Molina, Juan José Fallas-Monge, Pablo Soto-Quiros (2022) Effective implementation to reduce execution time of a low-rank matrix approximation problem, *Journal of Computational and Applied Mathematics*, 401, 113763. <https://doi.org/10.1016/j.cam.2021.113763>.

УДК 004.4

**ПРОБЛЕМНІ ПИТАННЯ ВИКОРИСТАННЯ ОПЕРАЦІЙНИХ
СИСТЕМ WINDOWS У КОМПЛЕКСНИХ СИСТЕМАХ
ЗАХИСТУ ІНФОРМАЦІЇ**

***Автор:** Васєв В.В., 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. Під час роботи в сфері захисту інформації, часто виникали проблемні питання пов'язані з сім'єю ОС Windows. В перелік таких питань входить: повторна активація на АС класу 1, проблеми з закупкою ліцензій для створення нових систем, порушення роботи системи при налаштуванні політик безпеки

Метою роботи є аналіз недоліків ОС Windows та визначення обмеженості у доступі до ядра системи, переповненість системи функціями та програмами (видалення яких не передбачено системою) які не використовуються в роботі та створюють додаткове навантаження на систему або передумови для витоку інформації.

Основна частина.

Згідно з Умовами використання продукції Майкрософт (Terms of Use ("TOU")) [1] користувачеві заборонено модифікувати, копіювати, передавати, розмножувати, публікувати тощо продукцію корпорації Майкрософт. У зв'язку з цими обмеженнями створення спеціалізованої або модифікованої версії під конкретні потреби легально неможливе. Також використання сервісів компанії передбачає реєстрації та створення акаунту з вказанням актуальної та достовірної інформації, що не є можливим у випадку створення системи під службові нужди та підводить нас до питання відношення компанії Майкрософт до конфіденційної інформації.

Згідно "Декларації компанії Майкрософт про конфіденційність"[2], корпорація Майкрософт збирає дані під час взаємодії через продукти, зокрема під час створення нового облікового запису при першому запуску є перелік обов'язкових питань, які неможливо пропустити. При цьому параметри конфіденційності Windows часто

ігноруються при налаштуванні автоматизованих систем, що дозволяє Майкрософт та відвідуваним сайтам отримувати дані для можливої ідентифікації призначення системи з підключенням до мережі.

Надані дані також можуть використовуватися корпорацією для розробки та навчання штучного інтелекту (далі – ШІ), що створює додаткові передумови витоку.

Також Майкрософт отримує дані від афілійованих структур, дочірніх компаній і третіх сторін та передає дані дочірнім компаніям, поставальникам, що працюють від імені компанії та за законом або судовим наказом (варто відмітити, що компанія розташована в Сполучених Штатах Америки та переважно підконтрольна законам цієї країни та міжнародним, що не входить в рамки нашого впливу).

Також корпорація активно використовує файли cookie в тому числі інших компаній, що підводить нас до необхідності вивчення “Сторонньої інвентаризації файлів cookie”[3]. Даний ресурс містить перелік третіх осіб, які встановлюють файли cookie на веб-сайтах компанії, крім тих, які вказані безпосередньо на сайті. Повний список потребує окремого дослідження та аналізу, однак навіть поверхневий огляд дозволяє виявити компанії які не порушуючи власних декларацій і відповідно законів можуть передавати дані до компаній партнерів, що може стати причиною витоку інформації до недружніх країн.

Враховуючи кількість методів якими корпорація Майкрософт отримує дані користувачів, варто розглянути загрозу кібератак на підконтрольні їй ресурси.

Відповідно до Microsoft Digital Defence Report[4] за 2024 рік, кількість кібератак постійно збільшується і навіть користувачі Microsoft зазнають понад 600 млн. атак кіберзлочинців та національно-державних атак щодня. Загалом атаки розподіляються таким чином:

ІТ – 24%, навчання та наукова сфера – 21%, державні апарати – 12%, недержавні організації, транспорт, споживча торгівля, фінансова сфера – по 5%, сфера виробництва та сфера комунікацій – по 4% та решта – 16%

При цьому такі країни як Росія, Китай, Іран та Північна Корея придбали доступ до ІТ продуктів та серверів частково для проведення атак

на ланцюги поставок. При цьому кількість кібер атак усіх типів суттєво зростає з кожним роком. Хоча корпорація Майкрософт і володіє великою кількістю інженерів та систем захисту постійно зростаюча кількість атак створює постійні ризики витоку даних.

Під час аналізу ліцензійної угоди Windows 11[5], можна виділити декілька проблемних аспектів:

- програмне забезпечення можна також активувати вручну через Інтернет або по телефону, однак якщо програмне забезпечення визначити, що інстальований екземпляр програмного забезпечення піратський, не має ліцензії або містить несанкціоновані зміни, активація не буде успішною. Подібні випадки мають місце бути у Автоматизованих системах класу 1 і дана проблема не має досконалого рішення;

- приймаючи угоду ви погоджуєтесь на автоматичні оновлення продукту без отримання повідомлень про це, крім того коли ви підключаєтесь до Інтернету програмне забезпечення автоматично підключається до серверів корпорації Майкрософт, для активації ліцензії та щоб пов'язати її з певним пристроєм.

Іншими словами у продукції Майкрософт є ряд функцій підключення до серверів та оновлень, непідконтрольних користувачеві навіть з правами адміністратора. Звісно є можливість вручну відключити ряд процесів які відповідають за оновлення, однак це призведе до того, що операційна система не буде оновлюватися взагалі і попри те, що неможливо сегрегувати частини оновлення одне від одного, в самих оновленнях часто фігурують такі, що покращують захист системи, усувають баги, недоліки та експлойти. У зв'язку з чим використання моделей які більше не підтримуються є недоцільним, оскільки їх не виправлені недоліки можуть бути використані для компрометації системи.

Згідно з “Сторінкою пошуку інформації про життєвий цикл продуктів і послуг” життєвий цикл продукції Windows 10 та його варіантів закінчився 14 жовтня 2025 року. У зв'язку з чим офіційна закупівля та оновлення неможливе. Це створює необхідність переходу на нові продукти компанії Майкрософт.[6]

Висновки

Враховуючи ситуацію в країні, на політичні відносини з іншими країнами, аналіз виявив критичну залежність будь-яких систем від трьох сторін та інших країн. Виникає потреба в створенні незалежної

системи, з можливістю її контролю та модифікації внутрішніми засобами без залучення третіх сторін та відповідне полегшення системи отримання/закупівлі нових копій.

Список літератури:

1. Умови використання продукції компанії Майкрософт. URL: <https://www.microsoft.com/en-us/legal/terms-of-use>

2. Декларація компанії Майкрософт про конфіденційність. URL: <https://www.microsoft.com/uk-ua/privacy/privacystatement>

3. Сторонній інвентаризація файлів cookie. URL: <https://support.microsoft.com/uk-ua/topic/%D1%81%D1%82%D0%BE%D1%80%D0%BE%D0%BD%D0%BD%D1%96%D0%B9-%D1%96%D0%BD%D0%B2%D0%B5%D0%BD%D1%82%D0%B0%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F-%D1%84%D0%B0%D0%B9%D0%BB%D1%96%D0%B2-cookie-81ca0c3d-c122-415c-874c-55610e017a6a>

4. Microsoft Digital Defence Report. URL: <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024>

5. EULA windows 11. URL: [https://www.microsoft.com/content/dam/microsoft/usetm/documents/windows/11/oem-\(pre-installed\)/Useterms_OEM_Windows_11_Ukrainian.pdf](https://www.microsoft.com/content/dam/microsoft/usetm/documents/windows/11/oem-(pre-installed)/Useterms_OEM_Windows_11_Ukrainian.pdf)

6. Життєвий цикл Windows 10. URL: <https://learn.microsoft.com/uk-ua/lifecycle/products/?terms=windows%2010&products=windows>

УДК 004.8

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ФАЛЬСИФІКОВАНОЇ ІНФОРМАЦІЇ ДЛЯ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

***Автори:** Кобзєв В.Г., к.т.н., с.н.с., професор кафедри Програмної інженерії; Ховрат А.В., аспірант, Харківський національний університет радіоелектроніки, м. Харків, Україна*

Одна зі складових інформаційної безпеки полягає у забезпеченні обігу правдивої інформації в усіх важливих сферах діяльності. Особливого значення це набуває у період активного інформаційного протистояння під час кризових явищ.

Розвиток технологій виявлення фальсифікованої інформації спрямований на забезпечення доступу до інформації без коригувань і прямої фабрикації, що має місце у засобах масової інформації і соціально орієнтованих інформаційних системах зі значним навантаженням з боку користувачів. Причому в останні роки таке коригування носить масовий і цілеспрямований характер. У цій роботі аналізуються тенденції розвитку таких технологій на основі сучасних публікацій.

Питанню застосування нейронних мереж для ідентифікації рейкових новин присвячена стаття [1]. Новий підхід до класифікації фейкових новин з використанням моделей глибокого навчання на основі LSTM запропонований у статті [2]. Використання різних засобів штучного інтелекту для виявлення і класифікації фейкової інформації представлено у публікаціях авторів цієї роботи, зокрема [3, 4].

Запропоновано створення двошарової моделі класифікації фейкової інформації на основі поєднання наївного баєсівського класифікатора й гібридної рекурентно-згорткової нейромережі RCNN. Демонструється розв'язання таких завдань: експертне оцінювання та доменний аналіз для визначення базових класів фейкової інформації; аналіз лінгвістичних маркерів дезінформації та розроблення векторів ознак для класифікації; створення моделей для сегрегації даних з використанням наївного баєсівського класифікатора; експериментальна перевірка запропонованої двошарової моделі та порівняння з підходом RCNN. Упроваджено такі методи: аналітичний (для формування набору маркерів дезінформації);

індуктивний (з метою визначення цільового набору індикаторів для реалізації другого шару моделі); експертне оцінювання (для встановлення найбільш впливових факторів ефективності та вагових коефіцієнтів ознак); експериментальний і багатокритеріальний методи оцінювання (з метою визначення найбільш ефективної моделі).

Основні результати. Сформовано класифікаційну структуру для типів фейкової інформації, що містить п'ять категорій – від жартів до глобально шкідливих новин. Розроблено набір дискримінативних ознак, властивих для сфабрикованої інформації, зокрема первинні лінгвістичні маркери та вторинні стилOMETричні індикатори. Визначено, що підхід з використанням двошарової моделі продемонстрував у середньому 15% підвищення ефективності порівняно з прямим застосуванням гібридної рекурентно-згортокової нейромережі.

Застосування двошарової моделі класифікації даних успішно розширює можливості базового виявлення факту фальсифікації інформації, зокрема оцінювання масштабу й аналіз навмисності фабрикації. Емпіричний аналіз демонструє, що імплементація двошарової моделі з нав'язним баєсівським класифікатором досягає підвищення продуктивності в середньому на 15%, на відміну від простого застосування нейронної мережі. Ця різниця в продуктивності стає особливо значущою в системах з високою пропускнуою здатністю, де швидка ідентифікація та реагування на сфабриковану інформацію є критичними операційними параметрами. Здобутий результат дає змогу стверджувати про доцільність упровадження запропонованого підходу, а відповідно, сприяє зменшенню впливу подібної інформації в соціально орієнтованих системах, особливо під час кризових явищ.

Список літератури:

1. Afanasieva, I., Golian, N., Golian, V., Khovrat, A., Onyshchenko, K. Application of Neural Networks to Identify of Fake News. Proceedings of the 7th International Conference Computational Linguistics and Intelligent Systems (COLINS 2023). Kharkiv, April 20–21, 2023. CEUR Workshop Proceedings, No. 3396, P. 346–358.
2. Padalko H., Chomko V., Chumachenko D. A novel approach to fake news classification using LSTM-based deep learning models. Frontiers

in Big Data, Sec. Machine Learning and Artificial Intelligence. V. 6 – 2023. 18 pp. <https://doi.org/10.3389/fdata.2023.1320800>

3. Yakovlev S., Khovrat A., Kobziev V., Uzlov D. Decision support algorithm in the development of information sensitive socially oriented systems. Proceedings of the 4th International Workshop of IT-professionals on Artificial Intelligence (ProFIT AI 2024). Cambridge, MA, USA, September 25-27, 2024. CEUR Workshop Proceedings, 2024, 3777, pp. 315-326.

