МІНІСТЕРСТВО
ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ

КАФЕДРА
ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

КИЇВ - 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА
ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

ВСЕУКРАЇНСЬКА
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

Дата проведення:
05 листопад 2025 року.

Початок о 10:00.

Київ 2025

УДК 004.89:621.39(043.2)

Організатори:

Іванченко Євгенія Вікторівна кандидат технічних наук, професор, Директор навчально-наукового інституту кібербезпеки та захисту інформації ДУІКТ;

Туровський Олександр Леонідович, доктор технічних наук, професор, завідувач кафедри Технічних систем кіберзахисту ДУІКТ;

Пепа Юрій Володимирович, професор кафедри Технічних систем кіберзахисту ДУІКТ, кандидат технічних наук, доцент.

Комп'ютерна верстка та редагування:
Поночовний Петро Михайлович, доцент кафедри
технічних систем кіберзахисту ДУІКТ.

Рекомендовано до друку Вченою радою Навчально-наукового інституту
телекомунікацій Державного університет інформаційно-комунікаційних технологій
(протокол № 3 від 14.10.2025 р.)

Актуальні проблеми безпеки інформаційно-комунікаційних систем: збірник тез всеукраїнської науково-практичної конференції (м. Київ, 05 листопада 2025 року), Київ: РВЦ ДУІКТ. – 2025. – 61с.

Збірник тез призначений для аспірантів, науковців, викладачів
та інших зацікавлених осіб.

Редакційна колегія не несе відповідальності за зміст матеріалів, що опубліковані у збірнику. Всі вони надані в авторській редакції та виражають персональну позицію учасників конференції.

Є.О. Васін, студент СЗДМ 61,
Державний університет інформаційно-комунікаційних технологій

СУЧАСНІ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ

Захищеність інформації визначається і певними властивостями, а саме конфіденційність, цілісність та доступність. За визначенням конфіденційність це властивість інформації бути захищеною від несанкціонованого ознайомлення. Одним зі шляхів втрати інформацією конфіденційності є її виток матеріально-речовим каналом. В жодному з НД ТЗІ не висвітлюється яким чином захищати інформацію від витоку матеріально-речовим каналом.

Проведемо оцінку можливості протидії витоку інформації матеріально-речовим каналом шляхом використання системи контролю та управління доступом (СКУД).

До складу СКУД входять [1] (рис. 1): пристрій ідентифікації особи, контролер та виконавчий пристрій.

Рис. 1. Складові СКУД

Функціональним призначенням СКУД є автоматичне надання допуску особам яким вхід дозволений на певну територію, або приміщення. Всі її інші функції (збереження матеріальних цінностей, контроль і облік робочого часу і ін.) є результатом основного призначення.

До основних характеристик СКУД відносяться [1]:

- вартість;
- надійність функціонування;
- швидкодія;
- час реєстрації користувача;
- ємність пам'яті;
- стійкість до зловмисних дій;
- ймовірність помилкового відхилення законного користувача (помилки 1-го роду);
- ймовірність помилкового надання доступу незаконному користувачеві (помилки 2-го роду).

Припустимо, що у якості приміщення, що охороняється є об’єкт інформаційної діяльності (ОІД) у якому наявні матеріальні носії інформації з обмеженим доступом (ІзОД). Загрозою для ІзОД, у даному випадку, буде несанкціоноване переміщення матеріального носія за межі ОІД спричинене діями порушника інформаційної безпеки (ІБ), тобто виток інформації матеріально-речовим каналом.

Згідно з наведеною класифікацією [2], порушники ІБ бувають зовнішні і внутрішні. Якщо припустити, що ОІД обладнано СКУД, то фактор зовнішнього порушника ІБ можна

викреслити. Дійсно, у сторонньої для ОІД людини не може бути унікальних біометричних ознак, властивих співробітникам ОІД, щоб СКУД здійснила допуск цієї людини у ОІД. Тобто можна зробити висновок, що СКУД здатна протидіяти витоку інформації матеріально-речовим каналом, або по іншому - забезпечити конфіденційність інформації.

Проте при проектування СКУД для охорони ОІД треба враховувати параметри надійності роботи СКУЛ, ймовірність виникнення помилок другого роду, вибір стійкого ідентифікатора користувача.

Список використаних джерел:

1. Котенко А.М. Курс лекцій для студентів зі спеціальності 125 «Кібербезпека та захист інформації» з дисципліни «Системи контролю та управління доступом на об'єкти інформаційної діяльності». –К, ДУІКТ, 2024. – 79 с.

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

Д. О. Калалб, студент
Державний торгівельно-економічний університет

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАСОБІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ЗОБРАЖЕННЯ ОБЛИЧЧЯ

У роботі розглянуто результати експериментального дослідження ефективності біометричної автентифікації за зображенням обличчя, реалізованої у мобільному пристрої Xiaomi Note 10 Pro. Проаналізовано вплив зовнішніх факторів — відстані, освітленості та кутів зйомки — на точність розпізнавання. Проведено порівняння із системами Apple Face ID та Samsung Face Recognition. Запропоновано рекомендації щодо підвищення надійності біометричних систем.

Ключові слова: біометрична автентифікація, розпізнавання обличчя, Face Unlock, точність, антиспуфінг, безпека мобільних пристроїв.

Біометричні системи автентифікації — один із найперспективніших напрямів розвитку інформаційної безпеки, який дозволяє реалізувати доступ до систем за унікальними фізіологічними ознаками користувача. На відміну від традиційних паролів чи токенів, біометричні дані не потребують запам'ятовування та практично не можуть бути забутими чи втраченими[1].

Розпізнавання обличчя стало найпоширенішим методом біометричної автентифікації у споживчих пристроях завдяки його швидкодії та зручності. Однак 2D-реалізації, що ґрунтуються на зображенні з фронтальної камери, часто демонструють низьку стійкість до змін зовнішніх умов та спроб спуфінгу (імітації обличчя через фото чи відео).

З огляду на це, метою роботи є оцінка практичної ефективності технології Face Unlock (2D) на смартфоні Xiaomi Note 10 Pro та аналіз перспектив її використання в інформаційно-комунікаційних системах із підвищеними вимогами до безпеки.

Експериментальна частина включала:

- визначення еталонних умов автентифікації (відстань 0.3–0.6 м, нормальне освітлення, нульові кути);
- серію вимірювань точності при зміні одного параметра (відстані, горизонтального або вертикального кута);
- інтегральні тести, що поєднували кілька факторів одночасно;
- оцінку показників ефективності:
    1. *TAR (True Acceptance Rate)* — частка успішних розпізнавань легітимного користувача;
    2. *FAR (False Acceptance Rate)* — частка помилкових прийняттів;
    3. *FRR (False Rejection Rate)* — частка помилкових відмов[2].

Для контролю впливу середовища проводились тести при різному рівні освітлення (денне, штучне, затемнене) та відстані до 5 метрів.

В еталонних умовах середня точність Face Unlock становила ≈ 90%, що свідчить про задовільну роботу системи у типових сценаріях використання. Проте навіть у цьому режимі фіксувалися окремі випадки False Acceptance (10%).

При зміні відстані результати демонстрували експоненціальне зниження точності:

- у зоні 0.3–0.6 м — точність 92–94%;
- при відстані >2 м — падіння до 0–5%.

Вплив кутів був не менш значним: при горизонтальних або вертикальних відхиленнях понад ±45° система втрачала здатність до стабільної ідентифікації (точність <10%).

Інтегральні тести (комбінація трьох факторів) показали, що навіть незначне відхилення від оптимальних умов призводить до зменшення точності у 2–3 рази, що свідчить про низьку адаптивність системи до реальних сценаріїв використання.

Таблиця 1

Порівняльний аналіз

Параметр	Xiaomi Note 10 Pro (2D Face Unlock)	Apple Face ID (3D)(3)	Samsung Face Recognition (3D)(4)
Точність (FRR / FAR)	FRR ~10%, FAR ~10%	FRR <1%, FAR ≈ 0.0001%	FRR ~2%, FAR ≈ 0.001%
Технологія	2D-зображення RGB	3D-сканування з IR та структурованим світлом	3D ToF + IR
Стійкість до освітлення	Висока залежність	Незалежна (IR)	Незалежна (IR)
Антиспуфінг	Відсутній (можливий обхід фото/відео)	Захист за рахунок аналізу глибини та мікро-рухів	Середній рівень
Рівень безпеки	2/5	5/5	4/5

Отримані результати підтверджують, що 2D-біометрія має значні обмеження. Вона придатна для некритичних застосувань — наприклад, швидкого розблокування смартфона, але не для захисту фінансових або корпоративних систем.

Основними виявленими недоліками є:

1. Висока залежність від умов освітлення та позиції обличчя.
2. Відсутність глибинного аналізу, що робить систему вразливою до підробок.
3. Відсутність механізму «liveness detection» (визначення “живого” обличчя).

Для підвищення надійності пропонується:

- впровадження інфрачервоної підсвітки та сенсорів глибини;
- використання моделей машинного навчання, здатних адаптуватися до різних умов зйомки;
- комбінування біометрії з PIN-кодом або токеном у межах мультифакторної автентифікації (MFA);
- додаткове зашифроване зберігання біометричних шаблонів із апаратною ізоляцією (наприклад, Secure Enclave або Knox Vault).

Висновок

1. Оптимальні параметри для стабільної автентифікації — відстань 0.3–0.6 м і фронтальне положення обличчя.
2. При відхиленні понад ± 45° або поганому освітленні точність знижується у 3–10 разів.
3. Технологія 2D Face Unlock не забезпечує достатнього рівня безпеки та не повинна використовуватися як єдиний фактор автентифікації.

4. Найбільш ефективними залишаються системи 3D-розпізнавання, які поєднують IR-сканування, аналіз текстури та мікрорухів.
5. Для забезпечення інформаційної безпеки в критичних ІКС доцільно впроваджувати багатофакторну біометричну ідентифікацію з інтеграцією декількох методів (face + fingerprint + behavioral biometrics).

Список використаних джерел:

1. Jain, A. K., Ross, A., Nandakumar, K. Introduction to Biometrics. - New York: Springer, 2011. - 370 p. (розд. 2, с. 45–72.)

2. ISO/IEC 19795-1:2021. Information technology - Biometric performance testing and reporting - Part 1: Principles and framework. - Geneva: International Organization for Standardization, 2021. - 67 p.

3. Apple Inc. Face ID Security Overview. - Apple Support. URL: https://support.apple.com/en-us/HT208108 (дата звернення: 30.10.2025).

4. Samsung Electronics. Face Recognition and Biometrics Security. - Samsung Knox. URL: https://www.samsungknox.com/en/solutions/biometric (дата звернення: 2.11.2025).

А.М. Котенко,
доцент каф. Технічних систем кіберзахисту,
І.С. Карпенко, студент
Державний університет інформаційно-комунікаційних технологій

ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ МАТЕРИАЛЬНО-РЕЧОВИМ КАНАЛОМ ЩЛЯХОМ ВИКОРИСТАННЯ ТЕХНІЧНИХ СИСТЕМ ОХОРОНИ.

Обробка інформації з обмеженим доступом здійснюється в спеціалізованих приміщеннях – об’єктах інформаційної діяльності (ОІД). Отже загрозою витоку інформації, що зберігається на матеріальних носіях, з об’єкту інформаційної діяльності є крадіжка цього матеріального носія, тобто порушення конфіденційності інформації.

Відомо [1], що технічні системи охорони, (ТСО) встановлені на об'єктах охорони, повинні в комплексі з силами фізичної охорони, забезпечувати захист ОІД від потенційного порушника. В загальному випадку ТСО складаються з наступних елементів [2]: сповіщувачі (засоби виявлення) – чутливі елементи ТСО які реагують на тривожні події (проникнення, або спроба проникнення об’єкт), і характеристики яких визначають основні характеристики всієї ТСО: прилад приймально-контрольний охоронний (ППКО) – пристрій, який отримує сигнал тривоги від сповіщувачів; виконавчі пристрої – агрегати, які забезпечують виконання заданого алгоритму дій системи у відповідь на те чи інше тривожне повідомлення; шлейф охоронний – електрична мережа, яка з’єднує електричні ланцюги сповіщувачів, допоміжні елементи (діоди, резістори і т.і.).

Виникає питання побудови ефективної технічної системи охорони для унеможливлення витоку інформації матеріально-речовим каналом. Для вирішення такого завдання пропонується використання теорію оптимізацію, із застосуванням методу послідовного перебору варіантів систем.

Цільова функція реалізації варіантів ТСО має вигляд:

$$\max\left(\frac{F}{I}\right) = \max\left(\frac{\sum_i f_i}{\sum_i I_i}\right) \quad (1)$$

де:
F – показний корисності i – ої реалізації ТСО;
I – вартість i – ої реалізації ТСО.

Методом послідовного перебору варіантів ТСО знайдемо оптимальний склад ТСО, що задовольняє критерію якості виконання функцій ТСО при мінімальній вартості системи.

Розрахунок показнику корисності кожної складової системи *М* (сповіщувач, ППКОП, виконавчий пристрій) проводиться за виразами лінійної трансформації. Якщо відповідному показнику якості приладу (системи) x_1 більш максимальне значення відповідає більш якісній роботі, то вираз переходу від ненормованого значення показника x_n до нормованого має вигляд:

$$X_n = \frac{x_1 - f_1^{min}}{f_1^{max} - f_1^{\min}}$$

$f_1\text{^}min$і f_1^{max}відповідно абсолютні мінімальне (найгірше) й максимальне (найкраще) значення показника якості роботи серед усіх варіантів;

x_1 – абсолютне значення показника, що нормується.

Якщо для деякого показника x_1 абсолютне мінімальне значення відповідає більш якісному функціонуванню, то вираз трансформації матиме вигляд:

$$X_n = \frac{f_1^{max} - x_1}{f_1^{max} - f_1^{\min}}$$

необхідно визначити вагові коефіцієнти показників якості кожної зі складових ТСО. У найпростішому випадку можна використати метод експертного оцінювання. Далі розраховується показник корисності f_i для кожної складової ТСО, як сума перемножень значимості показника якості на вагу цього показника:

$$f_i = \sum a_i Kc_i \qquad (2)$$

де:

a_i – вага показника якості складової ТСО;

Kc_i – нормоване значення показника якості складової ТСО.

Усього варіантів побудови ТСО у відповідності з методом повного перебору буде:

$$N = \prod_{i=1}^{n} K_i$$

де:

n – число елементів у ТСО;

K – число альтернатив кожного елементу ТСО.

Далі за виразом (1) з урахуванням отриманого показників корисності за виразом (2) та розрахованої вартості кожної з *N* – ої реалізації системи розраховується значення цільової функції для кожної з реалізацій.

За максимальним значенням цільової функції обираємо кращий варіант ТСО.

Список використаних джерел:

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации / Под ред. В.А. Хорошко. – К.: , 2010. –465 с.

2. https://psytest.wordpress.com/data_treatment/normalization_indicator/

А.А. Клен, студент
Державний торговельно-економічний університет

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОВЕДЕННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

В сучасних реаліях задача забезпечення кібербезпеки стає все більш складною через розвиток технологій, зростання вектору атак а також масштабування інформаційно-комунікаційних систем, зокрема через використання генеративних ШІ-моделей для створення коду, що значно спрощує процес для людей без значного досвіду у написанні застосунків. Ця тенденція породжує появу більшої кількості систем із вразливостями внаслідок погано написаного коду.[1]

Враховуючи окреслену проблему, класичне «ручне» тестування на проникнення потребує нового підходу, оскільки цей процес є ресурсомістким. Для оптимізації тестування новітньою практикою є використання ШІ-агентів. Застосування інструментів на основі машинного навчання(ML) чи великих мовних моделей(LLM) дозволяють автоматизувати процес тестування і суттєво зекономити час. Дослідження показують, що LLM можливо залучити до всіх 5 фаз тестування на проникнення: планування, розвідка, експлуатація, стійкість(збереження доступу) та звітування.[2]

Водночас, автоматизація відкриває нові ризики: якість навчання моделей та їх здатність адекватно оцінити середовище, в якому вони працюють – критичні чинники. Часто проблемою є визначення невідомих вразливостей, навченість ШІ стосовно старих специфічних вразливостей, хибні спрацювання, помилки та галюцинування мовних моделей. Саме для уникнення подібних проблем, сучасні підходи йдуть у напрямку гібридних архітектур, що об’єднують людський досвід та штучний інтелект, розподіляючи контроль над процесом(human-in-the-loop). ШІ-агенти виконують рутинні або масштабні завдання(сканування системи, пошук корисних точок входу серед великої кількості інформації), а спеціалісти залишаються залучені для оцінки знайдених вразливостей, прийняття остаточних рішень, управління випадками, що виходять за межі шаблонів.[3]

Висновки: Інтеграція штучного інтелекту у тестування на проникнення має високий потенціал для підвищення ефективності тестування та його масштабування, що цілком виправдано враховуючи сучасні виклики. Однак при впровадженні подібного рішення необхідно забезпечити якісні та релевантні навчальні дані для моделей та використовувати гібридну архітектуру human-in-the-loop, щоб забезпечити ефективність та точність безпекового тестування.

Список використаних джерел:

1. Aalto University. Agentic AI for Penetration Testing – Viktoria Kovalenko. C.9
2. E. Hilario, S. Azam, J. Sundaram, K. I. Mohammed, B. Shanmugam. Generative AI for pentesting: the good, the bad, the ugly. International Journal of Information Security, 2024, 23:2075-2097.[Електронний ресурс] Режим доступу: https://doi.org/10.1007/s10207-024-00835-x
3. Siva Krishna Jampani. Revolutionizing Penetration Testing: AI-Powered Automation for Enterprise Security. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., 10(6):1562-1569, 2024. [Електронний ресурс] Режим доступу: https://ijsrcseit.com/index.php/home/article/view/CSEIT241061201

Т.В. Німченко,
Доцент каф. Технічних систем кіберзахисту,
М.В. Крощенко, студент
Державний університет інформаційно-комунікаційних технологій

ПЕРСПЕКТИВИ ЗАХИСТУ ПРИМІЩЕНЬ ЗА ДОПОМОГОЮ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Актуальність. У сучасному світі питання безпеки прміщень набуває дедалі найбільшої актуальності. Системам відеоспостереження відводиться надзвичайно важлива роль, оскільки вони дозволяють не лише фіксувати несанкціоновану активність, але й забезпечувати перевенцію, створювати докази у разі інциденту, а також інтегруватися з іншими системами безпеки. Саме тому впровадження таких систем має майбутнє і потребує подальшого дослідження.

Сучасні системи відеоспостереження - це не просто камери, які фіксують події. Це розумні комплекси, здатні аналізувати зображення, розпізнавати обличчя, номери автомобілів, відстежувати рух тощо. Застосування штучного інтелекту в цих системах дало змогу суттєво підвищити їх ефективність. Відеоаналітика дозволяє не лише фіксувати події, але й попереджати про потенційні загрози в реальному часі [1, 2].

Історично відеоспостереження пройшло довгий шлях розвитку. Перші камери з'явилися ще в середині двадцятого століття та використовувалися переважно для спостереження за промисловими процесами. У 80-х роках відеокамери почали активно застосовуватись у сфері безпеки, однак їх можливості були обмежені низькою якістю зображення та відсутністю автоматичного аналізу. Сьогодні відеокамери мають високу роздільну здатність, інфрачервоне підсвічування, можливість хмарного запису та віддалений доступ.

Використання відеоспостереження дало змогу значно підвищити рівень безпеки. Камери не лише фіксують правопорушення, але й мають психологічний ефект - запобігають злочинам самим фактом своєї наявности. У юридичному контексті це значно підвищує ймовірність притягнення винних до відповідальности чи відшкодування збитків.

Окрім безпеки, відеоспостереження має важливу роль в оптимізації бізнес-процесів. Грамотний моніторинг робочих процесів, оцінка якости обслуговування, контроль логістики, або аналіз поведінки клієнтів перетворює систему відеоспостереження на багатофункціональний інструмент управління [3].

Для захисту приміщень з підвищенем рівнем контролю найчастіше застосовуються різні типи відеокамер, серед яких виділяють аналогові, цифрові, купольні, корпусні, поворотні та приховані. Аналогові камери забезпечують базову якість зображення та простоту підключення, проте поступаються у гнучкости та роздільній здатності сучасним системам. Цифрові (IP-камери) передають дані через мережу, підтримують високу роздільну здатність та функції відеоаналітики. Купольні камери використовуються в приміщеннях завдяки компактности та антивандальному корпусу, тоді як корпусні - для зовнішнього спостереження, бо мають змінну оптику та кращу стійкість до погодних умов. Поворотні (PTZ) моделі дозволяють віддалено змінювати кут огляду, нахил і масштабування, що зручно для великих об'єктів або великих територій. Приховані камери забезпечують непомітний контроль коли важливо зберегти конфіденційність, або уникнути психологічного тиску на персонал чи відвідувачів.

Висновки. Підсумовуючи, можна стверджувати, що перспективи використання систем відеоспостереження надзвичайно широкі. Завдяки постійному вдосконаленню технологій, впровадженню штучного інтелекту та підвищенню доступності обладнання, ці системи стають

невід'ємною частиною сучасної інфраструктури. Вони забезпечують не лише захист приміщень, а й підвищують ефективність управління, сприяють комфорту, довірі та стабільності у суспільстві.

Список використаних джерел:

1. History of Security Cameras: How Did CCTV Evolve [https://www.dtiq.com/blog/video-surveillance/history-of-security-cameras]
2. First Security Cameras [https://innotech.ge/en/first-security-cameras/]
3. How Surveillance Cameras Evolved from Curiosity to Ubiquity [https://statetechmagazine.com/article/2019/04/how-surveillance-cameras-evolved-curiosity-ubiquity]

А.В. Макаренко, студент УБД-61
Державний університет інформаційно-комунікаційних технологій

СИСТЕМА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

У тезі запропоновано концепцію системи забезпечення кіберстійкості критичної інфраструктури України в умовах гібридних загроз, що поєднують кібератаки, інформаційні операції, фізичні диверсії та ланцюгові ефекти у суміжних секторах. Підхід спирається на сучасні рамкові документи NIST CSF 2.0, NIS2, CER, стандарти безпеки OT/ICS, NIST SP 800-82r3, ISA/IEC 62443, а також на актуальні оцінки загроз ENISA, MITRE ATT&CK for ICS та практичні рекомендації CISA. Досліджено, що інтегроване впровадження принципів Zero Trust, сегментації OT-мереж, безпечного управління активами та сценарійного тренування підвищує здатність КІ запобігати інцидентам, витримувати удари та швидко відновлюватися, зберігаючи безперервність критичних послуг. Основні висновки підкріплені європейськими та національними нормативами щодо КІ.

