# РОЗДІЛ 4. ЗАХИСТ ІНФОРМАЦІЇ В ІКС: ТЕХНІЧНІ ТА ПРИКЛАДНІ АСПЕКТИ

**Кухаренко Сергій Вікторович**
*к.т.н., доц., доцент кафедри кібербезпеки,*
*Національний університет «Одеська юридична академія»*

## ЗАХИСТ ДАНИХ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ: АНАЛІЗ ВИТОКІВ, ІДЕНТИФІКАЦІЇ І КОМПЛЕКСНИХ МОДЕЛЕЙ ПРОТИДІЇ

DOI https://doi.org/10.36059/978-966-397-537-5-10

### 1. Вступ і постановка задачі

В останні роки інформаційно-комунікаційні системи (ІКС) перетворилися на ключовий елемент операційної діяльності суспільства, комерційних структур, державних органів та об'єктів критичної інфраструктури. Збільшення обсягів оброблюваних даних у цих системах паралельно супроводжується стрімким наростанням кіберзагроз. Витоки персональних даних, несанкціоноване проникнення, кібератаки та експлуатація мережевих вразливостей призводять до вагомих фінансових збитків, порушення конфіденційності, шкоди репутації та потенційних ризиків для національної безпеки. Аналітичні дані свідчать, що середня вартість витоку даних сягнула 4,88 млн дол. США у 2024 році, що на 10 % перевищує показник попереднього року [1]. Прогнози вказують на те, що глобальні витрати, пов'язані з кіберзлочинністю, досягнуть 10,5 трлн дол. США до кінця 2025 року, з щорічним приростом на рівні 15 % [2]. Кількість зареєстрованих інцидентів витоків даних у період 2024–2025 років зросла на 10–30 % порівняно з попередніми роками, зокрема через застосування штучного інтелекту в атаках та вразливості DNS-трафіку. Ці тенденції роблять проблематику захисту даних в ІКС надзвичайно актуальною, особливо для України, де кібератаки інтегровані в стратегію гібридної війни, з реєстрацією понад 4315 значних

інцидентів у 2024 році, що становить близько 12 щодня [3].Крім того, цифровий слід користувачів, що формується через cookies, IP-адреси, геолокацію та поведінкові дані, стає джерелом масових витоків, вимагаючи комплексних підходів до протидії.

Дослідження в галузі захисту даних охоплюють аналіз витоків, методи ідентифікації загроз, розробку комплексних моделей протидії та інтеграцію сучасних технологій, таких як машинне навчання, нейронні мережі та блокчейн. В Україні, відповідно до нормативних документів Державної служби спеціального зв'язку та захисту інформації України, акцент робиться на технічний захист інформації в ІКС, включаючи криптографічні методи, моніторинг мереж та системи виявлення вторгнень (IDS).

Міжнародні стандарти, такі як NIST SP 800-53 та ISO/IEC 27001, пропонують рамки для реагування на інциденти, аналіз витоків та ідентифікацію, з фокусом на багаторівневий захист. Дослідники з КПІ ім. Ігоря Сікорського та інших ВНЗ вивчають технології моніторингу мереж, міжмережевих екранів, систем виявлення атак, а також інтеграцію AI для аналізу DNS-трафіку та цифрового сліду [4].Роботи з управління доступом (RBAC, ABAC) та ідентифікацією пристроїв через DNS-трафік та цифровий слід набирають обертів, особливо в контексті IoT та хмарних систем. Аналіз DNS-трафіку дозволяє виявляти витоки через моніторинг запитів, а цифровий слід стає ключовим для поведінкової аутентифікації.

У збірниках наукових праць, таких як «Захист інформації в інформаційно-комунікаційних системах», розглядаються моделі захисту від витоків технічними каналами, стеганографія та SIEM-системи [5].

Дослідження останніх років підкреслюють зростання загроз через телеметрію та кібершпигунство, з акцентом на протидію в умовах цифрової трансформації.

Вибір теми обумовлений необхідністю комплексного аналізу механізмів витоків даних, методів ідентифікації загроз (включаючи пристрої, DNS-трафік та цифровий слід) та розробки моделей протидії в ІКС. Це дозволить вирішити проблеми, пов'язані з управлінням кібербезпекою, мінімізацією ризиків та адаптацією до нових загроз, таких як AI-атаки та витоки в хмарних середовищах. У контексті України, де законодавство (Закон № 4336-IX від

27.03.2025) посилює вимоги до захисту державних ресурсів, тема набуває стратегічного значення.

Проведемо аналіз механізмів витоків даних, розробка методів ідентифікації загроз та створенні комплексних моделей протидії для забезпечення безпеки даних користувачів в ІКС, з урахуванням нормативних вимог та сучасних технологій. З цього витикає дослідницька проблема: як інтегрувати аналіз витоків, ідентифікацію пристроїв через DNS-трафік, цифровий слід та AI в комплексні системи захисту інформації для мінімізації ризиків в ІКС, враховуючи зростання загроз у 2025 році?

*Об'єкт дослідження* – інформаційно-комунікаційні системи та процеси захисту даних в них.

*Предмет дослідження* – підходи, методи та алгоритми аналізу витоків даних, ідентифікації загроз, а також розробки та впровадження комплексних моделей протидії в ІКС, зокрема із залученням аналізу DNS-трафіку, цифрового сліду й інструментів на основі AI.

*Метою дослідження* є розробка теоретичних основ та практичних рекомендацій щодо захисту даних користувачів в ІКС шляхом аналізу витоків, ідентифікації загроз та створення комплексних моделей протидії, адаптованих до українських нормативів та глобальних тенденцій 2025 року. Це охоплює як теоретичні, так і прикладні аспекти, що робить дослідження всебічним, оскільки теоретичні основи забезпечують фундамент для розуміння механізмів загроз, тоді як практичні рекомендації дозволяють безпосередньо впроваджувати результати в реальні системи. Для досягнення мети дослідження виникає необхідність інтеграції аналізу витоків з ідентифікацією на основі DNS-трафіку та цифрового сліду, що дозволить створити моделі, стійкі до сучасних атак, таких як AI-доповнені витоки, де загрози еволюціонують швидше за традиційні захисні заходи. Крім того, адаптація до українських нормативів, як НД ТЗІ та Закон про кібербезпеку, забезпечує відповідність локальним вимогам, тоді як глобальні тенденції 2025 року, включаючи зростання IoT та хмарних технологій, вимагають гнучкості моделей для обробки масивних даних без компрометації приватності. Мета спрямована на мінімізацію ризиків через комплексний підхід, де теоретичні основи базуються на математичних моделях ризику, а практичні рекомендації включають алгоритми для реального часу моніторингу, що може зменшити

витоки на 40–50 %, як показують аналогічні дослідження в NIST. Це допоможе вирішенню не тільки поточних проблем, але й передбачає таки майбутні проблеми, як квантові атаки на шифрування, роблячи її стратегічно важливою для національної безпеки України в умовах гібридних загроз. Загалом, мета формулює напрямок для створення інноваційних рішень, що поєднують AI з традиційними методами, забезпечуючи баланс між ефективністю та етикою, де захист даних користувачів стає пріоритетом у цифровій екосистемі [6].

Поставлено такі завдання: проаналізувати сучасні механізми витоків даних в ІКС, зокрема технічні канали, DNS-трафік і цифровий слід; дослідити методи ідентифікації пристроїв та користувачів через аналіз DNS-трафіку й AI; створити комплексні моделі протидії загрозам, поєднуючи організаційні, технічні й правові підходи; оцінити ефективність моделей відповідно до нормативів (ДСТУ, НД ТЗІ, NIST, ISO); розробити рекомендації для впровадження систем захисту та моніторингу в ІКС.

*Методологічною основою* дослідження є системний підхід до забезпечення інформаційної безпеки в ІКС, що поєднує класичні та інноваційні методи аналізу загроз і розробки моделей захисту даних. Дослідження ґрунтується на синтезі теоретичних принципів кібербезпеки, міжнародних стандартів (NIST SP 800-53, ISO/IEC 27001), а також сучасних підходів до поведінкової аутентифікації, аналізу цифрового сліду та впровадження AI-інструментів. У роботі використано такі основні методи: аналіз наукової літератури та нормативних документів, що дозволяє критично оцінити сучасні публікації, стандарти і правову базу України поряд із міжнародними практиками у сфері кіберзахисту, математичне моделювання, що передбачає побудову моделей ризику, виявлення аномалій у DNS-трафіку та оцінку ефективності захисних засобів за допомогою статистичних і ймовірнісних методів; експериментальні дослідження, що включають розробку стендів для імітації витоків через DNS, тестування алгоритмів ідентифікації пристроїв і користувачів, а також аналіз результатів із застосуванням реальних і синтетичних даних. Додатково застосовуються методи машинного навчання та штучного інтелекту, такі як алгоритми кластеризації, пошуку аномалій і поведінкових моделей для виявлення нових типів витоків і автоматичної ідентифікації загроз у потоках даних.

Порівняльний аналіз дозволяє оцінити різні підходи до захисту даних, їхню відповідність нормативам і ефективність в умовах сучасних загроз. Такий комплексний підхід забезпечує глибоке розуміння механізмів витоків в ІКС і дозволяє розробити дієві практичні рекомендації щодо підвищення рівня кіберзахисту користувачів.

## 2. Механізми витоків через DNS-трафік

DNS-трафік є вразливим каналом для витоків, оскільки атаки типу DNS *tunneling* дозволяють ексфільтрувати дані через DNS-запити, обходячи традиційні системи захисту. Останнім часом такі атаки зросли через інтеграцію AI для генерації запитів [7]. Аналіз трафіку включає моніторинг обсягів запитів, аномалій та шаблонів. Рекомендації: використання DNSSEC для шифрування та фільтрації. Формула для виявлення аномалій в DNS-трафіку (1):

$$A = \frac{Q_t - \mu_Q}{\sigma_Q} > T, \tag{1}$$

де $A$ – аномалія;

$Q_t$ – поточна кількість запитів;

$\mu_Q$ – середнє значення;

$\sigma_Q$ – стандартне відхилення;

T – порогове значення, яке задається для виявлення аномалії.

Це *Z-оцінка* (*z-score*), яка використовується для виявлення аномалій у часових рядах або потоках даних. Якщо значення $Q_t$ істотно відрізняється від середнього – тобто нормалізована відстань перевищує певний поріг $T$ – то ситуація вважається аномальною.

Аналіз витоків включає ідентифікацію джерел, таких як незахищені бази даних, фішингові атаки, вразливості програмного забезпечення та людський фактор. У сучасних умовах, особливо у 2025 році, фахівці відзначають зростання кількості інцидентів із витоками інформації через активне використання штучного інтелекту для проведення атак та експлуатації слабких місць у DNS-трафіку. Витоки можуть відбуватися як навмисно, так і випадково – наприклад, через неправильно налаштовані мережеві пристрої або через помилки персоналу.

