Державний торговельно-економічний університет
Кафедра інженерії програмного забезпечення
та кібербезпеки

ПРОГРАМУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ

Збірник наукових статей студентів,
які здобувають освітній ступінь «магістр»
за спеціальностями 121 «Інженерія програмного забезпечення», 125 «Кібербезпека та захист інформації»

Частина 2

Київ 2024

УДК 004.056.5
П 78

П 78 **Програмування** та захист інформації [Електронний ресурс] : зб. наук. ст. студ. / відп. ред. Т. О. Жирова. – Київ : Держ. торг.-екон. ун-т, 2024. – Ч. 2. – 180 с.

У збірнику наукових статей студентів висвітлено результати теоретичних та експериментальних досліджень у галузі інженерії програмного забезпечення й кібербезпеки та захисту інформації.

Матеріали подано в авторській редакції. Відповідальність за зміст матеріалів несуть автори.

УДК 004.056.5

Відповідальна за випуск О. В. Криворучко, д-р техн. наук, проф.

Видається за рекомендацією вченої ради факультету інформаційних технологій ДТЕУ
(протокол № 13 від 28 травня 2024 року)

ЗМІСТ

СУЧАСНІ ТРЕНДИ В ЗАХИСТІ ОНЛАЙН-ГАМАНЦЯ

БАЛАН О.О., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто сучасні тренди в захисті онлайн гаманців.. Зазначено основні онлайн гаманці, їх переваги, способи застосування та можливі недоліки у вкористанні. Більш детальна розповідь про всі види онлайн гаманців. Актуальність у використанні та актуальність теми.

The article examines modern trends in the protection of online wallets. The main online wallets, their advantages, methods of use and possible disadvantages in use are indicated. A more detailed account of all types of online wallets. Relevance in use and relevance of the topic.

Актуальність. З наближенням 2024 року сфера цифрових платежів розвивається шаленою швидкістю, змінюючи спосіб проведення транзакцій і управління нашими фінансами. Зі стрімким розвитком мобільних пристроїв, зростаючим попитом на зручні способи оплати та невпинним прагненням до інновацій у фінансовій галузі не дивно, що цифрові гаманці стають основним рішенням для споживачів і компаній.

Очікується що ринок мобільних гаманців зросте з 220 мільярдів доларів у 2021 році до 970 мільярдів доларів у 2030 році. Цьому зростанню сприятиме технологія Near Field Communication (NFC), банки, фінтех-компанії, лише цифрові рішення та інші передові платіжні технології.. Оскільки все більше споживачів використовують цифрові гаманці для онлайн-транзакцій, важливість цих методів оплати в галузі електронної комерції зростатиме.

Однією з головних переваг цифрових гаманців із білою міткою є швидкість, з якою вони можуть бути розгорнуті. Компанії можуть використовувати наявну інфраструктуру та технології, скорочуючи час і витрати на розробку. Це дозволяє компаніям швидко вийти на ринок цифрових гаманців і скористатися зростаючим попитом на зручні та безпечні фінансові послуги.

Метою статті є дослідження онлайн гаманців, їх види, способи використання. Захист конфеденційних данних користувачів, та їх коштів.

Об'єктом дослідження є сучасні тренди в захисті онлайн гаманця.

Предмет дослідження – інформаційно-захисна система.

Аналіз попередніх досліджень. Дослідженню інформаційно-захисних систем, визначенню структури, основних характерних рис присвячені праці вітчизняних та закордонних науковців: Ю. В. Борсуковський, В. Л. Бурячок і В. Ю. Борсуковська, В.О. Хорошко, М.Є. Шелест, О.В. Рибальський та ін.

Виклад основного матеріалу. Цифрові гаманці White label можуть підтримувати різні варіанти оплати, включаючи кредитні та дебетові картки, банківські перекази та платежі в криптовалюті. Ця гнучкість дозволяє підприємствам задовольняти різноманітні платіжні переваги своїх клієнтів. Крім того, інтеграція з мобільними платіжними рішеннями, такими як Apple Pay і Google Pay, ще більше розширює можливості оплати, роблячи транзакції зручнішими для користувачів.

В епоху, коли порушення безпеки та викрадення особистих даних викликають серйозне занепокоєння, цифрові гаманці виводять безпеку на новий рівень завдяки біометричній автентифікації. Хоча сканування відбитків пальців було початковим кроком у біометричній перевірці, очікуйте, що більше гаманців включатимуть розпізнавання обличчя та навіть сканування райдужної оболонки ока для підвищення безпеки. Біометрія забезпечує надійний рівень захисту від несанкціонованого доступу та забезпечує безперебійну та безпроблемну роботу користувача. Простіше кажучи, ваше обличчя або відбиток пальця стає ключем до розблокування вашого цифрового гаманця.

Крипто-гаманці зберігають ваші приватні ключі – паролі, які надають вам доступ до ваших криптовалют – у безпеці та доступності, дозволяючи вам надсилати та отримувати криптовалюти, такі як Bitcoin та Ethereum. Вони бувають у багатьох формах, від апаратних гаманців, таких як Ledger (який виглядає як USB-накопичувач), до мобільних додатків, таких як Coinbase Wallet, які роблять використання криптовалюти таким же простим, як покупки за допомогою кредитної картки в Інтернеті.