Надійна система забезпечення кіберстійкості критичної інфраструктури має спиратися на перевірені рамки управління ризиками й чітко пов'язувати технічні контролі з безперервністю суспільно важливих послуг, що системно викладено у NIST Cybersecurity Framework 2.0 з його функціями Govern–Identify–Protect–Detect–Respond–Recover [1]. Для технологічних середовищ особливого значення набувають підходи з безпеки операційних технологій, детально описані в NIST SP 800-82 Rev.3, які вимагають сегментації, урахування специфічних протоколів та безпечного режиму експлуатації контролерів і мостів між IT та OT [2]. Європейський вимір формує директива NIS2, що задає мінімальні заходи керування ризиками, інцидент-репортинг і вимоги до ланцюгів постачання для широкого переліку секторів, уніфікуючи підходи в державах-членах [3]. Комплементарно до цього діє директива CER, яка фокусує увагу на фізичній та операційній стійкості критичних суб'єктів і вимагає національних стратегій, періодичних оцінок ризиків і планів забезпечення стійкості [4]. Україна закріпила правові та організаційні засади захисту КІ Законом №1882-IX, який визначає принципи побудови національної системи, ролі суб'єктів і критерії віднесення об'єктів до критичних [5]. Для промислових систем безпеки застосовуються стандарти ISA/IEC 62443, що пропонують модель зон і каналів, рівні захисту та процесний підхід до розбудови електронно захищених IACS з урахуванням балансу між безпекою та технологічною надійністю [6]. Плануванню оборони допомагає таксономія MITRE ATT&CK for ICS, яка дозволяє моделювати поведінку противника, пріоритезувати виявлення та

формувати сценарні тренування з урахуванням тактик і технік, притаманних OT-середовищам [7].

Реальний контекст загроз демонструє стале зростання складності та кількості інцидентів, що ENISA систематизує у щорічних оглядах ландшафту кіберзагроз із виділенням провідних типів атак і міжсекторних залежностей [8]. Оператори КІ мають підтримувати підвищений рівень готовності, імплементуючи рекомендації CISA «Shields Up» як набір пріоритетних практик для швидкого зміцнення кібергігієни, моніторингу та реагування під час загострення ризиків [9]. Гібридний характер загроз підтверджують і розвіддані європейських партнерів: на тлі фіксації спроб кібератак і саботажів проти об'єктів КІ у країнах ЄС наголошується на картографуванні морської інфраструктури та тестуванні вразливостей у кабельних і енергетичних мережах [10]. Уразливість підводних кабелів, трубопроводів і вітрових парків підсилює потребу в скоординованому нагляді та оперативному виявленні аномалій, адже пошкодження таких ліній здатні спричиняти каскадні збої в економіці та безпеці [11]. Паралельно Європол попереджає про зростання «проксі-активності», коли організована злочинність використовує штучний інтелект для дезінформації, фішингу та технічних атак в інтересах ворожих держав, що ускладнює атрибуцію та пришвидшує цикл загроз [12].

З огляду на це пропонується інтегрована цільова архітектура, де управління ризиками ведеться «governance-first» із чіткими ролями ризик-власників і прив'язкою до бізнес-функцій, а технічна реалізація спирається на сегментацію OT за моделлю зон/каналів, розмежування IT/OT через DMZ та запровадження принципів Zero Trust для доступу персоналу і підрядників. Плавний перехід до таких практик потребує інвентаризації активів, ведення SBOM/ABOM, політик безпечного оновлення, контролю віддалених сесій через брокери з MFA та JIT-привілеями, а також протокольного моніторингу (Modbus, DNP3 тощо) з поведінковою аналітикою. Узгоджене виявлення та реагування підсилюється вбудованими планами безпечного зупину технологічних процесів, офлайн-резервуванням даних і регулярними сценарними тренуваннями за ATT&CK для підвищення колективної спроможності до відновлення. Для міжвідомчої координації доцільно розгорнути обмін індикаторами та тактиками через національні та галузеві CERT/CSIRT, а також проводити міжсекторні «table-top» вправи, що поєднують кібер, фізичні й інформаційні компоненти гібридних сценаріїв. Практична ефективність контролюється метриками на кшталт MTTD/MTTR, відсотка сегментованих вузлів OT, частки доступів із MFA та регулярності тренувань, що дозволяє демонструвати відповідність вимогам і керувати залишковими ризиками на рівні ради директорів.

У підсумку, кіберстійкість КІ формується як безперервний цикл керування ризиками, технологічної дисципліни й спільної оборони, де нормативні опори NIST CSF 2.0, NIS2 і CER поєднуються з доменно-специфічними вимогами NIST SP 800-82 та ISA/IEC 62443 і підкріплюються розвідкою загроз та оперативними ініціативами на кшталт «Shields Up». Такий підхід зменшує імовірність каскадних збоїв, підвищує готовність операторів до витримування ударів і скорочує час відновлення критичних сервісів у середовищі гібридного протистояння.

Список використаних джерел:

1. NIST. The NIST Cybersecurity Framework (CSF) 2.0. URL: https://www.nist.gov/cyberframework

2. NIST. Guide to Operational Technology (OT) Security, SP 800-82 Rev.3. URL: https://doi.org/10.6028/NIST.SP.800-82r3.

3. European Commission. NIS2 Directive: securing network and information systems, 2023–2025. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

4. EUR-Lex. Directive (EU) 2022/2557 on the resilience of critical entities (CER). URL: https://eur-lex.europa.eu/eli/dir/2022/2557.

5. Верховна Рада України. *Закон України «Про критичну інфраструктуру» №1882-IX, 16.11.2021. URL: https://zakon.rada.gov.ua/laws/ show/1882-20.

6. ISA/IEC. ISA/IEC 62443 Series of Standards — Industrial Automation and Control Systems Security. URL: https://www.isa.org/isa62443.

7. MITRE. ATT&CK for ICS: Matrix & Techniques. URL: https://attack.mitre.org/matrices/ics/.

8. ENISA. Threat Landscape — overview of prime threat types and methodology. URL: https://www.enisa.europa.eu/topics/threat-risk-management/ threats -and-trends.

9. CISA. Shields Up — Guidance for Organizations, 2022–2025. URL: https://www.cisa.gov/shields-up.

10. Reuters. Russia is ramping up hybrid attacks against Europe, Dutch intelligence says. URL: https://www.reuters.com/world/europe/russia-ramping-up-hybrid-attacks-against-europe-dutch-intelligence-says-2025-04-22.

11. The Guardian. Undersea ‘hybrid warfare’ threatens security of 1bn, NATO commander warns, 16.04.2024. URL: https://www.theguardian.com/world /2024/apr/16/nato-commander-warns-undersea-hybrid-warfare-threatens-security.

12. Financial Times. Criminals use AI in ‘proxy’ attacks for hostile powers, warns Europol, 18.03.2025. URL: https://www.ft.com/content/ai-proxy-attacks-europol-2025.

В.В. Мацкевич, студент
Державний університет інформаційно-комунікаційних технологій

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ФІЗИЧНОГО РІВНЯ БЕЗПЕКИ В MIMO-СИСТЕМАХ ЗВ’ЯЗКУ

Сучасні інформаційно-телекомунікаційні системи дедалі активніше використовують технології багатоканальної передачі даних. Архітектури з множиною передавальних і приймальних антен (MIMO) лягли в основу стандартів 4G, 5G та формують основу для майбутніх систем шостого покоління (6G). Основними перевагами MIMO є збільшення пропускної здатності, покращення якості обслуговування абонентів та підвищення спектральної ефективності.

Водночас зростання кількості бездротових сервісів породжує нові виклики у сфері безпеки. Традиційні криптографічні методи захисту не завжди можуть ефективно застосовуватись через обмежені обчислювальні ресурси пристроїв Інтернету речей (IoT) та високі вимоги до затримок. Це актуалізує дослідження фізичного рівня безпеки (Physical Layer Security, PLS), що використовує особливості каналу зв’язку для підвищення конфіденційності переданих даних.

Основні підходи до забезпечення фізичного рівня безпеки

Одним із ключових напрямів є використання просторового рознесення сигналів. Наявність декількох антен дозволяє формувати просторові промені (*beamforming*), які забезпечують спрямовану передачу сигналу в сторону легітимного користувача та мінімізують потужність випромінювання у напрямку потенційного зловмисника.

Другим перспективним методом є застосування штучного шуму (*artificial noise*), який накладається на інформаційний сигнал у тих просторових напрямках, де потенційно можуть перебувати зловмисники. Такий підхід ускладнює процедуру коректного декодування для сторонніх приймачів, не погіршуючи якість прийому легітимного абонента.

Важливим завданням є також оптимізація алгоритмів оцінювання каналу. Точне визначення параметрів каналу дозволяє ефективніше реалізовувати просторове кодування та

розподіл потужності. Водночас хибна або навмисно спотворена інформація про канал (наприклад, у результаті атаки типу *pilot contamination*) може призвести до втрати безпеки.

Використання MIMO у захисті від атак

MIMO-системи забезпечують високий рівень стійкості до завад завдяки можливості реалізації адаптивної обробки сигналів. Зокрема, алгоритми просторового фільтрування дозволяють пригнічувати сигнали від сторонніх джерел, тим самим підвищуючи стійкість до *jamming*-атак.

У багатокористувацьких системах важливим завданням є захист від міжкористувацьких перешкод. Застосування методів багатопроменевої обробки (multiuser MIMO) у поєднанні з алгоритмами динамічного розподілу ресурсів дозволяє гарантувати не лише високу пропускну здатність, а й безпечність комунікаційного процесу.

Перспективні напрямки досліджень

Серед актуальних напрямків розвитку фізичного рівня безпеки можна виділити:

- використання методів машинного навчання для виявлення аномалій та атак у каналі зв’язку;
- інтеграцію PLS-алгоритмів у мережі наступних поколінь (5G/6G), зокрема у сценаріях масового підключення IoT;
- поєднання методів PLS із класичними криптографічними підходами для формування багаторівневої системи захисту.

Висновки:

Фізичний рівень безпеки в MIMO-системах є одним із найперспективніших напрямів розвитку телекомунікаційних технологій. Методи просторового кодування, формування променю та штучного шуму дозволяють значно підвищити захищеність інформації без додаткових обчислювальних витрат на рівні абонентських пристроїв. Подальші дослідження у цьому напрямку мають велике значення для створення безпечних і надійних мереж зв’язку майбутнього.

Список використаних джерел:

1. Коваленко О. О., Шматков С. В. Методи просторового кодування та обробки сигналів у MIMO-системах // *Вісник Харківського національного університету радіоелектроніки*. – 2020. – № 3. – С. 45–53.

2. Гавриленко О. І., Сидоренко М. П. Фізичний рівень безпеки у бездротових мережах 5G // *Проблеми телекомунікацій*. – 2021. – № 2. – С. 21–29.

3. Кравченко В. В., Іванченко О. С. Використання адаптивних антенних решіток для підвищення безпеки систем зв’язку // *Наукові праці Одеської національної академії зв’язку*. – 2019. – № 1. – С. 55–61.

А.М. Котенко,
доцент каф. Технічних систем кіберзахисту,
Н.М. Ніколаєв, студент
Державний університет інформаційно-комунікаційних технологій

ЗАХИСТ ІНФОРМАЦІЇ У СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Системи електронного документообігу дозволяють державним службовцям працювати не тільки над виконанням внутрішньовідомчих задач, але і спільними зусиллями вирішувати більш широкий спектр державних проблем та полегшують процес управління знаннями. Відсутність необхідності вручну розмножувати документи, відслідковувати переміщення

паперових документів всередині організації, контролювати порядок передачі конфіденційної інформації істотним образом знижує трудовитрати діловодів, але при цьому виникають певні завдання пов'язані із захистом електронних інформаційних ресурсів [1].

Електронний документообіг це високотехнологічний процес, який включає в себе процеси: створення документів, їх обробку, передачу, збереження, вивід інформації, що циркулює в організації чи підприємстві, на основі використання комп'ютерних мереж. Головним призначенням є організація, збереження електронних документів, а також робота з ними (їх пошук, редагування і т.д.)

Забезпечення конфіденційності досягається наступними послугами [2]: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

Для забезпечення цілісності використовуються послуги: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

Критерій доступності може забезпечуватися в ІКС послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

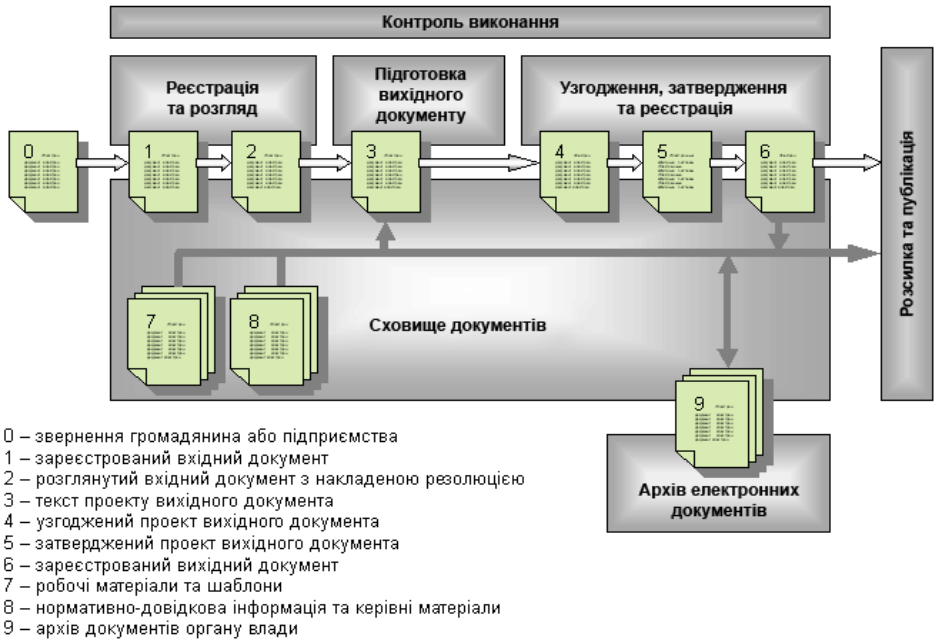

Рис. 1. Схема електронного документообігу організації

З метою забезпечення та підвищення якості захисту інформації у системах електронного документообігу (рис. 1), доцільно застосування наступних кроків: автоматизація ділових процесів, прийом та електронна реєстрація документів, застосування реєстраційно-контрольних карток, організація контролю за виконанням документообігу. Такий підхід реалізовано наприклад у базі даних діловодства "Документ" (рис. 2) [3].

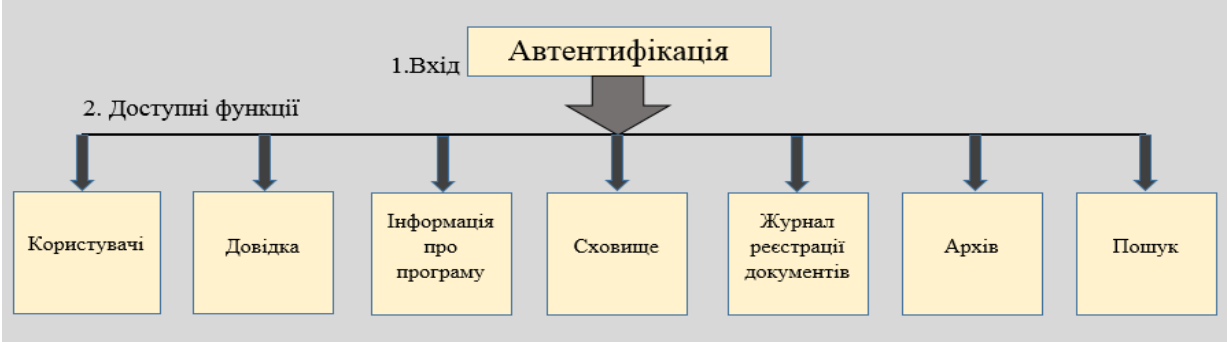

Рис. 2. База даних діловодства "Документ"

Режим *Користувачі* дозволяє адміністратору в будь-який момент змінювати раніше введені дані про користувачів, включаючи видалення користувача із системи. Для зміни пароля користувача, обраного в списку, адміністратор повинен вибрати закладку «Пароль», увести новий пароль і після повторного введення пароля натиснути кнопку «Застосувати». За допомогою функції *Довідка* можна переглянути інформацію щодо користування системою. Режим *Сховище* використовується для перегляду, синхронізації й адміністрування (додавання, видалення, перейменування місць обробки і збереження документів системи (сховищ). Також у даному режимі можливе призначення користувачам доступних сховищ**.** *Журнал реєстрації документів м*ає вкладки «вхідні документи» та «Вихідні документи». Обравши одну з вкладок відкриється таблиця зі списком зареєстрованих документів; текстові поля для відображення реквізитів вибраного документу; функціональні кнопки дій, які можна виконати з обраним документом. *Архів* це своєрідна база, що містить відомості про документи, які зберігаються в архіві, їх розміщення, номер справи, опис, термін зберігання (програма автоматично видає інформацію, що стосується строку зберігання.

Для використання позитивних функціоналів електронного документообігу необхідно використання програмних та апаратних засобів підтримки процесу електронного документообігу.

Список використаних джерел:

1. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення. – К.: Держстандарт України, 1998. – 16 с.

2. Макарчук О.А. Документообіг як основа діяльності органу влади. Визначення термінів [Електрон. ресурс] URL: http//www.atlas.ua/ukr/hum-rm.html

3. Закон України «Про електронні документи та електронний документообіг» ВРУ, 2003

Д.С. Пічкур, студент УБДМ-61
Державний університет інформаційно-комунікаційних технологій

МЕТОДИ ЕТИЧНОГО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ МОНІТОРИНГУ В ІНФОРМАЦІЙНІЙ ТА КІБЕРБЕЗПЕЦІ: БАЛАНС МІЖ ПРИВАТНІСТЮ ТА НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ

Методи етичного використання технологій моніторингу в інформаційній та кібербезпеці вимагають балансу між захистом приватності та забезпеченням національної безпеки, оскільки сучасні інструменти спостереження, аналізу даних і штучного інтелекту ефективно виявляють загрози, але часто конфліктують з індивідуальними правами, викликаючи ризики надмірного нагляду, зловживань і дискримінації. Для вирішення цих проблем необхідно впроваджувати етичні підходи, включаючи правові рамки, технічні заходи приватності та суспільний контроль, що дозволить зберегти довіру та уникнути порушень прав людини в цифровому середовищі.

У сучасному цифровому світі, де кіберзагрози стають дедалі складнішими та глобальними, технології моніторингу, такі як системи спостереження, аналіз даних і штучний інтелект, відіграють ключову роль у забезпеченні інформаційної та кібербезпеки, дозволяючи виявляти загрози на ранніх етапах і захищати критичну інфраструктуру. Однак їхнє використання часто вступає в конфлікт з правом на приватність, викликаючи етичні дилеми, такі як надмірний нагляд, потенціал зловживань і ерозія громадянських свобод, що вимагає пошуку балансу між колективною безпекою та індивідуальними правами.[1] Це зумовлено швидким розвитком технологій, як-от біометрія та AI-аналітика, які посилюють можливості моніторингу, але також підвищують ризики, наприклад, створення "суспільства нагляду" чи дискримінації через упереджені алгоритми, як це видно з викриттів Едварда Сноудена в 2013

році щодо масового збору даних NSA.[2] Без етичних методів ці інструменти можуть призвести до втрати довіри до влади, соціальних нерівностей і навіть порушень людських прав, особливо в контексті пандемій, як COVID-19, коли контакт-трекінг став нормою, але без належного контролю загрожував приватності.

Етичні виклики в використанні технологій моніторингу включають конфлікт між національною безпекою та приватністю, де масове спостереження, як у програмах типу PRISM, може запобігати тероризму, але порушує автономію індивідів, створюючи профілі без згоди. Наприклад, AI-системи для передбачення загроз аналізують поведінкові патерни, але якщо треновані на упереджених даних, вони можуть дискримінувати певні групи, як у випадку з передбачувальною поліцією, що посилює расові стереотипи. Правові рамки, такі як GDPR в ЄС, що вимагає згоди, мінімізації даних і оцінок впливу на приватність (PIA), намагаються вирішити ці проблеми, але прогалини існують, наприклад, у США з фрагментарними законами на кшталт CISA чи Patriot Act, які дозволяють широкий доступ до даних для безпеки, але недостатньо захищають приватність. У Китаї Cybersecurity Law фокусується на державному контролі, що часто ігнорує індивідуальні права, тоді як в Індії справа Puttaswamy визнала приватність фундаментальним правом, вимагаючи пропорційності в моніторингу. Ці приклади показують необхідність гармонізованих міжнародних стандартів, аби уникнути зловживань, як у системі соціального кредиту в Китаї, де моніторинг пригнічує інакодумство.

Методи етичного використання включають "privacy by design", де приватність інтегрується з самого початку, наприклад, через енд-то-енд шифрування, анонімізацію даних і диференційну приватність, яка додає шум до запитів, аби запобігти ідентифікації. У кібербезпеці це означає обмеження моніторингу легітимними цілями, з обов'язковими аудитами та прозорістю, як у рекомендаціях NIST чи ISO 27001, де організації проводять PIA перед впровадженням систем спостереження. Наприклад, у боротьбі з кібератаками AI може виявляти аномалії в мережевому трафіку без доступу до особистих даних, використовуючи гомоморфне шифрування для аналізу зашифрованої інформації. Поведінковий аналіз фіксує відхилення, як незвичайний доступ до баз даних, але етично вимагає згоди та мінімізації збору, аби не створювати профілі без потреби. Громадська участь, через діалоги та незалежний нагляд, допомагає будувати довіру, як у випадку з реформами після Сноудена, де Freedom Act обмежив масовий збір даних.