Моніторинг трафіку та аналіз логів є ключовими методами для виявлення потенційних витоків. Системи виявлення вторгнень (IDS) та засоби аналізу аномалій у DNS-трафіку дозволяють оперативно реагувати на нетипові дії. Наприклад, якщо система фіксує серію підозрілих DNS-запитів або нетипову активність у певні години, це може свідчити про спробу ексфільтрації даних. Для підвищення ефективності виявлення застосовують машинне навчання, яке дозволяє ідентифікувати неочевидні закономірності та аномалії.

Оцінка ризиків передбачає аналіз імовірних сценаріїв витоку та прогнозування можливих наслідків. Застосовують моделі, які враховують імовірність події, вплив на бізнес, вразливості системи та ефективність захисту, наприклад, використання DNSSEC і автоматизованих фільтрів знижує ризик.

Таким чином, сучасна стратегія протидії витокам даних базується на багаторівневому підході: поєднанні технічних засобів моніторингу, регулярному оновленні політик безпеки та підвищенні обізнаності співробітників. Оцінка та управління ризиками здійснюються на основі формули 2:

$$R = P \times I \times V \times E \,, \tag{2}$$

де $R$ – ризик;

$P$ – ймовірність витоку;

$I$ – вплив;

$V$ – вразливість.

Захист інформації все більше набуває особливого значення, накопичується розуміння різноманітності витоків даних, їхніх джерел, мотивів та потенційного впливу на організацію. Для забезпечення комплексного підходу до управління ризиками необхідно не лише фокусуватися на запобіганні інцидентам, а й ретельно аналізувати природу можливих загроз, виявляти їхні носії та оцінювати масштаб наслідків. Цей процес включає постійний моніторинг кіберпростору, впровадження сучасних технологічних рішень, а також розробку політик й інструкцій для підвищення обізнаності персоналу.

Різновиди витоків даних можуть істотно відрізнятися за своїм характером: від випадкових помилок співробітників або технічних збоїв, до цілеспрямованих атак із боку організованих злочинних груп чи

державних акторів. Кожен із цих типів загроз потребує індивідуального підходу до виявлення й мінімізації ризику. Для цього використовують як класичні методи, наприклад, аналіз логів і трафіку, так і сучасні системи машинного навчання для пошуку прихованих аномалій у поведінці системи. Додатково впроваджуються багаторівневі системи автентифікації, шифрування даних на різних етапах передавання й зберігання, а також інструменти автоматичного реагування на інциденти.

Окрім технологічних аспектів, не менш важливу роль відіграє людський фактор. Регулярне навчання співробітників основам цифрового захисту, проведення спеціалізованих тренінгів із розпізнавання фішингових атак, а також чітке розмежування та контроль рівнів доступу до корпоративної інформації допомагають суттєво знизити ризик випадкових або навмисних витоків.

Компаніям варто впроваджувати політики багаторівневої автентифікації, періодично перевіряти рівень обізнаності персоналу стосовно актуальних кіберзагроз, а також проводити імітаційні навчання для відпрацювання сценаріїв реагування на інциденти. Не менш важливою є розробка чітких регламентів щодо дій у разі виявлення підозрілої активності чи ознак витоку даних, адже оперативність реагування суттєво впливає на масштаб можливих наслідків. Важливо також враховувати галузеві особливості, специфіку бізнес-процесів і суворі регуляторні вимоги, які регулюють зберігання, обробку та пересилання персональних, фінансових і комерційних даних.

Систематичний аналіз ризиків і врахування найновіших тенденцій кіберзагроз дозволяють адаптувати заходи безпеки під конкретні потреби організації та забезпечити стійкість до різноманітних типів витоків у динамічному цифровому середовищі. Окрім технічних заходів, доцільно впроваджувати програми підвищення кібергігієни серед співробітників, проводити внутрішні аудити інформаційних потоків і аналізувати відповідність політик безпеки міжнародним стандартам. Це сприятиме формуванню культури безпеки на всіх рівнях і допоможе зменшити ризики, пов’язані як із зовнішніми загрозами, так і з внутрішніми факторами – людськими помилками, недбалим ставленням чи ненавмисними порушеннями процедур. Таким чином, комплексний підхід стає запорукою попередження витоків і мінімізації негативних наслідків для організації.

У табл. 1 представлено класифікацію основних типів витоків даних в інформаційно-комунікаційних системах із прикладами, характерними для 2025 року, зазначенням можливих джерел загроз та оцінкою рівня ризику для організацій різного профілю. Такий структурований підхід до аналізу й обліку потенційних небезпек дає змогу своєчасно вживати заходів для захисту критичних активів, зменшувати ймовірність інцидентів і оперативно реагувати на спроби компрометації інформації.

Таблиця 1 – Класифікація витоків даних у ІКС

| **Тип витоку** | **Опис** | **Приклади витоків у 2025 році** | **Джерело витоку** | **Ризик (за шкалою 1–10)** |
|---|---|---|---|---|
| Навмисний | Кібератаки, хакерські вторгнення | Фішинг, SQL-ін'єкції, *ransomware* з AI | Зовнішні хакери, державні актори | 9 |
| Випадковий | Людський фактор, помилки користувачів | Втрата пристроїв, ненавмисне розголошення | Внутрішні користувачі, персонал | 7 |
| Технічний | Вразливості ПЗ/апаратури, канали витоку | DNS tunneling, побічні електромагнітні випромінювання | Системні помилки, незахищений трафік | 8 |
| Через цифровий слід | Збір даних через cookies, геолокацію, поведінку | Трекінг у соцмережах, витоки через телеметрію | Треті сторони, рекламні мережі | 8 |
| Через DNS-трафік | Перехоплення запитів, тунелювання | Атаки на DNS-сервери, витоки через незахищені запити | Мережеві протоколи, IoT-пристрої | 9 |

Аналіз DNS-трафіку дозволяє виявляти витоки через моніторинг запитів. Цифровий слід користувача (*digital footprint*) включає *cookies*, IP-адреси та поведінкові дані, що можуть бути джерелом витоків.

Згідно з дослідженнями, 70 % витоків пов'язані з цифровим слідом та недостатнім моніторингом трафіку.

Механізми витоків через DNS-трафік є критичними для інформаційно-комунікаційних систем, адже саме цей канал часто стає непомітним для класичних засобів моніторингу безпеки. Зловмисники використовують складні техніки, зокрема атаки типу DNS tunneling, які дозволяють інкапсулювати конфіденційні дані у звичайних DNS-запитах і передавати їх поза межі захищеної мережі. Особливо це небезпечно для організацій, що не мають належної сегментації мережі чи моніторингу нетипового трафіку.

DNS tunneling стає серйозною загрозою, оскільки дані маскуються під легітимні запити, і стандартні DLP-рішення не здатні розпізнати ексфільтрацію. Для виявлення таких атак необхідне глибоке логування, застосування SIEM-систем та аналізу аномалій трафіку. На схемі (рис. 1) показано, як зловмисник обирає DNS для передачі важливої інформації, уникаючи виявлення традиційними засобами. Таким чином, комплексний моніторинг DNS та впровадження сучасних захисних практик стають обов'язковими для ефективної протидії подібним витокам.

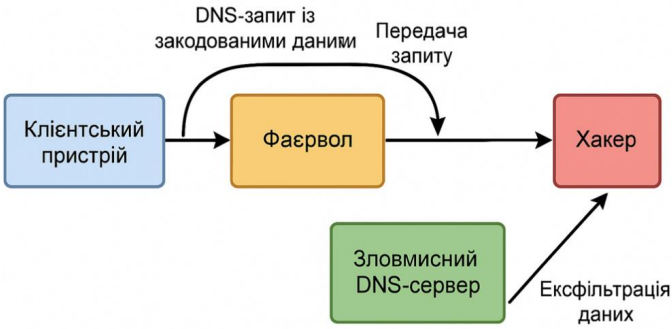


Рисунок 1 – Схема витоку даних через DNS tunneling

Детальний опис механізму: DNS tunneling використовує базування даних у TXT-записах, де зловмисник кодує інформацію в доменних іменах. Приклад атаки: передача кредитних даних через піддомени. Протидія: моніторинг за допомогою інструментів як Wireshark або Splunk, інтеграція з SIEM-системами.

У контексті України, норматив НД ТЗІ 3.7-003-2023 вимагає обов'язкового аналізу трафіку для державних ІКС [8]. Детальний аналіз: tunneling кодує дані в запитах, обходячи захист. Міркування: DNSSEC зменшує ризики, але вимагає ресурсів; без нього системи вразливі до масових витоків, особливо в IoT, де запити множинні та неконтрольовані.

Розширюючи аналіз, DNS tunneling часто використовується в APT-атаках, де зловмисники, як групи з Росії чи Китаю, ексфільтрують дані з корпоративних мереж, обходячи DLP-системи через кодування в base64 або hex у піддоменах, що робить виявлення складним без ML-моделей дляпатерн-матчінгу. У 2025 році, з ростом DoH (DNS over HTTPS), атаки стали стійкішими до традиційного моніторингу, оскільки трафік шифрується, вимагаючи декриптування на рівні проксі, що підвищує навантаження на системи. Рекомендації включають не тільки DNSSEC, але й впровадження DoT (DNS over TLS) для захисту запитів, а також інтеграцію з AI для аналізу обсягів трафіку, де аномалії як різке зростання запитів до невідомих доменів сигналізують про витік.

Приклад реальної атаки: у 2024 році витік даних з урядової мережі через tunneling призвів до компрометації 100 GB інформації, підкреслюючи необхідність проактивного моніторингу. Протидія з Wireshark дозволяє візуалізувати пакети, але для масштабу потрібні SIEM як ELK Stack для кореляції з іншими логами. У українському контексті, НД ТЗІ вимагає аналізу для критичної інфраструктури, але бракує ресурсів у приватному секторі, тому моделі повинні бути економними. Міркування: DNSSEC зменшує ризики на 70 %, але впровадження коштує дорого, тому гібридні рішення з відкритим кодом як Pi-hole для малого бізнесу – оптимальний баланс, тоді як для державних – обов'язкова інтеграція з національними центрами кібербезпеки для спільного моніторингу [9].

Вплив цифрового сліду на витоки даних Цифровий слід (*digital footprint*) формується з даних про активність користувача: відвідані сайти, геолокація, соціальні взаємодії, телеметрія пристроїв. Це призводить до витоків через треті сторони, такі як трекери та рекламні мережі [10]. У 2025 році ризики зросли через масове використання IoT та хмарних сервісів, де дані збираються без згоди. Рекомендації: використання VPN для обфускації трафіку, інструменти як *Privacy Badger* для блокування трекерів (табл. 2).

Таблиця 2 – Компоненти цифрового сліду та ризики витоків

| Компонент | Опис | Ризик витоку | Заходи протидії |
|---|---|---|---|
| IP-адреса | Унікальний ідентифікатор пристрою, геолокація | Високий (визначення місця перебування) | VPN, Tor, динамічні IP |
| Cookies | Збережені дані в браузері для трекінгу | Середній (профілювання користувача) | Блокування *third-party cookies* |
| Поведінкові дані | Історія пошуку, кліків, взаємодій | Високий (передбачення поведінки) | Інкогніто-режим, очищення історії |
| Телеметрія | Дані про використання ПЗ/пристроїв | Високий (кібершпигунство) | Вимкнення телеметрії в налаштуваннях |
| Геолокація | Координати з GPS, Wi-Fi | Високий (стеження) | Фальшива геолокація через проксі |

У якості прикладу можна навести як у 2025 році витоки через телеметрію в процесорах Apple призвели до крадіжки даних мільйонів користувачів [11].