4. Yakovlev S., Khovrat A., Kobziev V. A Dual-Layered Artificial Intelligence Solution for Classifying Disinformation in Socially Oriented Systems. Proceedings of the Computational Linguistics Workshop (CLW-CoLInS 2025) at the 9th International Conference on Computational Linguistics and Intelligent Systems (CoLInS 2025). Kharkiv, Ukraine, May 15-16, 2025. CEUR Workshop Proceedings, 2025, 3976, pp. 69-81.

УДК 004.056.55: 681.3.06

ВИКОРИСТАННЯ ЕЛЕМЕНТІВ ЗАДАЧІ ПОКРИТТЯ ДЛЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ УДОСКОНАЛЕНОГО СПОСОБУ СИМЕТРИЧНОГО ШИФРУВАННЯ ДАНИХ

***Автори:** Лученко Я.В., аспірант; Тавдгірідзе Д.Д., студент,
Харківський національний університет радіоелектроніки, м. Харків,
Україна*

***Науковий керівник:** Кобзев В.Г., к.т.н., с.н.с., професор кафедри
Програмної інженерії; Харківський національний університет
радіоелектроніки, м. Харків, Україна*

Суттєве зростання обсягів використання цифрової інформації різного призначення вимагає забезпечення високого рівня її захисту при зберіганні і, особливо, при передачі різними каналами зв'язку. Загальновідомі способи захисту передбачають шифрування інформації тим чи іншим методом. Вибір таких методів, безумовно, має враховувати необхідний рівень конфіденційності самої інформації, кількість її користувачів, частоту оновлення і т.п. [1, 2].

Найбільший рівень захисту цифрової інформації забезпечують методи асиметричного шифрування, але складність реалізації обумовлює їх використання для шифрування лише найбільш важливої частини

інформації (особисті дані, паролі, ключі і т.п.). Їх практичну реалізацію забезпечує мережа центрів сертифікації ключів з використанням спеціальних протоколів. Для суттєво більшої за розміром частини інформації застосовуються методи симетричного шифрування зі зміною в часі таємного шифру або його частин [3].

Один з варіантів такого підходу до криптографічних перетворень покладений в основу патенту [4]. Він передбачає виконання блокового шифрування/дешифрування повідомлень з використанням мережі Фейстеля і гамування з використанням спеціальних масок.

В якості масок пропонується застосувати результати вирішення задачі покриття обмеженого простору цифрових даних фігурами певних, в тому числі різних, геометричних форм [5] з контрольованим рівнем перекриття, що відповідає нечіткому покриттю вихідного простору. Вибір і формування масок відбувається менш часто у порівнянні з етапом безпосереднього шифрування. Тому вимоги швидкодії до цього етапу менш жорсткі, він може виконуватися у фоновому режимі.

Метою роботи є аналіз можливостей програмної реалізації кроків криптографічних перетворень, передбачених у патенті [4], на основі спеціальної організації маскування та оцінка їх ефективності. У роботі проаналізовані існуючі програмні рішення, використовувані для виконання перестановок і перемішування, а також формування і накладання масок шляхом гамування. До уваги бралися мова програмування, обсяг програмного коду, розмір пам'яті для його розгортання, часові характеристики етапів шифрування/дешифрування, використання засобів паралелізації обчислювальних операцій. Останнє стосується як обрання нових масок, так і паралельного опрацювання декількох елементів блоків, частково за відомим принципом використання конвеєру. Перші два з трьох етапів формування ключів і підключів, на яких, згідно [4], виконується передача інформації щодо зображення, передача інформації про локальні фрагменти на зображенні, реалізуються в межах багатоваріантного вирішення вищезгаданої задачі покриття.

Експериментальні дослідження підтверджують, що при безпосередньому виконанні шифрування/дешифрування найбільш ефективним з точки зору швидкодії є використання низькорівневих мов

програмування з безпосереднім виконанням бітових операцій, передбачених алгоритмами мережі Фейстеля. В першу чергу це стосується операцій з різними частинами машинних слів.

Подальші дослідження перспективні у напрямку реалізації випадкового характеру чередування (обрання послідовності) рішень задачі покриття для забезпечення практично достатнього рівня криптостійкості описаної комбінованої системи шифрування.

Таким чином, комбінування відомих принципів симетричного шифрування з новітніми способами формування і зміни ключів за рахунок використання елементів задачі покриття для вибору масок є перспективним напрямом розвитку засобів криптографічного захисту інформації.

Список літератури:

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: монографія. – Харк. нац. ун-т радіоелектроніки, ПАТ "Ін-т інформ. технологій". – Вид. 2-ге, перероб. і доповн. – Х.: Форт, 2012. – 878 с.
2. Горбенко Ю.І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем: монографія / Ю.І. Горбенко. – Харків: Форт, 2016. – 959 с.
3. Ціхоцький М.С., Лужецький В.А. Аналіз методів розподілу секрету // Кібербезпека: освіта, наука, техніка. №1 (25), 2024. – С. 279-293.
4. Бритік В.І., Кобзєв.В.Г., Маркова Л.І., Путятін Є.П., Струков Є.В. Спосіб симетричного шифрування даних. – Патент на винахід № 96826, МПК H04L 9/06 (2006.01), Бюл. №23 від 12.12.2011.
5. Bulat A., Kiseleva E., Yakovlev S., Prytomanova O., Lebediev D. Solving the Problem of Fuzzy Partition-Distribution with Determination of the Location of Subset Centers. Computation, 2024, vol. 12, no. 10, article 199. Pp. 1-20.

УДК 004.056.5: 534.843: 621.391.883

ЩОДО АДАПТАЦІЇ ТОНАЛЬНОГО МЕТОДУ ВИЗНАЧЕННЯ РОЗБІРЛИВОСТІ МОВИ ДО ЗАДАЧ ЗАХИСТУ ІНФОРМАЦІЇ

***Автор:** Лях О.Д., студент, 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. До недавнього часу загальноприйнятим критерієм нормування та оцінювання захищеності мовної інформації було відношення сигнал/шум в точці можливого знімання інформації контрольній точці. Однак, враховуючи неінваріантність даного критерію до виду маскувальної завади, в провідних країнах світу відбувся перехід до критерію залишкової словесної розбірливості мови [1]. При цьому більшість сертифікованих методик оцінювання захищеності мовної інформації за цим критерієм ґрунтовані на формантному методі визначення розбірливості, який має певні недоліки, зокрема він не дозволяє повністю врахувати ряд факторів, що впливають на розбірливість мови і пов'язані з суб'єктивними властивостями і характеристиками людської слухової системи. Це обумовлює необхідність його удосконалення та пошуку нових підходів і методів.

Одним з ефективних методів визначення розбірливості мови, який вже давно використовується для оцінювання якості каналів мовного зв'язку є тональний метод, стандартизований варіант якого представлений в ГОСТ 8031-78 «Апарати телефонні. Тональний метод вимірювання розбірливості мови». Широко використовується цей метод також в медицині при проведенні таких досліджень, як тонова і мовленнєва аудіометрія.

Але використати цей метод в задачах оцінювання захищеності мовної інформації безпосередньо за існуючими методиками не можна через його суб'єктивний характер, що впливає на оперативність і економічність досліджень.

Метою роботи є визначення способу адаптація тонального методу визначення розбірливості мови до задачі оцінювання захищеності мовної інформації.

Основна частина. Тональний метод характеризується простотою і не потребує складних апаратних засобів (в якості тестових сигналів використовуються тональні сигнали). Він оснований на властивості людського слуху чітко визначати момент зникнення та появи звуку на рівні порогу чутності. За порогоми чутності тону розраховуються рівні відчуття тону, як різниця між рівнем сигналу і визначеним пороговим рівнем та визначається формантна розбірливість в заданих частотних смугах і залишкова словесна розбірливість. Результати оцінювання захищеності мовної інформації тональним методом та їх порівняння за результатами, отриманими формантним методом, показали відмінність до 5% [2]. Однак, тональний метод є суб'єктивним, тобто використовує слухову систему людини для визначення порогів чутності тону і потребує участі аудиторів в проведенні досліджень. Це збільшує час і необхідні людські ресурси на проведення досліджень та обмежує його використання в задачах оцінювання захищеності мовної інформації, для яких важливими є оперативність, економічність і конфіденційність.

Таким чином, потрібно вирішити задачу створення об'єктивного тонального методу, де замість аудиторів використовувались би узагальнені характеристики порогу чутності тонових сигналів для середньостатистичного слухача. Це забезпечить вказані вимоги при достатній точності оцінювання.

Основні аспекти створення інструментально-розрахункового тонального методу та етапи методики оцінювання захищеності мовної інформації за критерієм розбірливості мови таким методом визначено в [3]. Для об'єктивізації тонального методу потрібно мати значення порогів чутності тону тональних сигналів з частотами, що відповідають середньгеометричним частотам октавних (або третьоктавних) смуг мовного діапазону (частотну характеристику порогу чутності тональних сигналів) при різних шумових завадах. Це можна зробити:

- чисто розрахунком – для типових видів шуму (з відомими спектрами) при різних інтегральних рівнях шуму;
- експериментально-розрахунковим способом – коли частотна характеристика шуму знімається експериментально, а пороги чутності тональних сигналів розраховуються;

– чисто експериментально – коли пороги чутності тональних сигналів визначаються акустичним експериментом за допомогою аудиторів.

Наразі отримано частотні характеристики порогу чутності тональних сигналів при заваді "білий" шум розрахунковим та експериментальним шляхом [3]. Потрібно отримати аналогічні характеристики для інших видів шумових завод.

Висновок: Визначено основні шляхи адаптації тонального методу до задач оцінювання захищеності мовної інформації шляхом створення його об'єктивної версії та першочергові задачі в цьому напрямку.

Список літератури:

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

2. Касьянов Ю.І. Використання тонального методу визначення розбірливості мови для задачі оцінки захищеності мовної інформації / Ю.І. Касьянов, С.В. Дума // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали V всеукраїнської науково-практичної конференції з міжнародною участю. – Миколаїв: НУК, 2015. – С. 32 – 38.

3. Касьянов Ю.І. Основні аспекти об'єктивного тонального методу визначення розбірливості мови / Ю.І. Касьянов, С.О. Трізно // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали X всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2022. – С. 85–90.

УДК 004.42:004.056

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ПРОГРАМУВАННЯ ГЕНЕРАТОРІВ ВИПАДКОВИХ ЧИСЕЛ

***Автор:** Нестерович Е.Р., Харківський національний університет
радіоелектроніки, м. Харків, Україна*

***Науковий керівник:** Лановий О.Ф., к.т.н., доцент кафедри
Програмної інженерії; Харківський національний університет
радіоелектроніки, м. Харків, Україна*

Основою надійності сучасних криптографічних систем та протоколів вважається якість джерел ентропії. В детермінованому обчислювальному середовищі отримання істинної випадковості й досі залишається складною інженерною задачею. Застосування в програмних системах виключно програмних псевдовипадкових генераторів (ГПВЧ) або програмних криптостійких генераторів (ГКВЧ) створює погрози, що пов'язані з передбачуваністю станів або недостатньою ентропією початкового стану. З огляду на це сучасні процесори (зокрема Intel 64 та AMD64) мають інтегровані апаратні генератори випадкових чисел, ключовим елементом яких є інструкція RdRand, яка використовує тепловий шум в якості фізичного джерела ентропії [1].

Разом з тим, не зважаючи на апаратну стандартизацію, програмна абстракція доступу до RdRand суттєво залежить від екосистеми розробки. Різні мови програмування та середовища виконання використовують різні підходи до виклику цієї інструкції, обробки виключних ситуацій та інтеграції з власними криптографічними бібліотеками. В рамках проведеного дослідження було розглянуто особливості виклику інструкції RdRand та виконано порівняльний аналіз механізмів її використання у контексті різних мов програмування та операційних систем.

Опис експериментів. Емулюється N кидків абсолютно симетричної монети та перевірка випадання «орла» чи «решки». З теорії ймовірностей відомо, що при N , яка спрямована до нескінченності, кількість ймовірності випадання «орла» (або «решки») наближається до 0,5.

Програмна модель, реалізована на певній мові програмування, викликає функцію генерації дійсного числа в діапазоні від 0 до 1; якщо отримане число менше за 0,5, то будемо вважати, що випав «орел», в

іншому випадку – «решка». Звернення до функції повторюється N разів та підраховується кількість випадіння «орлів», визначається частота випадання «орла», яка порівнюється з теоретичним значенням 0.5 (береться різниця). Далі N кратно збільшується і багаторазово повторюється для деякого набору значень N .