Інтеграція цих методів у корпоративну та державну інфраструктуру створює багатошаровий підхід, де моніторинг захищає від загроз, як DDoS чи ransomware, але не порушує права, наприклад, через блокчейн для прозорого зберігання даних чи нульового довіри моделі, де доступ перевіряється постійно. У перспективі, з розвитком IoT та AI, етичні рамки мусять адаптуватися, впроваджуючи міжнародну співпрацю, як у Five Eyes чи EU Cybersecurity Act, аби балансувати безпеку з приватністю. У підсумку, етичне використання технологій моніторингу можливе через комбінацію правових, технічних і суспільних заходів, що забезпечують пропорційність і прозорість, дозволяючи захищати національну безпеку без значного ущемлення приватності та сприяючи стійкому цифровому суспільству.

Список використаних джерел:

1. Ethics of Surveillance Technologies: Balancing Privacy and Security in a Digital Age / Premier Science. 2024. URL: https://premierscience.com/pjds-24-359/

2. The case of Edward Snowden URL: https://www.whistleblowers.org/news/the-case-of-edward-snowden/

3. Analysis of the Impact of the USA PATRIOT Act, CISA, and Gag Orders on Privacy URL: https://vpnpick.com/non-us-based-vpn/

А.М. Котенко,
доцент каф. Технічних систем кіберзахисту,
М.М. Площинський, студент
Державний університет інформаційно-комунікаційних технологій

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ЗА РАХУНОК ВИКОРИСТАННЯ ЦИФРОВИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ.

Системи відеоспостереження (СВ) знайшли широке застосування в усіх галузях людської діяльності починаючи від безпеки власного житла і закінчуючи сучасною інфраструктурою (кінотеатри, аеропорти, банки, торгові центри та навіть стали однією зі складових проекту «безпечне місто»). Зважаючи на швидкість розвитку нового світу, завдяки досягненням науки і техніки, було створено СВ, в яких втілено інтелектуальні функції, що дозволяють відстежувати рухомі об'єкти, аналізувати траєкторію руху, нестандартну поведінку, автоматично реєструвати можливі потенційно небезпечні предмети. Використання систем відеоспостереження для захисту інформації від витоку матеріально-речовим відображено наприклад у публікації [1].

Склад типової СВ показано на рис. 1

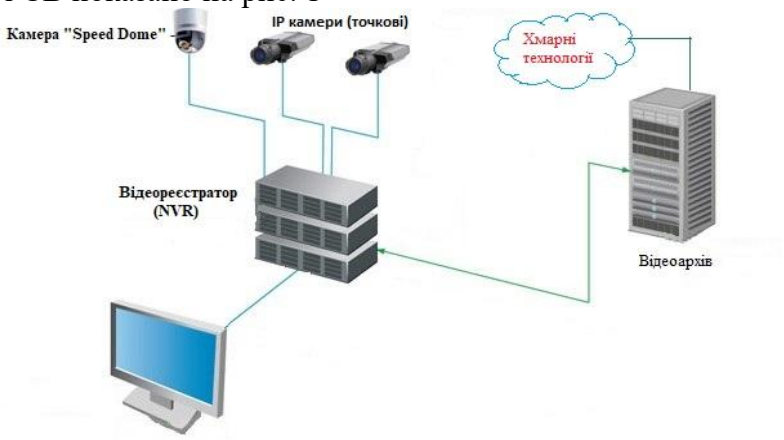

Рис. 1. Склад системи відеоспостереження

До складу СВ входять відеокамери та пристрій реєстрації відеоінформації. СВ бувають локальні і з можливістю віддаленого доступу. СВ бувають цифрові та аналогові. Цифрова система відео спостереження (ЦСВ) це це сучасна технологія, яка використовує цифрові камери (IP-камери) для отримання, передачі, запису та віддаленого перегляду відеоматеріалів. На відміну від аналогових систем, цифрові пропонують вищу якість зображення, гнучкість, розширені можливості та легкість керування через інтернет.

Типова ЦСВ складається з наступнихвих елементів:

- цифрові (IP) відеокамери. Їх функцією є: отримання зображення, перетворення його у цифровий сигнал. Вони можуть підключатися до мережі як через кабель (Ethernet), так і бездротовим способом;

- відеореєстратор (NVR). Мережевий відеореєстратор, який отримує інформацію від IP-камер, зберігає її на жорсткому диску та керує системою;

- Мережеве обладнання**.** Комутатори, маршрутизатори та проаводні лінії (для проводних систем) або Wi-Fi-точки доступу (для безпроводних) для інформаційного обміну;

- Програмне забезпечення для керування, налаштування та перегляду відео. Воно може бути встановлене на комп'ютер або доступне через веб-інтерфейс чи мобільний застосунок.

Застосування цифрових технологій у СВ дозволяє здійснювати:

- Серверну відеоаналітику - централізовану обробку відеоданих на сервері. Основною перевагою серверної відеоаналітики є можливість комбінування алгоритмів відеоаналітики на одній апаратній платформі.

- Вбудовану відеоаналітику - реалізується безпосередньо в джерелі відеоданих, тобто в камерах і кодерах. Головна перевага вбудованої відеоаналітики полягає в зменшення навантаження на канали зв'язку і на сервер обробки відеоданих. У порівнянні з серверною відеоаналітикою, вбудована відеоаналітика дозволяє збільшити ефективність використання каналів зв'язку і серверів.

- Розподілену відеоаналітику - гібридне рішення між серверної і вбудованою відеоаналітикою, в якому обробка розподілена між джерелом відеоданих і центральним устаткуванням. Наприклад, в системи багатокамерного стеження, виявлення об'єктів проводитися в джерелі відеоданих, а зіставлення результатів між декількома джерелами - на сервері.

Основні переваги ЦВС перед аналоговими [2].

Висока якість зображення. Цифрові камери забезпечують високу роздільну здатність, чіткість і деталізацію, що значно підвищує ефективність спостереження.

Віддалений доступ. Можливість переглядати відео в реальному часі з будь-якої точки світу через інтернет, використовуючи смартфон або комп'ютер.

Розширені функції. Багато IP-камер мають вбудовані інтелектуальні функції, такі як розпізнавання руху, аналітика відео, розпізнавання облич, що робить систему ще ефективнішою.

Гнучкість та масштабованість. СВ легко розширювати, додаючи нові камери без необхідності прокладання додаткових кабелів до відеореєстратора.

Таким чином можна зробити висновок про необхідність використання ЦСВ для захисту інформації, що у поєднанні з перевагами цифрових технологій робить їх якісним засобом.

Список використаних джерел:

1. Котенко А.М., Запобігання витоку інформації з обмеженим доступом матеріально-речовим каналом за рахунок використання систем відеоспостереження – К:. Сучасний захист інформації № 1, 2017.

2.https://bezpeka.com.ua/ua/stati/chem-otlichaetsya-analogovoe-i-tsifrovoe-videonabludenie/?srsltid=AfmBOootZoddAf_mIJ5jjtejfcbEBx4EDw4EQDPa08I-J2klusok8pu8

Г.І. Рибачок, полковник
Національний університет оборони України
ад'юнкт кафедри кіберборотьби

ПАСПОРТ МЕТРИК РЕАКЦІЇ НА КІБЕРІНЦИДЕНТИ ДЛЯ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ: ВІД MTTD/MTTR ДО ОХОПЛЕННЯ УРАЖЕНЬ

Органи військового управління (ОВУ) оперують у середовищі з високою інтенсивністю загроз і вимогами до часу реагування. Класичні показники Mean Time to Detect (MTTD) і Mean Time to Respond/Recover (MTTR) лишаються базовими, але не відображають реального «покриття загроз» та якості детекції. Доцільно розширювати паспорт метрик через прив’язку до життєвого циклу інцидентів за NIST SP 800-61r3, узгодження з NIST CSF 2.0 та впровадження програми вимірювань за NIST SP 800-55 [1–3; 8–9]. З огляду на практику CSIRT/SOC у держсекторі, варто вводити метрики effective coverage ATT&CK, якості сигналів і готовності плейбуків [4–7; 10].

Постановка проблеми. Типовий набір показників у більшості ОВУ фокусується на швидкості реагування, ігноруючи: 1) ступінь покриття технік противника; 2) надмірність/перекриття контролів без приросту ефективності; 3) якість оповіщень (precision/recall) та навантаження на аналітиків; 4) узгодженість метрик із регуляторними вимогами та сумісність міжвідомчих обмінів [1–3; 5–7].

Мета і завдання. Мета — сформувати паспорт метрик реакції на кіберінциденти для ОВУ, що поєднує часові, метрики покриття та якісні показники, сумісні з NIST CSF 2.0 та ISO/IEC 27035-1/-2.

Завдання:

- визначити таксономію метрик;
- запровадити індикатори effective coverage з урахуванням перекриття контролів;
- встановити пороги рішень;
- продемонструвати застосування на синтетичному прикладі [1–4; 8–10].

Методи

Основа — модель життєвого циклу інцидентів у SP 800-61r3 з мапуванням на функції CSF 2.0 (Govern-Identify-Protect-Detect-Respond-Recover) [1–2]. Процес вимірювань — за SP 800-55 (вибір, операціоналізація, програмне впровадження, звітність) [8–9]. Покриття загроз оцінюється через матрицю «техніка ATT&CK × контроль» [5]. Ролі/послуги SOC/CSIRT — за FIRST CSIRT Services Framework v2.1 [6]. Готовність плейбуків і відповідність звітуванню — за CISA Playbooks та рекомендаціями ENISA/NIS2 [7; 10].

Основна частина.

1) Таксономія метрик паспорта.

Часові: MTTD, MTTA (acknowledge), MTTC (contain), MTTR (recover), dwell time [1–2].

Метрики покриття: raw coverage (частка пріоритетних технік ATT&CK з ≥1 детектором), effective coverage (EC) з урахуванням зменшення віддачі від дублювання; redundancy index (середня кількість контролів на техніку) [5].

Якісні: precision/recall алертів; частка автоматизованих дій; частка інцидентів з валідованою TTP-прив'язкою; відповідність плейбуків і частота навчань/тестів [1–2; 7–9].

Організаційні: покриття ролей/змін, час ескалації, узгодженість форматів обміну (STIX/TAXII) [1; 6–7].

Таблиця 1.

Паспорт базових метрик для ОВУ (фрагмент)

Код	Метрика	Визначення	Одиниці	Джерело даних	Орієнтир/поріг*	Призначення
T-1	MTTD	середній час від події до детекції	хв	SIEM/EDR/NDR	≤15 хв (High)	швидкість виявлення [1–2]
T-2	MTTR	середній час до відновлення сервісу	год	тикети/CMDB	≤24 год (High)	швидкість відновлення [1–2]
C-1	Raw coverage	частка пріоритетних технік з ≥1 детектором	частка	матриця ATT&CK× контроль	≥0.85	повнота покриття [5]
C-2	EC (effective coverage)	покриття з урахуванням зменшення віддачі від дублювання	частка	те саме	≥0.80	реальна «сила» покриття [1;5]
Q-1	Precision	TP/(TP+FP) по High-alerts	частка	SOC QA	≥0.70	якість сигналу [8–9]

Q-2	Recall	TP/(TP+FN) по High-інцидентах	частка	пост-мортеми	≥0.60	повнота спрацювань [8–9]
O-1	Playbook readiness	частка сценаріїв з актуальним плейбуком і тренуванням ≤90 днів	частка	SOAR/wiki	≥0.90	готовність реагування [7;10]

● Пороги — стартові для пілотного впровадження; коригуються за класом систем та об'єктів [1–2; 7].

2) Метрична модель «effective coverage».

Нехай (T) — множина пріоритетних технік ATT&CK, (n_t) — кількість незалежних детекторів для техніки (t). Введено граничну віддачу від дублювання: [EC = \frac{1}{|T|} \sum_{t \in T} \left(1 - \alpha^{,n_t}\right),\quad \alpha \in (0,1).] За (n_t=1) внесок дорівнює (1-альфа); додаткові детектори дають щораз менше, стимулюючи диверсифікацію покриття [1;5;8].

3) Мапування метрик на життєвий цикл.

Таблиця 2.

Прив'язка метрик до функцій CSF 2.0 та фаз ISO/IEC 27035

Функція CSF 2.0	**Фаза ISO 27035**	**Ключові метрики**
Govern/Identify	планування/готовність	O-1, покриття ролей, SLA ескалації [2–4;6]
Protect	превентивні контролі	частка активних плейбуків на превентивні дії [2;7]
Detect	виявлення	T-1, Q-1, Q-2, C-1, C-2 [1–2;5;8]
Respond	стримування/усунення	MTTC, частка автоматизованих дій, час кореляції [1–2;7]
Recover	відновлення/уроки	T-2, RTO-критика, частота уроків [1–4]

4) Синтетичний приклад (ОВУ-SOC).

Набір (T) з 25 пріоритетних технік ATT&CK. Елементи покриття: EDR (18 технік), NDR (12), SIEM-правила (14). Об'єднання дає raw coverage (=22/25=0{.}88). Розподіл (n_t): 10 технік — 1 детектор, 9 — два, 3 — три, 3 — нуль. За (\alpha=0{.}5): [EC = \tfrac{1}{25}\bigl(10\cdot0{.}5 + 9\cdot0{.}75 + 3\cdot0{.}875 + 3\cdot0\bigr) = 0{.}755.] Ефективне покриття ≈ 0.76; слід додати незалежні детектори на 3 «сліпі» техніки та зменшити зайве дублювання [1;5;8].

5) Практичні пороги для старту (High-severity).

- **MTTD ≤ 15 хв**, **MTTC ≤ 60 хв**, **MTTR ≤ 24 год**; медіана dwell time ≤ 24 год [1–2; 7].
- **Raw coverage ≥ 0.85**, **EC ≥ 0.80** на наборі пріоритетних технік [1;5].
- **Precision ≥ 0.70**, **Recall ≥ 0.60** на High-alerts; FP/аналітик/год ≤ 4 [8–9].
- **Playbook readiness ≥ 0.90**, тренування кожні ≤ 90 днів; відповідність форматів обміну [7;10].

Висновок.

Запропонований паспорт метрик поєднує часові, метрики покриття та якісні показники, узгоджені з NIST CSF 2.0 та ISO/IEC 27035. Введення ЕС дозволяє уникати хибного відчуття «повноти» при дублюванні контролів і фокусує ОВУ на реальних «сліпих зонах». Пілотні пороги підлягають адаптації під класи систем і оперативні режими [1–5; 7–10].

Список використаних джерел:

1. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST SP 800-61r3. Gaithersburg, MD: NIST, 2025. DOI: 10.6028/NIST.SP.800-61r3. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final (data звернення: 28.10.2025).
2. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD: NIST, 2024. DOI: 10.6028/NIST.CSWP.29. URL: https://www.nist.gov/cyberframework (data звернення: 28.10.2025).
3. ISO/IEC 27035-1:2023. Information technology — Information security incident management — Part 1: Principles of incident management. Geneva: ISO/IEC, 2023. URL: https://www.iso.org/standard/78973.html (data звернення: 28.10.2025).
4. ISO/IEC 27035-2:2023. Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response. Geneva: ISO/IEC, 2023. URL: https://www.iso.org/standard/78974.html (data звернення: 28.10.2025).
5. MITRE ATT&CK® Enterprise Matrix. MITRE, 2025. URL: https://attack.mitre.org/matrices/enterprise/ (data звернення: 28.10.2025).
6. FIRST. CSIRT Services Framework, Version 2.1. Forum of Incident Response and Security Teams, 2023–2025. URL: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1 (data звернення: 28.10.2025).
7. CISA. Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Washington, DC: CISA, 2024. URL: https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks (data звернення: 28.10.2025).
8. Schroeder K., Trinh H., Pillitteri V. Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures. NIST SP 800-55 v1. Gaithersburg, MD: NIST, 2024. DOI: 10.6028/NIST.SP.800-55v1. URL: https://csrc.nist.gov/pubs/sp/800/55/v1/final (data звернення: 28.10.2025).
9. Schroeder K., Trinh H., Pillitteri V. Measurement Guide for Information Security: Volume 2 — Developing an Information Security Measurement Program. NIST SP 800-55 v2. Gaithersburg, MD: NIST, 2024. DOI: 10.6028/NIST.SP.800-55v2. URL: https://csrc.nist.gov/pubs/sp/800/55/v2/final (data звернення: 28.10.2025).
10. ENISA. Technical Implementation Guidance on Cybersecurity Risk Management Measures (v1.0). European Union Agency for Cybersecurity, 2025. URL: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance (data звернення: 28.10.2025).

О.М. Кодимський, студент УБДМ-61
Державний університет інформаційно-комунікаційних технологій

БАЛАНС МІЖ БЕЗПЕКОЮ ТА ПРИВАТНІСТЮ: ЕТИЧНІ ДИЛЕМИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРЗАХИСТІ

Розвиток технологій штучного інтелекту (ШІ) відкриває нові можливості для забезпечення кібербезпеки, особливо у сфері захисту критичних інформаційних систем. Проте впровадження таких технологій супроводжується низкою етичних викликів, пов'язаних із захистом приватності, автономністю прийняття рішень, а також відповідальністю за наслідки дій автоматизованих систем. Кіберзагрози стають дедалі складнішими, а атаки на критичну інфраструктуру — більш цілеспрямованими та руйнівними. Традиційні методи захисту, засновані на людському контролі, вже не забезпечують необхідного рівня реагування. Саме тому штучний інтелект розглядається як ключовий інструмент для автоматизації моніторингу, виявлення аномалій і запобігання атакам у режимі реального часу [1]. Водночас зростає ризик того, що надмірна автоматизація процесів без належного етичного контролю може призвести до зловживань, порушення приватності користувачів і навіть дискримінаційних рішень.

Однією з центральних етичних проблем є конфлікт між безпекою та правом на приватність. Для ефективного функціонування систем ШІ у сфері кіберзахисту необхідний збір і аналіз великих обсягів даних, включно з особистими. Це створює ризик надмірного втручання у приватне життя громадян, особливо у випадках, коли системи моніторингу працюють без прозорих критеріїв або з обмеженим доступом до механізмів контролю. Таким чином, виникає потреба у визначенні меж допустимого спостереження, що не суперечитиме етичним і правовим нормам.

Другою важливою дилемою є питання автономності та відповідальності. Якщо система ШІ самостійно приймає рішення щодо блокування підозрілих дій або нейтралізації кіберзагроз, хто несе відповідальність у разі помилки — розробник, оператор чи сама система? Проблема ускладнюється тим, що алгоритми машинного навчання часто є «чорними скриньками», тобто процес прийняття рішень не є прозорим для користувача [2]. Така непрозорість може призвести до ситуацій, коли кіберзахисна система виявляє не лише атаки, а й законні дії, порушуючи при цьому права користувачів.

Ще один аспект — етичний контроль та довіра до технологій. Ефективність ШІ у сфері безпеки значною мірою залежить від довіри суспільства. Якщо громадяни не розумітимуть принципів роботи таких систем або сумніватимуться в їх неупередженості, це може призвести до відторгнення технологій навіть попри їхню користь. Тому необхідно розробляти політику прозорості — пояснювати, як і для чого використовуються алгоритми, яким чином забезпечується захист даних та запобігання зловживанням.

Важливу роль у розв'язанні цих дилем відіграють етичні стандарти та нормативне регулювання. У світі вже ведуться активні дискусії щодо створення універсальних принципів етики ШІ (наприклад, ініціативи UNESCO чи Європейської комісії) [3]. Для України актуальним є формування національних підходів до етичного регулювання, що враховували б як міжнародні стандарти, так і специфіку українського кіберпростору.

Застосування ШІ у сфері кіберзахисту відкриває широкі перспективи для підвищення безпеки критичних систем. Проте ефективність таких рішень залежить від того, наскільки вони впроваджуються з урахуванням етичних принципів. Баланс між безпекою та приватністю повинен стати ключовим орієнтиром при розробці, впровадженні й контролі технологій ШІ. Лише за умови прозорості, відповідальності та поваги до прав людини штучний інтелект зможе стати надійним інструментом захисту, а не потенційним джерелом нових загроз.

Список використаних джерел:

1. Peltz J., Street A. C. Artificial intelligence and ethical dilemmas involving privacy. *Artificial intelligence and global security*. 2020. P. 95–120. URL: https://doi.org/10.1108/978-1-78973-811-720201006

2. Cyber security risk assessment and management using artificial intelligence and machine learning / S. Ganesan et al. *Advances in information security, privacy, and ethics*. 2023. P. 198–217. URL: https://doi.org/10.4018/978-1-6684-9317-5.ch010

3. Mann G., Anglina, Gaur P. Ethical consideration regarding patient privacy and data security. *Advances in cancer detection, prediction, and prognosis using artificial intelligence and machine learning*. Singapore, 2025. P. 383–406. URL: https://doi.org/10.1007/978-981-96-9346-7_17

О.О. Верголяс, Лейтенант, к.ю.н, старший викладач,
Харківський національний університет Повітряних сил України

ЗАХИСТ LLM У КІБЕРБЕЗПЕЦІ: ЗАГРОЗИ, МОДЕЛІ АТАК І ПРАКТИЧНІ КОНТРЗАХОДИ

Генеративні моделі великого масштабу (LLM) стрімко інтегруються в IT-сервіси та операції безпеки. Паралельно формується окремий клас загроз: ін’єкції промптів, несанкціонований доступ до інструментів (tooling), ексфільтрація конфіденційних даних через вивід моделі, отруєння даних і зловмисні залежності в ланцюзі постачання моделей. Галузеві ініціативи вже систематизують типові ризики та практики захисту [1–5].

Постановка проблеми. Класичні підходи до безпеки застосунків не враховують поведінкову природу LLM і контекстне виконання інструкцій. Системи з агентською логікою та інструментами розширюють площину атаки: достатньо нав’язаного промпту або композиції вразливостей, щоб модель виконала небезпечну дію. Потрібні специфічні архітектурні й процесні контрзаходи з урахуванням загроз і рекомендацій OWASP/MITRE [1–3].

Мета і завдання. Мета — запропонувати практичний набір архітектурних, процесних і правових контрзаходів для безпечної експлуатації LLM. Завдання: (1) зіставити спектр загроз за OWASP LLM Top-10 та MITRE ATLAS; (2) окреслити архітектурні патерни ізоляції та санітизації; (3) адаптувати вимоги відповідності за AI Act і профілем NIST AI RMF для генеративних систем [4–5, 7].