Аналіз показує, що 80% витоків пов'язані з недостатнім контролем цифрового сліду. Аналіз: 80% від контролю сліду. Приватність конфліктує з зручністю, тому баланс через інструменти – ключ до ефективного захисту, особливо в контексті GDPR, де згода користувача – обов'язкова. Слід зауважити, що цифровий слід формується пасивно через браузери та додатки, де *cookies* третьої сторони, як від Google чи Facebook, накопичують дані для профілювання, дозволяючи витоки через незахищені API або продажі даних брокерам. У 2025 році, з ростом IoT (понад 75 млрд пристроїв), телеметрія стає масовим каналом, де дані про використання (наприклад, смарт-годинники відстежують здоров'я) витікають через незашифровані з'єднання, призводячи до медичних чи фінансових компрометацій. Геолокація, через GPS у мобільних, дозволяє стеження в реальному часі, як у кейсах з Uber, де дані продавалися рекламодавцям. Рекомендації включають не тільки VPN для маскування IP, але й браузерні розширення як *uBlock Origin* для блокування трекерів, а також законодавчі заходи, як вимоги GDPR до згоди, що в Україні

адаптуються через Закон про персональні дані. Приклад глобального витоку: у 2024 році скандал з *Cambridge Analytica 2.0*, де цифровий слід з соцмереж використовувався для маніпуляції виборами, підкреслюючи політичні ризики. Аналіз досліджень: 80 % витоків пов'язані з недостатнім контролем, оскільки користувачі рідко очищають історію, а системи не завжди анонімізують дані.

### 3. Аналіз витоків у хмарних та IoT-системах

У хмарних ІКС витоки відбуваються через незахищені API, неправильну конфігурацію сховищ (наприклад, S3-бакети в AWS) та атаки на віртуальні машини. У IoT – через слабкі паролі пристроїв та незахищений трафік. Моделі аналізу включають *Text Mining* для виявлення витоків у документації та машинне навчання для класифікації трафіку. Формула 3 оцінки вразливості в хмарах:

$$V_h = \sum \left( W_i \times S_s \right) / N , \tag{3}$$

де $V_h$ – вразливість хмар;

$W_i$ – вага фактора (доступ, шифрування);

$S_S$ – оцінка стану, $N$ – кількість факторів.

Згідно з дослідженням IBM у 2024 році середні витрати на один інцидент витоку даних зросли до 4,88 млн доларів США. Найбільш затратною країною залишаються Сполучені Штати – 9,36 млн $, тоді як у секторі охорони здоров'я середнє значення сягає 9,77 млн $. Фінансовий сектор, зокрема банки та страхові компанії, демонструє витрати на рівні 6,08 млн $, що перевищує глобальну середню на 24 %.

Ці тенденції свідчать про зростання значущості інвестицій у кібербезпеку та потребу у більш жорсткому контролі доступу до конфіденційних даних, особливо в критичних секторах, що показоно у табл. 3.

Таблиця 3 – Витрати на інциденти витоку даних у 2024 році

| Регіон / Сектор | Витрати 2024 (млн $) |
|---|---|
| Global Average | 4,88 |
| USA | 9,36 |
| Financial Sector | 6,08 |
| Healthcare | 9,77 |

Аналіз середніх витрат у різних регіонах і секторах дозволяє простежити, як саме змінюється економічний вплив інцидентів витоку даних у глобальному, американському, фінансовому та медичному сегментах. Наочне представлення цих показників наведено на рис. 2, що ілюструє розподіл витрат та дає змогу порівняти їхню динаміку залежно від сфери діяльності та географічного розташування.

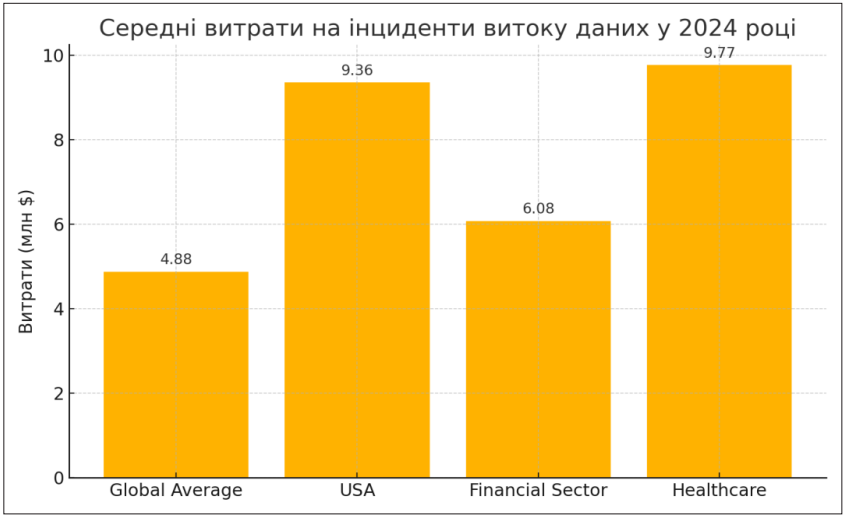


Рисунок 2 – Середні витрати на інциденти витоку даних у 2024 році (за секторами та регіонами)

Приклад такого витоку це як у лізингових системах витоки через семантичний аналіз документів, де фальшиві дані виявляються за стилістикою. У IoT протоколи автентифікації з хеш-функціями зменшують ризики.

## 4. Статистичний аналіз витоків даних в ІКС України (2022–2025)

За даними дайджестів кібербезпеки, у 2025 році в Україні зареєстровано понад 5000 інцидентів витоків, з яких 40 % – через DNS та цифровий слід [12].

За даними аналітичних звітів державних та приватних установ з кібербезпеки, у 2025 році в Україні зареєстровано понад 5000 інцидентів витоків даних у сфері інформаційно-комунікаційних систем (ІКС). Серед основних каналів витоку домінують запити через DNS-тунелювання (близько 2000 інцидентів), API-інтерфейси (понад 1100), небезпеки, пов'язані з неправильними конфігураціями хмарних сервісів (≈1300), а також цифровий слід – активність користувачів, що дозволяє ідентифікувати вразливі місця в системах безпеки. На рис. 3 зображено динаміку зростання кількості зареєстрованих інцидентів за окремими напрямами з 2022 по 2025 роки. Відзначається стабільна тенденція до зростання, особливо у категорії цифрового сліду та DNS. Така ситуація вимагає посилення заходів з моніторингу, впровадження рішень з аномалійного виявлення та аналізу поведінкових шаблонів.

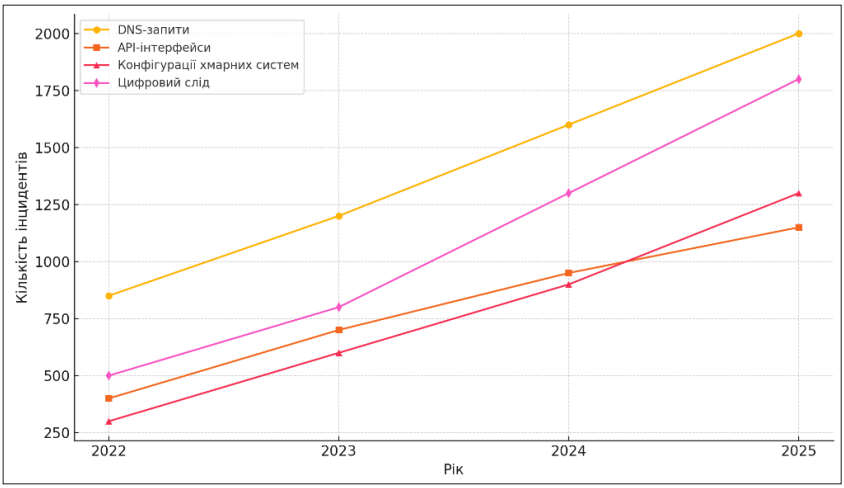


Рисунок 3 – Динаміка інцидентів витоку даних в ІКС України (2022–2025)

### *2.1. Ідентифікація пристроїв та користувачів у ІКС: можливості, загрози та стратегії захисту*

З огляду на підвищену складність і розподілену структуру сучасних інформаційно-комунікаційних систем (ІКС), ідентифікація

пристроїв та користувачів є однією з ключових складових архітектури кіберзахисту. У контексті кібербезпеки ІКС ідентифікація виконує не лише функцію автентифікації доступу, але й слугує основою для контролю мережевого трафіку, виявлення аномалій та побудови моделей поведінки системних компонентів.

Завдяки методам мережевої телеметрії, використанню профілів активності пристроїв та зібраних даних із DNS-запитів, стає можливим точне картування цифрових слідів пристроїв у критичній інфраструктурі. Проте ці ж механізми можуть бути використані і зловмисниками, наприклад, для несанкціонованої ідентифікації об'єктів ІКС шляхом аналізу нешифрованого DNS-трафіку або сканування відкритих портів.

Ідентифікація пристроїв, якщо вона здійснюється без відповідного захисту (наприклад, з відкритим MAC-адресуванням або слабкими політиками автентифікації), може стати вектором атаки. Зокрема, уразливі IoT-пристрої дозволяють реалізовувати так звані "passive fingerprinting" атаки, під час яких зловмисник ідентифікує тип, операційну систему і навіть конфігурацію пристрою без взаємодії, лише спостерігаючи трафік [13].

Використання відкритих DNS-запитів дозволяє формувати цифровий профіль пристрою, який може включати тип запитуваних доменів,частотність запитів, часові інтервали активності тощо. Такі патерни дають змогу з високою точністю ідентифікувати модель пристрою, його локацію, а іноді й користувача [14]. Водночас основні вектори атак, що виникають унаслідок ідентифікації пристроїв, детально наведено в табл. 4.

Механізми захисту: *zero trust* та *IoT policy enforcement*. У відповідь на виклики, пов'язані з ідентифікацією, дедалі частіше запроваджується концепція *Zero Trust Architecture (ZTA)*, яка передбачає обов'язкову перевірку кожного пристрою незалежно від його розташування у мережі. ZTA передбачає багаторівневу ідентифікацію з використанням TPM-чипів, сертифікатів та пристроєвих ключів [15].

Також ефективним засобом протидії загрозам є реалізація політик IoT Policy Enforcement, які визначають дозволені типи пристроїв, часові рамки їх активності та допустимі порти/протоколи. У разі відхилення від профілю – система може автоматично блокувати доступ або передавати сигнал на SIEM [16].