Таблиця 1

Види онлайн гаманців

Назва	Опис
Криптогаманці	програма, яка дозволяє взаємодіяти з криптовалютою в блокчейні
Картки для оплати покупок у мережі певного бренду	віртуальна вітрина магазину
Гаманці міжнародних платіжних систем	інструмент онлайн-платежів, який дозволяє користувачам здійснювати швидкі цифрові транзакції по всьому світу
Мобільні гаманці	Додатки для смартфонів, які дозволяють користувачам здійснювати платежі, зберігати карти лояльності та керувати фінансами

Джерело: розроблено автором.

На відміну від звичайного гаманця, який може містити реальну готівку, крипто-гаманці технічно не зберігають вашу криптовалюту. Ваші активи знаходяться в блокчейні, але доступ до них можливий лише за допомогою закритого ключа. Ваші ключі підтверджують ваше право власності на цифрові гроші та дозволяють здійснювати транзакції. Якщо ви втратите особисті ключі, ви втратите доступ до своїх грошей. Ось чому важливо зберігати апаратний гаманець у безпеці або користуватися надійним постачальником гаманців, таким як Coinbase.

Криптогаманці варіюються від простих у використанні програм до більш складних рішень безпеки

Таблиця 2

Види криптогаманців

Вид	Спосіб використання
Паперові гаманці	ключі записуються на фізичному носії, як папір, і зберігаються в безпечному місці
Апаратні гаманці	ключі зберігаються на флеш-накопичувачі, який зберігається в безпечному місці та підключається до комп'ютера лише тоді, коли ви хочете використовувати свою криптовалюту. Ідея полягає в тому, щоб спробувати збалансувати безпеку та зручність.
Онлайн-гаманці	ключі зберігаються в додатку чи іншому програмному забезпеченні – шукайте програмне забезпечення, захищене двоетапним шифруванням. Це робить надсилання, отримання та використання вашої криптовалюти таким же простим, як використання будь-якого онлайн-банківського рахунку, платіжної системи чи брокерської компанії.

Джерело: розроблено автором.

Кожен вид має свої компроміси. Зловмисникам важче отримати доступ до паперових і апаратних гаманців, оскільки вони зберігаються в автономному режимі, але вони обмежені в функціях і ризикують бути втраченими або знищеними. Онлайн-гаманці, які пропонує велика біржа, як-от Coinbase, є найпростішим способом почати роботу з криптовалютою та пропонують баланс безпеки та легкого доступу. Оскільки ваша особиста інформація

знаходиться в Інтернеті, ваш захист від хакерів настільки ж хороший, як і безпека вашого постачальника гаманця, тому переконайтеся, що ви шукаєте такі функції, як двофакторна перевірка.

Використання таких програм, як Coinbase Wallet або Exodus, дає вам легкий доступ до ваших криптохолдингів.

Можливості при використанні:

- Керувати всіма своїми цифровими активами в одному безпечному місці.
- Керувати своїми приватними ключами
- Надсилайти та отримуйте криптовалюту в будь-яку точку світу
- Взаємодіяти з іменами користувачів, а не з довгими шістнадцятковими адресами «відкритого ключа».

Картки для оплати покупок у мережі певного бренду

Кредитна картка певного бренду – це картка, яку роздрібний продавець або інший бізнес пропонує в партнерстві з емітентом кредитної картки або мережею. Зазвичай із логотипами компанії, що видає кредитні картки, і роздрібного продавця, спільні картки дають знижки на товари, бали чи інші винагороди за використання в продавця-спонсора, але їх також можна використовувати будь-де, де приймаються картки цієї мережі.

Як працюють спільні картки

Кобрендові картки працюють як будь-яка звичайна кредитна картка. Їх можна використовувати для будь-яких покупок, де приймаються картки в цій мережі (наприклад, Mastercard, Visa, American Express або Discover).

Кобрендові карткові відносини можуть бути структуровані різними способами. Але загалом, щоб випустити кобрендову кредитну картку, продавець (наприклад, універмаг, автозаправна станція чи авіакомпанія) або інша організація (наприклад, університет чи некомерційна організація) має співпрацювати з фінансовою установою.

Хоча картку буде випущено певним банком, на її лицьовій стороні, як правило, буде помітно логотип роздрібного продавця чи іншої компанії, а також логотип мережі обробки.

Кредитна картка певного бренду спонсорується двома сторонами – як правило, роздрібним продавцем і емітентом картки чи мережею карток – і зазвичай містить логотипи обох. Спільні картки можна використовувати будь-де, де приймають кредитні картки такого типу (наприклад, Visa або Mastercard). Багато роздрібних магазинів пропонують суміжні картки на додаток до своїх власних карток.

Міжнародна платіжна система – це масштабна організація, що функціонує у багатьох країнах, пропонує різні типи рахунків та великий перелік валют у своєму обігу.