Експерименти проводились для RdRand, ГКВЧ та ГПВЧ бібліотечних функцій для мов програмування Python 3.13.5, JavaScript (Node.js v22.18.0), C# 7.3 та Microsoft Macro Assembler зі складу Microsoft Studio 2022 в середовищі операційних систем Windows 11 та Ubuntu Linux 18.04.

Для переносу на різні апаратно-програмні платформи програмний код було максимально уніфіковано і спрощено, кінцевий псевдокод виглядає наступним чином:

```
for attempts_count in range(start, stop, step):  
    counter = 0  
    for i in range(attempts_count):  
        if [виклик ГПВЧ/ГВЧ/RdRand] <= 0.5:  
            counter += 1  
    print(attempts_count, counter / attempts_count)
```

Оскільки в деяких модулях відсутня функція, що повертає випадкове дійсне число, то було використано виклик функцій, що повертають невід’ємне ціле число з 64 випадковими бітами з подальшим масштабуванням в діапазон від 0 до 1 за допомогою ділення на 2^{64} (максимальне значення беззнакового 64-бітного цілого числа).

Через те, що мови програмування Python, JavaScript та C# не підтримують пряме використання асемблерних інструкцій у програмному коді, було використано спеціалізовані wrappers (обгортки) для забезпечення доступу високорівневих мов програмування до інструкцій процесора.

Тестування ГКВЧ на Python проводилось з використанням функції randbits() модуля secrets [2]. Модуль secrets забезпечує доступ до найбільш безпечного джерела випадкових чисел, яке надає ОС (джерелом ентропії можуть виступати, наприклад, таймінги руху миші або введення з клавіатури, стан пам’яті, кластери вільних дисків тощо).

Тестування ГКВЧ на JavaScript проводилось за допомогою методу `getRandomValues` модуля `Crypto` [3]. Він повертає масив, заповнений випадковими (у криптографічному сенсі) числами. Для того, щоб гарантувати достатню продуктивність, реалізації використовують не справжній ГВЧ, а ГПВЧ, якому надано початкове зерно з достатньою ентропією.

Тестування ГКВЧ на мові C# проводилось за допомогою методу `GetNonZeroBytes` класу `RandomNumberGenerator` (простір імен `System.Security.Cryptography`), який використовує системні сервіси генерації випадкових послідовностей на основі ентропії ОС [4].

До переліку некриптостійких ГПВЧ увійшли: функція `random.random()` у Python (алгоритм Mersenne Twister), метод `Math.random()` у JavaScript (алгоритм xorshift128+) та функція `NextDouble()` класу `System.Random` у C# на базі субтрактивного алгоритму Дональда Кнута.

Проводилось порівняння часу на один виклик ГВЧ для різних ОС/МП з `RdRand` та без неї. На графіках (рис.1) можна побачити, що при збільшенні кількості повторів відсутня деградація за часом (уповільнення) на виклик (про це свідчить горизонтальність графіків).

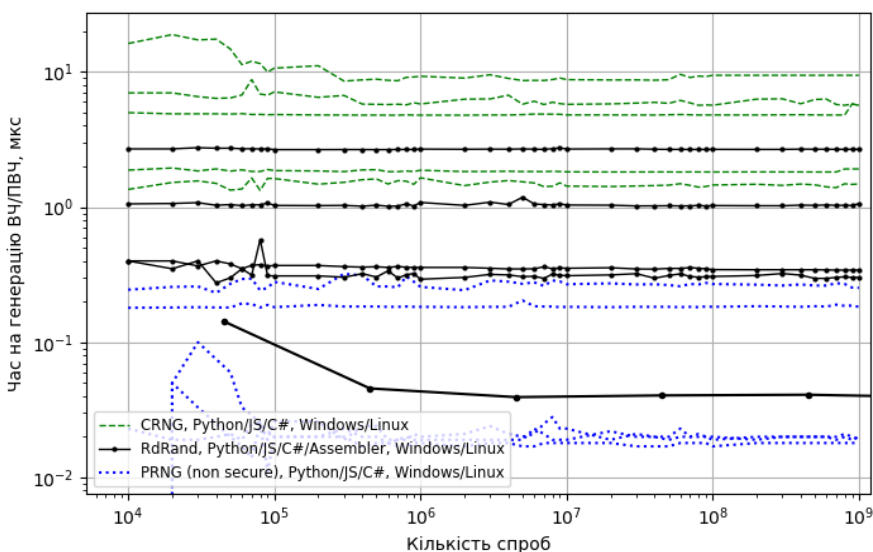


Рис. 1. Порівняння часу на один виклик ГВЧ

Візуальне порівняння графіків дозволяє зробити висновки про те, що:

- зі збільшенням кількості повторів (досліджено до 10^9 повторів) деградація за часом на виклик відсутня;
- апаратний ГВЧ працює вразі швидше ніж ГКВЧ, що використовують ентропію ОС.

Слід зазначити, що при проведенні експериментів спостерігалась несподівана поведінка програмної моделі ГВЧ на C#, що потребує подальшого дослідження.

Підсумовуючи порівняння:

- проведені експерименти не виявили суттєвих відмінностей у роботі RdRand та ГКВЧ, що свідчить про можливість та надійність використання ГКВЧ на слабких апаратних платформах, на яких відсутня підтримка RdRand;

- усереднена похибка ГПВЧ в рази менша ніж при використанні RdRand;

- програмні моделі на мовах програмування Python/JavaScript/C# для виклику RdRand використовують обгортки над кодом C/C++ який, у свою чергу, викликає RdRand за допомогою асемблерних вставок, що уповільнює роботу моделі.

Список літератури:

1. Intel® Digital Random Number Generator (DRNG). URL: <https://cdrdv2-public.intel.com/864722/drng-software-implementation-guide.pdf> (дата звернення 15.10.2025).

2. Documentation for the rdrand python module. URL: <https://rdrand.readthedocs.io/en/latest/> (дата звернення 29.10.2025).

3. JS метод Math.random(). URL: <https://css.in.ua/js/object/Math/method/random> (дата звернення 06.11.2025).

4. RdRand. Library to use Intel's Secure Key (rdrand instruction) in .NET URL: <https://github.com/JebteK/RdRand> (дата звернення 11.11.2025).

УДК 004.056:004.75

РОЗПОДІЛЕНА СИСТЕМА ЗБЕРІГАННЯ ТА РЕЗЕРВНОГО КОПІЮВАННЯ ДАНИХ

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

Цифрова трансформація транспортної галузі вимагає створення стійкої IT-інфраструктури, де дані є критичним активом для безпеки та безперервності перевезень. У 2026 році стратегія резервного копіювання стає основою кіберстійкості, оскільки програми-вимагачі (ransomware) фігурують у 44% випадків порушень безпеки, а для транспортних вузлів швидкість відновлення має прямий вплив на оперативні результати.

Традиційне правило «3-2-1» (три копії, два типи носіїв, одна копія поза об'єктом) залишається мінімальним базовим рівнем. Проте сучасні виклики вимагають переходу до архітектури «3-2-1-1-0», яка додає два критичні елементи:

1 незмінна (immutable) копія: дані, які фізично неможливо змінити або видалити протягом заданого періоду, навіть за наявності прав адміністратора.

0 помилок відновлення: досягається шляхом автоматизованого тестування кожної резервної копії (наприклад, технологія Veeam SureBackup).

Для географічно рознесених транспортних мереж рекомендується розподілене розгортання систем під управлінням єдиного центру (наприклад, Veeam Backup Enterprise Manager), що дозволяє керувати завданнями на різних сайтах через єдину консоль.

Особливу увагу варто приділити технологіям Peer-to-Peer (P2P), таким як Resilio Sync. На відміну від централізованих систем, P2P-архітектура:

- усуває єдину точку відмови, забезпечуючи стійкість до збоїв центральних серверів;
- оптимізує використання смуги пропускання шляхом паралельної передачі фрагментів файлів між усіма вузлами мережі одночасно;
- забезпечує низьку затримку та автоматичне балансування навантаження, що критично для терміналів із нестабільним зв'язком.

Ефективна розподілена система базується на комбінації апаратних і програмних рішень:

- Локальні сховища (NAS): використання Synology або QNAP для швидкого оперативного відновлення в локальній мережі. Для відкритих систем рекомендовано TrueNAS (на базі ZFS) або OpenMediaVault.
- Файлові системи: застосування ZFS або Btrfs, що підтримують миттєві знімки (snapshots) та функцію самовідновлення даних (Self-Healing).
- RAID-масиви: для забезпечення відмовостійкості на рівні дисків рекомендовано використовувати RAID 6 або RAID 10.

Згідно зі статистикою, 68% організацій не мають незмінних копій даних, що є їхньою найбільшою вразливістю. Розподілена система повинна включати Hardened Linux Repositories, які використовують файлову систему XFS із функцією блокування об'єктів (Object Lock). Крім того, сучасні системи у 2025/2026 роках впроваджують AI-сканування під час резервного копіювання для виявлення аномальних патернів шифрування ще до того, як заражені дані потраплять у сховище.

Оптимальний сценарій для транспортної інфраструктури включає три рівні захисту:

1. Рівень 1 (Локальний): NAS-сервери з RAID 5/6 для миттєвого відновлення.
2. Рівень 2 (Offsite/Cloud): зберігання копій у хмарних об'єктних сховищах (наприклад, AWS S3 або Wasabi) з підтримкою незмінності.
3. Рівень 3 (Синхронізація): використання P2P-клієнтів для дзеркалювання критичних документів у реальному часі між віддаленими офісами та терміналами.

У системі резервного копіювання та зберігання даних, зображений на рис. 1, реалізовано багаторівневу архітектуру захисту інформації, яка поєднує оперативність відновлення, кіберстійкість та глобальну доступність.

На першому етапі джерелами даних виступають сервери, бази даних і транспортні термінали, які генерують критично важливу інформацію. Для забезпечення її збереження виконується регулярне резервне копіювання на локальне сховище – мережевий накопичувач (NAS). Локальний рівень (рівень 1) забезпечує швидке відновлення даних (низький показник RTO) завдяки використанню відмовостійких конфігурацій RAID 6/10 та сучасних файлових систем (ZFS або Btrfs). Це дозволяє мінімізувати простой системи у разі збоїв або втрати даних.

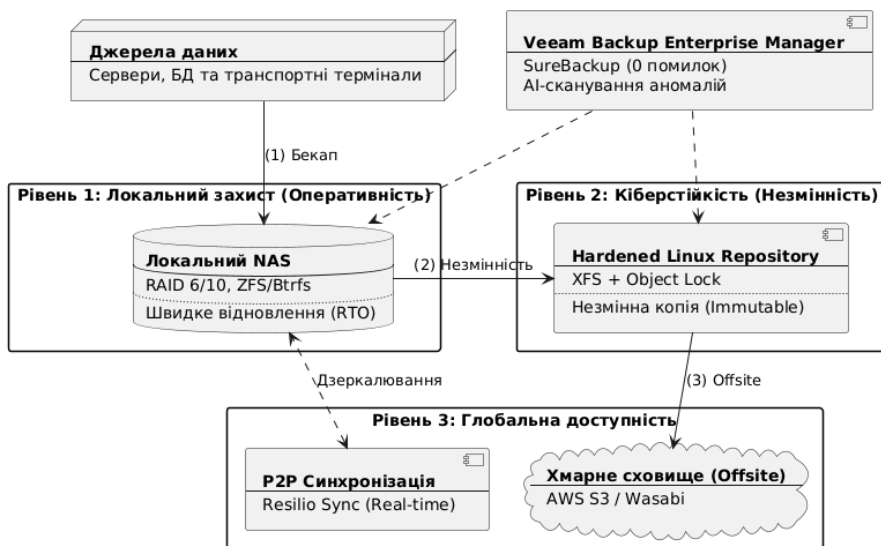


Рисунок 1 – Система резервного копіювання та зберігання даних

Керування процесами резервного копіювання та контроль їхньої цілісності здійснюється за допомогою програмного забезпечення Veeam Backup Enterprise Manager, яке забезпечує централізований моніторинг, перевірку резервних копій (SureBackup) та виявлення аномалій із використанням інтелектуального аналізу. Це підвищує загальний рівень надійності системи.

На другому рівні (рівень 2) реалізовано підхід кіберстійкості через використання захищеного сховища типу Hardened Linux Repository. У ньому застосовується файлова система XFS із механізмом Object Lock, що дозволяє створювати незмінні (immutable) резервні копії. Такий підхід гарантує захист даних від несанкціонованого видалення або модифікації, зокрема внаслідок атак типу ransomware.