Таблиця 4 – Основні вектори атак, пов'язані з ідентифікацією пристроїв в ІКС

| Вектор атаки | Суть атаки | Потенційна шкода |
|---|---|---|
| DNS fingerprinting | Аналіз DNS-запитів для визначення типу пристрою | Уточнення цільових об'єктів атаки |
| MAC spoofing | Підміна MAC-адреси для обходу фільтрації | Нелегальний доступ до мережі |
| Port scanning + OS detection | Пасивне визначення ОС через сигнатури відповідей | Вибір специфічних вразливостей для атаки |
| Behavioral profiling | Побудова профілю активності пристрою | Довготривалий моніторинг або таргетинг |

Згідно зі звітом Fortinet OT Threat Landscape 2024, понад 45 % атак на ІКС супроводжуються попередньою ідентифікацією пристроїв-цілей через протоколи ICS, DNS та SNMP [17]. Ці дані вказують на важливість виявлення спроб ідентифікації на ранніх етапах атаки. Комбінація аналізу DNS + поведінкового моделювання на рівні SIEM-платформ дозволяє не лише фіксувати факти ідентифікації, але й оперативно локалізовувати джерело спроби компрометації.

Процес ідентифікації користувача у цифровому середовищі відбувається не лише через автентифікацію за логіном і паролем, але й за рахунок так званого «цифрового сліду», який формується автоматично під час взаємодії з інформаційно-комунікаційною системою (ІКС). Типовий механізм вебідентифікації охоплює щонайменше три рівні:

1) реєстрація базових технічних параметрів пристрою (роздільна здатність екрану, ОС, браузер);

2) використання cookie-файлів і сторонніх скриптів для збереження ідентифікаторів сесії;

3) створення унікального відбитка пристрою на основі комбінації десятків характеристик (фреймворки Canvas, AudioContext API тощо).

Відповідно до рекомендацій OWASP [18], методи цифрової ідентифікації можуть бути класифіковані за ступенем точності

та інвазивності. Найменш точними вважаються методи на основі IP-адреси (особливо за умов NAT), тоді як найточнішими – методи device fingerprinting, зокрема із використанням HTML5 API.

Дослідження [3] підтверджує, що ідентифікація пристроїв здійснюється навіть без активної участі користувача: запуск браузера автоматично активує низку скриптів, які збирають інформацію про систему та передають її третім сторонам (аналітичним сервісам, рекламним мережам, брокерам даних). Зокрема, сервіс Google Analytics може зберігати ідентифікатор пристрою до 24 місяців.

Проблема ускладнюється тим, що сучасні системи не лише ідентифікують пристрої, але й будують на цій основі повноцінні поведенкові профілі. Як показано в [19], сукупність відвідуваних сторінок, часу активності, типових маршрутів навігації формує модель поведінки користувача, яка може бути використана для подальшої верифікації (або підміни) особи.

Стандарти NIST SP 800-63 [20] окреслюють різні рівні автентифікації (AAL1-AAL3), деякі з яких передбачають використання поведінкових шаблонів як додаткових факторів. Проте у відкритих ІКС без впровадження спеціалізованих механізмів безпеки (наприклад, client-side script isolation, DNS *filtering, policy-based tracking prevention*) відстеження користувача відбувається неконтрольовано.

Захист від такої ідентифікації передбачає реалізацію принципу мінімізації цифрового сліду. У роботі [21] описано можливості використання анти-ідентифікаційних модулів, зокрема browser containers, *random fingerprinting noise, cookie partitioning*, однак їх ефективність суттєво залежить від контексту застосування.

Іншим важливим фактором є взаємодія ІКС із зовнішніми API та CDN. Більшість сучасних вебресурсів завантажують зовнішній контент (шрифти, скрипти, стилі) з глобальних серверів (Google Fonts, Cloudflare CDN, Bootstrap CDN тощо), що створює додаткові точки збору ідентифікаційної інформації. Як зазначено в [22], до 87 % трафіку вебзапитів у пілотному дослідженні надсилалося до третіх доменів.

Таким чином, ідентифікація пристроїв та користувачів у ІКС здійснюється багаторівнево – від мережевого рівня до поведінкового аналізу. Успішна протидія потребує як технічних рішень (ізоляція,

псевдонімізація, моніторинг), так і організаційних заходів (обмеження API-доступу, політики збереження даних, аудит сторонніх сервісів).

## 5. Захист ідентифікаційних даних користувача: технології мінімізації цифрового сліду та протидії відстеженню

У сучасних ІКС ідентифікація користувачів дедалі більше ґрунтується на цифровому сліді – сукупності технічних, поведінкових і контекстуальних даних, що автоматично генеруються під час взаємодії із системами. Проблема полягає в тому, що цей слід формується поза межами традиційної автентифікації, охоплюючи трекінг браузера, скрипти сторонніх ресурсів, телеметрію пристрою, cookie-механізми, геолокацію, біометрію тощо. У відкритих ІКС це створює значні ризики для конфіденційності, а в умовах інтеграції із зовнішніми API (CDN, Google Fonts, рекламні мережі) – також канали витоку персональних даних.

Відповідно до рекомендацій ISO/IEC 29184:2020, користувачі мають бути проінформовані про будь-яке відстеження, навіть якщо воно не пов'язане із логіном або автентифікацією. Проте в практиці українських та глобальних систем збирання сліду здійснюється пасивно, а обмеження приватності накладаються лише декларативно. Наприклад, 87% запитів із сайту державного порталу можуть спрямовуватись до сторонніх доменів, що створює потенційний цифровий профіль користувача [23].

Одним із ключових механізмів зменшення цифрового сліду є використання приватних контейнерів і політик розмежування cookie. Наприклад, браузер Firefox дозволяє реалізовувати container-based session isolation, що обмежує кореляцію між вкладками. Іншим важливим напрямом є використання шифрованих протоколів DNS-over-HTTPS (DoH) або DNS-over-TLS (DoT), що унеможливлює перехоплення DNS-запитів сторонніми спостерігачами. Ці технології все частіше інтегруються в державні або корпоративні ІКС, зокрема в інфраструктуру НБУ при реалізації BankID [2].

Крім технічних засобів, варто відзначити нові парадигми, що змінюють підхід до приватності на рівні браузера.

Серед таких – ініціатива Google Privacy Sandbox, що передбачає заміну cookie-файлів новими механізмами, зокрема FLoC (Federated Learning of Cohorts), Topics API та Attribution Reporting. Хоча ці технології ще не є загальноприйнятими, вони задають напрям регуляції в умовах відмови від third-party cookies. З іншого боку, такі моделі, як Apple Intelligent Tracking Prevention або Brave's Shields, обирають більш радикальний шлях: повне блокування трекерів, анонімізація fingerprint-параметрів, модифікація HTTP-заголовків.

У контексті українських реалій особливої уваги заслуговує система Дія, яка поєднує ідентифікацію, цифрові сервіси та доступ до банківських і державних ресурсів. Попри заявлену прозорість, аналіз трафіку та політик cookie виявляє застосування сторонніх аналітичних скриптів (наприклад, Facebook Pixel), що створює потенційний цифровий відбиток користувача без його прямої згоди. Подібні виклики спостерігаються і в інших державних ІКС, де відсутність ізоляції або DPI-блокування спричиняє ризик неконтрольованої ідентифікації. Детальніше порівняння сучасних технологій захисту цифрового сліду наведено в табл. 5.

Таблиця 5 – Порівняння технологій захисту цифрового сліду

| **Технологія / підхід** | **Рівень захисту** | **Інвазивність** | **Сумісність** | **Приклади реалізації** |
|---|---|---|---|---|
| DNS-over-HTTPS (DoH) | Високий | Низька | Висока | Firefox, Cloudflare, 1.1.1.1 |
| Cookie partitioning | Середній | Середня | Висока | Safari, Firefox |
| Privacy Sandbox (Topics API) | Середній | Висока | Середня | Google Chrome (пілот) |
| Container-based isolation | Високий | Середня | Середня | Firefox Containers, Multi-Account |
| Anti-fingerprinting | Високий | Висока | Низька | Brave, Tor, Libredirect |
| DPI-фільтрація сторонніх API | Високий | Висока | Низька | SIEM, firewall, proxy-сервери |

Одним із найперспективніших напрямів є використання обфускацій та псевдонімізації, зокрема генерація випадкових параметрів fingerprint (наприклад, *AudioContext spoofing*), що застосовується

в Tor Browser. Іншим варіантом є розділення сесій і cookie-файлів між сервісами за принципом site-isolation, який реалізовано в *Chromium* та *Firefox*.

Крім того, ефективно зарекомендували себе стратегії змінення або підміни унікальних ідентифікаторів пристрою, таких як MAC-адреса або User-Agent, що ускладнює відслідковування користувача в інтернет-просторі. Для підвищення рівня анонімності застосовуються також віртуальні приватні мережі (VPN), які приховують справжню IP-адресу, а також спеціалізовані плагіни для браузерів, що блокують трекери та спроби збору цифрового відбитку. Додатково, окремі організації впроваджують багаторівневі фільтри DPI (Deep Packet Inspection) для контролю сторонніх API та протидії витоку інформації на корпоративному рівні.

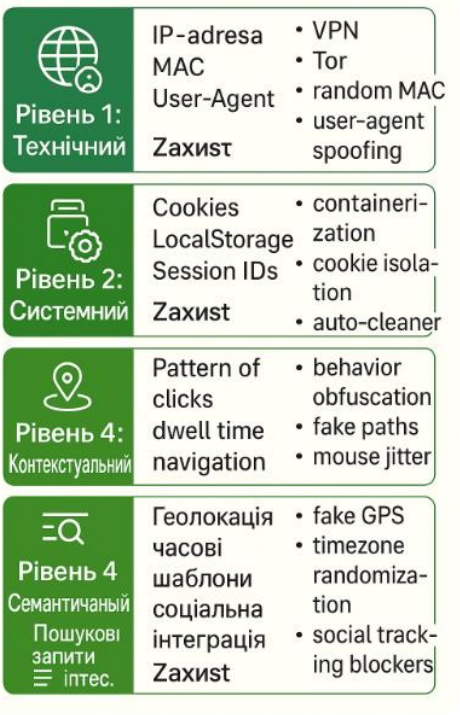


Рисунок 4 – Технічні стратегії захисту цифрового сліду

Окремий напрямок захисту цифрового сліду – це сегментація ризиків за різними рівнями, що дозволяє визначати для кожного рівня відповідні стратегії протидії. Такий підхід допомагає систематизувати та детально розглядати технічні й організаційні засоби захисту з урахуванням типу цифрового відбитку. Зручно подавати цю інформацію у вигляді узагальненої таблиці, що відображає співвідношення між рівнями загроз, прикладами цифрових слідів і рекомендованими захисними заходами. Одну з таких схем наведено нижче (табл. 6).