Таблиця 3

Найпопулярніші в Україні електронні гаманці та їхні головні особливості

Назва	Головні особливості
Paysera	Електронний гаманець популярної європейської платіжної системи, який підтримує понад 30 валют та пропонує просту реєстрацію. Мобільний додаток Paysera доступний 14 мовами, у тому числі українською. З його допомогою після обов'язкової верифікації можна за кілька хвилин відкрити особистий чи бізнес-рахунок IBAN, що належить європейській системі SEPA. Через Paysera можна виконувати перекази, обмінювати валюту за вигідним курсом та виводити гроші на банківські картки. Важливо: щоби працювати із системою, потрібно замовити фізичну картку, але отримати її можна лише на адресу в зоні ЄС. Тому, якщо ви перебуваєте в Україні, доведеться звернутися за допомогою до родичів та знайомих, які мешкають у Європі.
Payoneer	Власники облікового запису Payoneer використовують цей гаманець, щоб отримувати плату за свої послуги із США та Європи. Сервіс дає можливість відкрити рахунки в чотирьох валютах – доларах, євро, японських єнах та британських фунтах. За кожним з рахунків можна випустити віртуальну чи фізичну картку. Після реєстрації Payoneer зараховує на рахунок новому користувачеві $25

Закінчення табл. 3

Назва	Головні особливості
PayPal	Популярний у світі електронний гаманець для швидких грошових переказів між різними країнами. В Україні сервіс доступний, але поки що працює з обмеженнями, а гривні немає в списку валют. Надсилати та отримувати гроші на український акаунт можна в доларах США та Канади, британських фунтах та євро. До 31 березня 2023 року сервіс скасував для українських клієнтів власну стандартну комісію 4 %. Реєстрація в PayPal проста та зрозуміла. Сервіс працює з прив'язкою до банківського рахунку або кредитної картки. Отримавши гроші на гаманець, можна витратити їх на оплату товарів і послуг в іноземному інтернет-магазині або вивести на банківську картку за допомогою сервісу-посередника. Найпопулярніші з них – Western Bid і Seller Online.
SettlePay Wallet	Криптовалютний гаманець, який називають місточком між цифровими та фіатними валютами. Він дозволяє поповнювати баланс та виводити гроші з різних криптобірж, а також виконувати перекази між гаманцями, оплачувати різні послуги та зараховувати гроші на банківську картку. Сервіс підтримує понад 40 валют. SettlePay Wallet відрізняється низькими комісіями. Нещодавно сервіс запустив можливість підтверджувати особу за допомогою Дія за кілька хвилин. Верифікація потрібна, щоби поповнювати гаманець через Apple Pay та Google Pay, виводити гроші та переводити їх на інші гаманці. Крім того, верифіковані користувачі мають вищі ліміти на транзакції.

Джерело: розроблено автором.

Підключення такої системи є необхідним кроком для розвитку бізнесу в електронній комерції: платформа дозволяє приймати платежі від клієнтів з інших країн.

Основним завданням системи є автоматизація міжнародних платежів і розрахунків. Інтеграція такого сервісу в сайт або мобільний додаток – це спосіб зробити оплату замовлень зручною для клієнтів, заощадити час на обробці транзакцій, організувати відстеження статусу платежу через особистий кабінет і збір статистики.

Багато платформ дозволяють приймати платежі не тільки з банківських карток, а й через електронні гаманці та локальні платіжні методи, а також обробляти різні валюти.

Висновки. Використання онлайн гаманців тільки набуває своєї основної популярності не тільки в Україні, а і в усьому світі. Безпека онлайн гаманця має першочергове значення для забезпечення ваших фінансів та фінансових операцій, вашого бізнесу. З розвитком технологій створення онлайн гаманців, розвиваються і методи які використовують кібер-злочинці.

Список використаних джерел

1. Карась П.М.Приходько Н.В.Пащенко О.В.Гришина Л.О. // Банківська система. Видання від 2013 року.

2. Матеріали основної криптобіржі в світі компанія «Binance» // Режим доступу: https://www.binance.com/UA

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

СТВОРЕННЯ ТА ОПТИМІЗАЦІЯ КОНФІГУРАЦІЇ MQTT-БРОКЕРА ДЛЯ ЕФЕКТИВНОГО КОНТРОЛЮ ЗА БЕЗПЕКОЮ В IOT-СИСТЕМАХ

БРАТУНЕЦЬ Д.С., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

Ця стаття присвячена проблемі створення та оптимізації конфігурації MQTT-брокера для забезпечення ефективного контролю за безпекою в системах Інтернету речей. MQTT-брокери є основними складовими для обміну даними в мережі Інтернету речей, тому належне налаштування та оптимізація їх конфігурацій важлива для забезпечення безпеки. Результати дослідження можуть бути корисними для розробників та адміністраторів систем Інтернету речей, які прагнуть забезпечити надійність та безпеку своїх пристроїв та мереж.

This article is devoted to the problem of creating and optimizing the configuration of an MQTT broker to ensure effective security control in Internet of Things systems. MQTT brokers such as Mosquitto are the main building blocks for data exchange in the Internet of Things network, so properly configuring and optimizing their configuration is important to ensure security. The results of the study can be useful for developers and administrators of Internet of Things systems who seek to ensure the reliability and security of their devices and networks.

Актуальність. З розвитком IoT(Internet of Things) збільшується кількість підключених пристроїв, які передають інформацію через мережу, що створює велике навантаження на мережеву інфраструктуру та вимагає надійного забезпечення безпеки цієї комунікації.