Методологія. Аналіз побудовано на відкритих рамках: OWASP GenAI/LLM Top-10 (2025), MITRE ATLAS (таксономія технік атак на ШІ), NIST AI RMF 1.0 та Generative AI Profile (NIST AI 600-1), а також нормах ЄС (AI Act) і аналітиці ENISA ETL 2024 [1–7]. Рекомендації структуровано за принципами «захист через дизайн», розділення довіри та найменших привілеїв.

Основні результати.

1) Модель загроз для LLM-систем: ін’єкції промптів і непрямі ін’єкції; інструментальні атаки; отруєння даних; витік даних через вивід/журнали/аналітику; підміна/екфільтрація моделей і ваг; ескалація через інтеграції [1–3].

2) Архітектурні контрзаходи: ізоляція LLM-ядра від інструментів; політики маршрутизації та явні переліки дозволених дій; санітизація введення/виводу (включно з детекторами prompt-injection); маркування даних і контроль доступу до секретів; контейнери з найменшими привілеями; токен-бюджети і дроселювання; захист ланцюга постачання (SBOM/MBOM, підпис артефактів) [1–3].

3) Процесні практики: LLM-red teaming із каталогом сценаріїв; політики використання і заборонених дій; навчання користувачів щодо непрямих ін’єкцій; аудит відповідності для високоризикових застосувань [1, 6–7].

4) Відповідність і управління: узгодження контролів із NIST AI RMF та профілем для генШІ; мапінг правових вимог AI Act на технічні й організаційні заходи [4–5, 7].

Обговорення. Ключовий компроміс — між функціональністю та безпекою в системах з агентською поведінкою. Сувора ізоляція інструментів і підтвердження дій зменшують ризики, але коштують часу й UX. Першочерговим є контроль вихідних каналів, дефолт-відключення небезпечних інструментів та поетапне впровадження політик [1–3, 8].

Висновки.

Захист LLM поєднує класичні засоби кібербезпеки і специфічні для ШІ контролі. Гармонізація з OWASP GenAI, MITRE ATLAS, NIST AI RMF і AI Act забезпечує технічну та регуляторну узгодженість. Практичний пріоритет — санітизація, ізоляція інструментів, простежуваність даних і регулярний LLM-red teaming [1–7].

Список використаних джерел:

1. OWASP. Top 10 for Large Language Model Applications. URL: https://owasp.org/www-project-top-10-for-large-language-model-applications/ (дата звернення: 29.10.2025).

2. OWASP. Top 10 for LLM Applications (v2025). URL: https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-v2025.pdf (дата звернення: 29.10.2025).

3. MITRE. ATLAS — Adversarial Threat Landscape for AI Systems. URL: https://atlas.mitre.org/ (дата звернення: 29.10.2025).

4. NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). URL: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf (дата звернення: 29.10.2025).

5. NIST. Generative AI Profile for the AI RMF (NIST AI 600-1). URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf (дата звернення: 29.10.2025).

6. ENISA. ENISA Threat Landscape 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 29.10.2025).

7. European Union. Regulation (EU) 2024/1689 (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення: 29.10.2025).

8. NIST. Computer Security Incident Response Recommendations and Considerations (SP 800-61 Rev.3). URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf (дата звернення: 29.10.2025).

Д.О. Кондратюк, студент УБДМ-51
Державний університет інформаційно-комунікаційних технологій

МЕХАНІЗМИ УПРАВЛІННЯ ІКІБЕРБЕЗПЕКОЮ З УРАХУВАННЯМ ПСИХОЛОГІЧНИХ АСПЕКТІВ ПОВЕДІНКИ КОРИСТУВАЧІВ

Кібербезпека — це битва технологій, але найчастіше вона програється через одну вразливість: людину. Традиційні механізми захисту зосереджені на IT-інструментах, систематично ігноруючи психологічні аспекти (стрес, втома, когнітивні упередження), які роблять користувачів мішенями соціальної інженерії.

Ця теза досліджує, як інтегрувати глибинні знання про людську поведінку у процеси управління кібербезпекою. Ми пропонуємо механізми, які не карають за помилки, а змінюють поведінку на рівні свідомості, перетворюючи співробітників зі "слабкої ланки" на ключовий елемент захисту.

У сучасному цифровому середовищі, де захисні периметри організацій розмиваються, а обсяги даних зростають експоненційно, парадокс кібербезпеки стає все більш очевидним: ми інвестуємо мільярди у найсучасніші фаєрволи, системи виявлення вторгнень та шифрування,

але 90% успішних кібератак досі починаються з елементарної соціальної інженерії та людської помилки.

Найдосконаліший технологічний захист є безсилим перед натисканням користувачем на фішингове посилання, спричиненим поспіхом, втомою чи страхом. Отже, людський фактор є не просто ризиком, а фундаментальною точкою відмови в системі кіберзахисту.

Проблема є критичною і має реальні наслідки на національному та корпоративному рівнях. Яскравим прикладом є атака на американську компанію Colonial Pipeline у 2021 році, яка забезпечує паливом значну частину Східного узбережжя США. Кіберзлочинці отримали доступ до її мережі через компрометацію облікового запису VPN, який, як виявилося, не був захищений двофакторною автентифікацією (MFA). Це був не злам коду, а людський недогляд у налаштуванні безпеки, що призвів до зупинки критично важливої інфраструктури та паніки на ринку палива.

Інший показовий випадок — злам компанії RSA у 2011 році, світового лідера у сфері кібербезпеки та виробника SecurID-токенів. Атака почалася з фішингового листа, надісланого двом групам співробітників. Зміст листа був настільки невинним, що його навіть не заблокували спам-фільтри. Зрештою, один зі співробітників відкрив вкладення, дозволивши хакерам отримати контроль над мережею. Цей інцидент продемонстрував, що навіть експерти з кібербезпеки вразливі до психологічної маніпуляції, а наслідком стала компрометація даних мільйонів корпоративних клієнтів RSA по всьому світу.

Проблема кібербезпеки у 21 столітті більше не є суто технічною; це криза менеджменту людської поведінки. Ми дійшли висновку, що традиційні технологічні бар'єри не здатні захистити організацію, якщо не усунуто першопричину — психологічну вразливість співробітників.

Список використаних джерел:

1. Стаття «Докладно про кібератаку на Colonial Pipeline» URL: https://ussd.org.ua/2021/06/03/dokladno-pro-kiberataku-na-colonial-pipeline

2. Стаття «Що таке фішинг та як від нього захиститися» URL: https://whitepay.com/uk/news/shho-take-fishing-ta-yak-vid-nogo-zahistitisya

М. В. Чайка, студент
Державний торговельно-економічний університет м. Київ, Україна

OSINT ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВНИХ СТРУКТУР

Ключові слова: OSINT, кібербезпека, розвідка з відкритих джерел, державна безпека, інформаційна розвідка.

У сучасному світі, де інформаційна війна стає ключовим елементом гібридних конфліктів, інструменти OSINT (Open Source Intelligence) відіграють важливу роль у забезпеченні кібербезпеки державних структур. OSINT передбачає збір, аналіз та інтерпретацію даних з відкритих джерел, таких як соціальні мережі, новинні ресурси, державні реєстри, супутникові знімки та інші публічні бази даних.

Використання OSINT у державному секторі дозволяє своєчасно виявляти потенційні кіберзагрози, моніторити інформаційні операції, ідентифікувати джерела витоку даних і виявляти фейкові інформаційні кампанії. Завдяки цьому державні структури можуть формувати обґрунтовану систему реагування на кібератаки та мінімізувати ризики дестабілізації критичної інфраструктури.

Ключовими напрямами використання OSINT є: моніторинг соціальних медіа, аналіз мережевої активності, геолокаційна розвідка, а також автоматизований аналіз великих обсягів

даних за допомогою інструментів, таких як Maltego, Shodan, theHarvester, SpiderFoot та Recon-ng. Поєднання цих рішень із системами штучного інтелекту дозволяє створювати прогностичні моделі та прогнозувати потенційні інциденти.

Ефективне впровадження OSINT у діяльність державних структур вимагає дотримання етичних та правових норм, зокрема Закону України «Про основні засади забезпечення кібербезпеки України» та міжнародних стандартів ENISA. Крім того, важливо забезпечити належну підготовку кадрів, здатних працювати з відкритими джерелами у рамках державної кіберрозвідки.

Таким чином, OSINT виступає не лише інструментом інформаційної розвідки, а й фундаментальним елементом стратегічної кібероборони держави, який дозволяє своєчасно виявляти загрози, запобігати кібератакам та підвищувати загальну стійкість інформаційних систем публічного сектору.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. ENISA. Open Source Intelligence (OSINT) Tools. URL: https://www.enisa.europa.eu

3. Maltego Documentation. URL: https://docs.maltego.com

В.І. Богом'я,
д.т.н., професор,
І.М. Загурський, студент
Київського університету інтелектуальної власності та права

ЗАГРОЗИ ДЛЯ СТЕГАНОГРАФІЇ

Загроза для стеганографії, викликана появою квантових обчислювальних технологій, пов'язана з тим, що квантові комп'ютери здатні вирішувати завдання, які є обчислювально складними для класичних систем, значно швидше. Це створює кілька ризиків, пов'язаних із виявленням прихованої інформації та порушенням конфіденційності.

Дослідження цього впливу важливе для майбутнього цифрової безпеки, адже розвиток квантових обчислень продовжує змінювати обчислювальну парадигму [1].

Розглянемо основні аспекти цієї загрози. Це, по-перше, прискорення виявлення прихованої інформації, а саме використання алгоритму Гровера, коли квантові обчислення дозволяють значно пришвидшити процес пошуку прихованої інформації. Наприклад, якщо для аналізу стеганографічного носія потрібен перебір усіх можливих варіантів (таких як позиції бітів у файлі), алгоритм Гровера може зменшити час пошуку, що значно підвищує ймовірність викриття.

Також використання детектування аномалій, коли квантові комп'ютери можуть швидше ідентифікувати аномалії в цифрових файлах, мережевому трафіку або інших середовищах, що ускладнює приховування інформації.

По-друге, злам криптографічних алгоритмів, а саме використання алгоритм Шора, коли квантові обчислення здатні розкладати великі числа на множники надзвичайно швидко. Це ставить під загрозу класичні криптографічні алгоритми, такі як RSA, які часто використовуються для шифрування даних перед їх стеганографічним приховуванням. Злам криптографії робить приховані дані вразливими [1,2].

Також використання атаки на симетричні алгоритми: Навіть симетричні алгоритми (наприклад, AES) стають частково вразливими, оскільки квантові обчислення можуть зменшити складність перебору ключів.

По-третє, покращення аналізу великих обсягів даних за рахунок використання квантової обробки даних. Завдяки здатності квантових комп'ютерів швидко аналізувати великі

масиви даних, вони можуть ефективніше знаходити шаблони, які вказують на стеганографічну активність.

Також за рахунок використання машинного навчання на квантових комп’ютерах. Інтеграція квантових обчислень із машинним навчанням дозволяє створювати моделі, здатні швидко ідентифікувати приховану інформацію навіть у складних структурах даних.

По-четверте, збільшення можливостей атак, яке відбувається за рахунок здійснення ефективних атак на стеганографічні канали та використання підробок. Що стосується ефективних атак на стеганографічні канали, то квантові технології можуть використовуватися для аналізу каналів передачі даних. Наприклад, аналіз часових проміжків у мережевому трафіку або флуктуацій сигналу. Що стосується використання підробок, то квантові комп'ютери можуть допомогти зловмисникам створювати фальшиві стеганографічні повідомлення або виявляти справжні [2,3].

По-п’яте, загроза для квантових стеганографічних методів. Хоча квантова стеганографія має високий рівень захисту (завдяки законам квантової механіки), квантові обчислення можуть спробувати обходити її через складні атаки на квантові стани, такі як атаки на джерела фотонів або приймачі.

Прикладами впливу квантових технологій на стеганографічні методи є методи LSB у зображеннях, коли квантові комп'ютери можуть швидше проаналізувати пікселі зображення на предмет статистичних аномалій, що вказують на приховані дані.

Також до прикладів можна віднести приховування у мережевому трафіку, коли квантові обчислення дозволяють проводити аналіз трафіку в реальному часі, виявляючи приховані сигнали у часових інтервалах або розмірах пакетів.

До прикладів впливу квантових технологій на стеганографічні методи можна віднести шифрування стеганографічного повідомлення, коли злам криптографічного алгоритму, який використовується для шифрування перед приховуванням, відкриває доступ до самого повідомлення [3].

Що можна зробити для захисту стеганографії? На цей час існують таки можливості, як: перехід до постквантових криптографічних алгоритмів, коли використовується криптографія, стійка до квантових обчислень (наприклад, заснованої на решітках, кодах або ізогеніях); інтеграція квантових методів, коли застосовуються квантові розподіли ключів (QKD) для захисту стеганографічних каналів; динамічні методи приховування, коли розробляються стеганографічні алгоритми, які адаптуються в реальному часі, використовуючи випадковість і змінність даних.

Таким чином, з появою квантових обчислювальних технологій класична стеганографія стикається з новими загрозами, які ускладнюють приховування інформації. Водночас це стимулює розвиток нових підходів, таких як постквантова стеганографія, яка враховує потенціал квантових обчислень.

Список використаних джерел:

1. Bennett, C. H., & Brassard, G. (1984). Quantum Cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 498 p.

2. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information.* Cambridge University Press. 256 p.

3. Shor, P. W. (1995). Scheme for reducing decoherence in quantum computer memory. Physical Review A, 52(4), R2493-R2496. 320 p.

Н.А. Андрієнко, студент
І.С. Волковецький, студент
Є. О. Васін, студент
Державний університет інформаційно-комунікаційних технологій

ПРИНЦИПИ ТА МЕТОДИ ЗАСТОСУВАННЯ СИСТЕМИ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ ЗАПОБІГАННЯ ВИТОКУ КОНФІДЕНЦІЙНИХ ДАНИХ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Сучасні об'єкти інформаційної діяльності (ОІД) функціонують в умовах зростання кількості цілеспрямованих кібератак, інсайдерських загроз та спроб несанкціонованого доступу до конфіденційних даних. Класичні однофакторні механізми автентифікації, що базуються переважно на паролях, вже не забезпечують належного рівня захисту через низку вразливостей: використання слабких або однакових паролів, їх перехоплення, підбір, соціальну інженерію тощо. У таких умовах впровадження системи багатофакторної автентифікації (Multi-factor authentication systems- MFA) є одним з ключових напрямів підвищення рівня інформаційної безпеки та запобігання витоку конфіденційних даних.

Обґрунтування принципів та вибір ефективних методів застосування системи багатофакторної автентифікації для зменшення ймовірності несанкціонованого доступу та витоку конфіденційної інформації на об'єкті інформаційної діяльності є метою даної статті.

Для досягнення цієї мети необхідно вирішити такі завдання:

- проаналізувати типові загрози і вразливості, пов'язані з автентифікацією користувачів;
- визначити вимоги до MFA на ОІД; класифікувати основні фактори автентифікації;
- сформулювати принципи побудови та впровадження системи MFA;
- розглянути практичні методи її реалізації з урахуванням технічних, організаційних та людських чинників.

Об'єктом дослідження є процес доступу користувачів до інформаційних ресурсів ОІД.

Предметом дослідження є принципи та методи побудови й застосування системи багатофакторної автентифікації для захисту конфіденційної інформації від несанкціонованого доступу та витоку.

Система MFA базується на використанні декількох незалежних факторів автентифікації, які умовно поділяються на три основні групи: «те, що знає користувач» (паролі, PIN-коди, відповіді на контрольні запитання), «те, що має користувач» (апаратні токени, смарт-картки, одноразові паролі, надіслані на мобільний пристрій), «те, чим є користувач» (біометричні характеристики: відбитки пальців, геометрія обличчя, райдужка ока, голос, поведінкові біометричні ознаки тощо). Використання щонайменше двох різних факторів, що належать до різних груп, істотно ускладнює компрометацію облікових записів і, відповідно, знижує ризик витоку конфіденційних даних [1].

Основні принципи застосування системи MFA на ОІД можна сформулювати таким чином [1,2]:

- **Принцип достатності та доцільності** — набір факторів автентифікації має відповідати рівню критичності інформаційних ресурсів, щоб забезпечити баланс між безпекою та зручністю користувачів.
- **Принцип незалежності факторів** — компрометація одного фактору не повинна автоматично призводити до компрометації інших; фактори мають ґрунтуватися на різних механізмах.

- **Принцип мінімізації впливу людського фактору** — необхідно по можливості зменшити залежність від дій користувача (наприклад, за рахунок біометрії, апаратних токенів, автоматизованих перевірок контексту доступу).
- **Принцип контекстної та ризик-орієнтованої автентифікації** — посилення вимог (наприклад, запит додаткового фактору) має відбуватися в ситуаціях підвищеного ризику: підозріла IP-адреса, невідомий пристрій, нетипична геолокація, високочутливий ресурс тощо.
- **Принцип інтегрованості та масштабованості** — MFA повинна інтегруватися в існуючу інфраструктуру керування доступом (Active Directory, системи єдиного входу тощо) та мати можливість розширення без радикальної перебудови архітектури.

До основних методів реалізації MFA на ОІД можна віднести: застосування одноразових паролів (OTP) на основі часових алгоритмів (TOTP) чи лічильника (HOTP), використання мобільних додатків-аутентифікаторів, апаратних криптотокенів і смарт-карток, біометричних систем доступу, а також комбінованих схем з використанням сертифікатів відкритого ключа (PKI) [2,3]. Важливим є також впровадження механізмів адаптивної автентифікації, коли система автоматично оцінює ризик операції та визначає, чи потрібно запитувати додаткові фактори.

При побудові системи MFA для запобігання витоку конфіденційних даних необхідно враховувати специфіку ОІД: категорію інформації, що обробляється; наявність сегментованих мереж; вимоги нормативних документів; технічні можливості обладнання; рівень підготовки персоналу. Запровадження MFA має супроводжуватися розробленням і впровадженням локальних нормативних актів, політик керування обліковими записами, регламентів відновлення доступу, а також навчанням користувачів правилам безпечного використання засобів автентифікації [1,3].

Очікуваним результатом впровадження системи багатофакторної автентифікації є зменшення ймовірності несанкціонованого доступу до інформаційних ресурсів, зниження ризику витоку конфіденційних даних як унаслідок зовнішніх кібератак, так і через інсайдерські дії, підвищення загального рівня захищеності інформаційного середовища об’єкта. Подальші дослідження доцільно спрямувати на розроблення моделей оцінювання ефективності MFA з урахуванням конкретних сценаріїв загроз, а також на інтеграцію систем багатофакторної автентифікації з засобами виявлення аномальної активності та системами керування подіями інформаційної безпеки (SIEM).

Ключові слова: багатофакторна автентифікація, конфіденційні дані, витік інформації, об’єкт інформаційної діяльності, інформаційна безпека, фактори автентифікації, інсайдерські загрози.

Список використаних джерел:

1. Temoshok, D., Galluzzo, R., LaSalle, C., Lefkovitz, N., Regenscheid, A., Choong, Y.-Y., Proud-Madruga, D., & Gupta, S. (2025). *Digital identity guidelines* (NIST Special Publication 800-63, Revision 4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-4

2. European Union Agency for Cybersecurity. (2025). *Technical implementation guidance on cybersecurity risk management measures* (Version 1.0). ENISA. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

3. International Organization for Standardization, & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. ISO.

О.В. Матвійчук, студентка
В.М. Савченко, студент
Державний університет інформаційно-комунікаційних технологій

ПОБУДОВА ТА ПРИНЦИПИ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИЩЕНОГО ДОПУСКУ КОРИСТУВАЧІВ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

Сучасні об’єкти інформаційної діяльності обробляють значні обсяги інформації з обмеженим доступом, порушення конфіденційності, цілісності чи доступності якої може призвести до серйозних організаційних, фінансових або репутаційних втрат. Значна частина інцидентів пов’язана не стільки з технічними вразливостями, скільки з недосконалістю процедур допуску користувачів до інформації, слабким контролем повноважень та недостатнім розмежуванням доступу. Тому побудова цілісної системи захищеного допуску користувачів до роботи з інформацією з обмеженим доступом є ключовою складовою забезпечення інформаційної безпеки.

Метою доповіді є обґрунтування підходів до побудови та визначення принципів функціонування системи захищеного допуску користувачів до інформації з обмеженим доступом на об’єкті інформаційної діяльності. Для досягнення поставленої мети сформульовано такі завдання: проаналізувати вимоги до організації допуску; визначити етапи життєвого циклу прав доступу користувачів; запропонувати структурну модель системи допуску; сформулювати базові принципи її функціонування; окреслити механізми контролю та аудиту, що знижують ризик несанкціонованого доступу та витоку інформації.

Об’єктом дослідження є процес керування доступом користувачів до ресурсів інформаційної системи, що містить інформацію з обмеженим доступом. Предметом дослідження є організаційно-технічні рішення та принципи побудови системи захищеного допуску користувачів, включно з процедурами ідентифікації, автентифікації, авторизації, розмежування прав доступу та реєстрації дій.

У доповіді розглядається узагальнена модель системи захищеного допуску, що включає такі основні підсистеми:

– підсистему керування обліковими записами (створення, модифікація, блокування, видалення);

– підсистему ідентифікації та автентифікації користувачів (у т.ч. з використанням багатофакторних механізмів);

– підсистему авторизації та розмежування доступу (на основі ролей, атрибутів або політик доступу);

– підсистему криптографічного захисту (шифрування даних, захист каналів, керування ключовою інформацією);

– підсистему реєстрації та аудиту дій користувачів (журнали безпеки, контроль цілісності записів, аналіз інцидентів).

Побудова системи допуску розглядається як життєвий цикл управління доступом, що включає етапи: попереднього оформлення допуску (перевірка повноважень, визначення необхідного рівня доступу), реєстрації користувача та створення облікового запису, надання початкових прав доступу за принципом «мінімально необхідних повноважень», періодичного перегляду прав (recertification), тимчасового підвищення привілеїв у разі службової необхідності та своєчасного відкликання прав при зміні посади або звільненні. Для кожного етапу визначаються відповідальні особи та контрольні заходи.