Третій рівень (рівень 3) відповідає за глобальну доступність даних і передбачає їх дублювання за межами основної інфраструктури (offsite). Це може реалізовуватись двома способами: або через P2P-синхронізацію за допомогою програмного забезпечення Resilio Sync, що забезпечує передачу даних у режимі реального часу між вузлами, або

шляхом використання хмарних сервісів, таких як AWS S3 чи Wasabi. Це дозволяє забезпечити збереження інформації навіть у випадку фізичного знищення локальної інфраструктури.

Таким чином, запропонована система реалізує комплексний підхід до захисту даних відповідно до принципу 3-2-1-1-0, що передбачає наявність кількох копій даних, використання різних носіїв, зберігання однієї копії поза межами основної локації, а також створення незмінної резервної копії та постійний контроль відсутності помилок. Це забезпечує високий рівень надійності, безпеки та доступності інформаційних ресурсів.

Висновки. Головною проблемою сучасних систем є ілюзія безпеки: «зелений дашборд» не означає можливість успішного відновлення. Стійкість транспортної системи визначається не наявністю копій, а гарантованим часом їх відновлення (RTO) та мінімізацією втрат даних (RPO) через впровадження незмінних розподілених сховищ.

Список літератури:

1. Katai, N. (2026, February 21). Business backup solutions guide (2026): 3-2-1 architecture, vendor options, and rollout plan. Valydex.
2. Mouleeswaran, C., & Ghetau, C. (2023, September 6). Reference Architecture: Lenovo Backup Solution with ThinkSystem DE/DM/DG Storage and Veeam for ThinkAgile and ThinkSystem Platforms (Version 1.1). Lenovo Press.
3. National Instructional Media Institute. (2024). Computer Hardware & Network Maintenance - Trade Theory (1st ed.).
4. Resilio, Inc. (2026). Geo-diverse high availability deployment. Resilio Help Center.
5. Resilio, Inc. (2026). Implementing Resilio Active Everywhere as a Global File System (GFS). Resilio Help Center.
6. Veeam Software. (2026). Distributed Deployment - Veeam Backup & Replication User Guide (Build 13.0.1.1071). Veeam Help Center.

УДК 004.056:004.738.5

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМАХ РОЗУМНОГО БУДИНКУ

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

Сучасний «розумний будинок» перетворився зі збірки ізольованих приладів на складну взаємопов'язану екосистему, яка охоплює все: від енергоменеджменту до фізичної безпеки. Прогнозується, що до 2030 року кількість пристроїв Інтернету речей (IoT) зросте до 50 мільярдів, що експоненціально розширює поверхню для потенційних кібератак. Кожна «розумна» одиниця стає потенційною точкою входу для зламників у приватну мережу користувача.

Згідно з аналізом OWASP та іншими дослідженнями, основними проблемами безпеки є:

Слабкі або заводські паролі. Багато пристроїв постачаються зі стандартними обліковими даними (наприклад, admin/12345), які хакери легко використовують для масових атак.

Відсутність механізмів оновлення. Виробники часто нехтують регулярним випуском патчів безпеки, а користувачі не встановлюють їх, що залишає «діри» в прошивках відкритими роками.

Небезпечні налаштування за замовчуванням. Пристрої часто налаштовані на максимальну зручність підключення на шкоду безпеці, наприклад, із відкритими портами, що прослуховуються з інтернету.

Низькорівневі вразливості (напр., Ripple20). Помилки в широко використовуваних бібліотеках (як-от стек TCP/IP) можуть скомпрометувати мільйони пристроїв різних брендів одночасно.

Вибір протоколу безпосередньо визначає рівень стійкості системи розумного будинку до кіберзагроз.

Zigbee працює на частоті 2,4 ГГц (аналогічно Wi-Fi), що підвищує ризик інтерференції сигналу та атак типу jamming. Хоча протокол використовує шифрування AES-128, відомі випадки вилучення ключів при фізичному доступі до пристрою.

Z-Wave вважається більш безпечним завдяки жорсткій сертифікації та використанню альтернативних частот. Водночас він є пропрієтарним рішенням, що обмежує гнучкість використання та підвищує вартість впровадження.

Matter – сучасний стандарт, побудований за принципом security by design із використанням інфраструктури відкритих ключів (PKI) для атестації пристроїв. Проте навіть у ньому вже виявлені специфічні вразливості, зокрема атаки типу Delayed DoS (DeeDoS), які можуть блокувати керування пристроями.

Злам системи розумного будинку може мати серйозні наслідки:

- Фінансові втрати – наприклад, через несанкціоноване відкриття електронних замків.
- Кіберфізичний саботаж – маніпуляції з термостатами або іншими пристроями можуть призвести до аварій (наприклад, розриву труб).
- Зловживання ресурсами – використання пристроїв для майнінгу криптовалют або участі в ботнетах.

Особливу загрозу становить порушення приватності. Скомпрометовані камери та мікрофони (зокрема в роботах-пилососах чи системах відеоспостереження) можуть використовуватися для шпигунства: фіксації конфіденційних документів або інформації з екранів пристроїв.

Крім того, самі виробники нерідко збирають надмірні обсяги даних про поведінку користувачів з маркетинговою метою, що створює додаткові ризики витоку інформації.

Типова архітектура системи розумного будинку має багаторівневу структуру, в якій кожен рівень виконує окремі функції та має власні вектори атак. На рис. 1 представлено узагальнену модель такої системи із зазначенням ключових компонентів і потенційних загроз.

Прикладний рівень (Application) забезпечує взаємодію користувача із системою через мобільні додатки, хмарні сервіси та програмне забезпечення керування. Саме на цьому рівні реалізується бізнес-логіка та віддалений доступ до пристроїв. Основними загрозами є використання слабких паролів, відсутність двофакторної автентифікації, а також наявність незахищених API. Компрометація цього рівня може призвести до повного контролю над системою з боку зловмисника.

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

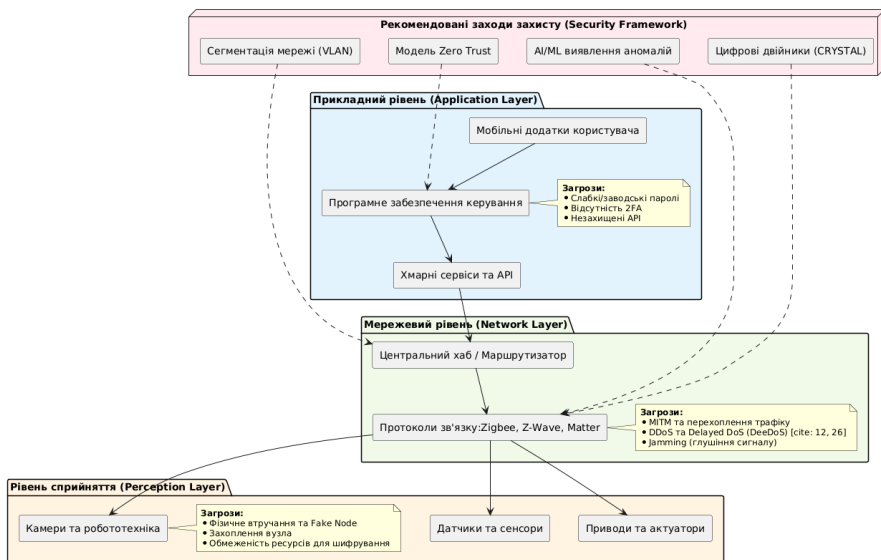


Рисунок 1 – Багаторівнева модель IoT-системи розумного будинку та основні загрози безпеці

Мережевий рівень (Network) відповідає за передачу даних між компонентами системи. До нього належать маршрутизатори (hub) та бездротові протоколи, такі як Zigbee, Z-Wave і Matter. Серед основних загроз — атаки типу «людина посередині» (MITM), DDoS-атаки, а також глушіння сигналу (jamming), що особливо актуально для бездротових протоколів. Успішна атака на цьому рівні дозволяє перехоплювати або змінювати мережевий трафік.

Рівень сприйняття (Perception) включає фізичні пристрої — датчики, сенсори, камери та роботизовані системи, які безпосередньо взаємодіють із середовищем. Основні загрози на цьому рівні пов'язані з фізичним доступом до пристроїв: захоплення вузла, втручання в роботу обладнання або підміна легітимного пристрою на фальшивий (Fake Node). Такі атаки можуть призвести до викривлення даних або повної компрометації системи.

Як показано на рис. 1, усі рівні системи тісно взаємопов'язані: дані передаються від рівня сприйняття через мережеву інфраструктуру до

прикладного рівня, тоді як керуючі команди рухаються у зворотному напрямку. Відповідно, порушення безпеки на будь-якому рівні може вплинути на функціонування всієї системи.

Для підвищення рівня безпеки експерти рекомендують застосовувати комплексний підхід:

Сегментація мережі (VLAN) – ізоляція IoT-пристроїв в окремий сегмент, щоб компрометація одного пристрою не відкривала доступ до критичних систем.

- Модель Zero Trust – жоден пристрій або користувач не вважається довіреним без постійної перевірки та автентифікації.

- Використання штучного інтелекту (AI/ML) – алгоритми машинного навчання дозволяють виявляти аномалії мережевого трафіку та ідентифікувати атаки з високою точністю.

- Цифрові двійники (наприклад, фреймворк CRYSTAL) – моделювання поведінки пристроїв для своєчасного виявлення відхилень, що можуть свідчити про кібератаку.

В умовах війни питання безпеки розумних будинків набуває особливої актуальності. Відомі випадки, коли хакерські групи використовують домашні маршрутизатори та IoT-пристрої для маскування атак на державні установи. Це підвищує значення захисту навіть побутових мереж як елементу загальної кібербезпеки країни.

Висновки. Повна безпека в IoT наразі недосяжна, проте керована стійкість є обов'язковою. Майбутнє за системами «прозорої безпеки», де автоматизований захист поєднується з повним контролем користувача над власними даними.

Список літератури:

1. Aldahmani, A., Ouni, B., Lestable, T., & Debbah, M. (2023). Cybersecurity of embedded IoTs in smart homes: Challenges, requirements, countermeasures, and trends. *IEEE Open Journal of Vehicular Technology*, 4, 281–292.
2. ENISA. (2024, December). 2024 report on the state of cybersecurity in the Union. European Union Agency for Cybersecurity.

3. Ghobakhlou, A., Al-Hamid, D. Z., Zandi, S., & Cato, J. (2025, July 25). A comprehensive analysis of security challenges in ZigBee 3.0 networks. *Sensors (Basel)*, 25(15), 4606. <https://doi.org/10.3390/s25154606>
4. Iturbe Araya, J. I. (2025, May). Anomaly-based detection of cyberattacks on smart homes [PhD Thesis, Universitat Oberta de Catalunya]. TDX.
5. Iturbe-Araya, J. I., & Rifà-Pous, H. (2024). Impact of dataset composition on machine learning performance for anomaly detection in smart home cybersecurity. *Proceedings of the 2024 International Symposium on Networks, Computers and Communications (ISNCC)*, 1–10. <https://doi.org/10.1109/ISNCC62547.2024.10759024>
6. Iturbe-Araya, J. I., & Rifà-Pous, H. (2025). Enhancing unsupervised anomaly-based cyberattacks detection in smart homes through hyperparameter optimization. *International Journal of Information Security*, 24(1), 45. <https://doi.org/10.1007/s10207-024-00961-6>
7. Mazhar, T., Talpur, D. B., Al Shloul, T., Ghadi, Y. Y., Haq, I., Ullah, I., Ouahada, K., & Hamam, H. (2023). Analysis of IoT security challenges and its solutions using artificial intelligence. *Brain Sciences*, 13(4), 683. <https://doi.org/10.3390/brainsci13040683>
8. Peterson, E., & Mujeye, S. (2025). Addressing IoT vulnerabilities in smart homes. *Proceedings of the 2025 8th International Conference on Software Engineering and Information Management (ICSIM 2025)*, 116–121. <https://doi.org/10.1145/3725899.3725918>

СЕКЦІЯ 3. ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 004.056.52.:53

ДОСЛІДЖЕННЯ РОЗВИТКУ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ НА БАЗІ NIS 2

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

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

Анотація. Інформація, що є власністю держави, а особливо інформація з обмеженим доступом, потребує захисту. Нормативно-правова база країни потребує постійної адаптації та вдосконалення. Ефективне управління інформаційною безпекою є одним з аспектів збереження цілостності та суверенітету держави.