Проблеми безпеки в IoT-системах є важливими як науковим, так і практичним завданням, оскільки недостатньо захищена мережа може призвести до серйозних наслідків, таких як порушення конфіденційності даних, несанкціонований доступ до системи та злам пристроїв. Отже, ефективний контроль за безпекою в IoT-системах стає критично важливим завданням для забезпечення захищеної та надійної роботи цих систем.

Мета статті полягає в розгляді та аналізі методів створення та оптимізації конфігурації MQTT-брокера для ефективного контролю за безпекою в IoT-системах. Основним завданням є надання рекомендацій щодо налаштування MQTT-брокера з урахуванням специфіки застосування в IoT-системах.

Предметом статті є технології та методи забезпечення безпеки в IoT-системах з використанням протоколу MQTT та MQTT-брокера.

Об'єктом дослідження є сам MQTT-брокер та його можливості щодо налаштування та оптимізації для забезпечення безпеки в IoT-системах.

Аналіз попередніх досліджень. Вивченню забезпечення безпеки в IoT-системах, що використовують MQTT протокол присвячено багато робіт науковців, таких як: Biswajeeban Mishra, Attila Kertesz, Syaiful Andy та інші.

Виклад основного матеріалу. Зважаючи на значення безпеки в інтернеті речей (IoT), важливо ретельно проаналізувати її вплив та визначити стратегії для забезпечення захисту в мережах IoT. Відсутність належних заходів безпеки може призвести до серйозних наслідків, таких як порушення конфіденційності, порушення цілісності даних та навіть загрози життю та здоров'ю в разі використання IoT в критичних областях, таких як медицина або автономні автомобілі. Тому аналіз вимог до безпеки в IoT-системах є першочерговим завданням при проектуванні та розгортанні мереж IoT. Для цього необхідно провести глибоке дослідження потенційних загроз та вразливостей, визначити вимоги до конфіденційності, цілісності та доступності даних відповідно до специфіки конкретного застосування IoT. Тільки після такого аналізу можна буде ефективно розробити та впровадити відповідні заходи безпеки,

включаючи налагодження конфігурації MQTT-брокера для забезпечення високого рівня захисту в мережах IoT.

MQTT (Message Queuing Telemetry Transport) є легковаговим протоколом обміну повідомленнями, який широко використовується в IoT-системах для передачі даних між пристроями та серверами. Він пропонує простий, ефективний та масштабований механізм комунікації, що робить його популярним в IoT-системах.[1] Однак, даний протокол без додаткових налаштувань має багато вразливостей, що є критичними та мають бути усунені перед його використанням. Найочевиднішою вразливістю є те, що даний протокол не має ввімкненої автентифікації за замовчуванням та транспортує паролі у відкритому вигляді, без жодного шифрування.

MQTT-брокер – це посередник у системі IoT, який відповідає за передачу повідомлень між пристроями, що публікують дані (видавець) та пристроями, які підписуються на ці дані (підписники). Загальна концепція IoT-системи, що використовує MQTT протокол зображена на рис. 1.

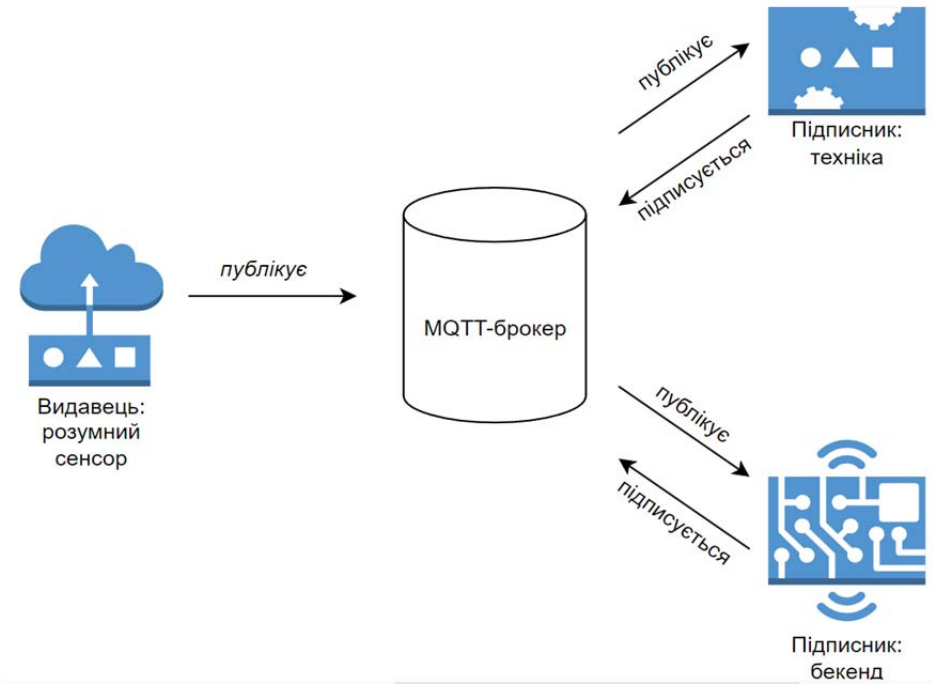


Рис. 1. Архітектура MQTT публікація/підписка

Джерело: розроблено автором

У цьому контексті MQTT-брокер відіграє ключову роль у забезпеченні безпеки мережі IoT. Деякі з основних функцій MQTT-брокера, які сприяють забезпеченню безпеки, включають:

- можливість встановлення захищеного каналу зв'язку з використанням протоколу TLS/SSL, що дозволяє шифрувати трафік між клієнтами та брокером, забезпечуючи конфіденційність інформації;
- можливість налаштування механізмів автентифікації, таких як імена користувачів та паролі або використання сертифікатів, щоб перевірити ідентичність клієнтів перед наданням доступу до брокера;
- можливість налаштовувати правила доступу до тем та повідомлень, що дозволяє обмежувати доступ до конкретних даних лише вповноваженим користувачам або пристроям; здатність ведення журналу подій та моніторингу активності, що дозволяє виявляти потенційні загрози та вживати відповідних заходів;
- можливість інтеграції з іншими системами безпеки, такими як системи моніторингу подій або системи виявлення вторгнень, для підвищення рівня безпеки мережі IoT.

Вибір правильного брокера та його налаштування з урахуванням вимог до безпеки є важливими завданнями для забезпечення ефективного захисту мережі IoT.

Вибір MQTT-брокера відбувався за наступними параметрами: можливості, щодо налаштувань безпеки, легкість встановлення, підтримка TLS/SSL, стабільність, навантаження на центральний процесор пристрою, використання постійної пам'яті пристрою. Для роботи був обраний MQTT-брокер Mosquitto. Були проаналізовані різні роботи з порівняння MQTT-брокерів. Mosquitto працював краще, ніж інші брокери в середовищі з обмеженими ресурсами[2]. Також даний брокер мав менший відсоток використання центрального процесора при великих навантаженнях.

Основними параметрами безпеки, що потребують налаштування для даного MQTT-брокера – це TLS/SSL, контроль доступу за допомогою ACL, автентифікація користувачів, логування основних подій.

При описі оптимізації заходів безпеки будуть розглянуті й інші брокери для створення відповідних рекомендацій щодо вибору.

Приклад налаштувань MQTT-брокера показано на рис. 2.

```
persistence true
persistence_location /var/lib/mosquitto/

log_dest file /var/log/mosquitto/mosquitto.log

include_dir /etc/mosquitto/conf.d

allow_anonymous false
password_file /etc/mosquitto/passwd

tls_version tlsv1.2
listener 8883
cafile /etc/mosquitto/certs/ca.crt
certfile /etc/mosquitto/certs/server.crt
keyfile /etc/mosquitto/certs/server.key
require_certificate true

plugin /usr/lib/x86_64-linux-gnu/mosquitto_dynamic_security.so
plugin_opt_config_file /etc/mosquitto/dynamic-security.json

acl_file /etc/mosquitto/acl.acl

max_connections 1000

log_timestamp true
log_timestamp_format %d-%m-%YT%H:%M:%S
log_type all
```

Рис. 2. Приклад налаштувань Mosquitto брокера

Джерело: розроблено автором

Було налаштовано шифрування даних за допомогою TLS, це забезпечить безпечне передання даних через мережу без ризику їх перехоплення. Довжина ключа не має бути занадто великою, бо пристрої IoT не мають багато ресурсів для шифрування даних.[3] В даному прикладі був використаний ключ довжиною 2048 біт.

Був вимкнений анонімний доступ до тем та створений файл з логінами та хешованими паролями користувачів.

Комбінація сертифікації та автентифікації може вважатися двофакторною автентифікацією, що покращує безпеку систему та не навантажує пристрої складними алгоритмами.

Також був доданий файл ACL в якому описані доступи окремих користувачів до певних тем. Це дасть змогу обмежити користувачів від отримання даних до яких вони не мають доступу. Окрім безпекових переваг, додавання ACL також зменшує навантаження на брокер, бо обмеження користувачів не дає їм змогу підписатись на всі теми, яких може бути тисячі, та навантажувати систему.

Були ввімкнені обмеження максимальної кількості одночасних підключень. Це налаштування є практичним, якщо система є закритою та не буде динамічно збільшуватись. В інших випадках найкращою практикою буде налаштувати механізми динамічного розподілення ресурсів, наприклад кластеризація.

Також було ввімкнено логування подій, що пов'язані з підключеннями та отриманням даних з клієнтів. Це може бути в подальшому використано для аналізу інцидентів.

Також необхідно встановити IDS/IPS, найкраще буде, якщо вони будуть встановлені як окремі пристрої, щоб зменшити навантаження на брокер.

Для зменшення навантаження на брокера рекомендується налаштувати також QOS (quality of service) для клієнтів. QOS існує трьох типів: 0 – повідомлення буде отримане максимум один раз, 1 – повідомлення буде отримане хоча б один раз та 2 – повідомлення буде отримане тільки 1 раз. Найбільше навантажує пристрій тип 2, найменше – тип 0, тому для пристроїв, що не є критичним рекомендується встановлювати тип 0, щоб зменшити навантаження. Тип 2 встановлювати, тільки тоді, коли повторне отримання повідомлення може нашкодити роботі системи.