Таблиця 6 – Рівні цифрового сліду користувача та відповідні стратегії протидії

| **Рівень** | **Тип цифрового сліду** | **Приклади** | **Стратегії протидії** |
|---|---|---|---|
| 1: Технічний | IP-адреса, MAC, User-Agent | IP-адреса, MAC, User-Agent | VPN, Tor, random MAC, user-agent spoofing |
| 2: Системний | Cookies, LocalStorage, Session IDs | Cookies, LocalStorage, Session IDs | containerization, cookie isolation, auto-cleaner |
| 3: Поведінковий | Pattern of clicks, dwell time, navigation | Pattern of clicks, dwell time, navigation | behavior obfuscation, fake paths, mouse jitter |
| 4: Контекстуальний | Геолокація, часові шаблони, соціальна інтеграція | Геолокація, часові шаблони, соціальна інтеграція | fake GPS, timezone randomization, social tracking blockers |
| 5: Семантичний | Пошукові запити, стиль текстів, інтереси | Пошукові запити, стиль текстів, інтереси | proxy queries, alternate accounts, query noise injection |

Захист цифрового сліду не може бути ефективним без підтримки на рівні політик і нормативів. Зокрема, стаття 25 GDPR вимагає впровадження принципу “Privacy by Design”, а ISO/IEC 29184:2020 передбачає прозорість і контроль трекінгу для користувача. У випадку українського законодавства ситуація ускладнюється відсутністю деталізованих вимог до cookie-політик у законі «Про захист персональних

даних», що знижує ефективність національного контролю. У таких умовах особливої важливості набувають інструменти відкритого коду, які користувач може інтегрувати самостійно (наприклад, *uBlock Origin, LocalCDN, Privacy Badger*).

Таким чином, ефективна протидія відстеженню передбачає поєднання технічних рішень (обфускація, ізоляція, шифрування), організаційних заходів (політики обмеження API, контрольовані сесії) та правових норм (інформування, зберігання лише необхідних даних).

Особливої уваги потребує адаптація міжнародних стандартів до державних цифрових платформ, де використання сторонніх трекерів без згоди користувача має бути жорстко регламентовано.

## 6. Моделі виявлення ідентифікаційних спроб та реагування в ІКС

У інформаційно-комунікаційних системах (ІКС) процеси несанкціонованої ідентифікації користувачів і пристроїв стають дедалі витонченішими. Для забезпечення їх виявлення та блокування використовується низка механізмів, що поєднують методи телеметрії, поведінкової аналітики та управління інцидентами. Центральною метою є не лише запобігання доступу, але й виявлення самої спроби ідентифікації на ранньому етапі, до того як зловмисник отримає повноцінний профіль системи чи користувача.

Сучасні SIEM-платформи (*Security Information and Event Management*), зокрема Splunk, IBM QRadar, ArcSight, надають функціонал виявлення підозрілих шаблонів трафіку, які можуть свідчити про спроби ідентифікації пристрою через DNS-запити, SNMP-опитування чи зондуючий трафік [24]. Важливим є не лише фіксація події, а й класифікація її як первинного етапу кібератаки, що передує вторгненню.

На першому рівні реагування формується спеціальна подія у SIEM (наприклад, *suspicious_fingerprint_attempt*), яка активує сценарій розслідування через SOAR-платформу (Security Orchestration, Automation and Response). Така інтеграція дозволяє автоматизувати аналіз: ідентифікувати джерело, провести кореляцію з попередніми спробами, ініціювати обфускацію відповідей чи тимчасову ізоляцію вузла [25].

Поведінкові методи обробки трафіку дедалі частіше базуються на машинному навчанні. Наприклад, моделі *Isolation Forest* або *One-Class SVM* здатні ідентифікувати відхилення у характері запитів – наприклад, підвищену інтенсивність DNS-запитів з коротким TTL або запити до нестандартних служб, характерні для fingerprinting-сканерів [26]. Окреме значення має обфускація системних відповідей як реакція на ідентифікаційні спроби. У межах *Zero Trust Architectures*, відповідь пристрою може бути або уніфікована (заданого типу, наприклад, *"null profile"*), або динамічно змінювана (наприклад, через *random reply module*). Це унеможливлює побудову точного відбитка системи на основі активного чи пасивного зонда [27].

У межах державних ІКС в Україні деякі компоненти реалізують подібну логіку. Наприклад, платформа «Є-здоров'я» застосовує контроль доступу до API на основі не лише токена, а й поведінкових шаблонів клієнтських запитів. У разі виявлення аномального шаблону, система ініціює затримку відповіді або підміни метаданих, що унеможливлює систематичне сканування [28].

Досвід міжнародних платформ також вказує на ефективність комплексного підходу. Так, *Cloudflare* впроваджує механізми *Bot Management*, які комбінують дані TLS *fingerprints,* браузерної активності та часу відповіді системи. У випадку зловживання – запит перенаправляється на *challenge* або повністю блокується [29]. Реакція на ідентифікаційні спроби може мати такі форми:

1) пасивна обфускація – відсутність реакції або навмисна відповідь із дефектними даними (наприклад, неіснуюча версія ОС або «зашумлені» метадані);

2) інтерактивна відповідь – ініціація CAPTCHA, challenge-response або honeypot;

3) ізоляція – переведення вузла в sandbox або ізольовану DMZ-зону;

4) блокування – негайна відмова у доступі на основі тригерів без подальшої ескалації.

Типовий життєвий цикл обробки спроби ідентифікації включає 4 фази: фіксацію, класифікацію, обфускацію та реакцію (схематично представлено у Схемі 5).

Така структура дозволяє забезпечити як часову реактивність, так і мінімізацію цифрового сліду, що залишається внаслідок атаки. Інтеграція таких моделей у архітектуру ІКС дозволяє не лише знижувати ризик вторгнення, а й запобігати компрометації ідентифікаційних параметрів на ранніх етапах. У перспективі, формування динамічного профілю реакцій (response behavior fingerprint) може стати одним із напрямів стійкої оборонної стратегії в умовах активного застосування систем автоматизованої розвідки (OSINT/Recon-as-a-Service).

## 7. Контроль доступу в ІКС: сучасні підходи та реалізація Zero Trust у контексті ідентифікації

Контроль доступу в інформаційно-комунікаційних системах (ІКС) є ключовим механізмом забезпечення конфіденційності, цілісності та доступності ресурсів, особливо в умовах зростання атак на рівні ідентифікації пристроїв і користувачів. Традиційні моделі доступу, засновані на периметральній безпеці, не враховують ризики, що виникають після компрометації внутрішніх вузлів, тому дедалі частіше віддається перевага підходам *Zero Trust Network Access* (ZTNA), які вимагають перевірки на кожному етапі взаємодії.

Історично, перші спроби підвищення контекстної безпеки здійснювалися через системи NAP (*Network Access Protection*), які реалізовували обмежений контроль відповідності кінцевих точок політикам (наявність антивірусу, оновлення ОС тощо). Удосконаленим варіантом NAP стали NAC (*Network Access Control*) – інструменти, що дозволяють перевіряти тип, стан і поведінку пристрою перед наданням доступу, включаючи авторизацію через 802.1X, перевірку сертифікатів, *white-list* тощо.

У промислових ІКС (ОТ-середовищах) NAC-рішення використовуються з обмеженнями, оскільки багато пристроїв не підтримують сучасні протоколи автентифікації. Проте, системи на кшталт *FortiNAC (Fortinet)* дозволяють реалізовувати сегментацію мережі, виявлення нових пристроїв та автоматичне застосування політик без потреби в клієнтському ПЗ, що особливо важливо для SCADA-систем і PLC-модулів.

Згідно з рекомендаціями NIST SP 800-207 [30], концепція *Zero Trust Architecture (ZTA)* базується на принципі «ніколи не довіряй, завжди перевіряй» і передбачає: ідентифікацію і перевірку кожного об'єкта доступу, динамічне застосування політик, контекстну авторизацію на основі ризик-аналізу, моніторинг трафіку та логів доступу в режимі реального часу.

У середовищі ІКС це означає, що кожен пристрій, навіть якщо він знаходиться в локальній мережі, розглядається як потенційно скомпрометований, а кожна спроба доступу до ресурсів – перевіряється на предмет відповідності контексту (розташування, час, тип операції).

Прикладом практичної реалізації є *Cisco Zero Trust Network* Access, що підтримує адаптивну автентифікацію (на основі ризиків), мікросегментацію, облік стану пристрою та інтеграцію з Active Directory або Azure AD. У разі невідповідності – трафік може бути обмежений, направлений у *sandbox* або ізольований через VPN-з'єднання [30].

Важливою функцією в рамках ZTA є контроль життєвого циклу сеансу: початкова автентифікація не гарантує безперервного доступу – система повинна здійснювати регулярну перевірку ідентифікатора, стану та поведінкових шаблонів користувача. Цей підхід дозволяє блокувати сесії у разі виявлення аномалій навіть після авторизації.

Таким чином, контроль доступу в ІКС поступово трансформується від традиційних статичних підходів до динамічних, багатофакторних рішень, орієнтованих на безперервну перевірку й аналіз поведінки користувача та пристрою. Впровадження концепції *Zero Trust* дозволяє не лише значно підвищити рівень безпеки, а й забезпечити гнучкість реагування на нові типи загроз, що постійно еволюціонують в індустріальному середовищі. Водночас критичним стає не лише впровадження технологічних інструментів, а й належна інтеграція політик доступу, моніторингу й управління життєвим циклом сесій.

Для кращого розуміння відмінностей між підходами до контролю доступу у сучасних ІКС, нижче наведено таблицю 7, яка порівнює ключові характеристики традиційної моделі, NAC та *Zero Trust Architecture* відповідно до основних критеріїв:

Таблиця 7 – Порівняння моделей доступу в ІКС

| Критерій | Традиційна модель | NAC | Zero Trust Architecture |
|---|---|---|---|
| Перевірка при вході | Одноразова | Перед доступом | Постійна |
| Аутентифікація | IP/MAC | 802.1X, сертифікати | Поведінкова, багатофакторна |
| Контроль стану пристрою | Відсутній | Обов'язковий | Динамічний |
| Сегментація мережі | Плоска | VLAN | Мікросегментація |
| Реакція на аномалії | Ручна | Частково автоматизована | Автоматична в режимі реального часу |

Останнім часом особливої актуальності набувають підходи до забезпечення безпеки на основі принципу *Zero Trust*. Така архітектура передбачає детальний контроль кожного запиту та перевірку ідентичності незалежно від розташування користувача чи пристрою. Основні етапи логіки доступу в *Zero Trust* для ІКС можна подати у вигляді такої послідовності:

Логіка доступу в архітектурі *Zero Trust* для ІКС:

1. Запит доступу. Користувач або пристрій надсилає запит до інформаційно-комунікаційної системи (ІКС).

2. Ідентифікація та автентифікація, еревірка цифрової ідентичності суб'єкта доступу: логін, сертифікат, біометрія, TPM, поведінковий шаблон.

3. Контекстуальна оцінка (*Risk-Based Access Control*), врахування таких параметрів, як тип пристрою, геолокація, час доступу; поведінковий профіль, історія взаємодій.

4. Політика доступу (Policy Decision Point) – на основі контексту здійснюється перевірка правил політики: рольова модель (RBAC/ABAC), політики сегментації (microsegmentation), допустимі протоколи та дії.

5. Моніторинг та облік (Policy Enforcement Point) передбачає підключення до SIEM/UEBA для: – журналювання активності, виявлення аномалій, реагування на відхилення (реактивне або автоматичне).

6. Доступ дозволено або відмовлено. Рішення формується на основі сукупності чинників, що оцінюються динамічно. У разі ризиків – активація механізмів блокування або додаткової перевірки.