Сформульовано ключові принципи функціонування системи захищеного допуску:

– принцип необхідності та достатності (need-to-know, least privilege) – користувач отримує лише ті повноваження, які об’єктивно потрібні для виконання його службових обов’язків;

– принцип розподілу повноважень (separation of duties) – критичні операції не повинні

виконуватися однією особою без контролю чи дубляжу, що знижує ризик зловживань;

– принцип ідентифікованості та персональної відповідальності – кожна дія з інформацією має бути однозначно пов'язана з конкретним користувачем;

– принцип багатошаровості захисту (defense in depth) – допуск забезпечується сукупністю організаційних, технічних та програмних засобів, а не одним механізмом;

– принцип керованості та контролю – усі зміни прав доступу здійснюються за формалізованими процедурами з обов'язковою реєстрацією та можливістю аудиту;

– принцип відповідності нормативним вимогам – система допуску має бути узгоджена з чинними законами, стандартами та внутрішніми документами організації.

Наголошується, що ефективність системи захищеного допуску значною мірою залежить від узгодженості організаційної та технічної складових: наявності структурованих політик інформаційної безпеки, регламентів доступу, навчання користувачів, а також впровадження технічних засобів підтримки (системи керування ідентичністю та доступом, SIEM-рішення, засоби контролю дій привілейованих користувачів тощо). Важливим є регулярний аналіз журналів безпеки, періодичний перегляд прав доступу та тестування на відповідність встановленим політикам.

У висновках підкреслюється, що системний підхід до побудови та функціонування системи захищеного допуску користувачів дозволяє суттєво знизити ризик несанкціонованого доступу та витоку інформації з обмеженим доступом. Перспективними напрямами подальших досліджень є розроблення формалізованих моделей оцінювання ризиків, використання методів інтелектуального аналізу даних для виявлення аномальної поведінки користувачів та інтеграція систем допуску з сучасними засобами автоматизованого управління інформаційною безпекою.

Ключові слова: інформація з обмеженим доступом, система захищеного допуску, керування доступом, ідентифікація, автентифікація, авторизація, розмежування прав, інформаційна безпека.

Список використаних джерел:

1. Гуз, А. М., Довгань, О. Д., Марущак, А. І., та ін. (2011). Організація захисту інформації з обмеженим доступом [Підручник]. Національна академія Служби безпеки України.

2. Кавун, С. В., Носов, В. В., & Манжай, О. В. (2008). Інформаційна безпека [Навчальний посібник]. Вид-во ХНЕУ.

3. Остапов, С. Е., Євсеєв, С. П., & Король, О. Г. (2013). Технології захисту інформації [Навчальний посібник]. Вид-во ХНЕУ.

Ю.В. Жеребок, студент
І.В. Довбня, студент
О.І. Лихогод, студент
Державний університет інформаційно-комунікаційних технологій

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ТА ЗАВДАННЯ СИСТЕМИ ЗАХИСТУ ТЕХНІЧНИХ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ ОБ'ЄКТІВ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

Сучасні об'єкти банківської діяльності характеризуються високим ступенем інформатизації та використанням розгалужених технічних каналів передачі інформації: локальних комп'ютерних мереж, каналів зв'язку між філіями, каналів взаємодії з платіжними системами, системами інтернет- та мобільного банкінгу, міжбанківських електронних розрахунків тощо. Ці канали є критично важливими для забезпечення безперервності банківських операцій, але одночасно виступають основним середовищем реалізації загроз

перехоплення, модифікації, підміни та блокування інформації, а також використання технічних каналів витоку [1].

Метою доповіді є обґрунтування особливостей функціонування системи захисту технічних каналів передачі інформації в банківській сфері та визначення її основних завдань з позицій забезпечення конфіденційності, цілісності, доступності та автентичності інформації. Для досягнення цієї мети розв'язуються такі завдання: аналізуються специфічні загрози для банківських інформаційних ресурсів у каналах передачі; визначаються особливості побудови системи захисту на різних рівнях банківської інфраструктури; формулюються ключові функціональні завдання системи захисту; окреслюються напрямки вдосконалення технічних та організаційних заходів.

Об'єктом дослідження є технічні канали передачі інформації об'єктів банківської діяльності (проводові, безпроводові, мережеві, оптичні, радіоканали, корпоративні та публічні IP-мережі). Предметом дослідження є система захисту цих каналів, її структура, принципи функціонування та комплекс завдань, спрямованих на протидію загрозам несанкціонованого доступу та витоку інформації.

Особливість функціонування технічних каналів у банківській сфері полягає в їхній критичності до затримок, відмов та порушень якості сервісу, а також у необхідності одночасно забезпечити високий рівень захисту та безперервність обслуговування клієнтів. Банківські канали використовуються для передавання платіжних доручень, автентифікаційних даних, даних клієнтів, ключової інформації криптозахисту, службової інформації між підрозділами тощо [1,2]. Це зумовлює підвищені вимоги до захищеності як самих каналів, так і кінцевих вузлів, через які здійснюється оброблення даних.

До основних загроз технічним каналам передачі інформації у банківській сфері належать [2,3]:

перехоплення мережевого трафіку (у тому числі з використанням засобів аналізу трафіку та «прослуховування» мережевих сегментів);

організація атак «людина посередині»; модифікація або підміна повідомлень у процесі передавання;

несанкціонований доступ до мережевого обладнання;

використання побічних електромагнітних випромінювань та наведень, радіоканалів, безпроводових сегментів як технічних каналів витоку інформації; порушення доступності каналів шляхом DDoS-атак.

Система захисту технічних каналів передачі інформації в банківській діяльності розглядається як багаторівневий комплекс організаційних та технічних заходів, що включає: класифікацію інформаційних потоків за рівнем чутливості; логічне та фізичне сегментування мереж; застосування криптографічних протоколів захисту (VPN, TLS, захищені канали для міжбанківських розрахунків); використання міжмережевих екранів, систем виявлення та запобігання вторгненням; контроль цілісності мережевого трафіку; технічний захист від побічних випромінювань та наведень у приміщеннях, де розміщено критичне обладнання.

До **ключових завдань системи захисту технічних каналів** належать [2,3]:

– формування та підтримка актуальної моделі загроз і вразливостей для каналів передачі інформації;

– забезпечення конфіденційності даних у каналах шляхом шифрування, захищеної автентифікації сторін та протоколів обміну ключами;

– забезпечення цілісності та автентичності повідомлень (виявлення підміни, спотворення, несанкціонованих змін);

– забезпечення доступності каналів та протидія мережевим атакам, що спрямовані на блокування або деградацію сервісів;

– контроль та реєстрація подій безпеки в каналах (журналювання, кореляція подій, інтеграція із системами моніторингу та SIEM);

– організація технічного захисту приміщень і комунікацій, де прокладено лінії зв'язку, встановлене критичне телекомунікаційне й серверне обладнання;

– періодична оцінка ефективності заходів захисту, проведення тестувань на проникнення, аудит захищеності каналів.

Особливе значення мають принципи побудови системи захисту [2,3]:

системність та комплексність (узгодження мережевих, криптографічних, фізичних та організаційних заходів);

диференціація доступу та розмежування повноважень при роботі з мережевою інфраструктурою;

мінімізація довіри до зовнішніх каналів та використання захищених шлюзів;

принцип «мінімально необхідних привілеїв» для адміністраторів та операторів; регулярне оновлення засобів захисту і підтримка їх відповідності актуальним вимогам регулятора та стандартам інформаційної безпеки.

У доповіді підкреслюється, що ефективне функціонування системи захисту технічних каналів передачі інформації в банківській сфері можливе лише за умови тісної взаємодії організаційних, нормативно-правових, технічних та кадрових складових.

Своєчасне виявлення та нейтралізація загроз у каналах передачі дозволяє суттєво знизити ризик несанкціонованого доступу, фінансових втрат та репутаційних збитків банківської установи. Перспективними напрямами розвитку є впровадження інтелектуальних систем аналізу трафіку, адаптивних механізмів виявлення аномалій, подальша автоматизація процедур моніторингу та реагування на інциденти.

Ключові слова: банківська діяльність, інформація з обмеженим доступом, технічні канали передачі інформації, система захисту, мережна безпека, криптографічний захист, технічні канали витоку інформації, аудит безпеки.

Список використаних джерел:

1. **Іванченко, С. О., Гавриленко, О. В., Липський, О. А., & Шевцов, А. С. (2016).** *Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації* **[Навчальний посібник]. ІСЗЗІ НТУУ «КПІ».**

2. **Корченко, А. О., Скачек, Л. М., & Хорошко, В. О. (2014).** *Банківська безпека* **[Підручник]. ПВП «Задруга».**

3. **Національний банк України. (2017).** *Постанова Правління Національного банку України від 28 вересня 2017 року № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України»*. https://bank.gov.ua

Є.В. Бакум, студент
Є.М. Шиньковий, студент
Є.І. Нагаєв, студент
Державний університет інформаційно-комунікаційних технологій

ТИПИ ТА МЕХАНІЗМИ КІБЕРАТАК НА МЕРЕЖЕВІ КАНАЛИ ПЕРЕДАЧІ ДАНИХ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Сучасні об'єкти інформаційної діяльності (ОІД) – органи державної влади, банки, підприємства критичної інфраструктури, освітні та медичні установи – залежать від безперервного та захищеного функціонування комп'ютерних мереж. Мережеві канали передачі даних забезпечують виконання основних бізнес-процесів, віддалену взаємодію підрозділів, доступ до державних і корпоративних сервісів. Порушення роботи цих каналів або компрометація даних, що ними передаються, може призвести до витоку конфіденційної інформації, фінансових втрат та зупинки діяльності організації.

Кібератаки на мережеві канали є одним із ключових ризиків для ОІД. Вони можуть здійснюватися на різних рівнях мережевої моделі – від фізичного до прикладного – із застосуванням широкого спектра технічних та програмних засобів.

1. Класифікація кібератак на мережеві канали

За основною ціллю впливу виділяють атаки на:

- конфіденційність – перехоплення та несанкціоноване ознайомлення з даними;
- цілісність – модифікація, підміна або знищення інформації;
- доступність – блокування або істотне уповільнення роботи сервісів;
- автентичність – підміна сторін взаємодії, фальсифікація повідомлень.

За характером дій розрізняють пасивні (спостереження, аналіз трафіку) та активні (втручання в трафік, генерація шкідливих пакетів, зміна маршрутів) атаки.

2. Пасивні та активні атаки на трафік

До пасивних атак належить перехоплення мережевого трафіку (sniffing) та аналіз метаданих. Зловмисник може отримувати паролі, службові дані, відомості про структуру мережі та критичні вузли. Особливо небезпечним є використання незашифрованих протоколів або спільних мережевих сегментів.

Активні атаки включають зміну, підміну чи вставку пакетів, а також організацію повторних (replay) атак, коли перехоплені раніше коректні повідомлення відтворюються повторно для ініціювання небажаних дій (наприклад, транзакцій).

Окрему групу становлять атаки типу «людина посередині» (Man-in-the-Middle, MITM) та перехоплення сеансу (session hijacking), коли зловмисник «вбудовується» між сторонами обміну даними, отримуючи змогу переглядати й змінювати трафік, підмінювати сторони, спрямовувати користувача на фальшиві ресурси. Для цього можуть використовуватися ARP- та DNS-spoofing, створення фальшивих точок доступу Wi-Fi тощо.

3. Атаки на доступність: DoS та DDoS

Атаки на доступність реалізуються переважно у вигляді **DoS/DDoS-атак**, коли на сервіс або канал генерується надмірний обсяг трафіку. Це призводить до вичерпання ресурсів серверів, мережевого обладнання чи каналів зв'язку. Застосовуються як «примітивні» флуди (масова розсилка пакетів), так і протокольні атаки (TCP SYN-flood, UDP-flood, зловживання ICMP).

Для ОІД такі атаки можуть означати недоступність критичних сервісів (кабінетів користувачів, сервісів електронного урядування, систем управління тощо), що має суттєві організаційні й репутаційні наслідки.

4. Специфіка атак на мережеві канали ОІД

Особливістю об'єктів інформаційної діяльності є:

- наявність віддалених філій і партнерів, з якими організація взаємодіє через мережу;
- використання VPN та каналів віддаленого доступу;
- можливе підключення до державних інформаційних ресурсів та спеціалізованих інформаційних систем;
- застосування бездротових сегментів (Wi-Fi, мобільний зв'язок).

Це створює додаткові точки атаки: компрометація VPN-доступу, підміна шлюзів, несанкціонований доступ через неправильно налаштовані бездротові мережі, використання вразливостей протоколів службових систем.

5. Узагальнені підходи до протидії кібератакам

Ефективний захист мережевих каналів ОІД можливий лише за умови комплексного підходу, що включає:

1. Технічні заходи:
2. Організаційні заходи:
3. Навчання персоналу:
4. Моніторинг і реагування:

Висновки

Кібератаки на мережеві канали передачі даних об'єктів інформаційної діяльності становлять серйозну загрозу для конфіденційності, цілісності та доступності інформації.

Різноманітність атак – від пасивного перехоплення до складних MITM та DDoS – вимагає від організацій побудови комплексної системи захисту, яка поєднує технічні засоби, організаційні заходи та належну підготовку персоналу.

Лише системний підхід до захисту мережевих каналів, регулярний аналіз загроз і вразливостей, модернізація інфраструктури безпеки та розвиток культури кібербезпеки дозволяють істотно знизити ризики порушення роботи об'єктів інформаційної діяльності та витоку критично важливої інформації.

Список використаних джерел:

1. Костюк, Ю., Складанний, П., Рзаєва, С., Мазур, Н., Черевик, В., & Аносов, А. (2025). ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ МЕРЕЖЕВИХ АТАК ЧЕРЕЗ TCP/IP-ПРОТОКОЛИ. *Кібербезпека: освіта, наука, техніка, 1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915 csecurity.kubg.edu.ua

2. Полотай, О. І., Фединець, Н. І., & Кухарська, Н. П. (2024). Дослідження загроз інформаційної безпеки та способів їх вирішення в комп'ютерних мережах на канальному рівні. *Вісник Львівського державного університету безпеки життєдіяльності, 29.* sci.ldubgd.edu.ua+1

3. Kak, A. (2025). *Lecture 16: TCP/IP vulnerabilities and DoS attacks: IP spoofing, SYN flooding, and the Shrew DoS attack* (Lecture notes for "Computer and Network Security"). Purdue University. Retrieved from https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture16.pdf en

Н.О. Струк, студент
М.С. Максимчук, студент
Ю.Л. Іванов, студент
Державний університет інформаційно-комунікаційних технологій

СТРУКТУРА, ПЕРЕЛІК ТА ЗМІСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ КОМЕРЦІЙНОЇ ТОРГОВЕЛЬНОЇ УСТАНОВИ ТА КАНАЛИ ЇЇ НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Сучасні комерційні торговельні установи функціонують в умовах високої конкуренції та постійної цифровізації бізнес-процесів. Інформація стає одним з основних активів, а її втрата або розголошення можуть призвести до прямого фінансового збитку, втрати ринкових позицій та репутаційних ризиків. Особливого значення набуває конфіденційна інформація, яка містить відомості про фінансові показники, клієнтів, постачальників, ціноутворення, маркетингові стратегії тощо.

Для побудови ефективної системи інформаційної безпеки необхідно чітко визначити структуру, перелік та зміст конфіденційної інформації, а також проаналізувати можливі канали її несанкціонованого доступу.

1. Поняття та загальні підходи до класифікації конфіденційної інформації

Під конфіденційною інформацією комерційної торговельної установи розуміють відомості, що не є загальнодоступними, мають комерційну цінність, створюють конкурентні переваги та підлягають захисту згідно з внутрішніми політиками, договорами або законодавством.

Для зручності управління такою інформацією її доцільно класифікувати:

за змістом (фінансова, комерційна, технологічна, персональні дані тощо);

за джерелом походження (власна інформація, інформація партнерів, дані клієнтів);

за рівнем критичності (високої, середньої, низької важливості);

за формою подання (електронні дані, паперові документи, усні відомості, візуальна інформація).

Така класифікація дозволяє структурувати підхід до захисту та визначити пріоритети при впровадженні організаційних і технічних заходів.

2. Структура та перелік основних видів конфіденційної інформації торговельної установи

У типових умовах діяльності комерційної торговельної установи можна виділити такі основні блоки (структуру) конфіденційної інформації.

2.1. Фінансова та управлінська інформація

внутрішня управлінська звітність (прибутки, витрати, рентабельність по підрозділах, товарних групах);

бюджети, фінансові плани, бізнес-плани розвитку;

інформація про інвестиційні проєкти, кредити, фінансові зобов'язання;

внутрішні аналітичні звіти про ефективність напрямів діяльності.

Ці дані відображають реальний фінансовий стан установи та використовуються для стратегічного управління.

2.2. Комерційна та договірна інформація договори з постачальниками та оптовими покупцями;

умови поставок, знижки, відстрочки платежів;

комерційні пропозиції, специфікації товарів, прайси для різних категорій клієнтів;

дані про участь у тендерах, конкурси, закриті переговори з партнерами.

Розголошення такої інформації може створити конкурентні переваги іншим учасникам ринку та погіршити позиції установи.

2.3. Інформація про клієнтів та контрагентів бази клієнтів (як юридичних, так і фізичних осіб);

історія покупок, обсяг і структура замовлень, середній чек;

контактні дані, умови індивідуального обслуговування, програми лояльності;

відомості про платіжну дисципліну, кредитні ліміти (для B2B-клієнтів).

Ця інформація часто підпадає під дію законодавства про захист персональних даних і є цінною з точки зору маркетингу та конкурентної розвідки.

2.4. Маркетингова та стратегічна інформація маркетингові стратегії, плани рекламних кампаній, бюджети на промо-активності;

результати маркетингових досліджень, аналіз поведінки клієнтів;

дані про цінову політику, плановані акції, знижки, ребрендинг;

інформація про позиціонування, асортиментну політику, виведення нових товарів.

Дострокове розкриття такої інформації може дозволити конкурентам адаптувати власні дії або нейтралізувати переваги.

2.5. Інформація про логістику, склади та запаси дані про складські залишки, оборотність товарів;

маршрути постачання, графіки відвантаження та доставки;

інформація про логістичних партнерів, тарифи, умови зберігання.

Компрометація цієї інформації може створити ризики для фізичної безпеки вантажів, можливості махінацій із запасами, організації крадіжок.

2.6. Внутрішньоорганізаційна та кадрова інформація внутрішні регламенти, політики, посадові інструкції;

інформація про структуру управління, схеми підпорядкування;

дані про персонал (посади, оклади, преміювання, дисциплінарні заходи).

Ця інформація важлива для підтримання стабільності колективу та запобігання внутрішнім конфліктам і корупційним ризикам.

2.7. Технічна та IT-інформація

структури корпоративної мережі, схеми підключень, конфігурації серверів і мережевого обладнання;

облікові записи, права доступу, резервні копії, ключі та сертифікати;

параметри інформаційних систем (ERP, CRM, касові системи, інтернет-магазини).

Це «критична» конфіденційна інформація з точки зору кібербезпеки.

3. Канали несанкціонованого доступу до конфіденційної інформації

Канал несанкціонованого доступу — це шлях, способом якого зловмисник може отримати доступ до інформації в обхід встановлених правил і механізмів захисту. Для комерційної торговельної установи можна виділити кілька основних груп таких каналів.

3.1. Людський фактор та організаційні канали

Інсайдерські дії співробітників: свідоме копіювання баз клієнтів, прайсів, звітів, комерційних умов з метою передачі конкурентам або використання при переході на нове місце роботи.

Порушення правил роботи з документами: залишення конфіденційних документів у відкритому доступі, неналежне знищення паперових носіїв, неврегульований доступ до архівів.

Соціальна інженерія: отримання інформації шляхом маніпуляції співробітниками (телефонні дзвінки під виглядом «служби підтримки», «перевіряючих», «партнерів» тощо).

3.2. Технічні та мережеві канали

Несанкціонований доступ через мережу Інтернет: використання вразливостей веб-сайтів, інтернет-магазинів, систем віддаленого доступу;

Атаки на IT-інфраструктуру: експлуатація уразливостей серверів, робочих станцій, мережевого обладнання, систем управління базами даних;

Шкідливе програмне забезпечення: віруси, трояни, шпигунське ПЗ, яке фіксує натискання клавіш, перехоплює трафік, копіює файли;

Перехоплення трафіку в локальній мережі або бездротових сегментах: використання незашифрованих протоколів, слабких паролів Wi-Fi, відсутність сегментування мережі.

3.3. Фізичні канали

Несанкціонований доступ до приміщень: складів, серверних, касових вузлів, кабінетів керівництва;

Крадіжка або втрата носіїв інформації: ноутбуків, смартфонів, флеш-накопичувачів, зовнішніх дисків;

Спостереження та підглядання (shoulder surfing): підгляд за введенням паролів, знімання екранів за допомогою камер, використання прихованих засобів запису.

3.4. Канали, пов’язані з контрагентами та підрядниками

доступ стороннього персоналу (аутсорсингових IT-компаній, охорони, прибирання) до інформації або приміщень;

недостатній рівень захисту інформації у партнерів, яким передаються дані (логістичні компанії, маркетингові агенції, сервісні центри);

відсутність чітких договірних зобов’язань щодо збереження конфіденційності та технічних вимог до захисту.

Висновки

Конфіденційна інформація комерційної торговельної установи має складну структуру та охоплює широкий спектр відомостей — від фінансових показників та комерційних умов до IT-інфраструктури та внутрішніх регламентів. Чітке визначення **структури, переліку та змісту** такої інформації є необхідною передумовою для побудови ефективної системи її захисту.

Аналіз каналів несанкціонованого доступу показує, що загрози походять як з **зовнішнього середовища**, так і з **внутрішнього** — через людський фактор, організаційні недопрацювання, технічні вразливості та слабкі точки у взаємодії з контрагентами.

Таким чином, система захисту конфіденційної інформації має будуватися на поєднанні організаційних, технічних та правових заходів, включати класифікацію інформації, регламентацію доступу, навчання персоналу, впровадження засобів технічного та криптографічного захисту, а також постійний контроль і аудит дотримання встановлених вимог.