В Таблиці 1 приведена порівняльна характеристика деяких популярних MQTT-брокерів[4].

Таблиця 1

Порівняльна характеристика популярних MQTT-брокерів

Характеристик	Mosquitto	RabbitMQ	Eclipse Paho MQTT	HiveMQ
Відкритий вихідний код	Так	Так	Так	Так
Підтримка TLS/SSL	Так	Так	Так	Так
Підтримка ACL	Так	Так	Ні	Так
Легкість встановлення	Дуже легка	Помірна	Дуже легка	Легка
Ефективність	Висока	Висока	Висока	Висока
Стабільність	Дуже стабільний	Стабільний	Стабільний	Стабільний
Підтримка розширень	Обмежена	Широка	Обмежена	Широка
Налаштування безпеки	Достатньо розширений	Обмежені можливості	Обмежені можливості	Розширені можливості

Джерело: розроблено автором

Для визначення критерію оптимальності безпекових рішень запропонована наступна формула:

$$k=w_1*e_ш+w_2*e_а+w_3*e_д+w_4*e_м,\ldots \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

де w_1, w_2, w_3, w_4 – вагові коефіцієнти, які відображають важливість кожного з аспектів безпеки, сума яких дорівнює 1;

$e_ш$ – показник ефективності шифрування;

$e_а$ – показник ефективності автентифікації;

$e_д$ – показник ефективності контролю доступу;

$e_м$ – показник ефективності моніторингу;

Переведення показників ефективності заходів безпеки в числовий формат:

Шифрування:

- Оцінка рівня шифрування: 0 (відсутній) – 10 (максимальний рівень).

- Стійкість до атак: 0 (нестійкий) – 10 (дуже стійкий).
- Навантаження на пристрої: 0 (велике) – 10 (низьке).

Автентифікація:

- Час автентифікації: 0 (повільний) – 10 (швидкий).
- Використання двофакторної аутентифікації: 0 (відсутня) – 10 (повністю реалізована).
- Навантаження на пристрої: 0 (велике) – 10 (низьке).

Контроль доступу:

- Кількість неавторизованих доступів: 0 (часті) – 10 (рідкісні).
- Швидкість реакції на несанкціонований доступ: 0 (повільна) – 10 (швидка).
- Навантаження на пристрої: 0 (велике) – 10 (низьке).

Моніторинг:

- Кількість сповіщень та подій: 0 (мало) – 10 (багато).
- Час реакції на виявлення загроз: 0 (повільна) – 10 (швидка).
- Навантаження на пристрої: 0 (велике) – 10 (низьке).

Показник ефективності кожного з заходів безпеки дорівнює середньому арифметичному відповідних показників. Отже, максимальне значення критерію оптимальності дорівнює 10 і означатиме, що система безпеки MQTT-брокера оптимізована для потреб певної IoT-системи.

Висновки. В даній роботі було розглянуто важливі аспекти безпеки в мережах Інтернету речей із використанням MQTT-брокера. Було проаналізовано основні функції MQTT-брокера, спрямовані на забезпечення безпеки мережі IoT, такі як шифрування трафіку, механізми автентифікації, контроль доступу та моніторинг подій.

Для визначення критерію оптимальності безпекових рішень була запропонована формула, яка враховує ефективність заходів безпеки на основі таких показників, як шифрування, автентифікація, контроль доступу та моніторинг.

Отже, використання відповідно налаштованого MQTT-брокера разом з відповідними заходами безпеки є ключовим для забезпечення ефективного захисту мереж IoT, а зазначена методика визначення критерію оптимальності дозволить здійснити обґрунтований вибір заходів безпеки для конкретної IoT-системи.

Список використаних джерел

1. Adil Bashir and Ajaz Hussain Mir. Securing Communication in MQTT enabled Internet of Things with Lightweight security protocol. – Режим доступу: https://publications.eai.eu/index.php/IoT/article/view/672/538

2. Biswajeeban Mishra, Biswaranjan Mishra and Attila Kertesz. Stress-Testing MQTT Brokers: A Comparative Analysis of Performance Measurements. – Режим доступу: https://www.mdpi.com/1996-1073/14/18/5817

3. Thomas Prantl, Lukas Iffländer, Stefan Herrnleben, Simon Engel, Samuel Kounev, Christian Krupitzer. Performance Impact Analysis of Securing MQTT Using TLS. – Режим доступу: https://research.spec.org/icpe_proceedings/2021/proceedings/p241.pdf

4. Heiko Koziolek, Sten Gruner, and Julius Ruckert. A Comparison of MQTT Brokers for Distributed IoT Edge Computing. – Режим доступу: https://www.koziolek.de/docs/Koziolek2020-ECSA-preprint.pdf

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

АНАЛІЗ ВРАЗЛИВОСТЕЙ CROSS-SITE SCRIPTING ВЕБДОДАТКУ ТА МЕТОДИ ДЛЯ ЇХ УСУНЕННЯ

ВОВЧЕНКО І.В., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

Стаття присвячена аналізу вразливостей Cross-Site Scripting (XSS) у веб-додатках та методам їх усунення. XSS є однією з найбільш поширених атак на веб-додатки, дозволяючи зловмисникам впроваджувати в шкідливий код на сторінки веб-сайтів. У статті розглянуто різновиди XSS, включаючи reflected, stored та DOM-based XSS, та їх можливі наслідки для безпеки веб-додатків. Детально описано методи обнаруження та запобігання XSS-атакам, такі як валідація введених даних, екранування виведених даних та використання безпечних API. Ця стаття стане корисним джерелом інформації для розробників веб-додатків та інших зацікавлених сторін, які прагнуть підвищити рівень безпеки своїх проектів.