Ключові слова: Захист інформації, нормативно-правова база, аналіз організації інших країн, ДСК, NIS2, NIST, НАТО, ЄС.

Вступ

Розвиток України полягає в її вступі в ЄС, що вимагає адаптації законодавчої та нормативно-правової бази України до вимог ЄС. В сфері захисту інформації ці процеси почались більше 20-и років тому, однак їх пік відбувається безпосередньо зараз. Керівництвом держави, в рамках підготовки України до вступу до ЄС, поставлене завдання по оновленню всієї нормативно-правової бази з максимальним врахуванням вимог NIS 2 та NIST. Однак, дія вказаних нормативних документів не розповсюджується на структуру та алгоритми дії систем безпеки щодо інформації з обмеженим доступом, особливо такої, що містить державну таємницю.

Мета роботи є проведення дослідження з визначення шляхів узгодження діючої в Україні нормативно-правової бази розробки та експлуатації систем безпеки інформації з базами США та ЄС.

Для досягнення поставленої мети вирішувалися такі завдання :

1. Проведено порівняльний аналіз нормативно-правового забезпечення з розробки та експлуатації систем захисту інформації США (NIST, NIST SP800), ЄС (NIS 2), Канади, НАТО та України;
2. Проведено маркування інформації в залежності від її важливості;
3. Створення методологічної основи для модернізації нормативно-методичних документів в Україні.

Викладення основного матеріалу

Результати порівняльного аналізу показали значну нерівномірність по об'ємам робіт щодо реконфігурації нормативно-правової бази України. Так, в питаннях забезпечення захисту інформації на об'єктах інформаційної діяльності критичної інфраструктури головним питанням є підвищення рівня теоретичної підготовки працівників. При цьому головне питання реконфігурації нормативно-правової бази України полягає в зменшенні рівня формалістики в їх роботі – колосальна кількість звітів, актів, протоколів та інше, що забирають більшість робочого часу.

В сфері кіберзахисту, Україна має значні проблеми в нормативно-правовому забезпеченні. Це багато в чому, пов'язане з неможливістю формалізувати звітність по виконаних роботах і небажанням молодих фахівців, що в більшості випадків мають високі теоретичні і практичні навички, до роботи з таким рівнем формалізації звітності. Ці проблеми, багато в чому, вже вирішені в Регламентах ЄС та США щодо побудови систем кібербезпеки. Тим більше, що питання побудови систем захисту інформації від загроз кібербезпеці, в більшості випадків, є інваріантним до інформації, що потребує захисту.

В Україні та й в Світі виникла ситуація, що характеризується наявністю двох методологій:

– Маркування ризиків в залежності від збитків, які виникають в наслідок інциденту, та розбудова систем безпеки спрямованих на запобігання виникнення інцидентів (зменшення збитків). Щодо інформації, яку повинна захистити система безпеки, то її важливість враховується на рівні величини збитків в наслідок втрати її конфіденційності та/цілісності та/або доступності. Більш того, NIS 2 та NIST взагалі не

призначені для розробки систем безпеки для захисту інформації що містить держану таємницю (методика розрахунку величини збитків не розрахована для таких випадків). Наявність в інформації, що потребує захисту, держаної таємниці розглядається в NIST SP-800, однак ці документи рекомендують як побудувати систему безпеки, мають рекомендаційний характер і не встановлюють певних (законодавчих) вимог до рівнів захисту безпосередньо самої інформації. На цій методології засновані нормативно-правові бази США, ЄС та інших.

– Маркування інформації в залежності від її важливості (наприклад наявності в ній державної таємниці) та розбудова систем безпеки спрямованих на її захист. Величина збитків (витрати на розбудову системи, її супровід, збитки від інциденту та інше) є додатковим фактором, який враховується шляхом підвищення окремих вимог (гарантій, критеріїв, та інше) в порівнянні з типовим рівнем і фактично може не впливати на структуру системи безпеки (витрати на розбудову системи та її експлуатацію можуть значно перевищувати величину збитків від інциденту). На цій методології засновані нормативно-правові бази НАТО та України.

Таким чином, нормативно-правова бази України з розробки та функціонування систем захисту інформації з базою ЄС потребує розуміння мети та шляхів вдосконалення.

Проведено порівняльний аналіз нормативно-правового забезпечення з розробки та експлуатації систем захисту інформації США (NIST, NIST SP800), ЄС (NIS 2), НАТО та України, що дозволило визначити основні розбіжності в підходах до формування принципів побудови систем безпеки.

В США та ЄС використовується «ризико-збитковий» підхід, що дає змогу побудувати системи захисту інформації з мінімізацією збитків від інцидентів. Однак при цьому не враховується суть самої інформації, не проводиться її маркування, а отже не враховується статус інформації, проти якої стався інцидент.

В НАТО і Україні побудова систем безпеки ведеться на основі маркування інформації, що забезпечує побудову ієрархічних систем захисту, спрямованих на оптимізацію структури системи захисту

інформації, їх спрямованість на захист інформаційного ресурсу. Недоліком таких систем є не врахування збитків на побудову та експлуатацію системи захисту та збитків від інциденту.

Висновки

У межах дослідження системного аналізу та структурного моделювання, з використанням тривимірної матриці відповідності, яка охоплює напрями гармонізації, країни (або організації) та стан нормативно-правових актів. Такий підхід дав змогу формалізувати взаємозв'язки між вимогами різних систем безпеки та визначити конкретні напрями вдосконалення.

У результаті створено універсальну методологічну основу для оцінки, порівняння та модернізації нормативно-методичних документів, щодо вдосконалення нормативно-правової бази НД ТЗІ та окремих вимог з метою її адаптації з міжнародними стандартами NIS2, NIST та НАТО у сфері технічного захисту інформації з обмеженим доступом, в тому числі й таку, що містить державну таємницю, що забезпечує узгодження української нормативної бази з міжнародними практиками та підвищує ефективність управління інформаційною безпекою на національному рівні.

Список літератури:

1. Закон України «Про державну таємницю» // сайт Верхов. Ради України (BBP). URL: <https://zakon.rada.gov.ua/laws/show/3855-12Text> (10.10.2024).
2. Захист конфіденційної інформації – персональних даних. Засоби захисту від несанкціонованого доступу. // ООО НИИ «Автопром». URL: <http://avtoprom.kiev.ua/avtoprom /ru/content/защита-конфиденциальной-информации-персональных-данных> (10.10.2024).
3. Верховна Рада України. (2019, 7 лютого). Закон України «Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору)» № 2680-VIII.
4. Постанова КМУ №373 (2018) – Типова інструкція з організації захисту інформації.
5. Постанова КМУ №92 (2022) – Порядок забезпечення кіберзахисту державних інформаційних ресурсів.

6. Постанова КМУ №667 (2006) – Порядок проведення державної експертизи в сфері технічного захисту інформації

7. Європейська Комісія. (2025). Звіт щодо виконання Угоди про асоціацію між Україною та ЄС за 2023–2024 роки

8. Служба безпеки України. (2020, 23 грудня). Наказ «Про затвердження Зводу відомостей, що становлять державну таємницю» (№ 383).

9. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2013, 15 квітня). Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці: НД ТЗІ 1.6-005-2013 (Наказ № 215).

10. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2024). НД ТЗІ 2.3-025-24: Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (Наказ № 45/ДСК).

УДК 004.056.52.:.53

РОЗРОБКА ШАБЛОНУ КОМПЛЕКТУ ДОКУМЕНТІВ ДЛЯ СТВОРЕННЯ АС-1 КЛАСУ 4 КАТЕГОРІЇ ДЛЯ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

***Автор:** Мельник І.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

Інформація з давніх давен була важливим важелем, не дарма кажуть «Проінформований – значить озброєний». З одного боку, у нас є інформація якою володіє певний підрозділ, а з іншого – особа або група осіб, які бажають заволодіти даною інформацією.

Під час розробки документів для створення АС-1 класу 4 категорії для об'єкту інформаційної діяльності в підрозділах Національної гвардії України треба враховувати усі можливі варіанти витоку інформації щоб запобігти втрати важливих даних.

Ключові слова

Комплексна система захисту інформації, канали витоку інформації, кіберзагроза, документообіг, інформаційна безпека

Вступ

У сучасному інформаційному просторі захист інформації на підприємствах набуває все більшої ваги через зростання кіберзагроз і глобалізацію. Забезпечення інформаційної безпеки є необхідною умовою збереження цілісності, конфіденційності та доступності даних, що роблять дослідження цієї теми актуальним і важливим. Метою роботи є комплексний аналіз існуючих підходів, нормативно-правової бази та розробка рекомендацій щодо покращення системи управління інформаційною безпекою підприємств.

Розробка документів, процес навчання персоналу необхідно перебудовувати та вдосконалювати, для цього необхідно включати в навчання сучасні курси з навчання співробітників із країн, які стоять вище за Україну в цьому питанні: ЕС, США, Канади та НАТО.

Метою роботи є дослідження існуючих систем захисту інформації в Національній гвардії України та розробка комплексного підходу до їхнього розвитку.

Теоретичні аспекти забезпечення інформаційної безпеки

Інформаційна безпека у підрозділах Національної гвардії України розглядається як сукупність заходів і процесів, спрямованих на захист інформаційних ресурсів від загроз. Основні зовнішні загрози включають кібернапади, витоки даних, технічні збої, а внутрішні – помилки персоналу, зловмисні дії чи недбалість. Управління інформаційною безпекою базується на принципах і методах оцінки ризиків, побудові політик безпеки та впровадженні захисних технологій.

Аналіз нормативно-правової бази України та міжнародний досвід

Детальний аналіз нормативних актів України, а також документів ЕС, США, Канади та НАТО показав, що на сучасному етапі державне регулювання потребує удосконалення. Запровадження міжнародних

стандартів і узгодження нормативних документів забезпечать підвищення ефективності захисту інформації та інтеграцію українських підприємств у світову систему кібербезпеки.

Постановка задачі дослідження

Визначено основні завдання, серед яких – аналіз нормативно-правових вимог до технічного захисту інформації, а також розробка конкретних заходів щодо вдосконалення системи захисту відповідно до сучасних стандартів.

Розробка системи управління інформаційною безпекою організації

В роботі запропоновано структуру системи управління, що включає детальний аналіз інформаційних потоків, розподіл інформації за рівнями доступу, формування політик безпеки та впровадження засобів технічного захисту. Особлива увага приділяється класифікації інформації та специфіці заходів безпеки для різних типів даних.

Рекомендації щодо вдосконалення системи управління інформаційною безпекою

Розроблені рекомендації містять організаційні заходи (підвищення кваліфікації персоналу, розробка внутрішніх політик), технічні кроки (впровадження сучасних технологій захисту, моніторинг безпеки) та нормативні пропозиції (оновлення нормативної бази, відповідність міжнародним стандартам). Визначено порядок і план впровадження цих рекомендацій, що забезпечить системний і комплексний підхід.

Практична значущість роботи та перспективи

Запропоновані рішення допоможуть підприємствам ефективно захищати інформаційні ресурси, знижуючи ризики кіберзагроз і внутрішніх порушень. Подальші дослідження можуть бути спрямовані на розробку адаптивних систем безпеки з урахуванням специфіки конкретних організацій, а також на вдосконалення нормативного регулювання в Україні.

Висновок

Отже, виконане дослідження підтверджує важливість комплексного підходу до забезпечення інформаційної безпеки підприємницьких структур, включаючи аналіз теоретичних основ, нормативної бази та практичних заходів. Запропоновані рекомендації мають вагоме наукове

і практичне значення, сприяють підвищенню безпеки інформації і можуть бути використані у подальшій роботі підприємств.