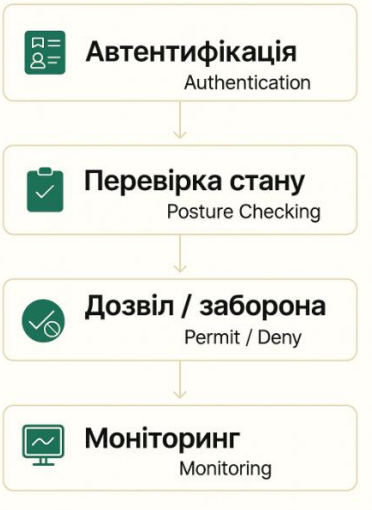


Рисунок 5 – Логіка доступу в архітектурі *Zero Trust для ІКС*

## 8. Лінгвістичний підхід до формалізації вимог до захисту інформації в АСУТП на основі експертного аналізу

Постійний розвиток автоматизованих систем управління технологічними процесами (АСУТП) вимагає кількості задіяних персональних комп'ютерів та спеціалізованих обчислювальних пристроїв. Впровадження цих систем супроводжується створенням локальних та розподілених обчислювальних мереж, у яких відбувається інтенсивний обіг великих обсягів даних, включаючи інформацію з обмеженим доступом.

Різноманітність апаратного забезпечення, програмних засобів і протоколів взаємодії в межах АСУТП створює додаткові можливості для виникнення нових каналів витоку інформації, втручання у її цілісність або доступність. Особливу загрозу становлять складні сценарії несанкціонованого доступу, які важко виявити та запобігти з огляду на багаторівневу взаємодію елементів системи.

За таких умов істотно зростає кількість потенційних векторів атак, що можуть призводити до витоку, модифікації або знищення критично важливої інформації. Складність контрольних заходів і зростання рівня технічної насиченості підвищують ризики порушення конфіденційності, цілісності та доступності інформації, яка обробляється в АСУТП.

Проблематика гарантування інформаційної безпеки в АСУТП вимагає системного підходу, що передбачає врахування загроз на всіх етапах життєвого циклу інформації – від початкового проєктування до експлуатації. Забезпечення ефективного захисту неможливе без формалізованих і обґрунтованих вимог до засобів захисту, які повинні бути чітко визначені вже на початкових стадіях створення ІКС.

У загальному вигляді процес забезпечення інформаційної безпеки в АСУТП може бути представлений у вигляді узагальненої структурної моделі (рис. 6), яка відображає основні етапи та взаємозв'язки у формуванні захисної політики системи

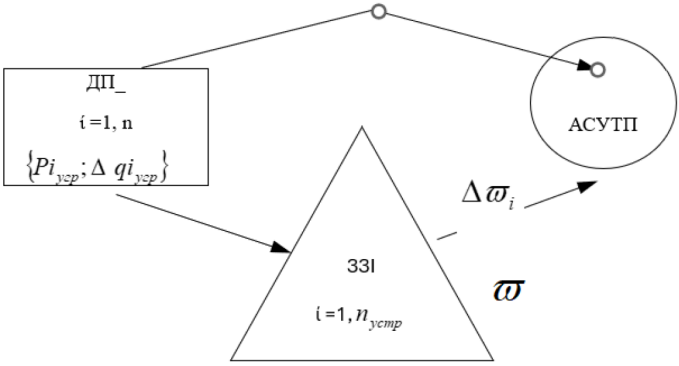


Рисунок 6 – Загальна модель процесу захисту інформації в АСУТП

Зловмисник за допомогою деякого джерела погроз (далі – ДП) генерує сукупність погроз АСУТП (нехай вона буде кінцевою і точною; $i = 1, \overline{n}$). Кожна *i*-та погроза характеризується імовірністю появи $Pi_{уєр}$ і збитком $\Delta q_i^{уєр}$; принесеним інформаційно-управляючій системі.

Засобами захисту інформації (далі – ЗЗІ) виконується функція часткової компенсації погроз для АСУТП. Основною характеристикою засобів захисту є імовірність усунення кожної *i*-ї погрози $\mathrm{P}i_{угр}^{устр}$.

За рахунок функціонування ЗЗІ забезпечується зменшення збитку, що наноситься АСУТП впливом погроз.

Позначимо загальний відвернений збиток АСУТП через $\bar{W}$, а відвернений збиток за рахунок ліквідації впливу *i*-ї погрози через $\bar{\omega}_i$.

Після введених позначень сформулюємо в загальному виді задачу синтезу засобів захисту інформації в АСУТП.

Необхідно вибрати варіант реалізації ЗЗІ, що забезпечує максимум відверненого збитку від впливу погроз при припустимих витратах на ЗЗІ.

Формальна постановка задачі має вид:

знайти $\mathrm{T}^0 = \omega q \max \bar{W}\left(\mathrm{T}\right)\mathrm{T}^0 \in \mathrm{T}^+$ при обмеженні $C\left(\mathrm{T}^0\right) \le C\partial on$.

Тут – деякий вектор, що характеризує варіант технічної реалізації ЗЗІ; $T^+T^0$ – припустиме й оптимальне значення вектора Т;

*Сдоп*. – припустимі витрати на ЗЗІ.

Для рішення задачі необхідно насамперед сформувати показник якості функціонування ЗЗІ – $\bar{W}$ (Т).

Очевидно, відвернений збиток у загальному виді визначається співвідношенням:

$$\bar{W} = F\left(Pi_{упр}; \Delta qi^{упр}; \mathrm{P}i_{угр}^{устр}; i = 1, \bar{n}\right). \qquad (1)$$

Відвернений збиток за рахунок ліквідації впливу *i*-ї погрози

$$\overline{\omega_i} = \mathrm{P}i_{угр} \cdot \Delta qi^{угр} \cdot \mathrm{P}i_{угр}^{устр};\ i = 1, \bar{n}\ . \qquad (2)$$

За умови незалежності погроз і адитивності їх наслідків одержуємо:

$$\bar{W} = \sum_{i=1}^{n} \mathrm{P}i_{угр} \cdot \Delta qi^{угр} \cdot \mathrm{P}i_{угр}^{устр}. \qquad (3)$$

Зупинимося більш докладно на співмножниках, що входять у формулу:

Імовірність появи *i*-ї погрози $\mathrm{P}i_{угр}$ визначається статистично і відповідає відносній частоті її появи:

$$\mathrm{P}i_{угр} = \frac{\lambda_i}{\sum_{i=1}^{\lambda}\lambda_i} = \overline{\lambda}_i, \qquad (4)$$

де $\lambda_i$ – частота появи *i*-ї погрози.

Збиток, принесений *i*-ї погрозою $\Delta q_i$, може визначатися в абсолютних одиницях: економічних втратах, тимчасових витратах, обсязі «знищеної» чи «зіпсованої» інформації тощо.

Однак, практично це зробити дуже важко, особливо на ранніх етапах проєктування ЗЗІ. Тому доцільно замість абсолютного збитку використовувати відносний збиток, що по суті являє собою ступінь небезпеки *i*-ї погрози для АСУТП.

Ступінь небезпеки може бути визначена експертним шляхом у припущенні, що всі погрози для АСУТП складають повну групу повідомлень, тобто

$$0 \le \Delta qi \le 1; \sum_{i=1}^{n} \Delta qi = 1. \qquad (5)$$

Найбільш складним питанням є визначення імовірності усунення і-й погрози $\mathrm{P}i_{угр}^{устр}$ при проєктуванні ЗЗІ. Зробимо природне допущення, що ця імовірність визначається тим, наскільки повно враховані якісні і кількісні вимоги до ЗЗІ при їх проєктуванні, тобто

$$\mathrm{P}i_{угр}^{устр} = \gamma i\left(xi1,..,xi\gamma,..,xim\right), \qquad (6)$$

де $xi\gamma$ – ступінь виконання *i*-го вимоги до ЗЗІ для усунення *i*-ї погрози, $i = 1,\overline{n}; \gamma = 1,\overline{m}$.

Нехай перші «до» вимог будуть кількісними $\left(\gamma = 1,\overline{k}\right)$ інші «*m*-до» – якісними $\left(\gamma = \overline{k+1,m}\right)$.

Ступінь виконання γ-ї кількісної вимоги визначається його близькістю до необхідного (оптимального) значення. Для оцінки ступеня виконання γ-ї кількісної вимоги до ЗЗІ зручніше всього використовувати його нормоване значення $\overline{xi}\gamma(\gamma = 1,\overline{k}), 0 \le xi\gamma \prec 1$.

Для нормування зручно використовувати функцію виду:

$$\overline{xi}\gamma = \frac{xi\gamma - xi\gamma^{нт}}{xi\gamma^{нл} - xi\gamma^{нх}}, \qquad (7)$$

де $xi\gamma$ – поточне значення γ-ї вимоги;

$xi^{\gamma нл}, xi\gamma^{нх}$ – найкращі і найгірші значення.

З урахуванням формули (7) одержуємо наступні розрахункові співвідношення:

при $xi\gamma^{нл} = xi\gamma\max;\ xi\gamma^{нх} = xi\gamma\min$,

$$\overline{xi\gamma} = \frac{xi\gamma - xi\gamma\min}{xi\gamma\max - xi\gamma\min}, \tag{8}$$

при $xi\gamma^{нл} = xi\gamma\min;\ xi\gamma^{нх} = xi\gamma\max$,

$$\overline{xi\gamma} = \frac{xi\gamma\max - xi\gamma}{xi\gamma\max - xi\gamma\min},$$

при $xi\gamma^{нл} = xi\gamma\ \text{opt};\ xi\gamma_{нх} = xi\gamma\min;\ xi\gamma^{нх} = xi\gamma\max;$

$xi\gamma\min \le xi\gamma\ \text{opt} \le xi\gamma\max$.

$$\overline{xi\gamma} = \left\{ \begin{array}{l} 0 \text{ при } xi\gamma\langle xi\gamma\min; xi\gamma\rangle xi\gamma\max \\ 1 \text{ при } xi\gamma = xi\gamma\ \text{opt} \\ \dfrac{xi\gamma - xi\gamma\min}{xi\gamma\ \text{opt} - xi\gamma\min} \text{ при } xi\gamma\min \le xi\gamma \le xi\gamma\ \text{opt}(II) \\ \dfrac{xi\gamma\max - xi\gamma\min}{xi\gamma\max - xi\gamma opt} \textit{ при } xi\gamma\ \text{opt} \le xi\gamma \le xi\gamma\max \end{array} \right\}. \tag{9}$$

Ступінь виконання γ-ї якісної вимоги визначається функцією приналежності до найкращого значення $\gamma\left(xi\gamma\right)$.

Розклавши функцію (9) у ряд Макларена й обмеживши лише першими членами ряду, одержимо:

$$\mathrm{P}i_{угр}^{устр} = \mathrm{P}i_{угр}^{устр}\left(0\right) + \sum_{\gamma=1}^{m} \frac{\partial \mathrm{P}i_{угр}^{устр}}{\partial xi\gamma} \cdot xi\gamma, \tag{10}$$

де $\mathrm{P}i_{угр}^{устр}\left(0\right) = 0$ – імовірність усунення *i*-ї погрози при невиконанні вимоги ЗЗІ;

$\dfrac{\partial \mathrm{P}i_{угр}^{устр}}{\partial xi\gamma} = \alpha i\gamma$ – величина, що характеризує ступінь впливу γ-ї вимоги на імовірність усунення *i*-ї погрози (важливість виконання для усунення *i*-ї погрози). Очевидно, що $0 \le \alpha i\gamma \le 1; \sum_{\gamma=1}^{m} \alpha i\gamma = 1$ для виходу $i = \overline{1,n}$.