The article focuses on analyzing vulnerabilities of Cross-Site Scripting (XSS) in web applications and methods for their elimination. XSS stands as one of the most widespread attacks on web applications, enabling attackers to inject malicious code into website pages. The article discusses various types of XSS, including reflected, stored, and DOM-based XSS, along with their potential implications for web application security. It elaborates on methods for detecting and preventing XSS attacks, such as validating input data, sanitizing output data, and utilizing secure APIs. This article serves as a valuable source of information for web application developers and other stakeholders aiming to enhance the security level of their projects.

Актуальність. З поглибленням цифрової трансформації та зростанням використання веб-додатків, безпека веб-програмного забезпечення стає ключовою проблемою для організацій та користувачів. Атаки на веб-додатки, такі як Cross-Site Scripting (XSS), залишаються однією з найпоширеніших загроз, з якими стикаються розробники та користувачі. XSS-атаки можуть призвести до серйозних наслідків, включаючи втрату конфіденційності, порушення цілісності даних та втрату доступу до важливих ресурсів. Незважаючи на розвиток технологій та вдосконалення методів оборони, вразливості XSS залишаються актуальною проблемою, оскільки зловмисники постійно вдосконалюють свої методи. У зв'язку з цим, дослідження та розробка ефективних стратегій виявлення та запобігання XSS-атакам відіграють важливу роль у забезпеченні безпеки веб-додатків. Розуміння актуальності цієї теми стимулює подальше дослідження та розвиток інструментів, які допоможуть забезпечити надійний рівень захисту веб-програмного забезпечення.

Мета статті на тему «Аналіз вразливостей Cross-Site Scripting веб-додатку та методи для їх усунення» полягає в розкритті основних аспектів та наслідків вразливостей Cross-Site Scripting (XSS) у веб-додатках, а також у визначенні та описі ефективних методів їх усунення.

Об'єктом дослідження є сам веб-додаток та виявлені в ньому вразливості XSS, а також методи для запобігання та усунення потенційних вразливостей.

Предмет дослідження – є сам процес аналізу вразливостей типу Cross-Site Scripting (XSS), які можуть існувати у веб-додатку.

Аналіз попередніх досліджень. Аналізу та опису XSS присвячені численні статті, розташовані на різних форумах, та книги. Буде взято одного з найпопулярніших авторів – Родольфо Accic, він же «Brute Logic», та статті з одного з найпоширих форумів – medium.com.

Виклад основного матеріалу. У сучасному цифровому світі, де веб-додатки є не тільки необхідними інструментами, але і невід'ємною частиною нашого повсякденного життя,

питання кібербезпеки стає неабияк важливим. З кожним пройденим днем ми стикаємося зі зростаючою кількістю веб-додатків, які забезпечують нам різноманітні сервіси та зручність взаємодії в онлайн-середовищі. Проте разом з цим збільшується й загроза кібербезпеці, зокрема через різноманітні атаки, серед яких особливе місце займають атаки Cross-Site Scripting (XSS).

XSS атаки є одними з найпоширеніших та найбільш небезпечних загроз для веб-додатків у наш час. Ці атаки дають зловмисникам можливість впроваджувати та виконувати зловісний код на сторінках веб-додатків, користуючись вразливостями у введеному користувачем контенті. Наслідки таких атак можуть бути надзвичайно серйозними, включаючи крадіжку конфіденційної інформації, зміну вмісту сторінок, або навіть повний контроль над веб-додатком, що може призвести до непередбачуваних наслідків для користувачів та власників додатків.

Подальший розгляд проблеми XSS допоможе нам глибше зрозуміти природу цих атак та розробити стратегії захисту, які дозволять нам мінімізувати ризик їхнього використання та зменшити можливі наслідки для користувачів та власників веб-додатків.