Список літератури:

1. Про державну таємницю // сайт Верхов. Ради України (ВВР). URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text> (25.11.2025).
2. Закон України “Про інформацію” [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/2657-12>;
3. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/2657-12>;
4. Указ Президента України "Про заходи щодо захисту інформаційних ресурсів держави" від 10 квітня 2000 р. № 582/2000.
5. Указ Президента України "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні" від 31 липня 2000 р. № 928/2000
6. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації;
7. ДБН А.2.2-3-97 Проектування. Склад, порядок розробки, узгодження і затвердження проектної документації для будівництва;
8. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
9. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
10. НД ТЗІ 1.1-004-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

УДК 004.056.52.:53:004.912

АНАЛІЗ ПРОЦЕСУ РЕКОНФІГУРАЦІЇ НОРМАТИВНО- ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

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

Анотація. Гармонізація нормативно-правової бази України з вимогами Європейського Союзу є ключовою передумовою інтеграції держави у спільний політичний та безпековий простір, що зумовлює необхідність модернізації підходів до технічного й кіберзахисту інформації. Попри багаторічний розвиток нормативних документів у сфері НД ТЗІ, найактивніша фаза їх реформування триває саме зараз, коли Україні поставлено завдання адаптувати національну систему до регламенту NIS2 та рекомендаційної бази NIST. Водночас зазначені стандарти не охоплюють вимоги щодо побудови систем захисту інформації з обмеженим доступом, включно з державною таємницею, що формує методологічний розрив між ризик-орієнтованими моделями США та ЄС і ієрархічним підходом України та НАТО, який ґрунтується на класифікації, маркуванні та регламентованому обігу інформації. У роботі проведено порівняльний аналіз вимог NIS2, стандартів NIST, документів НАТО та українських НД ТЗІ, визначено ключові концептуальні й процедурні відмінності між цими системами. Оцінено ступінь їх сумісності, а також виявлено напрями, у яких українська нормативна база потребує оновлення. На основі отриманих результатів сформовано рекомендації щодо модернізації НД ТЗІ з урахуванням міжнародних практик, забезпеченням методологічної узгодженості та збереженням вимог до захисту інформації з обмеженим доступом.

Ключові слова: інформаційна безпека, НД ТЗІ, NIS2, NIST, STANAG, державна таємниця.

Вступ

Після внесення змін до Конституції України у 2019 році стратегічний курс держави на членство в ЄС і НАТО став юридично визначеним.

Однією з передумов інтеграції є модернізація нормативно-правової бази у сфері інформаційної та кібербезпеки. Регламент NIS2 (Network and Information Security Directive 2, Директива ЄС про мережеву та інформаційну безпеку, друга редакція) визначає імперативні вимоги до підвищення стійкості критичної інфраструктури ЄС, а рекомендації NIST SP-800 (National Institute of Standards and Technology Special Publication 800 Series, Національний інститут стандартів і технологій США) сформували технічні стандарти кіберзахисту у США, Спеціальна серія публікацій 800).

Проте ці документи орієнтовані на захист інформації середнього та високого рівня чутливості і не регламентують вимоги до даних, що становлять державну таємницю. На відміну від цього, нормативні документи НАТО та українські НД ТЗІ побудовані на принципі інформаційної ієрархії: саме рівень секретності визначає структуру системи безпеки.

Історичні чинники (радянська модель ТЗІ, високий рівень документальної формалізації, відставання у сфері кіберзахисту) призвели до дисбалансу між сучасними потребами та нормативними процедурами. Це ускладнює введення ризик-орієнтованих підходів ЄС/США в українську систему.

Мета та задачі дослідження

Метою дослідження є визначення шляхів узгодження діючої в Україні нормативно-правової бази розробки та експлуатації систем безпеки інформації з нормативними моделями США, ЄС та НАТО.

Для досягнення цієї мети виконано такі **задачі**:

- 1) Проведено порівняльний аналіз NIS2, стандартів NIST, нормативних документів НАТО та українських НД ТЗІ.
- 2) Визначено концептуальні розбіжності між ризик-орієнтованим підходом (США/ЄС) та ієрархічним підходом, що базується на маркуванні інформації (Україна/НАТО).
- 3) Сформовано рекомендації щодо вдосконалення НД ТЗІ з метою гармонізації з вимогами NIS2/NIST і стандартами НАТО.
- 4) Побудовано тривимірну матрицю відповідності, яка дозволяє системно узгодити вимоги та визначити напрями оптимізації нормативної бази.

Порівняльний аналіз

1 Порівняння NIS2 та NIST

NIS2 є обов'язковою директивою ЄС, тоді як NIST – набір рекомендацій, що служать технічною основою для захисту інформації.

Критерій	NIS2	NIST
Правовий статус	Законодавчий акт	Добровільні стандарти
Мета	Підвищення кіберстійкості	Управління ризиками
Підхід	Організаційні вимоги	Технічні контролю
Класифікація	Відсутня	FIPS199 (Low/Moderate/High)

Примітка: FIPS199 – Federal Information Processing Standards 199, Федеральний стандарт обробки інформації №199)

2 НД ТЗІ України та стандарти НАТО

Україна і НАТО застосовують ієрархію рівнів секретності та комплексну систему норм щодо:

- маркування та обігу інформації,
- контролю доступу,
- фізичного захисту,
- криптозахисту,
- TEMPEST/EMSEC-вимог (TEMPEST (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions, Захист електронних систем від побічних електромагнітних випромінювань) / EMSEC (Emission Security, Захист від електромагнітних випромінювань (компрометувальних випромінювань)),
- процедур передачі,
- акредитації інформаційних систем.

3 Порівняння трьох систем

- НАТО забезпечує повну модель секретності.
- НД ТЗІ встановлюють суворі процедури атестації.
- NIST/NIS2 пропонують гнучкий технічний механізм управління ризиками.

4. Рекомендації щодо гармонізації НД ТЗІ

1. Класифікація та маркування – впровадити STANAG 4778/4779.
2. Життєвий цикл – повне журналювання та протоколи знищення.
3. IAM – MFA та least privilege (IAM – Identity and Access Management, Управління ідентичністю та доступом; MFA – Multi-Factor Authentication, Багатофакторна автентифікація).
4. Аудит – централізований моніторинг (SIEM).
5. TEMPEST – SDIP-27/28 (NATO SDIP-27 – Minimum Standards for the Security of Information Systems (Мінімальні стандарти безпеки інформаційних систем НАТО) / NATO SDIP-28 – Information System Security Assessment and Authorization (Оцінювання та авторизація безпеки інформаційних систем НАТО)).
6. Акредитація – узгодження з натівською моделлю.
7. Реагування на інциденти – строки за NIS2.
8. Фізичний захист – синхронізація з директивами НАТО.

Висновки

1. Проведено порівняльний аналіз нормативно-правового забезпечення з розробки та експлуатації систем захисту інформації США (NIST, NIST SP800), ЄС (NIS 2), НАТО та України, що дозволило визначити основні розбіжності в підходах до формування принципів побудови систем безпеки.

В США та ЄС використовується «ризико-збитковий» підхід, що дає змогу побудувати системи захисту інформації з мінімізацією збитків від інцидентів. Однак при цьому не враховується суть самої інформації, не проводиться її маркування, а отже не враховується статус інформації, проти якої стався інцидент.

В НАТО і Україні побудова систем безпеки ведеться на основі маркування інформації, що забезпечує побудову ієрархічних систем захисту, спрямованих на оптимізацію структури системи захисту інформації, їх спрямованість на захист інформаційного ресурсу. Недоліком таких систем є не врахування збитків на побудову та експлуатацію системи захисту та збитків від інциденту.

2. У межах дослідження розроблено рекомендації щодо вдосконалення нормативно-правової бази НД ТЗІ та окремих вимог з метою її гармонізації з міжнародними стандартами NIS2, NIST та НАТО.

Розроблення здійснено методом системного аналізу та структурного моделювання, з використанням тривимірної матриці відповідності, яка охоплює напрями гармонізації, країни (або організації) та стан нормативно-правових актів. Такий підхід дав змогу формалізувати взаємозв'язки між вимогами різних систем безпеки та визначити конкретні напрями вдосконалення.

У результаті створено універсальну методологічну основу для оцінки, порівняння та модернізації нормативно-методичних документів у сфері технічного захисту інформації з обмеженим доступом, в тому числі й таку, що містить державну таємницю, що забезпечує узгодження української нормативної бази з міжнародними практиками та підвищує ефективність управління інформаційною безпекою на національному рівні.

Список літератури:

1. Верховна Рада України. (2019, 7 лютого). *Закон України «Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору)» № 2680-VIII.*
2. European Council. (1993, June 21–22). *Conclusions of the Copenhagen European Council.* Copenhagen, Denmark
3. European Union, & Ukraine. (2014). *Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part.* Official Journal of the European Union, L 161, 3–2137.
4. Кабінет Міністрів України. (2025). *Звіт про виконання Угоди про асоціацію між Україною та Європейським Союзом за 2024 рік.* Офіційний вебсайт Кабінету Міністрів України.
5. Європейська Комісія. (2025). *Звіт щодо виконання Угоди про асоціацію між Україною та ЄС за 2023–2024 роки*
6. Рада Європейського Союзу. (2022). *Рішення Ради Європейського Союзу щодо кібербезпеки.*
7. National Institute of Standards and Technology. (2004). *Standards for security categorization of federal information and information systems (FIPS PUB 199).*

8. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Revision 5).
9. National Institute of Standards and Technology. (2020). *Protecting controlled unclassified information in nonfederal systems and organizations* (NIST Special Publication 800-171, Revision 2).
10. NATO. (2017, December 20). *Confidentiality Metadata Label Syntax (STANAG 4774 Ed 1; ADatP-4774 Ed A Ver 1)*. NATO.
11. NATO. (2018, October 26). *Metadata Binding Mechanism (ADatP-4778 Ed A Ver 1; STANAG 4778 Ed 1)*. NATO.
12. NATO (SECAN). (2009, August). *TEMPEST Product Qualification and Control (SDIP-55)*.
13. NATO (SECAN). (n.d.). *Emission Security / Compromising Emanations Standard (SDIP-27)*.
14. NATO (SECAN). (n.d.). *Zoning Procedures for Emission Security (SDIP-28)*.
15. NATO. (2002, 17 червня). *Security Within the North Atlantic Treaty Organization* (Document C-M(2002)49).
16. NATO. (2002, July 11). *The Management of Non-Classified NATO Information* (Document C-M(2002)60).
17. НІКС. (2024). Перелік нормативно-методичних документів в галузі захисту інформації [Звіт].
18. Інститут кібернетики імені В. М. Глушкова НАН України. (2025). *Історія*.
19. Верховна Рада України. (1994). *Закон України «Про державну таємницю»* (№ 3855-XII). Офіційний вісник України.
20. Служба безпеки України. (2020, 23 грудня). *Наказ «Про затвердження Зводу відомостей, що становлять державну таємницю»* (№ 383).
21. The White House. (2009, December 29). *Executive Order 13526: Classified National Security Information* (Vol. 75, No. 2). *Federal Register*.
22. North Atlantic Council. (2007, December 11). *The NATO Information Management Policy (NIMP)* (C-M(2007)0118).
23. North Atlantic Treaty Organization. (pik). *STANAG 4779: Confidentiality Metadata Binding*. NATO Standardization Office.

24. North Atlantic Treaty Organization. (2020). *Directive on personnel security* (AC/35-D/2000-REV8). NATO Security Committee.

25. North Atlantic Treaty Organization. (2020). *Directive on physical security* (AC/35-D/2001-REV3). NATO Security Committee.

26. North Atlantic Treaty Organization. (n.d.). *NATO Security Incident Reporting Procedures* [Internal document]. NATO Communications and Information Agency.

27. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2013, 15 квітня). *Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці: НД ТЗІ 1.6-005-2013* (Наказ № 215).

28. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2016). *НД ТЗІ 3.6-003-2016: Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації* (Наказ № 41/ДСК).

29. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2024). *НД ТЗІ 2.3-025-24: Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем* (Наказ № 45/ДСК).

30. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2023). *НД ТЗІ 3.7-003-2023: Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі* (Наказ № 924).

31. Державна служба спеціального зв'язку та захисту інформації України. (2003). *НД ТЗІ 2.5-010-2003: Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу*. Київ: Держспецзв'язку України. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

**СЕКЦІЯ 5. ПІДГОТОВКА КАДРІВ У ГАЛУЗІ ЗНАНЬ
«ІНФОРМАЦІЙНА БЕЗПЕКА»**

УДК 004.412

**ВИЗНАЧЕННЯ НЕОБХІДНОСТІ ТРАНСФОРМАЦІЇ
ПАРАДИГМИ ПІДГОТОВКИ КАДРІВ У СФЕРІ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПОТРЕБ ЗАХИСТУ
КРИТИЧНОЇ ІНФРАСТРУКТУРИ**

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

Проблеми персоналу набувають стратегічного значення для країни через посилення гібридних загроз та прискорену цифровізацію транспортного сектору. Транспортний сектор за останні кілька років зазнав зростання кібератак, які включають масштабні атаки на АТ «Укрзалізниця» та морську інфраструктуру України. Модель загроз еволюціонувала від атак на основі масової пошти до складних багатовекторних атак, що включають атаки на основі АРТ-груп проти систем автоматизації та управління ОТ, які ініціюються сусідніми країнами. Успіх захисту від цих загроз залежить від технічних засобів захисту та стратегій, пов'язаних з персоналом, які використовують організації. [1] Реальні потреби галузі та навчальні програми вищих навчальних закладів не узгоджені. Існує кілька критичних проблем, які потребують негайного вирішення за допомогою теоретичних та практичних підходів.