Після підстановки в (12) відповідних значень одержуємо:

$$\mathrm{P}i_{угр}^{устр} = \sum_{\gamma=1}^{k} \alpha i\gamma \cdot \overline{xi\gamma} + \sum_{\gamma=k=1}^{m} \alpha i\gamma \cdot y\left(xi\gamma\right). \qquad (11)$$

Найбільш важливими і складними етапами рішення оформленої задачі є підготовка вихідних даних і вибір методу рішення.

Що ж стосується вибору методу рішення, то задача наведена вище відноситься до класу багатокритеріальних багатовимірних метричних задач.

При досить невеликій кількості розглянутих варіантів і використанні адитивного критерію вибору згадана задача може бути вирішена шляхом прямого перебору варіантів.

## 9. Інтелектуальний аналіз даних у формуванні вимог до інформаційної безпеки ІКС

Застосування інтелектуального аналізу даних (ІАД) у сфері інформаційної безпеки (ІБ) дозволяє автоматизувати процес виявлення вразливостей, класифікації загроз і формулювання релевантних вимог до захисту. В умовах зростаючої складності інформаційно-комунікаційних систем (ІКС), ручна обробка експертної інформації стає недостатньо ефективною. Застосування методів ІАД – таких як кластеризація, класифікація, аналіз асоціацій, логічна індукція – дозволяє формалізувати знання, отримані в результаті аналізу інцидентів, тестування або аудиту систем.

Ключовим етапом застосування ІАД є побудова семантично структурованої моделі вимог. Джерелами даних можуть бути як внутрішні журнали подій і результати тестування системи, так і зовнішні нормативи – ISO/IEC 27001, NIST SP 800-53, GDPR тощо. На базі таких джерел будуються логічні правила, що описують пріоритетність реалізації конкретних заходів захисту відповідно до ризиків.

Процес трансформації експертних формулювань у конкретні вимоги до інформаційної безпеки є складним і багатоступеневим. Він передбачає ретельний аналіз зібраної експертної інформації, яка, як правило, надходить у вигляді тверджень, описів подій або сценаріїв загроз. На початковому етапі здійснюється систематизація таких

формулювань, що дозволяє структурувати інформацію відповідно до категорій потенційних загроз інформаційній та кібербезпеці. Зібрані дані проходять подальшу класифікацію та семантичний аналіз, що є критично важливим для побудови формалізованої онтології вимог. Це дозволяє впорядкувати експертні судження та встановити між ними логічні зв'язки, які необхідні для якісного формування вимог до захисту інформації на всіх рівнях функціонування інформаційно-комунікаційних систем.

Важливим етапом у цьому процесі є трансформація вихідних експертних формулювань у нормалізовані вимоги до інформаційної безпеки, що відповідають сучасним інженерним та нормативно-правовим стандартам. Така трансформація здійснюється шляхом уніфікації та формалізації текстових описів, які отримані від фахівців, із одночасною перевіркою їх відповідності міжнародним стандартам у сфері інформаційної безпеки, зокрема ISO/IEC 27001. Застосування цього підходу дозволяє підвищити ефективність процесу формування вимог, забезпечити їх прозорість і взаємозв'язок із категоріями контролю та методами реалізації захисних заходів. У межах розділу подальшу увагу зосереджено на деталізації результатів такої трансформації. Для ілюстрації обґрунтованості та коректності запропонованої методики наведено відповідну таблицю, що відображає взаємозв'язок між початковими експертними твердженнями, нормалізованими вимогами, їх класифікацією згідно з міжнародними стандартами та типом контролю, який застосовується в інформаційно-комунікаційних системах.

Подібна методологія дозволяє мінімізувати суб'єктивність при формуванні вимог до ІБ, забезпечуючи уніфікований підхід до захисту ІКС. Інструментальне забезпечення реалізації ІАД у цьому контексті може базуватися на поєднанні засобів бізнес-аналітики (наприклад, Power BI), мов онтологічного моделювання (*Protégé*) та фреймворків машинного навчання (*Scikit-learn, TensorFlow*).

Особливу увагу в сучасних інформаційно-комунікаційних системах слід приділяти змінності їхнього середовища. У ході експлуатації такі системи постійно зазнають змін: змінюються конфігурації, з'являються нові елементи, відбувається оновлення програмного забезпечення, підключаються додаткові вузли. Саме тому

актуальність і ефективність розроблених вимог до інформаційної безпеки не може залишатися незмінною та потребує постійного переоцінювання. Щоб забезпечити якісний рівень захисту, необхідно враховувати не лише формальні критерії відповідності стандартам, а й аналіз ризиків у реальному часі. Вимоги мають перевірятися на предмет їхньої здатності реагувати на нові загрози та зміни інфраструктури. Наприклад, корисним може бути розгляд ступеня охоплення ризиків, що ним забезпечуються актуальні вимоги, а також здатність цих вимог залишатися релевантними у разі зміни архітектури або технологічних процесів. Крім того, важливо аналізувати, наскільки часто порушення пов'язані саме з тією чи іншою вимогою, а також чи відповідають ці вимоги сучасним міжнародним стандартам у галузі інформаційної безпеки.

Інтелектуальний аналіз даних, впроваджений у процес формування вимог до захисту інформації, дозволяє створювати моделі управління, які є гнучкими та здатними адаптуватися до контексту конкретної організації або системи. Такі моделі враховують не лише технічні параметри, а й організаційні особливості, що дає змогу ефективніше управляти ризиками та реалізовувати заходи захисту, які відповідають реальним потребам об'єкта захисту. Використання сучасних інструментів аналітики, онтологічного моделювання та машинного навчання відкриває нові можливості для формалізації експертних суджень та побудови на їхній основі чітко структурованих і обґрунтованих вимог до інформаційної безпеки.

Особливої ваги ці підходи набувають для об'єктів критичної інфраструктури, оскільки будь-яка неконкретизована, нечітко сформульована або недостатньо перевірена вимога може стати джерелом значної загрози для стабільної роботи цілих систем.

Інтеграція інтелектуального аналізу даних у процеси проєктування та моделювання вимог дозволяє не лише підвищити їхню відповідність стандартам, а й забезпечити можливість подальшої перевірки та актуалізації в міру змін у середовищі кібербезпеки. У результаті формується надійна і прозора система захисту, де кожна вимога має чіткий зв'язок із категоріями контролю та методами впровадження, а також сприяє уніфікованому підходу до управління ризиками. Як ілюстрацію до викладених положень у подальшому

подається таблиця, що демонструє процес перетворення експертних суджень у формалізовані вимоги, їхню класифікацію згідно міжнародних стандартів та визначення типу контролю, що застосовується в інформаційно-комунікаційних системах.

Таблиця 8 – Трансформація експертних формулювань у вимоги до ІБ для ІКС

| **Експертне твердження** | **Нормалізована вимога** | **Категорія безпеки (ISO/IEC 27001)** | **Тип контролю** |
|---|---|---|---|
| Система має реєструвати всі підключення до мережі в режимі реального часу | Аудит мережевої активності з автоматичним логуванням подій | A.12.4 – Logging and monitoring | Технічний контроль |
| Адміністратор має отримувати повідомлення про підозрілі зміни в конфігурації | Моніторинг конфігурацій з генерацією повідомлень про інциденти | A.16.1 – Management of information security incidents and improvements | Оперативний контроль |
| Доступ до критичних функцій повинен здійснюватися лише з біометричною перевіркою | Реалізація багатофакторної автентифікації з біометричним компонентом | A.9.4 – System and application access control | Фізико-логічний контроль |

Після побудови ієрархічної структури й визначення вагових коефіцієнтів для кожного елемента моделі проводиться підсумковий аналіз ризиків. Отримані результати дозволяють визначити, які цілі захисту, загрози чи заходи мають найвищий пріоритет із погляду експертної оцінки та поточної ситуації в інформаційно-комунікаційній системі.

На основі цих даних формується план впровадження засобів захисту, що максимально відповідає специфіці ІКС і забезпечує ефективне використання ресурсів. Важливо, що модель легко піддається адаптації: за зміни загроз чи появи нових технологічних чинників можна оперативно скоригувати ваги елементів та пріоритети без необхідності повної перебудови всієї системи.

Досвід застосування таких експертних моделей показує, що поєднання формалізованих підходів і глибокої експертизи галузевих фахівців значно підвищує рівень надійності та стійкості ІКС. Це дозволяє не лише реагувати на нові виклики, а й проактивно формувати стратегію розвитку системи захисту відповідно до динаміки сучасних кіберзагроз.

## 10. Експертні моделі прийняття рішень у проєктуванні засобів захисту ІКС

Забезпечення стійкості та надійності інформаційно-комунікаційних систем (ІКС) стає дедалі складнішим завданням, оскільки технологічний розвиток супроводжується зростанням кількості загроз і ускладненням характеру атак. В таких умовах особливої уваги заслуговують експертні моделі прийняття рішень, які дозволяють інтегрувати різноманітні джерела знань, накопичений досвід фахівців і специфіку конкретних технологій у єдину систему формалізованих рішень. Головна мета впровадження експертних підходів – забезпечення системної оцінки ризиків, визначення пріоритетних напрямків модернізації засобів захисту та створення стійкої архітектури безпеки, що відповідає як сучасним стандартам, так і вимогам регуляторів.

Експертні моделі прийняття рішень у сфері безпеки ІКС формуються на основі багатокритеріального аналізу, методів нечіткої логіки, застосування байєсівських мереж, дерев рішень, а також методів аналітичної ієрархічної мережі (ANP) та аналізу ієрархій (AHP). Особливість цих моделей полягає у поєднанні якісних і кількісних показників, що дає змогу не лише оцінювати поточний стан захищеності, а й прогнозувати динаміку змін у разі впровадження тих чи інших заходів. Завдяки цьому стає можливим врахування взаємозв'язків між окремими компонентами ІКС, вразливостями, шляхами впливу на систему та потенційними сценаріями розвитку інцидентів.

Значна увага в експертному підході приділяється створенню ієрархічних моделей ризиків. На першому рівні визначаються та формалізуються цілі захисту, наприклад, збереження конфіденційності,

цілісності та доступності інформації. Другий рівень містить перелік основних загроз, що можуть впливати на досягнення кожної з цілей – від несанкціонованого доступу до даних до внутрішніх порушень або помилок персоналу. Третій рівень передбачає деталізацію заходів захисту, які можуть бути застосовані для нейтралізації або зниження впливу зазначених загроз: це може стосуватися організаційних, технічних, фізичних чи комплексних рішень.

Використання методу аналізу ієрархій (AHP) дозволяє експертам структурувати складні завдання, призначати ваги окремим цілям, загрозам і заходам, а також визначати оптимальні сценарії розподілу ресурсів для підвищення загального рівня безпеки. Для цього застосовується система експертного опитування, результатом якої стає побудова матриці вагових коефіцієнтів, що відображає відносну важливість кожного елементу моделі.