Список використаних джерел:

1. Килимник, І. І., & Харитонов, О. В. (2014). *Правова характеристика забезпечення комерційної таємниці на підприємстві в умовах ринкової економіки* [Монографія]. Харківський національний університет міського господарства імені О. М. Бекетова.

2. Немченко, Т. А. (2022). *Управління захистом комерційної таємниці* **[**Навчальний посібник]. Центральноукраїнський національний технічний університет.

3. А.М. Гузь, І.П. Касперський, С.О. КнязевьОрганізація захисту інформації з обмеженим доступом**.** К.: Нац.акад., СБУ, 2028._251 с.

О.А. Турчин, студент
В.І. Нетьоса, студент
Є.О. Кравченко, студент
Державний університет інформаційно-комунікаційних технологій

СПОСОБИ, МЕТОДИ ТА ПЕРЕВАГИ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ МЕРЕЖЕВИХ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ НА ОСНОВІ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Стрімкий розвиток телекомунікаційних мереж, хмарних сервісів та розподілених інформаційних систем призвів до різкого зростання обсягів даних, що передаються мережевими каналами, а також до ускладнення структури мережевої інфраструктури. На цьому фоні постійно збільшується кількість та складність кібератак на мережеві канали: від масових DDoS-атак до таргетованих проникнень, що використовують складні багатоступеневі сценарії та техніки ухилення від виявлення. Традиційні засоби захисту — класичні міжмережеві екрани, сигнатурні системи виявлення вторгнень, фільтрація трафіку за статичними правилами — дедалі частіше виявляються недостатніми, оскільки не встигають адаптуватися до динаміки сучасних загроз [1].

У цих умовах перспективним напрямом розвитку засобів захисту мережевих каналів передачі інформації є застосування технологій штучного інтелекту (ШІ), насамперед методів машинного навчання, інтелектуального аналізу трафіку та поведінкової аналітики. Використання ШІ дозволяє не лише автоматизувати виявлення відомих атак, але й виявляти нові, раніше невідомі (zero-day) загрози на основі аномалій у поведінці мережевих об’єктів.

1. Концепція системи захисту мережевих каналів на основі ШІ

Система захисту мережевих каналів передачі інформації на основі технологій ШІ можна розглядати як багаторівневий програмно-апаратний комплекс, у якому основні функції аналізу та прийняття рішень делегуються інтелектуальним модулям. Узагальнено її структуру можна подати у вигляді таких підсистем [1,2]:

- підсистема збору даних — перехоплення та попередня обробка мережевого трафіку (packet capture, NetFlow, журнали безпеки, телеметрія мережевого обладнання);
- підсистема попередньої обробки та нормалізації — очищення, агрегація, формування наборів ознак (feature engineering) з мережевих даних;
- аналітичне ядро на основі ШІ — моделі машинного навчання та глибинного навчання для класифікації, кластеризації, виявлення аномалій;
- підсистема кореляції та прийняття рішень — поєднання результатів аналізу з політиками безпеки, формування реакцій (сповіщення, блокування, обмеження);
- підсистема візуалізації та підтримки оператора — панелі моніторингу, звітність, інструменти для аналізу інцидентів та донавчання моделей.

Основна відмінність такої системи від класичних рішень полягає в можливості автоматичного навчання на реальному трафіку, адаптації до змінних умов, побудові поведінкових профілів користувачів і вузлів, а також виявленні складних прихованих закономірностей, недоступних для простих сигнатурних підходів [2,3].

2. Способи та методи застосування ШІ в захисті мережевих каналів

2.1. Інтелектуальне виявлення вторгнень (IDS/IPS з ШІ)

2.2. Аналіз трафіку для виявлення DDoS-атак та аномалій навантаження

2.3. Виявлення шкідливих доменів і трафіку командно-керувальних серверів

2.4. Застосування поведінкової аналітики (UEBA)

3. Переваги використання технологій ШІ в системах захисту мережевих каналів

Застосування технологій штучного інтелекту в системах захисту мережевих каналів передачі інформації забезпечує низку важливих переваг порівняно з традиційними підходами.

3.1. Підвищення точності виявлення атак

3.2. Адаптивність до нових загроз

3.3. Автоматизація аналізу великого обсягу даних

3.4. Інтеграція з іншими засобами кіберзахисту

4. Обмеження та виклики впровадження ШІ-рішень у захисті мережевих каналів

Попри очевидні переваги, використання технологій ШІ має і певні обмеження та виклики, які необхідно враховувати [3,4].

По-перше, побудова ефективних моделей потребує **якісних навчальних даних**, що включають як нормальний трафік, так і приклади атак. Збір, розмітка та актуалізація таких наборів даних — складне і ресурсоємне завдання.

По-друге, існує ризик «отрутних» даних (data poisoning), коли зловмисник навмисно впливає на дані, що використовуються для навчання моделі, з метою зменшення її ефективності.

По-третє, складні моделі глибинного навчання часто мають низьку інтерпретованість: важко пояснити причини конкретного спрацьовування, що створює труднощі для аудиту й прийняття управлінських рішень.

Також слід враховувати ресурсні вимоги (обчислювальні потужності, пам’ять, пропускна здатність) і необхідність залучення кваліфікованих фахівців з кібербезпеки та аналізу даних [4].

Висновки

Системи захисту мережевих каналів передачі інформації на основі технологій штучного інтелекту є логічним етапом еволюції засобів кіберзахисту в умовах зростання складності мережевих інфраструктур та спектра кібератак. Використання методів машинного навчання, поведінкової аналітики, інтелектуального аналізу трафіку дозволяє істотно підвищити точність виявлення загроз, скоротити час реагування, адаптуватися до нових типів атак та автоматизувати обробку великого обсягу мережевих даних.

Разом з тим упровадження таких систем потребує зваженого підходу: формування якісної навчальної вибірки, організації безпечного процесу навчання моделей, інтеграції з існуючою інфраструктурою інформаційної безпеки, а також підготовки персоналу. Подальші дослідження в цьому напрямі доцільно спрямувати на розроблення більш інтерпретованих моделей, стійких до атак на самі алгоритми ШІ, а також на створення комплексних рішень, у яких інтелектуальний аналіз мережевого трафіку поєднується з іншими напрямами кіберзахисту (захист кінцевих точок, управління ідентичностями, аналіз журналів тощо).

Список використаних джерел:

1. Ободяк, В., Отрощенко, М., & Любчак, В. (2025). МОЖЛИВОСТІ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АУДИТУ ТА УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ. *Кібербезпека: освіта, наука, техніка*, 1(29), 319–330. https://doi.org/10.28925/2663-4023.2025.29.872

2. Голдій, А., Шпур, О., & Масюк, А. (2024). Розроблення моделі системи виявлення та протидії кіберзагрозам із підтримкою та оновленням правил виявлення атак. *Інфокомунікаційні технології та електронна інженерія*, 4(2), 60–71. https://doi.org/10.23939/ictee2024.02.060

3. Kikissagbe, B. R., & Adda, M. (2024). Machine learning-based intrusion detection methods in IoT systems: A comprehensive review. *Electronics, 13*(18), 3601. https://doi.org/10.3390/electronics13183601
4. Sowmya, T., & Mary Anita, E. A. (2023). A comprehensive review of AI based intrusion detection system. *Measurement: Sensors, 28*, 100827. https://doi.org/10.1016/j.measen.2023.100827

М.В. Онищенко, студент
Д.П. Жуковський, студент
Державний університет інформаційно-комунікаційних технологій

ПРИНЦИПИ ПОБУДОВИ ТА ОСНОВИ ФУНКЦІОНУВАННЯ СИСТЕМИ КІБЕРЗАХИСТУ ПЕРЕДАЧІ КОНФІДЕНЦІЙНИХ ДАНИХ МЕРЕЖЕВИМИ КАНАЛАМИ НА ОСНОВІ СТЕГАНОГРАФІЧНИХ ТЕХНОЛОГІЙ

Сучасні інформаційні системи активно використовують мережеві канали для обміну даними між користувачами, сервісами та віддаленими ресурсами. В умовах зростання кількості кібератак, розвитку методів несанкціонованого доступу та перехоплення трафіку особливої актуальності набуває задача забезпечення конфіденційності передачі даних. Традиційні засоби криптографічного захисту (шифрування, протоколи TLS, VPN тощо) залишаються базовим інструментом, однак у ряді випадків сам факт застосування криптографії може викликати підвищену увагу з боку зловмисника або спеціальних служб аналізу трафіку.

В цих умовах додатковий рівень захисту може забезпечити **стеганографія** – технологія прихованої передачі інформації, коли факт передавання конфіденційних даних маскується в звичайному, на перший погляд нешкідливому, трафіку. Поєднання криптографічних і стеганографічних методів дає змогу реалізувати більш стійку систему кіберзахисту, де захищаються не лише зміст даних, але й сам факт їх існування та передавання [1,2].

2. Принципи побудови системи кіберзахисту на основі стеганографії [1,2].

Побудова системи кіберзахисту передачі конфіденційних даних мережевими каналами на основі стеганографічних технологій має ґрунтуватися на кількох ключових принципах.

2.1. Принцип комплексності та багаторівневості

Стеганографічна система не повинна розглядатися як повна заміна криптографічних засобів, а, навпаки, як додатковий рівень захисту. Загальна система кіберзахисту має включати:

2.2. Принцип стійкості до виявлення (неспостережуваності)

Основною вимогою до стеганографічного каналу є мінімальна ймовірність його виявлення. Це досягається:

2.3. Принцип криптостійкості

Навіть якщо стеганоканал буде виявлений, зміст передаваних даних має залишатися захищеним. Тому всі конфіденційні дані, що передаються стеганографічно, мають бути попередньо зашифровані сучасними криптографічними алгоритмами з надійним управлінням ключами.

2.4. Принцип прозорості для легітимного використання

Система не повинна суттєво погіршувати якість та працездатність легітимних сервісів, наприклад:

Стеганографічне вбудовування має бути **прозорим** для звичайних користувачів та сервісів.

2.5. Принцип керованості та масштабованості

Система має легко інтегруватися в існуючу інфраструктуру, підтримувати масштабування за кількістю користувачів та обсягами трафіку, а також забезпечувати централізоване управління параметрами вбудовування, ключами та політиками безпеки.

3. Узагальнена структура системи кіберзахисту на основі стеганографічних технологій

Типову систему можна подати у вигляді кількох взаємопов'язаних модулів [2,3]:

1. Модуль підготовки конфіденційних даних
2. Модуль вибору та формування контейнерів
3. Стеганографічний модуль вбудовування
4. Модуль передачі контейнерів мережевими каналами
5. Модуль витягання та відновлення даних на приймальній стороні
6. Модуль управління ключами та політиками

4. Переваги та обмеження використання стеганографії в системах кіберзахисту

5.1. Переваги [1,2]:

1. Прихованість факту передачі конфіденційних даних
2. Навіть за умови перехоплення трафіку зловмисник не завжди здогадується, що в ньому взагалі міститься секретне повідомлення.
3. Підсилення класичних криптозасобів
4. Шифротекст додатково «маскується» у звичайному трафіку, що ускладнює його вилучення та аналіз.
5. Можливість побудови прихованих резервних каналів зв'язку Наприклад, для обміну службовими сигналами, маркерами цілісності, службовою телеметрією без викликання підозри.
6. Адаптивність до різних середовищ Стеганографічні методи можуть бути адаптовані під специфіку конкретної мережевої інфраструктури, типів контенту та застосунків.

5.2. Обмеження та ризики [1,2]:

1. Обмежена пропускна здатність стеганоканалу
2. В один контейнер можна надійно вбудувати лише обмежений обсяг даних. Для великих масивів інформації потрібна багатократна або потокова передача.
3. Існування стеганоаналізу
4. Сучасні методи статистичного аналізу можуть виявляти спотворення в контейнерах. Тому необхідно використовувати стійкі стеганографічні алгоритми.
5. Складність реалізації та адміністрування
6. Порівняно з традиційними засобами захисту, стеганосистеми складніші в налаштуванні, потребують підготовки персоналу та ретельного тестування.
7. Ризики неправильної інтеграції
8. Некоректне використання стеганографії може, навпаки, підвищити помітність трафіку або порушити роботу сервісів.

Висновки

Система кіберзахисту передачі конфіденційних даних мережевими каналами на основі стеганографічних технологій є перспективним напрямом розвитку засобів інформаційної безпеки. Її ключова особливість полягає в можливості маскування самого факту передачі секретної інформації, що доповнює традиційні криптографічні підходи.

Принципи побудови такої системи – комплексність, стійкість до виявлення, криптостійкість, прозорість для легітимного використання та керованість – дозволяють створити гнучкі та адаптивні рішення для різних типів організацій. Водночас впровадження стеганографічних технологій потребує врахування їхніх обмежень, наявності кваліфікованого персоналу та ретельного тестування у реальних мережевих умовах.

Подальші дослідження доцільно спрямувати на розроблення **стійких до стеганоаналізу алгоритмів**, оптимізацію стеганоканалів для високошвидкісних мереж, інтеграцію стеганографії з інтелектуальними системами моніторингу та керування

кіберзахистом, а також на формування нормативно-методичної бази використання таких технологій в організаціях.

Список використаних джерел:

1. Кузнецов О. О., Євсеєв С. П., Король О. Г. Стеганографія : навч. посіб. Харків : Вид-во ХНЕУ, 2011.
2. Стасюк О. І., Гнатюк С. О., Довгич Н. І., Літош М. С. Сучасні стеганографічні методи захисту інформації // Захист інформації. 2011. Т. 13, № 1. С. 5–15.
3. Fridrich J. Steganography in digital media: Principles, algorithms, and applications. Cambridge : Cambridge Univ. Press, 2009.

О.Ю. Панчук, студент
М.О. Чернишов, студент
Н.І. Осадчий, студент
Державний університет інформаційно-комунікаційних технологій

ОСНОВНІ ЗАГРОЗИ ТА РИЗИКИ ПОРУШЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ В КОРПОРАТИВНІЙ МЕРЕЖЕВІЙ СИСТЕМІ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГ

Основні загрози та ризики порушення цілісності інформації, що циркулює в корпоративній мережевій системі електронного документообігу

Сучасні організації все частіше відмовляються від паперового документообігу на користь **корпоративних мережевих систем електронного документообігу (СЕД)**. Такі системи забезпечують швидкість обміну інформацією, автоматизацію бізнес-процесів, контроль виконання рішень, зручне зберігання й пошук документів.

Разом із перевагами зростають і вимоги до **інформаційної безпеки**, насамперед до **цілісності інформації**, яка циркулює в СЕД. Порушення цілісності електронних документів може призвести до помилкових управлінських рішень, юридичної недійсності документів, фінансових втрат і репутаційних ризиків [1].

1. Поняття цілісності інформації в системі електронного документообігу

Цілісність інформації – це властивість даних зберігати свою **повноту, правильність, несуперечливість та незмінність**, якщо зміни не були санкціоновані й належним чином задокументовані [1,2].

Для корпоративної СЕД це означає, що:

- електронний документ не може бути непомітно змінений сторонньою особою;
- усі зміни, що вносяться легітимно, мають бути **ідентифіковані й зафіксовані** (версіонування, журнали змін);
- не допускається приховане викривлення реквізитів, тексту, додатків, маршрутів погодження та затвердження.

Порушення цілісності може мати як **навмисний характер** (зловмисні дії), так і **випадковий** (помилки користувачів, програмні збої, технічні відмови).

2. Класифікація основних загроз цілісності в корпоративній СЕД

Загрози порушення цілісності інформації доцільно згрупувати за такими основними напрямами [2,3]:

1. **Програмно-технічні загрози**
2. **Мережеві та комунікаційні загрози**
3. **Організаційні загрози**
4. **Людський фактор**
5. **Зовнішні кібератаки та шкідливе програмне забезпечення**

Кожна група по-своєму впливає на життєвий цикл електронних документів – від створення до архівування.

3. Основні ризики від порушення цілісності інформації

Реалізація зазначених загроз призводить до таких ключових ризиків [3,4]:

1. **Управлінські ризики** – прийняття рішень на основі спотворених звітів, планів, наказів.

2. **Юридичні ризики** – визнання електронних документів недійсними, конфлікти з контрагентами, претензії регуляторів.

3. **Фінансові втрати** – помилкові розрахунки, некоректні договірні умови, штрафи, збитки від некоректних операцій.

4. **Репутаційні збитки** – втрата довіри партнерів, клієнтів, суспільства у випадку виявлення фальсифікацій чи грубих помилок у документах.

5. **Ризики безперервності діяльності** – у разі масового пошкодження або втрати документів порушуються ключові бізнес-процеси.

4. Коротко про напрями зниження ризиків

Хоча фокус доповіді – саме загрози та ризики, логічно згадати загальні напрямки їхнього зниження [3,4]:

- застосування **криптографічного захисту** (електронного підпису, хеш-контролю, шифрування);
- впровадження механізмів **версіонування й журналювання** змін документів;
- чітке **розмежування прав доступу** та принцип «мінімально необхідних привілеїв»;
- регулярне **резервне копіювання** та перевірка якості відновлення;
- розробка та дотримання **регламентів роботи в СЕД**, навчання користувачів;
- використання **засобів захисту від кібератак** (антивірус, міжмережеві екрани, IDS/IPS, моніторинг подій).

Висновки

Корпоративна мережева система електронного документообігу є критичною складовою інформаційної інфраструктури організації. Порушення цілісності інформації, що циркулює в такій системі, має комплексні наслідки – від локальних помилок у документах до масштабних управлінських, фінансових і юридичних проблем.

Основні загрози цілісності мають різну природу – технічну, мережеву, організаційну, людську та зовнішню (кібератаки). Усвідомлення цих загроз і пов’язаних з ними ризиків є базою для побудови ефективної системи захисту СЕД.

Комплексний підхід, що поєднує технічні засоби, організаційні заходи та культуру безпечної роботи з електронними документами, дозволяє суттєво знизити ймовірність порушення цілісності інформації та забезпечити надійність корпоративного електронного документообігу

Список використаних джерел:

1. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/851-15 (дата звернення: 16.11.2025).

2. Кукарін О. Б. Електронний документообіг та захист інформації : навч. посіб. Київ : НАДУ, 2015. 84 с.

3. Піддубна Л. В., Павліченко В. М. Інформаційна безпека в системах електронного документообігу // Науковий вісник Полтавського університету економіки і торгівлі. Серія : Економічні науки. 2019. № 4 (95). С. 59–66.

4. Федорук О. Безпека та захист інформації у системах електронного документообігу: підвищення рівня кіберзахисту // Вісник Книжкової палати. 2024. № 4. С. 39–44.

В.С. Герасимчук, аспірант
Державний університет інформаційно-комунікаційних технологій

ОЦІНКА ЯКОСТІ НАДАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ ТА ІНФОРМАЦІЙНИХ ПОСЛУГ

Як правило, досить важливо оцінити телекомунікаційні послуги, що надаються абонентам, а саме їх якість. Сучасні методи оцінки складових якості послуг ґрунтуються на використанні певного набору характеристик цих самих послуг [1], що належать до результату та процесу надання послуги, умов обслуговування.

Розглянемо один з найвідоміших методів оцінки якості послуг, який зберігає своє провідне значення і дотепер. Це метод SERVQUAL, запропонований А. Парасураманом, Л. Беррі та В. Цайтамлем [2]. В його основі лежить два ключові припущення: перше вказує на те, що споживач оцінює якість послуг, порівнюючи свої очікування зі сприйняттям якості послуг; друге – те що, що споживач оцінює якість послуг у межах його окремих складових, тобто: матеріальність, надійність, чуйність, переконаність, співчуття. Оцінка якості складається з оцінки цих двох етапів. Споживачі за допомогою семибальної шкали Р. Лайкерта («цілком не згоден» або «повністю згоден») оцінюють свої загальні очікування та сприйняття щодо цих п’яти вище перелічених складових якості послуги на основі 4 - 5 питань щодо кожної складової. На основі порівняння оцінок очікувань та сприйняття розраховуються коефіцієнти якості за кожною складовою та за допомогою методу середніх значень формується глобальний коефіцієнт якості послуги. Результати оцінки якості за допомогою методики SERVQUAL інтерпретуються в такий спосіб. Нульове значення якогось із коефіцієнтів якості означає збіг рівня очікування якості споживачем та рівня сприйняття якості за цим критерієм або підкритерієм. Негативні значення вказують на те, що очікування перевищують рівень сприйняття. Нарешті, позитивні значення вказують на те, що сприйняття якості вище за рівень очікувань.

Такий підхід дозволяє виявити причини низької якості послуг, які умовно назвемо «розбіжності». До них відносяться: розбіжність у знаннях про послугу, розбіжність у стандартах послуг, розбіжність у наданні послуг, розбіжність у внутрішніх комунікаціях, розбіжність у сприйнятті отриманої послуги, розбіжність в інтерпретації, розбіжність в обслуговуванні. Кожна складова має чисельний суб’єктивний показник, а при великій кількості абонентів, що отримують одну і ту саму послугу, цей метод стає ефективним на відміну від одиничних випадків. Це його головний недолік.

Іншими найбільш відомими спробами вдосконалити метод SERVQUAL став метод нормованої якості [3], в рамках якого абонент порівнює своє сприйняття окремих складових якості послуги з двома видами очікувань – ідеальними (очікування щодо того, яким має бути ідеальна якість послуг) і можливо досяжними (очікування щодо цієї послугу). Ще одним різновидом є метод QUALITOMETRO (Ф. Франчесчіні та С. Розетто), який передбачає поділ за часом моментів оцінки очікувань (щодо отримання послуги) та оцінки сприйняття (після отримання послуги). Саме від часових інтервалів навіть протягом доби очікування і запити абонента будуть різними, що впливає на об’єктивність показників.

Слід зазначити, що ці методи мають різне призначення. Поява першого методу пов’язана із спробою запропонувати абонентам загальну інтерпретацію очікувань. Він спрямований на виявлення узагальненої думки споживачів щодо якості послуги в цілому, на основі всього їхнього досвіду взаємодії з телекомунікаційними сервісами, а також дозволяє зрозуміти якою мірою якість послуги відповідає суб’єктивному ідеалу абонентів та очікуваним можливостям чи потребам самої організації, яка отримує такі послуги. Такий підхід до оцінки має більшу точність порівняно з SERVQUAL, проте ускладнює саму процедуру оцінки і, на мій погляд, має проводитись із залученням фокус-груп абонентів, а не за допомогою масового опитування всіх споживачів.