Ринок праці вже почав агресивно реагувати на цю суперечність. З одного боку, бізнес готовий прийняти щойно випущених студентів, але повинен приділяти значний час їхньому навчанню. Це призводить до появи молодшої посади з інформаційної безпеки, що означає, що спеціалісту знадобиться щонайменше 6 місяців (а зазвичай і більше) безперервного навчання, щоб мати змогу виконувати найпростіші завдання. Це призводить до додаткового тиску на старших керівників та керівників команд, відволікаючи їхню увагу від роботи із захисту життєво важливої інфраструктури. Бізнесу давно відомо, що у провідних національних університетах, на кафедрах інформаційної безпеки,

навчання студентів роботі в реальному середовищі (наприклад, у Цentraх операцій безпеки або кафедрах інформаційної безпеки) є вкрай недостатнім. Згідно з дослідженнями ринку праці (наприклад, IBM та ISC2), існує глобальна нестача персоналу, і кілька факторів погіршують ситуацію в Україні. Це не питання дефіциту знань, а питання браку навичок та досвіду.[2, 3]

Українська дослідницька та освітня спільнота може бути незрозумілою щодо того, що означають терміни інформаційна безпека та кібербезпека. Таке непорозуміння призведе до неправильного уявлення випускників вищих навчальних закладів про цю професію. Інформаційна безпека – це широкий термін, який включає захист усіх типів інформації, включаючи організаційну та фізичну безпеку. Спеціалізована галузь кібербезпеки зосереджена на захисті цифрової інформації, мереж та систем. Відсутність чіткого розмежування цих двох термінів під час навчання призводить до того, що випускники вищих навчальних закладів не можуть зрозуміти деталі своєї роботи. Зокрема, обов'язки щодо захисту інформації та кібербезпеки змішуються з обов'язками щодо мережевої безпеки та реагування на інциденти. [4]

У транспортному секторі ця різниця особливо актуальна, оскільки захист транспортної інфраструктури передбачає як кіберзахист (захист систем управління дорожнім рухом, SCADA), так і захист інформації (захист критичної інформації про вантажі, пасажирів, розклади руху та стратегічні активи). Нездатність розмежувати ці дві сфери призводить до побудови незбалансованих систем безпеки.

Огляд навчальних програм технічних університетів показує надлишок базових предметів на шкоду спеціальним. Математичні моделі криптографічних функцій студенти опановують, але практичні навички використання інструментів безпеки або аналізу журналів SIEM-систем представлені недостатньо. Відсутність доступу до анонімізованих даних про інциденти та матеріалів розслідування кіберзлочинів не дозволяє набуту аналітичних навичок та «полювання на загрози». Це особливо важливо в транспортному секторі, оскільки захист систем автоматизації залізниць передбачає знання специфічних протоколів та сценаріїв атак, які неможливо інтерпретувати виключно на теоретичному рівні.[5].

Варто також згадати про небезпечну упередженість, яка спостерігається у професійних уподобаннях студентів. Під впливом медійного іміджу «хакера», більшість студентів зацікавлені у спеціалізації лише в наступальній безпеці (Pentesting, Red Teaming). Тим часом, сфера GRC (Governance, Risk and Compliance), яка є основою інфраструктури безпеки будь-якої компанії, особливо в регульованих галузях, таких як транспорт (вимоги NBU, ISO 27001, NIST, NIS2), майже не досліджується. Це призвело до парадоксальної ситуації на ринку праці, де спостерігається надлишок претендентів на посаду молодшого пентестера (без досвіду) та гостра нестача інженерів зі стандартизації та майбутніх аудиторів. [6]

Впровадження штучного інтелекту у повсякденний та навчальний процес також має двійтий характер. З одного боку, це потужний інструмент автоматизації. З іншого – фіксується тренд на пошук «швидких шляхів» серед студентів, які делеguють вирішення навчальних та професійних задач AI-моделям, не розуміючи принципів їх роботи і отриманих результатів. Це призводить до формування покоління фахівців, неспроможних верифікувати результат, виявляти галюцинації ШІ та вирішувати нестандартні проблеми без допомоги алгоритмів. Така «сліпа віра» в технологію створює екзистенційні ризики для безпеки критичної інфраструктури, де помилка в коді або конфігурації може мати катастрофічні наслідки. [7]

У сфері інформаційної та кібербезпеки ціна помилки є настільки високою, що це може коштувати втрати цілого бізнесу або зупинити на певний час діяльність підприємства критичної інфраструктури. Згенеровані штучним інтелектом відповіді можуть бути результатом «галюцинацій» – дуже правдоподібних, але хибних відповідей. Те ж саме стосується вразливого коду в додатках. Молодий фахівець, який має дуже поверхневу теоретичну базу, не здатен верифікувати результат роботи ШІ. Він «сліпо» довіряє йому, що може призвести до впровадження вразливого коду або неправильних рішень у бізнес. Так само це стосується неправильної оцінки інциденту безпеки. [8]

Використання ШІ створює серйозну ілюзію компетентності. Студент відтепер може надати результат дуже швидко. Такий результат виглядає досить професійно сформульованим, але при детальному розгляді виявляється абсолютно непрацездатним або навіть небезпечним до

впровадження. Роботодавці на технічних співбесідах все частіше стикаються з кандидатами, які не можуть пояснити код, який вони нібито «написали» (насправді, згенерували).

Надмірна покладання на ШІ призводить до атрофії навичок критичного мислення та вирішення проблем (problem-solving). Процес навчання – це подолання труднощів, пошук рішень, налагодження (debugging). Коли цей процес делегується ШІ, мозок не формує необхідних нейронних зв'язків. Ми ризикуємо отримати покоління «операторів промптів», які без доступу до ШІ стають професійно недієздатними.

Список літератури:

1. Ukraine Railway Systems Attacked By Russian Hackers. URL: <https://www.cybersecurityintelligence.com/blog/ukraine-railway-systems-attacked-by-russian-hackers-8324.html>
2. The cybersecurity skills gap contributed to a USD 1.76 million increase in average breach costs. URL: <https://www.ibm.com/think/insights/cybersecurity-skills-gap-contributed-increase-average-breach-costs>
3. Growth of Cybersecurity Workforce Slows in 2024 as Economic Uncertainty Persists. URL: <https://www.isc2.org/Insights/2024/09/ISC2-Publishes-2024-Cybersecurity-Workforce-First-Look>
4. Information Security vs. Cybersecurity: What's the Difference? URL: <https://www.nu.edu/blog/information-security-vs-cybersecurity/>
5. OT Cybersecurity course (curriculum) applied to the Transport Sector. URL: <https://www.cci-es.org/en/c04-ot-cybersecurity-course-applied-to-the-transport-sector/>
6. 2025 ISC2 Cybersecurity Workforce Study. URL: <https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study>
7. Advancing Cybersecurity Education in the Era of Generative AI. Selina Demi, Bjørnar Guttormsen, Kevin Forberg Reinaas, Mats Hansen, Sofie Sand. URL: https://www.researchgate.net/publication/398004070_Advancing_Cybersecurity_Education_in_the_Era_of_Generative_AI

УДК 004.056.53

ПЕРСПЕКТИВИ ПІДГОТОВКИ СТУДЕНТІВ ДЛЯ УЧАСТІ В CTF-ЗМАГАННЯХ

Автор: Орел О.С., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

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

Вступ

У сучасних умовах цифрової трансформації та зростання кількості кіберінцидентів особливої актуальності набуває якісна підготовка фахівців з кібербезпеки. Одним із найбільш дієвих інструментів формування практичних умінь та командних компетенцій стали CTF-змагання (Capture the Flag). Вони моделюють реальні кіберситуації, вимагають швидкої аналітики, технічної підготовки та ефективної взаємодії учасників. Попри активний розвиток CTF-руху, питання методології командотворення, організації навчального процесу та створення умов для системної підготовки студентів залишаються відкритими та потребують подальшого дослідження.

Метою роботи є огляд перспективних завдань для створення команд для участі в CTF-змаганнях.

Основна частина

Ефективна підготовка фахівців з кібербезпеки ґрунтується на поєднанні теоретичних знань із практичними завданнями, що моделюють реальні кіберзагрози. Ключовими елементами такого навчання є міждисциплінарність, командна взаємодія, рольовий розподіл та робота з інструментами, які застосовуються у реальному середовищі.

Важливу роль у формуванні практичних навичок відіграють лабораторні заняття з дисципліни «Безпека інформаційних та комунікаційних систем», де студентів навчають основам червоної команди (red teaming) та синьої команди (blue teaming). У рамках red team-підходу відпрацьовуються методи аналізу та експлуатації вразливостей, отримання та утримання доступу, а також техніки обходу захисту. Blue team-напрямок охоплює основи SOC-аналізу, виявлення шкідливої активності, моніторинг, реагування на інциденти та роботу з матрицею MITRE ATT&CK. Практична частина включає виконання задач за

принципами CTF: Web, Crypto, Forensics, OSINT, Reverse, а також командну роботу над симуляціями атак. Планується опрацювання системи MITRE Caldera для моделювання реальних кібератак.

Додаткові можливості для розвитку навичок створює гурток кібербезпеки, де студенти проходять кімнати на платформі Hack The Box, працюють над командними CTF-завданнями та вдосконалюють навички взаємодії в команді. Окремий напрям гуртка присвячено програмуванню C++, що сприяє глибшому розумінню низькорівневих процесів і підготовці до задач типу Pwn та Reverse Engineering.

Комплексне поєднання занять з БІКС та роботи гуртка забезпечує студентам системний розвиток технічних та командних компетенцій, необхідних для участі у CTF-змаганнях.

Висновки:

Підготовка студентів до CTF-змагань вимагає комплексного підходу, який поєднує теоретичні знання з практичними вправами, симуляціями кіберзагроз та командною роботою. Використання методологій red team та blue team сприяє розвитку як атакувальних, так і захисних навичок, формуючи всебічну компетентність у сфері кібербезпеки. Регулярні практичні заняття та участь у гуртках дозволяють поглибити технічні знання, розвивати аналітичне мислення та навички ефективної командної взаємодії. Системний підхід до підготовки команд допомагає студентам опановувати технічні навички, стратегічне мислення, швидке ухвалення рішень та ефективну комунікацію, що є ключовим для успішної участі у CTF-змаганнях.

ПЕРШИЙ ПОГЛЯД НА ВИКОРИСТАННЯ ЗОВНІШНІХ ПЛАТФОРМ ПІДГОТОВКИ СПЕЦІАЛІСТІВ З КІБЕРЗАХИСТУ ДЛЯ ЗАЛУЧЕННЯ ЇХ В НАВЧАЛЬНИЙ ПРОЦЕС

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

На даний час підготовка спеціалістів у напрямку кібербезпеки набуває все більшої актуальності. Це зумовлено стрімкою цифровою трансформацією суспільства, активним впровадженням інформаційних технологій у всі сфери діяльності, а також зростанням кількості кіберзагроз і милітаризацією кіберпростору. Сучасні умови ведення кібервоєн та інформаційних операцій вимагають від фахівців високого рівня підготовки, практичного досвіду та здатності оперативно реагувати на нові виклики.

Одним із найбільш ефективних шляхів підвищення якості підготовки майбутніх фахівців з кіберзахисту є інтеграція онлайн-платформ для навчання та тренування. Такі платформи надають можливість студентам працювати з реалістичними сценаріями атак і захисту, що важливо для формування навичок, які складно чи неможливо відтворити в межах традиційних лабораторних робіт.

Метою роботи є огляд перспектив використання онлайн-платформ для навчання кібербезпеки, а також визначення можливостей їх інтеграції в освітній процес закладів вищої освіти.

Для оцінки ефективності таких платформ було проведено навчання студентів з використанням двох найбільш популярних ресурсів у сфері кібербезпеки – Hack The Box та TryHackMe. Обидві платформи активно застосовуються як у навчальних закладах, так і у корпоративному секторі для розвитку практичних навичок з етичного хакінгу, цифрової криміналістики, аналізу вірусів, роботи з мережевими протоколами тощо.