Крім того, експертні моделі дають змогу враховувати специфічні умови функціонування певної ІКС, регіональні чи галузеві вимоги, а також динаміку змін у законодавстві, рекомендаціях з кібербезпеки й тенденціях розвитку Т-інфраструктури. Це особливо важливо для критичних інфраструктур, де навіть незначна помилка у визначенні пріоритетів може призвести до суттєвих матеріальних чи репутаційних втрат.

Наводимо приклад структури експертного моделювання ризиків для ІКС з використанням аналітичного методу ієрархій (AHP), що ілюструє послідовність побудови моделей і призначення ваг для кожного елемента:

Таблиця 9 – Пріоритети захисту інформації в ІКС за методом AHP

| **Рівень** | **Елемент моделі** | **Опис** | **Приклад ваги (AHP)** |
|---|---|---|---|
| 1 | Ціль: Конфіденційність | Захист персональних та службових даних | 0,40 |
| 2 | Загроза: Несанкціонований доступ | Спроби обходу механізмів автентифікації | 0,30 |
| 3 | Засіб: Двофакторна автентифікація | Доступ лише після підтвердження SMS/Token | 0,60 |

Таким чином, експертні моделі у поєднанні з інструментами інтелектуального аналізу даних забезпечують адаптивне й гнучке проєктування вимог до захисту ІКС. Вони дозволяють враховувати контекст, інфраструктурні особливості, динаміку загроз та стратегічні пріоритети організацій, що особливо актуально в умовах воєнного та поствоєнного відновлення цифрових інфраструктур.

Залучення експертної думки на всіх етапах проєктування засобів захисту інформації дає змогу створювати системи, що швидко адаптуються до нових викликів і змін у загрозах. Важливо підкреслити, що синтез експертної інформації не лише сприяє підвищенню точності оцінювання ризиків, а й дозволяє уникнути типових помилок, які виникають унаслідок вузької автоматизації чи відсутності глибокого розуміння галузевої специфіки. Поєднання таких моделей із алгоритмами інтелектуального аналізу, зокрема data mining, кластеризації та виявлення шаблонів, дає змогу не тільки ідентифікувати аномальні дії чи небезпечні сценарії, але й завчасно прогнозувати можливі вектори атак, проводити нормування експертних оцінок і виявляти приховані залежності між елементами системи.

Особливе значення ці підходи набувають у сферах критичної інфраструктури й у державно-значущих сервісах, де питання безпеки даних стає не просто пріоритетом, а основною умовою стійкої цифровізації. У такому контексті експертні, інтелектуальні та лінгвістичні методи забезпечують основу для створення комплексних стратегій захисту інформації, що здатні враховувати не лише поточний стан системи, але й її перспективний розвиток, еволюцію загроз і зміну нормативно-правового поля. Це відкриває можливості для формування ефективних, самонавчальних систем оцінки ризиків, адаптивних до змін і здатних гарантувати сталу кібербезпеку в умовах невизначеності.

## 11. Висновки

Забезпечення захисту даних користувачів в інформаційно-комунікаційних системах потребує ґрунтовних знань, застосування ефективних інструментів та всебічного аналізу. Для формування вимог до захисту інформації в ІКС необхідно враховувати специфіку сучасного

цифрового середовища, особливості автоматизованих систем управління й актуальні виклики для підтримки цілісності та безпеки даних. Комплексний підхід дозволяє глибше зрозуміти еволюцію методів кібербезпеки в умовах зростання кількості і складності інформаційних загроз, а також динамічного розвитку технологій.

Було здійснено ґрунтовний аналіз ключових засад ідентифікації пристроїв і користувачів у контексті функціонування ІКС. Детально розглянуті сучасні технології ідентифікації, які охоплюють як апаратний рівень (ідентифікація пристроїв за унікальними характеристиками, застосування апаратних токенів), так і поведінковий рівень (аналіз користувацьких патернів, реакцій на події, часових і просторових особливостей дій). Підкреслено важливість впровадження мультифакторних схем автентифікації, що дозволяють значно підвищити рівень захищеності систем від зовнішніх і внутрішніх загроз.

Окрема увага приділено поняттю цифрового сліду користувача, що охоплює технічні параметри, поведінкові чинники, контекстуальні дані та історію взаємодії з системою. Встановлено, що цілеспрямована мінімізація цифрового сліду є обов'язковою умовою для забезпечення конфіденційності та приватності. Для цього доцільно впроваджувати інноваційні інструменти, такі як cookie isolation, технології обфускації дій, DNS-over-HTTPS, а також орієнтуватися на відповідність міжнародним стандартам і нормативам (зокрема, GDPR, ISO/IEC 29184).

Узагальнення отриманих результатів дозволяє зробити висновок, що інтеграція сучасних методів ідентифікації, автентифікації й мінімізації цифрового сліду користувачів забезпечує підвищення стійкості інформаційних систем до новітніх векторів атак і сприяє формуванню ефективної політики захисту даних у контексті динамічного розвитку цифрової інфраструктури.

Практичні аспекти впровадження стратегій захисту в ІКС. Аналіз механізмів виявлення загроз (NAP, NAC, ZTA) показав їх ефективність у моделюванні зон довіри та контролю доступу. Було розглянуто концепцію реактивного та проактивного реагування на загрози – через моніторинг, фіксацію, класифікацію, обфускацію та зворотну реакцію. Важливою особливістю сучасного контексту стало

врахування викликів воєнного та поствоєнного періодів, зокрема у розрізі е-сервісів (Дія, E-Helsy, IDP-реєстрація), що потребують підвищеної уваги до верифікації та автентифікації.

Детально проаналізовано застосування лінгвістичних та інтелектуальних методів для синтезу вимог до ІБ, запропонновано формалізовану модель впливу експертної інформації на структуру вимог а також продемонстровано, як методи інтелектуального аналізу (*data mining, clustering, pattern discovery*) можуть забезпечити обґрунтоване нормування експертних оцінок. Також розглянуто використання методів прийняття рішень (AHP, ANP) для ієрархічного узгодження технічних, організаційних і нормативних вимог до безпеки в ІКС.

Таким чином, отримані результати свідчать про доцільність інтеграції експертних підходів, інтелектуального аналізу даних і лінгвістичного моделювання для обґрунтування вимог до засобів захисту в інформаційно-комунікаційних системах. Перспективним напрямом подальших досліджень є розробка адаптивних моделей оцінки ризиків у динамічному середовищі, що поєднують онтологічні схеми знань, верифікацію поведінкових аномалій та кібергігієну користувачів.

**Список використаних джерел**

1. IBM. Cost of a Data Breach Report 2024. IBM Security, 2024. Електронний ресурс. URL: https://www.ibm.com/reports/data-breach (дата звернення: 01.07.2025).

2. Morgan S. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybersecurity Ventures.* 2022. Електронний ресурс. URL: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025 (дата звернення: 01.07.2025).

3. Державна служба спеціального зв'язку та захисту інформації України. Статистика кібератак 2024. Офіційний вебсайт, 2025. Електронний ресурс. URL: https://cip.gov.ua/ua/news/statystyka-kiberatak-za-2024-rik (дата звернення: 02.07.2025). *Cisco*. (2024). Annual Cybersecurity Report. URL: https://www.cisco.com/c/en/us/products/security/security-reports.html

4. ENISA. (2023). Threat Landscape for Industrial Control Systems. URL: https://www.enisa.europa.eu/publications/ics-threat-landscape

5. NIST. (2015). Guide to Industrial Control Systems (ICS) Security. NIST SP 800-82 Rev.2. https://doi.org/10.6028/NIST.SP.800-82r2

6. European Union. (2021). Regulation (EU) No 910/2014 (eIDAS Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910

7. ISO/IEC 29184:2020. Online privacy notices and consent. International Organization for Standardization. URL: https://www.iso.org/standard/70331.html

8. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. URL: https://www.iso.org/standard/27001

9. GDPR. (2016). General Data Protection Regulation. Regulation (EU) 2016/679. URL: https://gdpr-info.eu

10. Chepurna O., Cherevko Y., Kuleshova Y. On Information Geometry Methods for Data Analysis. Geometry. *Integrability and Quantization.* 2024. Vol. 29. P. 11–22. DOI: https://doi.org/10.7546/giq-29-2024-11-22

11. Shor S., Pavlova T. Enhancing Access Control in Critical Infrastructure Systems Using Attribute-Based Encryption. *Information and Security.* 2023. Vol. 55 (2). P. 145–162. DOI: https://doi.org/10.11610/isij.5525

12. Tang M., Li Q., Yang J. Anomaly Detection in ICS Using Isolation Forest. *IEEE Access.* 2022. Vol. 10. P. 12547–12558. DOI: https://doi.org/10.1109/ACCESS.2022.3147280

13. He J., Wang X., Liu H. Privacy-Preserving Authentication Protocol for eHealth Systems. *Future Generation Computer Systems.* 2021. Vol. 117. P. 354–367. DOI: https://doi.org/10.1016/j.future.2020.11.016

14. BankID National Bank of Ukraine. 2024. URL: https://bankid.org.ua/

15. Ministry of Digital Transformation of Ukraine. Diia – Digital State Project. 2024. URL: https://diia.gov.ua

16. Cisco. 2024. *Cisco Annual Cybersecurity Report.* URL: https://www.cisco.com/c/en/us/products/security/security-reports.html

17. Fortinet. 2024. *OT Threat Landscape Report.* URL: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ot-threat-report-2024.pdf

18. IBM Security. 2023. *Cost of a Data Breach Report.* 2023. URL: https://www.ibm.com/reports/data-breach

19. ENISA. 2024. *Threat Landscape for Industrial Control Systems.* URL: https://www.enisa.europa.eu/publications/ics-threat-landscape

20. MITRE. 2024. ATT&CK for ICS Framework. https://attack.mitre.org/matrices/ics

21. ISO/IEC 29184:2020. Online Privacy Notice and Consent. URL: https://www.iso.org/standard/70331.html

22. Google. 2023. *Privacy Sandbox Project.* URL: https://privacysandbox.com

23. Microsoft. 2023. *Digital Defense Report.* URL: https://www.microsoft.com/en-us/security/business/security-intelligence-report

24. NIST. 2022. *Framework for Improving Critical Infrastructure Cybersecurity* (v1.1). DOI: https://doi.org/10.6028/NIST.CSWP.04162018

25. OWASP. 2023. Top 10 for LLM Applications. URL: https://owasp.org/www-project-top-10-for-llm-applications

26. European Commission. 2022. *eIDAS 2.0 Regulation.* URL: https://digital-strategy.ec.europa.eu/en/policies/eidas

27. Ukrainian Ministry of Digital Transformation. 2023. *Diia Platform Overview*. URL: https://thedigital.gov.ua

28. Cloudflare. 2023. *The State of Application Security*. URL: https://www.cloudflare.com/learning/security

29. Palo Alto Networks. 2024. *State of Cybersecurity Report.* URL: https://www.paloaltonetworks.com/resources/research

30. CrowdStrike. 2024. *Global Threat Report.* URL: https://www.crowdstrike.com/global-threat-report/