Метод QUALITOMETRO призначений для оцінки якості одиничного, конкретного факту надання послуги клієнту. Це дозволяє дещо знизити суб'єктивність оцінок, завдяки тому, що споживачеві для виставлення оцінки не потрібно узагальнювати та осмислювати весь свій досвід взаємодії із телекомунікаційною компанією, у процесі чого оцінка збільшується.

Необхідно відзначити, що методи, спрямовані на оцінку якості окремих складових телекомунікаційних послуг, особливо нових або маловідомих, є досить формалізованими і дозволяють отримати порівняльну кількісну оцінку та обробляти її в подальшому за допомогою методів математики та статистики, робити прогнози, проводити порівняльний аналіз.

Таким чином слів враховувати:

1. Полісуб'єктність оцінки якості послуг;
2. Багатокритеріальність оцінки;
3. Множинність об'єктів оцінки;
4. Інтегральний характер оцінки;
5. Якісний характер оцінки;
6. Різнорідність нових послуг.

Список використаних джерел:

1. Abd-Elrahman. A Review of Telecommunications Service Quality Dimensions // Proceedings on Engineering Sciences, Egypt, June 2019. – Vol. 1(2). – P. 533-546.

2. Parasuraman A., Zeithaml V.A., Berry L.L. SERVQUAL: A Multiple-Item Scale for Measuring Consumer Perceptions of Service Ouality // Journal of Retailing, 1988. – Vol. 64. – No.1. – P. 12-40.

3. Kuo Y.F., Wu C.M., Deng W.J. The Relationships Among Service Quality, Perceived Value, Customer Satisfaction and Post-Purchase Intention in Mobile Value-Added Services // Computers in Human Behavior, 2009. – No. 25. – P. 887-896.

І.М. Аверічев,
доцент каф. Технічних систем кіберзахисту
П.М. Поночовний
доцент каф. Технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій

МЕТОДОЛОГІЯ АДАПТИВНОГО ЗАХИСТУ ГІБРИДНИХ ІКС ВІД APT-ЗАГРОЗ НА ОСНОВІ АНСАМБЛЕВИХ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Сучасна парадигма побудови інформаційно-комунікаційних систем (ІКС) характеризується масовою міграцією до гібридних архітектур, де поєднуються локальні обчислювальні потужності (On-premise) та хмарні середовища (Cloud). Така гетерогенність створює розширену поверхню атаки, яку активно експлуатують зловмисники за допомогою складних постійних загроз (Advanced Persistent Threats — APT).

Ключовою проблемою є неефективність класичних сигнатурних методів (IDS/IPS) та статичних правил SIEM-систем проти APT-атак, які використовують техніки "Living off the Land" (LotL) — легітимні інструменти адміністрування для зловмисних цілей. Існуючі засоби часто генерують надмірну кількість хибних спрацьовувань (False Positives), що призводить до "втоми від сповіщень" (alert fatigue) у операторів SOC [1].

Метою роботи є підвищення рівня захищеності гібридних ІКС шляхом розробки **адаптивної моделі виявлення кіберзагроз**, яка базується на поведінковому аналізі та ансамблевих методах машинного навчання.

Для досягнення мети вирішуються наступні завдання:

- Синхронізація потоків подій безпеки з різнорідних джерел (системні журнали серверів, логи хмарних провайдерів AWS/Azure, NetFlow).

• Розробка моделі для виявлення аномалій у часових рядах мережевої активності.

• Зменшення затримки між проникненням та виявленням (Time-to-Detect) за допомогою автоматизованого кореляційного аналізу.

В основу методології покладено концепцію **Zero Trust ("Нульова довіра")**, посилену модулем штучного інтелекту. Система працює за принципом замкненого циклу [2]:

1. **Рівень агрегації:** Збір "сирих" даних та їх нормалізація.
2. **Рівень аналітики (ML Core):** Використання гібридного підходу:
   - *Unsupervised Learning (навчання без учителя):* Автоенкодери (Autoencoders) для виявлення відхилень від базового профілю нормальної поведінки сутності (UEBA) [3].
   - *Supervised Learning (навчання з учителем):* Градієнтний бустинг (XGBoost) для класифікації виявлених аномалій на відомі типи атак (Lateral Movement, Exfiltration)[4].
3. **Рівень реагування:** на рисунку 1 представлено динамічне коригування політик доступу.

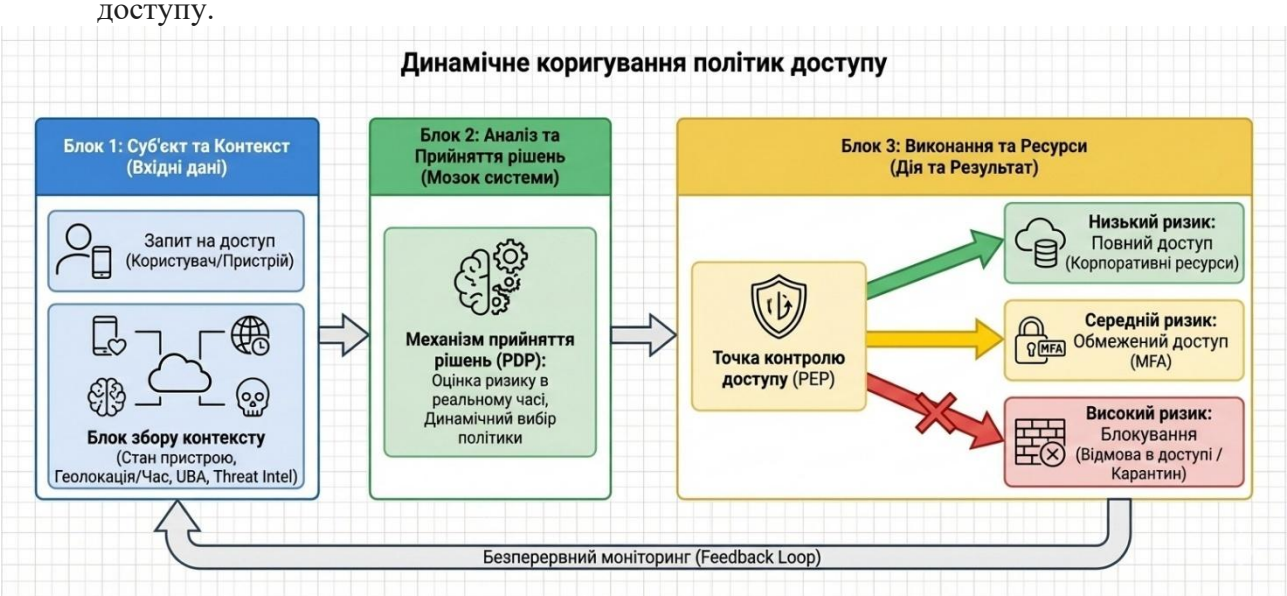

Рис. 1. Схема динамічного корегування політик доступу

4. Схема запропонованої архітектури. На рисунку 2 представлена структурна схема **автоматизованого конвеєра кібербезпеки**, що поєднує збір даних, штучний інтелект та автоматичне реагування. Вона описує повний цикл обробки інциденту:

- **агрегація (Блок 1):** Система збирає різнорідні "сирі" дані з операційних систем, хмари та мережі.
- **підготовка (Блок 2):** Дані нормалізуються та збагачуються контекстом для подальшого аналізу.
- **інтелектуальний аналіз (Блок 3):** Ключовий етап, де **Machine Learning** (автоенкодери, випадковий ліс) використовується для виявлення аномалій та класифікації конкретних типів загроз [7].
- **автоматична дія (Блок 4):** Система **SOAR** (Security Orchestration, Automation and Response) миттєво реагує на виявлену загрозу без участі людини (ізоляція, блокування) та сповіщає аналітиків (SOC) [5].

Схема демонструє перехід від реактивного моніторингу до **проактивного автоматизованого захисту** на основі даних.

Рис. 2. Схема запропонованої архітектури автоматизованого конвеєра кібербезпеки

Для опису запропонованої схеми необхідно визначити математичну модель перетворення вхідних даних (логів, трафіку) у керуючі впливи (реакцію SOAR). Нижче наведено математичний апарат, що описує кожен етап конвеєра: від векторизації даних до прийняття рішення про блокування.

Формалізація вхідних даних та попередньої обробки (Блок 1 та 2)

Нехай D — множина "сирих" подій, що надходять із джерел (Syslog, CloudTrail, Flow). Кожна подія $d_i \in D$ проходить процес **виділення ознак (Feature Extraction)** та перетворюється на вектор (1):

$$\boldsymbol{x} = \boldsymbol{\varphi}(\boldsymbol{d_i}) \in \boldsymbol{R^n} \quad (1)$$

де:

- $\boldsymbol{x}$ — вектор ознак (feature vector) розмірності n.
- $\boldsymbol{\varphi}$ — функція парсингу та векторизації.

Нормалізація даних: Для коректної роботи нейромереж виконується масштабування компонент вектора (наприклад, Min-Max нормалізація) (2):

$$\boldsymbol{x'_j} = \frac{\boldsymbol{x_j} - \mathbf{min}(\boldsymbol{X_j})}{\mathbf{max}(\boldsymbol{X_j}) - \mathbf{min}(\boldsymbol{X_j})} \quad (2)$$

де $\boldsymbol{x'_j}$ — нормалізоване значення j-ї ознаки.

Математична модель ядра аналізу (Блок 3)

Цей блок складається з двох підсистем, що працюють паралельно або послідовно.

А. Виявлення аномалій (Autoencoder / LSTM) Мета — виявити невідомі загрози $(0 - day)$, аналізуючи відхилення від "нормального" профілю. Використовуємо автоенкодер, який намагається стиснути і відновити вхідний вектор.

- Енкодер: $\boldsymbol{h} = \boldsymbol{f}(\boldsymbol{W_e x} + \boldsymbol{b_e})$
- Декодер: $\hat{\boldsymbol{x}} = \boldsymbol{g}(\boldsymbol{W_d h} + \boldsymbol{b_d})$

Функція прийняття рішення базується на **похибці реконструкції (Reconstruction Error)** (3):

$$\boldsymbol{L}(\boldsymbol{x}, \hat{\boldsymbol{x}}) = || \boldsymbol{x} - \hat{\boldsymbol{x}} ||^2 \quad (3)$$

Критерій аномалії (4):

$$\boldsymbol{A(x)} = \begin{cases} \mathbf{1}, \text{якщо } \boldsymbol{L(x, \hat{x})} > \boldsymbol{\theta} \\ \mathbf{0}, \text{інакше} \end{cases} \quad (4)$$

де $\boldsymbol{\theta}$ — порогове значення (threshold), визначене на етапі навчання. Якщо $A(x) = 1$, подія вважається аномальною.

Б. Класифікація загроз (Random Forest / XGBoost) Мета — визначити тип відомої атаки (DDoS, Bruteforce, Malware) [6]. Використовується ансамбль дерев рішень. Прогноз моделі для вхідного вектора $\boldsymbol{x}$ визначається як зважена сума прогнозів окремих дерев T_k (5):

$$\hat{y} = \arg max_{c \epsilon C} \sum_{k=1}^{K} f_k(x) \quad (5)$$

де:

- $\boldsymbol{C}$ — множина класів загроз (наприклад, {Normal, DDoS, SQLi}).
- $\hat{\boldsymbol{y}}$ — передбачений клас атаки.
- $\boldsymbol{P(\hat{y}|x)}$ — ймовірність (впевненість моделі) у цьому класі.

Функція реакції SOAR (Блок 4)

Блок реакції реалізує функцію відображення результатів аналізу на множину доступних дій: $R = \{Isolation, BlockIP, ResetSession, Notify\}$.

Функція прийняття рішення F_{SOAR} залежить від виявленої аномалії та класу загрози (6):

$$\boldsymbol{F_{SOAR}(x)} = \begin{cases} \boldsymbol{Block\ IP}, \text{якщо } \hat{\boldsymbol{y}} = \boldsymbol{DDoS} \text{ та } \boldsymbol{P(\hat{y})} > \mathbf{0.9} \\ \boldsymbol{Isolate\ Host}, \text{якщо } \hat{\boldsymbol{y}} = Malware \\ \boldsymbol{Reset\ Session}, \text{якщо } A(x) = 1 \text{ (аномалія поведінки)} \\ \boldsymbol{Notify\ SOC}, \text{якщо } P(\hat{y}) < 0.6 \text{ (низька впевненість)} \end{cases} \quad (6)$$

Запропонований математичний апарат дозволяє формалізувати задачу кіберзахисту як задачу **мінімізації ризику**, де:

1. **Автоенкодер** мінімізує пропуск невідомих атак через метрику відстані L.
2. **Класифікатор** максимізує точність розпізнавання відомих патернів.
3. **SOAR** виконує дискретну оптимізацію вибору контрзаходів на основі ймовірнісних оцінок ML-моделей.

5.Наукова новизна та очікувані результати

Наукова новизна полягає у вдосконаленні методу **динамічного профілювання сутностей** у гібридних системах. На відміну від існуючих аналогів, запропонована модель враховує крос-платформні кореляції (наприклад, аномальний вхід у хмару після підозрілого запиту до локальної бази даних).

Очікувані результати впровадження:

1. **Зниження False Positives Rate** на 15-20% завдяки використанню ансамблевих методів.
2. **Виявлення прихованих каналів** ексфільтрації даних, які пропускаються сигнатурними методами.
3. Забезпечення можливості **проактивного блокування** загроз на етапі розвідки (Reconnaissance).

6. Висновки

Інтеграція методів глибокого навчання в контур безпеки гібридних ІКС є необхідною умовою протидії сучасним APT-групуванням. Подальші дослідження будуть спрямовані на

використання навчання з підкріпленням (Reinforcement Learning) для повної автоматизації процесів реагування на інциденти.

Список використаних джерел:

1. **Di M., Gu L.** A Survey on Living-Off-The-Land Attacks: Detection and Mitigation. *IEEE Access*. 2021. Vol. 9. P. 91538–91556.
2. **Rose S., Borchert O., Mitchell S., Connelly S.** Zero Trust Architecture. *NIST Special Publication 800-207*. National Institute of Standards and Technology, 2020.
3. **Mirsky Y., Doitshman T., Elovici Y., Shabtai A.** Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. 2018.
4. **Chen T., Guestrin C.** XGBoost: A Scalable Tree Boosting System. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. 2016. P. 785–794.
5. **Islam C., Babar M. A., Nepal S.** Security Orchestration, Automation and Response (SOAR): A Systematic Mapping Study. *ACM Computing Surveys*. 2022.
6. **Ponochovny P.** Low-speed http ddos attack prevention model for end users. Cybersecurity: education, science, technique. 2024. Vol. 2, no. 26. P. 291–304. URL: https://doi.org/10.28925/2663-4023.2024.26.695.
7. Using the Latest Methods of Cluster Analysis to Identify Similar Profiles in Leading Social Networks. **Bohdan Zhurakovskyi, Ihor Averichev and Ivan Shakhmatov**. Information Technology and Implementation (Satellite) Conference Proceedings, 21 November, 2023. https://ceur-ws.org/Vol-3646/Paper_12.pdf

І.Д. Данилов, аспірант
Ю.В. Пепа,
професор каф. Технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій

ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ВИПРОМІНЮВАНЬ В ШУМОВИХ СИГНАЛАХ

Існуючі енергетичні виявлювачі радіосигналів здатні вловити сигнал з відношенням сигнал/шум не менше 20 дБ. Для енергетичних виявлювачів твердження про наявність сигналу робиться з його потужності [1]. LPI (Low-Probability-of-Intercept) – режим, який передбачає використання сигналів із низьким рівнем потужності. Зменшення випромінюваної пікової потужності призводить до зниження дальності передачі та ефективності радіомоніторингу.

Для станцій радіомоніторингу необхідна дальність виявлення в контрольованих зонах R1 або R2, що не можуть забезпечити енергетичні виявлювачі, які використовують тестові види сигналів. Отже, необхідно розробити виявлювач, здатний працювати не на потужності сигналу, а на інших фізичних принципах. Для вирішення цього завдання автори розглядають можливість застосування фрактального аналізу спектрограм прийнятого радіосигналу. Розглянутий варіант виявлювача слабких сигналів радіозакладних пристроїв на фоні широкосмугових сигналів на основі фрактального аналізу спектрограм дозволяє виявляти сигнали з відношенням сигнал/шум менше –5 дБ.

Результати були отримані на основі моделювання широкосмугових сигналів у середовищі PyCharm мовою програмування Python з низьким рівнем потужності та розрахунку фрактальних розмірностей спектрограм даних видів сигналів. За критерієм Пірсона доведено, що фрактальна розмірність підпорядковується нормальному закону розподілу, отже є можливість використання критерію виявлення Неймана-Пірсона. На його основі розраховані ймовірності правильного виявлення даних видів сигналів, які дозволяють зробити висновок, що при відношенні сигнал/шум менше –5 дБ забезпечується ймовірність правильного

виявлення більше 95%. Рішення про наявність слабкого сигналу приймається з урахуванням розрахунку фрактальної розмірності спектрограми прийнятого сигналу.

Висновки. Практична цінність даної роботи у тому, що фрактальний аналіз виявлених сигналів дозволяє виявити сигнал на більшій відстані (за межами зони R2) ніж із використанні енергетичного способу виявлення.

Результати фрактального аналізу спектрограм сигналу дозволяють виявляти слабкі сигнали радіозакладних пристроїв у широкосмугових сигналах з низьким рівнем потужності.

Список використаних джерел:

1. Diukov I. Algorithm for Adaptive Energy-Cyclostationary Detection of Noise-Like Signals // Military Science Journal, 2024. – No. 2(2). – P. 83-92.

Д.О. Римарчук, студент
А.О. Довгополий, студент
Державний університет інформаційно-комунікаційних технологій

ВИЯВЛЕННЯ ТА АНАЛІЗ АУДІО СПЕКТРУ

Цифровий спектральний аналіз є основою для обробки та дослідження сигналів у багатьох технічних та наукових галузях. Його розвиток тісно пов’язаний з цифровою обробкою сигналів. Перші методи спектрального аналізу [1] базувалися на аналогових фільтрах, що мали обмежену точність і гнучкість. З появою цифрових обчислювальних пристроїв з’явилася можливість більш точної, швидкої і гнучкої обробки сигналів.

Відомі методи – швидке перетворення Фур’є (FFT) значно знизило обчислювальні витрати. FFT дозволило виконувати спектральний аналіз у реальному часі навіть на обмежених за ресурсами мікропроцесорних системах.

Віконні методи використовуються для аналізу сигналів з часовою варіацією спектру, також були розроблені методи, що використовують віконні функції (наприклад, Хенінга, Хемінга) [2]. Такі методи допомагають зменшити спотворення спектру, які пов’язані з розривами сигналу.

Періодограми та спектральна оцінка застосовуються також для оцінки спектру сигналів. Розроблено різні підходи, такі як класична періодограма, усереднені періодограми та методи гладкої спектральної оцінки, що підвищують точність аналізу та зменшують вплив шуму.

Мультиплікативні та адаптивні методи — сучасні методи спектрального аналізу включають адаптивні алгоритми, які можуть змінювати параметри під час обробки сигналу, що дозволяє ефективніше виявляти зміни спектру в часі.

Досить часто використовують найпростіше вікно – прямокутне, це константа, яка не змінює форму сигналу. Воно еквівалентне відсутності вагового вікна. Одне з найпопулярніших вікон – вікно Хеммінга. Воно зменшує рівень розмиття спектру приблизно на 40 дБ щодо головного піку.

Вагові вікна розрізняються за двома основними параметрами: ступенем розширення головного піку та ступенем придушення розмиття спектру («бічних

пелюсток»). Чим сильніше є потреба придушити бічні пелюстки, тим ширшим буде основний пік. Прямокутне вікно найменше розмиває верхівку піку, але має

найвищі бічні пелюстки. Вікно Кайзера має параметр, який дозволяє вибирати потрібний ступінь придушення бічних пелюсток. Інший популярне вікно Хана. Воно придушує максимальну бічну пелюстку слабше, ніж вікно Хеммінга, проте інші бічні пелюстки швидше спадають при віддаленні від головного піку. Вікно Блекмана має більш сильне придушення бічних пелюсток, ніж вікно Хана.

Дуже важливо обрати «правильний» вид вагового вікна для аналізу аудіосигналу. Ефективними є вікна Хана чи Блекмана. Використання вагового вікна зменшує залежність форми спектра від конкретної частоти аудіосигналу та її збігу з сіткою частот FFT.

Створено ефективний та універсальний спектроаналізатор [2] аудіоспектру з вікнами Хана та Блекмана, що базується на платформі Arduino і відповідно програмується.

Його ключові особливості та переваги:

- необхідність такого пристрою виникає для аналізу спотвореного аудіо сигналу чи аудіозапису для виявлення на фоні шуму аудіо даних з їх подальшою обробкою;
- аналізатор аудіоспектру дозволяє вимірювати та візуалізувати спектральний склад аудіосигналів на цифровому дисплеї, що полегшує його сприйняття та оцінювання;
- програмований на Arduino Nano спектроаналізатор дозволяє розробляти та впроваджувати нові функції для аналізу звукових сигналів за рахунок зміни програмної прошивки;
- аналізатор спектру живиться від персонального комп'ютера через USB-перехідник та має можливість передачі візуальної інформації і відліків гармонік спектру на дисплей комп'ютера для подальшої математичної та графічної обробки та аналізу даних.

Список використаних джерел:

1. Спектральний аналіз звукових сигналів. URL: https://eduportal.com.ua/articles/spectral-audio-analysis.html (дата звернення: 03.11.2025 р.).

2. Спектроаналізатор – що ми бачимо на ньому? URL: https://prosound.ixbt.com/education/spektr-analys.shtml (дата звернення: 01.11.2025 р.)

А.М. Котенко,
доцент каф. Технічних систем кіберзахисту,
Н.С. Бондаренко, студент
Державний університет інформаційно-комунікаційних технологій

ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ У МЕРЕЖЕВИХ КАНАЛАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ШЛЯХОМ ВИКОРИСТАННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX

У тезі розглядається підхід до забезпечення безпеки конфіденційної інформації у мережевих каналах від несанкціонованого доступу шляхом використання операційної системи Linux.