Особливості процесу навчання:

- самостійне опрацювання теоретичних матеріалів, представлених у форматі інтерактивних лекцій, довідкових статей або навчальних модулів;
- виконання практичних завдань, що є ключовою частиною навчання. Такі завдання зазвичай зводяться до пошуку «прапора» (flag) — певної фрази або токена, що підтверджує успішне виконання вправи.

Пошук прапора може передбачати різні сценарії:

- аналіз частин програмного застосунку та виявлення прихованих даних;
- складання команди з відповідними параметрами, використання інструментів сканування, тестування чи експлуатації;
- пошук файлів на віртуальній машині чи сервері, до якого надано доступ у межах завдання;
- виконання повноцінних симульованих атак (у випадках платформ типу Hack The Box).

Завдяки цьому студенти не лише засвоюють матеріал, але й набувають реального досвіду взаємодії з сучасними інструментами кіберзахисту.

Переваги використання даних онлайн-платформ:

- широкий спектр напрямів та матеріалів. Платформи значно перевищують можливості стандартного курсу, надаючи доступ до десятків навчальних треків: від основ Linux до реверс-інжинірингу та аналізу шкідливого ПЗ;
 - індивідуалізація навчання. Кожен студент може обирати рівень складності та темп навчання, формуючи власну траєкторію професійного зростання;
 - дистанційність та доступність. Навчання не прив'язане до аудиторії – тренажери доступні 24/7, що особливо актуально для змішаного та дистанційного навчання;
 - сертифікація – студенти можуть отримувати офіційні сертифікати, які визнаються роботодавцями та можуть підвищити конкурентоспроможність на ринку праці;
 - підготовка до CTF-змагань. Формат завдань максимально наближений до реальних Capture The Flag турнірів, що дає змогу готувати команди для участі у професійних хакерських змаганнях;
 - реалістичність практики. Моделі вразливостей і сценарії на платформах часто ґрунтуються на реальних інцидентах у сфері кібербезпеки;
- Недоліки використання платформ
- платні підписки. Повний доступ до контенту часто потребує додаткових фінансових витрат, що може бути проблемою для окремих студентів;

– наявність готових рішень у мережі. Це може знижувати освітню цінність завдань і призводити до формального виконання роботи без реального засвоєння матеріалу;

– обмеженість формату «пошуку прапора». Такий підхід чудово підходить для тренування технічних навичок, але не завжди є повноцінною заміною лабораторних робіт, де потрібно, наприклад, самостійно розгорнути та налаштувати систему.

Висновки

Використання онлайн-платформ з кібербезпеки є доцільним і перспективним, проте їх варто інтегрувати продумано. Платформи доцільно застосовувати у рамках додаткового навчання, факультативів, практичних курсів або підготовки до змагань CTF. Вони чудово підходять для розширення та поглиблення знань, дають змогу студентам обирати власні траєкторії розвитку й отримувати унікальний досвід, який неможливо отримати в межах стандартної програми.

ВИКОРИСТАННЯ MITRE CALDERA В ПРОЦЕСІ ПІДГОТОВКИ СПЕЦІАЛІСТІВ З КІБЕРЗАХИСТУ

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

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

З кожним роком кількість і складність кібератак зростає, що створює серйозні ризики для державних структур, бізнесу та критичної інфраструктури. Саме тому підготовка спеціалістів із кіберзахисту останнім часом стає не просто важливою – вона стратегічна. В сфері кібербезпеки потрібні люди, які можуть не лише реагувати, а й передбачати дії нападника, а цьому складно навчитися з теорії – потрібні симуляції, лабораторії, практичні полігони. З цієї причини платформи на кшталт MITRE Caldera такі цінні – вони дозволяють просимулювати атаку, побачити, як вона розгортається, і зрозуміти, як її зупинити.

Мета роботи – обґрунтувати доцільність використання платформи MITRE Caldera як інструменту моделювання поведінки зловмисників у процесі підготовки фахівців з кіберзахисту, а також дослідити її

потенціал для формування практичних компетентностей у сфері виявлення, аналізу та реагування на кіберінциденти.

Основна частина

MITRE Caldera – це платформа з відкритим кодом, розроблена організацією MITRE на основі знань із MITRE ATT&CK Framework. Вона призначена для автоматизації, відтворення та оцінювання кібератак у контрольованому середовищі.

Автоматизація дозволяє послідовно повторювати сценарії без людського втручання; заощаджує час під час тестів і робить експерименти відтворюваними. За допомогою емуляції поведінки зловмисників замість абстрактних вправ отримуємо сценарії, які структурно відповідають реальним інцидентам, що покращує релевантність навчання і тестування засобів захисту.

Систематичне вимірювання результатів симуляцій дає змогу об'єктивно оцінити рівень кіберстійкості організації. Замість суб'єктивних висновків використовуються кількісні показники (метрики часу виявлення, реагування, виявлені техніки тощо), що дозволяє аргументувати прийняття рішень у сфері безпеки.

Використання MITRE ATT&CK Framework як концептуальної основи для Caldera забезпечує уніфікований підхід до опису й аналізу атак, що дає змогу стандартизувати результати оцінювання, спрощує порівняння між різними командами та організаціям.

Можливість інтеграції з існуючими інструментами (SIEM, EDR, IDS/IPS) забезпечує комплексність оцінювання кіберзахисту. Завдяки цьому з'являється можливість досліджувати не лише поведінку атак, а й ефективність систем моніторингу, логування та реагування.

Система побудована за архітектурою “сервер–агент”: сервер керує процесом симуляції, а агенти виконують дії на цільових машинах. Функціонал розширюється через плагіни, які додають нові можливості (наприклад, звітування чи взаємодію з іншими інструментами). Для тренувань використовуються сценарії (“operations”), що відтворюють послідовність дій зловмисників згідно з етапами ATT&CK – від початкового доступу до контролю над системою.

Платформа MITRE Caldera ефективно застосовується як у

університетському, так і у корпоративному середовищі для підготовки фахівців із кіберзахисту. Вона дає змогу створювати реалістичні навчальні сценарії, моделювати дії зловмисників і відпрацьовувати тактики реагування. У закладах освіти Caldera використовується для формування практичних компетентностей студентів, а в корпоративних програмах — для тренування команд безпеки (Red/Blue/Purple Team) та оцінювання готовності інфраструктури до атак.

Серед можливих прикладів застосування даної системи можна виокремити лабораторні вправи з відпрацювання етапів атаки, тренування команд у контрольованому середовищі, перевірка покриття детекції SIEM/EDR шляхом моделювання відомих TTP (тактик, технік і процедур), вправи з оцінки готовності до реагування на інциденти, аналізу мережевого трафіку та виявлення підозрілої активності, виявлення та усунення вразливостей веб-додатків, оцінки безпеки хмарної інфраструктури (AWS/Azure), управління доступом і автентифікації користувачів у корпоративній мережі.

До основних переваг використання MITRE Caldera відносяться швидке масштабування тестів, прив'язка до MITRE ATT&CK, можливість кількісної оцінки ефективності захисту, гнучкість та розширюваність. Проте слід мати на увазі, що неправильне розгортання або помилка в сценарії може спричинити порушення роботи або витоки даних, а інструменти емулявання можуть бути використані не за призначенням, якщо доступ до них потрапить до сторонніх осіб.

Також варто враховувати те, що деякі високоточні або кастомні техніки АРТ можуть не мати коректної емуляції, а налаштування, написання плагінів, інтеграція з логами і SIEM вимагають часу та компетенцій.

Висновки

MITRE Caldera є потужним інструментом для підготовки фахівців із кіберзахисту, оскільки дозволяє автоматизовано відтворювати реалістичні сценарії атак, оцінювати ефективність засобів захисту та розвивати практичні навички у студентів і корпоративних команд. Архітектура «сервер–агент», використання плагінів та сценаріїв на основі MITRE ATT&CK забезпечують масштабованість, стандартизацію та відтворюваність навчальних і тестових операцій.

Водночас застосування Caldera потребує уваги до обмежень і ризиків: неповне відтворення складних TTP, залежність від якості

сценаріїв, можливі негативні наслідки для експлуатаційних середовищ і потреба у захисті конфіденційних даних. Проте при належній організації і контролі Caldera стає ефективним інструментом навчання та оцінки кіберстійкості, що поєднує теоретичні знання з практичними навичками і сприяє формуванню компетентних спеціалістів із кіберзахисту.

Список літератури:

1. CALDERA room, TryHackMe | Cyber Security Training. URL: <https://tryhack-me.com/room/caldera> (date of access: 01.11.2025).
2. Welcome to MITRE Caldera's documentation! – caldera documentation. URL: <https://caldera.readthedocs.io/en/latest/> (date of access: 01.11.2025).

ЗМІСТ

Секція 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТРАНСПОРТНИХ ЗАСОБІВ І СИСТЕМ..... 3

Побудова реляційної моделі взаємовпливу факторів вразливостей на захищеність об'єкту водного транспорту <i>Бондаренко І.Ю.</i>	3
Порівняльний аналіз методів розпізнавання ознак в біометричних системах контролю доступу <i>Гальченко О.Л.</i>	8
Інформаційна модель вибору базового профілю безпеки <i>Ломова О.О.</i>	13
Інформаційна модель вибору альтернативних заходів захисту при створенні системи безпеки інформації <i>Ткаченко Д.О.</i>	19
Інформаційна модель вибору заходів захисту за НД ТЗІ 3.6-006-24 <i>Турти М.В.</i>	27
Інформаційна модель вибору заходів захисту за НД ТЗІ 3.6-006-24 <i>Шаповалова О.П.</i>	33

Секція 2. ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ..... 42

Обґрунтування методики оцінки часової складності алгоритмів на базі кореляційного аналізу <i>Бабенко Н.; Пантелєєв В.; Самойленко Д.М.; Суліма М.М.; Туманов О.А.</i>	42
Проблемні питання використання операційних систем Windows у комплексних системах захисту інформації <i>Васєв В.В.</i>	47
Технології виявлення фальсифікованої інформації для підвищення інформаційної безпеки <i>Кобзєв В.Г.; Ховрат А.В.</i>	51
Використання елементів задачі покриття для програмної реалізації удосконаленого способу симетричного шифрування даних <i>Лученко Я.В., аспірант; Тавдгірідзе Д.Д.</i>	53
Щодо адаптації тонального методу визначення розбірливості мови до задач захисту інформації <i>Лях О.Д.</i>	56
Дослідження особливостей програмування генераторів випадкових чисел <i>Нестерович Е.Р.</i>	59

Розподілена система зберігання та резервного копіювання даних <i>Трибулькевич С.Л.; Трибулькевич В.В.; Бачула Є.Г.</i>	63
Проблеми інформаційної безпеки системах розумного будинку <i>Трибулькевич С.Л.; Трибулькевич В.В.; Титарчук В.В.</i>	67
Секція 3. ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	72
Дослідження розвитку нормативно-правової бази забезпечення захисту інформації в Україні на базі NIS 2 <i>Гришко М.Ю.</i>	72
Розробка шаблону комплексу документів для створення АС-1 класу 4 категорії для об'єкту інформаційної діяльності в підрозділах Національної гвардії України <i>Мельник І.М.</i>	76
Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України <i>Нужний С.М.</i>	80
Секція 5. ПІДГОТОВКА КАДРІВ У ГАЛУЗІ ЗНАНЬ «ІНФОРМАЦІЙНА БЕЗПЕКА»	87
Визначення необхідності трансформації парадигми підготовки кадрів у сфері інформаційної безпеки для потреб захисту критичної інфраструктури <i>Гусева-Божаткіна В.А.; Божаткін С.М.; Пасюк Б.Б.</i>	87
Перспективи підготовки студентів для участі в СТФ-змаганнях <i>Орел О.С.</i>	91
Перший погляд на використання зовнішніх платформ підготовки спеціалістів з кіберзахисту для залучення їх в навчальний процес <i>Сірівчук А.С.</i>	93
Використання MITRE Caldera в процесі підготовки спеціалістів з кіберзахисту <i>Ферцович М.С.; Рибак А.Ю.</i>	95

Наукове видання

**СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ НА ТРАНСПОРТІ**

СПІБТ–2025

**XIII Всеукраїнська науково-технічна конференція
з міжнародною участю**

27–28 листопада 2025 року

*Національний університет кораблебудування
імені адмірала Макарова*

*Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв*

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

**У двох частинах
Частина 2**

(українською мовою)

Відповідальна за випуск В. В. Трибулькевич