Пропонується систему захисту мережевих каналів передачі даних на базі операційної системи Linux побудувати застосуванням технічних, організаційних, програмних засобів (рис. 1) [1].

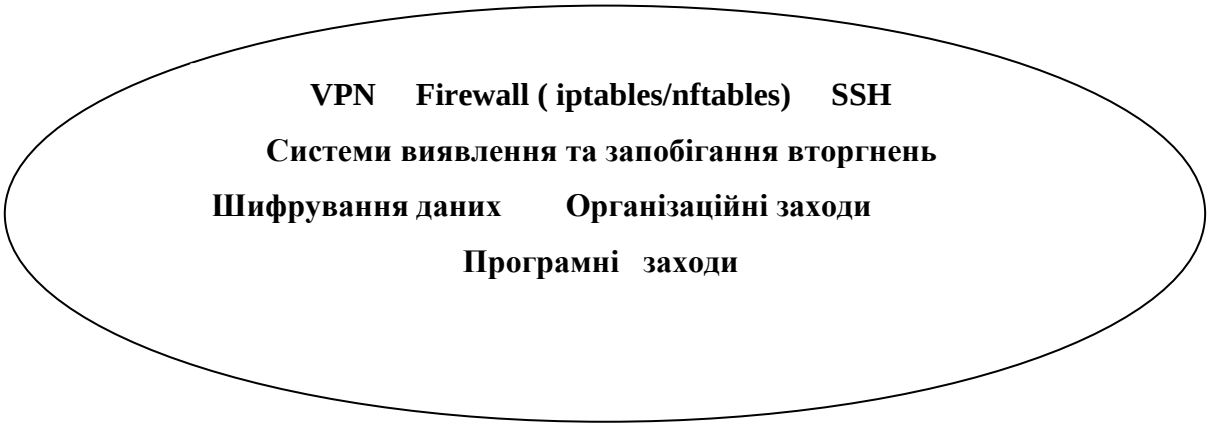

Рис. 1. Складові системи захисту мережевих каналів на базі ОС Linux

Розглянемо функціональність кожної складової.

Firewall (iptables/nftables) – міжмережеві екрани. Вони контролюють мережевий трафік, що входить в мережу і той що виходить з неї. Використання інтерфейсу налаштувань профілю доступу міжмережевого екрану, можливо для кожного користувача створити свій профіль. Цей профіль буде визначати права доступу цього користувача до мережі інтернет, і також права доступу до цього користувача з інтернету. Міжмережевий екран може блокувати передачу в мережу несанкціонованого трафіка та виконувати перевірку трафіка. Добре налаштований міжмережевий екран спроможний зупинити більшість відомих комп'ютерних атак. Міжмережеві екрани реалізуються програмно або апаратно.

VPN (Virtual Private Network). Даний засіб являє собою інтегрований з віртуальними мережами засіб захисту мережі, в цілому, її сегментів та кожного клієнта мережі окремо (захист TCP/IP трафіку який створюється додатками і програмами; захист робочих станцій, серверів WWW; автопроцесингу, транзакцій фінансових та банківських додатків, платіжних систем).

SSH (Secure Shell) - мережевий протокол прикладного рівня, який дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань. Забезпечує захист від перехоплення паролів та команд.

IDS/IPS - системи виявлення та запобігання вторгнень. Призначенням такого засобу є аналіз трафіку та виявлення підозрілої активності, що може свідчити про спробу несанкціонованого доступу. Для запобігання вторгненню, система або зупиняє здійснювану атаку перед її досягненням системи-жертви, або зупиняє дію атаки перед виконанням на системі-жертві коду, що використовує уразливість системи.

Шифрування даних. Метою даної складової є шифрування файлів та дисків для захисту даних на пристроях зберігання, та шифрування електронної пошти та файлів перед відправленням.

Призначенням *організаційних та програмних заходів* є [2]:

- *управління обліковими записами***.** Розуміється **в**икористання надійних паролів, їх регулярна зміна; обмеження прав доступу користувачів до необхідних.
- *регулярне оновлення системи.* Виконуються роботи з встановлення оновлень безпеки для операційної системи та програмного забезпечення для закриття відомих вразливостей.
- *роботи з навчання персоналу.* Проводяться тренінги з інформаційної безпеки для запобігання інцидентам які спричиняються людським фактором.

Застосування вищевикладених технічних, організаційних, програмних засобів дозволить забезпечити захист конфіденційної інформації у мережевих каналах від несанкціонованого доступу шляхом використання операційної системи Linux.

Список використаних джерел:

1. https://ela.kpi.ua/server/api/core/bitstreams/d99a0045-e907-4d17-afc1-5431f67d2444/content
2. https://elartu.tntu.edu.ua/bitstream/lib/29278/1/!!_Lek_print_zahust_123.pdf

Р.О. Чечко, студент
К.І. Раус, студент
Державний університет інформаційно-комунікаційних технологій

ОЦІНКА ЕФЕКТИВНОСТІ БІОМЕТРИЧНИХ СИСТЕМ

Широке використання біометричних систем у різних сферах людської діяльності, в тому числі і в сучасних інфо-комунікаційних системах, висуває на перший план надійність їх функціонування. Біометричні системи містять методи теорії перевірки статистичних гіпотез у математичній статистиці [1], які дуже широко та ефективно використовуються в сучасних

технічних системах. Надійність таких систем характеризується помилками першого та другого роду.

Розглянемо кількісну оцінку ефективності існуючих та нових біометричних систем. У відомих роботах [1, 2] щодо порівняльного аналізу біометричних систем, як правило, обговорюються їх характеристики та принципи роботи, однак, в них відсутні дані кількісної оцінки ефективності біометричних систем.

В роботі пропонується усунути цей недолік. В основу покладено критерій ефективність/вартість. При оцінці ефективності використовуються основні характеристики біометричних систем – помилки першого і другого роду, оцінки яких наводяться та аналізуються у науковій літературі [2]. При цьому є можливість врахування різних наслідків, зумовлених помилками першого та другого роду. Для цього запроваджується спеціальний коефіцієнт.

Проведено кількісний аналіз біометричних систем, які використовуються в сучасних системах контролю та управління доступом, а саме дактилоскопія, геометрія обличчя 2D та 3D і голос. За результатами досліджень найефективнішою виявилася дактилоскопія (відбитки пальців). Найгірші показники ефективності за розробленим критерієм має геометрія обличчя 2D, яка досить широко використовується в сучасних системах контролю та управління доступом.

Для підвищення ефективності голосових систем запропоновано знизити на порядок ймовірність помилкового розпізнавання за рахунок обліку фазових даних сигналів, що обробляються. Запропонований критерій відрізняється простотою, коректністю, ясністю, повнотою обліку основних характеристик надійності та достовірністю, а також може бути використаний для оцінки поточного становища відомих біометричних систем. Отримані результати можуть бути використані як на етапі розробки, так і вибору біометричних систем.

Список використаних джерел:

1. Горбенко І.Д., Олешко І.В. Методи біометричної автентифікації для використання в паспортній системі // Прикладна радіоелектроніка, 2011. – № 10(2). – С. 233-239.

2. Швець В.А., Фесенко А.А. Основні біометричні характеристики, сучасні системи та технології біометричної аутентифікації // Безпека інформації, 2013. –№ 19(2). – С. 99-111.

Є.В. Шарай, студент
Г.В. Чупрін, студент
Державний університет інформаційно-комунікаційних технологій

НЕБЕЗПЕЧНІ РАДІОВИПРОМІНЮВАННЯ ТЕХНІЧНИХ ЗАСОБІВ ОБРОБКИ ІНФОРМАЦІЇ

Технічні засоби, які не є радіопередавальними пристроями, також можуть бути джерелами небажаних електромагнітних випромінювань. Випромінювання таких технічних засобів обробки інформації називаються побічними електромагнітними випромінюваннями [1].

Існують різні причини виникнення побічних випромінювань. У ланцюгах різних пристроїв протікають змінні електричні струми, що породжують електромагнітні поля, що випромінюються в навколишній простір. Структура і параметри електромагнітних полів, створюваних струмопровідними елементами, визначаються конструктивними особливостями систем та засобів інформатизації та зв’язку, а також умовами їх розміщення та експлуатації. Такі електромагнітні випромінювання, наприклад випромінювання, що виникають при роботі ПЕОМ (випромінювання дисплея, підсилювачів запису та зчитування, кабельних з'єднань та ін.), є потенційними носіями небезпечного сигналу [2].

В окремих технічних засобах, наприклад у підсилювальних каскадах, можуть виникати паразитні випромінювання, зумовлені їх самозбудженням за рахунок паразитних позитивних зворотних зв'язків. Причини виникнення небажаних зворотних зв'язків у підсилювачах можуть бути різними. Параметри елементів радіоелектронної апаратури – конденсаторів, резисторів, котушок індуктивності, відрізків сполучних ліній – поза смужкою робочих частот істотно відрізняються від відповідних параметрів на робочих частотах. Наявність кінцевої індуктивності виводів елементів, різних паразитних ємностей, прояв властивостей ланцюгів з розподіленими параметрами, різні міжелементні сполуки утворюють велику кількість паразитних коливальних систем і зворотних зв'язків [2], властивості яких неможливо передбачити і врахувати заздалегідь.

На будь-якій частоті небажаний зворотний зв'язок може виявитися позитивним, а умови самозбудження – виконаними. Це призводить до виникнення паразитної генерації пристрою на цій частоті, передбачити яку заздалегідь практично неможливо. Причиною виникнення високочастотних коливань у транзисторних підсилювачах може стати їхнє перевантаження за рахунок впливу вхідного сигналу надмірно великого рівня. І тут нелінійність ємностей p-n переходів транзисторів призводить до параметричної генерації гармонік сигналу. Крім того, при впливі вхідних сигналів великого рівня може мати місце зміна внутрішнього зворотного зв'язку електронного приладу підсилювача, що за певних умов викликає самозбудження.

У цифрових інтегральних мікросхемах на відміну каскадів, виконаних на дискретних елементах, відстані між елементами значно менше, а самі елементи розташовані на підкладці, провідність якої вище провідності повітря. Це призводить до збільшення паразитних зв'язків. В інтегральних мікросхемах можлива також паразитна генерація, що виникає через відображення сигналу від кінців з'єднувальних ліній між цими мікросхемами внаслідок неузгодженості опорів джерела та навантаження з опором хвильовим сполучних ліній. Побічні випромінювання технічних засобів обробки інформації можуть мати місце в різних ділянках частотного діапазону і тому потрібно з ними боротися або здійснювати ефективний захист інформації від її витоку [3].

Небажані випромінювання різних пристроїв можуть містити небезпечні сигнали. У процесі функціонування технічних засобів обробки інформації елементи генераторів, підсилювачів та інших випромінюючих електромагнітних полів пристроїв можуть опинитися в зоні дії електромагнітних полів небезпечних сигналів. Вплив електромагнітного поля небезпечного сигналу на пристрої може призвести до зміни параметрів окремих елементів генератора або підсилювача (наприклад, крутизни S характеристики активного елемента, контурної ємності або індуктивності, ємностей p-n переходів транзисторів, опору навантаження каскаду та ін.). Результатом такої зміни є паразитна модуляція небезпечним сигналом небажаних випромінювань технічних засобів. Вид та кількісні параметри, що характеризують цю модуляцію, визначаються конкретною ситуацією.

Таким чином, зовнішній вплив електромагнітних полів небезпечних сигналів на елементи високочастотних генераторів, підсилювачів та інших технічних засобів може призвести до амплітудної та кутової модуляції високочастотних коливань у цих пристроях. Наслідком є поява у навколишньому просторі небажаних радіовипромінювань, модульованих небезпечними сигналами, тобто створюються передумови для витоку інформації, оброблюваної технічними засобами.

Список використаних джерел:

1. Горліченко С.О. Особливості формування технічних каналів витоку інформації від сучасних ІКС // Захист інформації, 2023. – Том 29. – № 2. – С. 80-87.

2. Любимов А.Я., Кудряшов В.О., Грабовський О.В., Богун В.Д., Добровольська С.В., Кудряшов С.В. Електроніка [Навч. посіб.]. – Одеса: ТОВ «ПЛУТОН», 2015. – 413 с.

3. Басюк Т.М., Литвин В.В. Технології захисту інформації. – Львів: Львівська політехніка, 2025. – 320 с.

Д.В. Мартиненко, студент
І.С. Іванченко,
доцент каф. Технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій

УДОСКОНАЛЕННЯ СИСТЕМИ БАГАТОФАКТОРНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА ПРИ РОБОТІ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

На сьогоднішній день питання захисту інформації з обмеженим доступом набуває критичного значення у контексті зростання кількості кіберзагроз та посилення вимог до інформаційної безпеки. Особливої актуальності це питання набуває для державних установ, фінансових організацій, медичних закладів та підприємств оборонно-промислового комплексу, де обробляється конфіденційна, таємна або персональна інформація. Традиційні методи ідентифікації та автентифікації, базовані на паролях, виявилися недостатньо надійними через вразливість до фішингу, підбору паролів та соціальної інженерії. Багатофакторна автентифікація стала стандартом захисту доступу до критичних систем, проте існуючі рішення потребують удосконалення для адаптації до сучасних загроз та вимог зручності використання.

Сучасні системи багатофакторної ідентифікації та автентифікації повинні забезпечувати баланс між високим рівнем безпеки та зручністю для користувачів. Класичні підходи до побудови таких систем включають комбінацію факторів знання (паролі, PIN-коди), факторів володіння (смарт-карти, токени, мобільні пристрої) та біометричних факторів (відбитки пальців, розпізнавання обличчя, голосу). Однак динаміка розвитку методів атак вимагає впровадження адаптивних механізмів автентифікації, які враховують контекст доступу, поведінкові характеристики користувача та рівень ризику операції.

Було розглянуто ряд сучасних релевантних наукових праць з точки зору удосконалення систем багатофакторної автентифікації. У роботі [1] досліджено ефективність різних комбінацій факторів автентифікації для систем з підвищеними вимогами до безпеки. Дослідження показує, що використання біометричних методів у поєднанні з криптографічними токенами забезпечує найвищий рівень захисту при прийнятному рівні зручності для користувачів. Робота [2] наголошує на важливості впровадження адаптивних систем автентифікації, які динамічно змінюють вимоги до автентифікації залежно від рівня ризику конкретної операції. Такий підхід дозволяє оптимізувати баланс між безпекою та зручністю, застосовуючи посилену автентифікацію лише у випадках підвищеного ризику. Дослідження [3] зміщує фокус уваги на поведінкову біометрію як додатковий фактор автентифікації. Аналіз патернів роботи користувача, динаміки набору тексту та навігації інтерфейсом дозволяє виявляти аномалії та потенційні спроби несанкціонованого доступу навіть після успішної первинної автентифікації.

У роботі [4] представлено архітектуру системи багатофакторної автентифікації з використанням технології блокчейн для забезпечення децентралізованого зберігання та верифікації ідентифікаційних даних. Така модель підвищує стійкість системи до атак на централізовані сервери автентифікації та забезпечує незмінність аудиційних записів про спроби доступу до інформації з обмеженим доступом.

Аналіз сучасних джерел дозволяє виокремити три найбільш перспективні напрямки удосконалення систем багатофакторної ідентифікації та автентифікації для роботи з інформацією з обмеженим доступом:

1. впровадження адаптивних систем автентифікації на основі оцінки ризику та контексту доступу;

2. інтеграція поведінкової біометрії як безперервного фактора верифікації користувача;

3. використання децентралізованих технологій для управління ідентифікаційними даними та протоколами автентифікації.

Перший напрямок надає можливість динамічно регулювати рівень захисту залежно від чутливості інформації, місця доступу, часу та інших контекстних параметрів, що забезпечує оптимальний баланс між безпекою та зручністю використання.

Другий напрямок дозволяє здійснювати безперервний моніторинг автентичності користувача протягом всієї робочої сесії без необхідності повторної явної автентифікації, що підвищує захист від атак типу перехоплення сесії.

Третій напрямок відкриває перспективні можливості для створення стійких до компрометації систем управління доступом, де відсутність єдиної точки відмови підвищує загальну надійність системи захисту інформації з обмеженим доступом.

Висновки

Таким чином, найбільш перспективним є перехід від статичних багатофакторних систем автентифікації до інтелектуальних адаптивних рішень, які інтегрують традиційні фактори автентифікації з поведінковим аналізом та контекстною оцінкою ризиків. Напрямки перспективних розробок включають створення гнучких архітектур, здатних адаптуватися до специфічних вимог різних категорій інформації з обмеженим доступом при врахуванні сучасних потенційних загроз та методів атак на системи ідентифікації та автентифікації.

Список використаних джерел:

1. NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management. *National Institute of Standards and Technology*. 2024. URL: https://pages.nist.gov/800-63-3/sp800-63b.html

2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. *International Organization for Standardization*. 2022. URL: https://www.iso.org/standard/27001

3. Continuous Authentication in the Digital Age: An Analysis of Reinforcement Learning and Behavioral Biometrics / P. Bansal et al. *Computers*. 2024. Vol. 13, № 4. DOI: https://doi.org/10.3390/computers13040103

4. Selecting Secure Multi-factor Authentication Solutions. *National Security Agency (NSA)*. 2020. URL: https://media.defense.gov/2024/Jul/31/2003515137/-1/-1/1/MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.PDF

5. Context-Aware Multi-Factor Authentication in Zero Trust Architecture: Enhancing Security Through Adaptive Authentication / S.R. Kandula, N. Kassetty. *International Journal of Global Innovations and Solutions (IJGIS)*. 2024. DOI: https://doi.org/10.21428/e90189c8.f525ef41

Г.В. Акулін, доцент кафедри ВП
В.А. Кононеко, викладач кафедри ВП
НТУУ «КПІ ім. Ігоря Сікорського»

«ОСОБЛИВОСТІ ЗАХИСТУ КАНАЛІВ УПРАВЛІННЯ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ В УМОВАХ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ».

Основні загрози для каналів управління БПЛА в умовах РЕБ включають наступні. Глушіння (jamming**)** - противник створює інтенсивні радіоперешкоди у діапазонах, якими користується БПЛА. Це призводить до: втрати керування; переходу апарата в аварійний

режим; зниження точності передачі телеметрії та відео. Спуфінг (підміна сигналу) - підміна навігаційних сигналів, особливо GPS/GNSS. Наслідки: БПЛА може відхилитися від маршруту; повернутися на фальшиву «точку домівки»; втратити орієнтацію в просторі. Перехоплення управління. Якщо канал погано захищений, противник може: зламати канал зв'язку; отримати контроль над БПЛА; заволодіти відеопотоком або телеметрією.

Особливості побудови захищених каналів управління

Шифрування

Надійне шифрування команд та телеметрії значно ускладнює перехоплення й декодування сигналу. Основні принципи:

- використання сучасних криптоалгоритмів;
- регулярна зміна ключів;
- мінімізація незашифрованих службових сигналів.

Стрибкоподібна зміна частот (FHSS)

Система швидко перемикає робочу частоту у випадковій або заздалегідь визначеній послідовності. Переваги:

- ускладнення глушіння;
- зменшення ймовірності визначення частоти роботи БПЛА;
- підвищена стійкість до завад.

Використання вузькосмугових, малопомітних сигналів

Сигнал низької потужності з малою шириною каналу важче виявити і заглушити. Це підвищує прихованість польоту.

Резервування каналів

Зазвичай використовують одночасно кілька каналів:

- радіоканал управління;
- супутниковий канал;
- автономні бортові алгоритми управління.

У разі глушіння один канал може заміняти інший.

Технологічні заходи підвищення стійкості БПЛА

Автономні режими керування

Для мінімізації впливу РЕБ дрон має мати:

- автономне утримання курсу;
- можливість завершити завдання без постійного зв'язку;
- алгоритми уникнення небезпечних зон.

інтеграція інерціальних навігаційних систем (INS)

INS забезпечує навігацію без зовнішніх сигналів, що важливо при глушінні GPS.

Використання альтернативних навігаційних систем

Наприклад:

- оптична навігація (за зображенням місцевості);
- радіомаяки;
- датчики руху та висоти.

Зниження радіопрофілю

Сюди входить:

- зменшення потужності передачі;
- короткі імпульсні сеанси зв'язку;
- спрямовані антени.

Тактичні та організаційні аспекти протидії РЕБ

Планування польотів з урахуванням РЕБ

- уникнення зон активних РЕБ;
- використання максимальних висот і траєкторій для зменшення впливу завад;
- розвідка частот і спектрів перед польотом.

Постійний аналіз сигналу

Бортові системи повинні:

- фіксувати рівні шуму;
- виявляти глушіння;
- автоматично перебудовувати частоту або режим.

Взаємодія з іншими засобами

Підрозділи РЕБ власної сторони можуть створювати «вікна» для роботи дронів — тимчасові ділянки простору, де завади мінімальні.

Висновок

Захист каналів управління БПЛА в умовах сучасної радіоелектронної боротьби є критично важливим елементом для збереження ефективності та живучості безпілотних систем. Поєднання технічних, криптографічних та тактичних заходів дозволяє істотно знизити вплив ворожих засобів РЕБ. Найбільш успішними є комплексні системи, які використовують одночасно шифрування, частотну маневреність, автономні алгоритми та інтелектуальну адаптацію до умов середовища.

Список використаних джерел:

1. Кочерга, І. О. (2023). *Підвищення ефективності застосування безпілотних літальних апаратів в умовах протидії засобів радіоелектронної боротьби*. Харків: ХНУВС. Отримано з https://dspace.univd.edu.ua/items/d39d59a3-a472-4a22-bfbb-99ef0d1451cc

2. Казіміров, О. О., Поліщук, М. М., & Бондар, С. В. (2025). Проблемні питання застосування засобів радіоелектронної боротьби для протидії БПЛА. *Збірник наукових праць Харківського національного університету Повітряних Сил*, 2(74), 56–61. https://journal-hnups.com.ua/index.php/zhups/article/download/1920/1745

3. Бибик, Р. В. (2025). Електромагнітні загрози в сучасних конфліктах: аналіз джерел РЕБ та їх вплив на системи ураження. *Сучасна безпека: науковий журнал*, 4(32), 88–97. https://csecurity.kubg.edu.ua/index.php/journal/article/download/748/608

ЗМІСТ