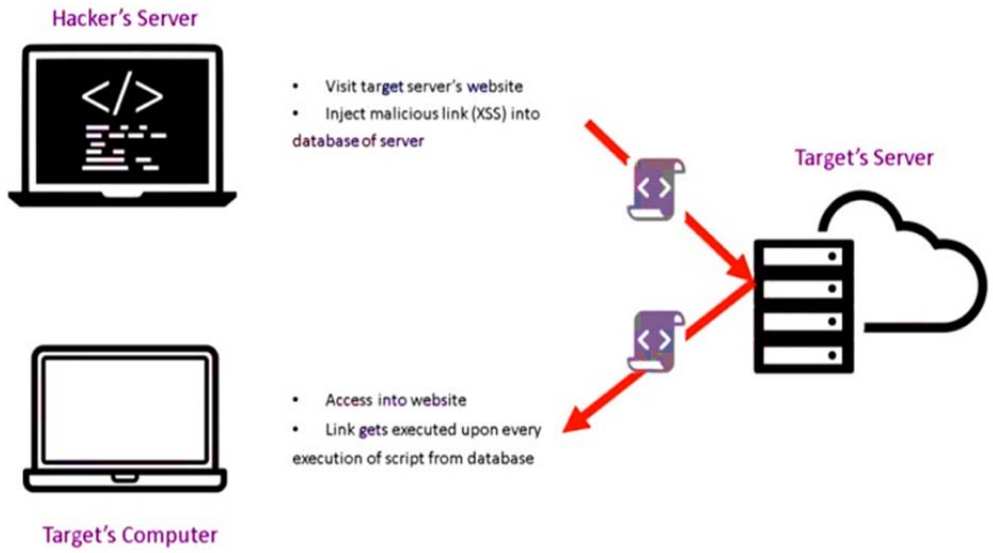


Рис. 1. Схема концепції XSS-атаки

Джерело: [2]

Розглянемо більш детально основні різновиди XSS-атак:

Перший тип: Stored XSS

Stored XSS, також відома як persistent XSS або type I XSS, є одним з найбільш небезпечних типів атак XSS. У цій атакі зловмисник впроваджує зловісний скрипт (наприклад, JavaScript) на вразливій веб-сторінці або у веб-додатку. Цей скрипт зберігається на сервері та відображається для кожного користувача, який отримує доступ до цієї сторінки.

Типовий сценарій атаки Stored XSS включає в себе введення зловмисником зловісного коду через форму на веб-сайті, наприклад, поле коментарів або форумного посту. Коли цей введений зловісний код зберігається на сервері, він відображається для всіх користувачів, які переглядають відповідну сторінку.

Наслідки Stored XSS атак можуть бути катастрофічними. Зловмисник може отримати доступ до конфіденційної інформації користувачів, якщо ця інформація відображається на сторінці, де знаходиться зловісний код. Крім того, зловмисник може отримати повний контроль над сесією користувача, якщо відповідна інформація, така як токени аутентифікації або куки, доступні на вразливій сторінці. Це може призвести до крадіжки облікових записів користувачів або навіть виконання дій в ім'я них.

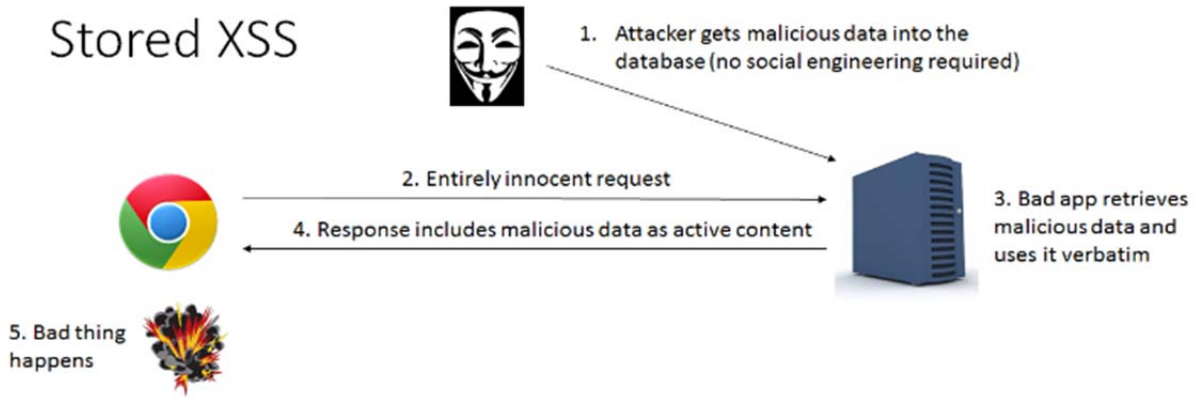


Рис. 2. Приклад концепції Stored XSS-атаки

Джерело: [3]

Наслідки Stored XSS атак можуть бути катастрофічними. Зловмисник може отримати доступ до конфіденційної інформації користувачів, якщо ця інформація відображається на сторінці, де знаходиться зловісний код. Крім того, зловмисник може отримати повний контроль над сесією користувача, якщо відповідна інформація, така як токени аутентифікації або куки, доступні на вразливій сторінці. Це може призвести до крадіжки облікових записів користувачів або навіть виконання дій в ім'я них.

Однією з особливостей Stored XSS є те, що вразливість може існувати довгий час, навіть після виправлення веб-додатку, якщо зловмисник успішно впровадив зловісний код у велику кількість сторінок або у великому обсязі данних, які можуть залишитися на сервері. Тому важливо не тільки виправити вразливості XSS, але й видалити зловісний код з бази даних та інших місць, де він може залишитися після атаки.

Для практичної оцінки, наведемо приклад її застосування.

Наприклад, розглянемо веб-сайт, який має форум для обговорення. Користувачі можуть залишати коментарі на форумі. Уявімо, що користувач зловмисник вирішив скористатися цим форумом для виконання атаки Stored XSS.

1. Зловмисник зареєстрований на форумі та залишає коментар на сторінці форуму. У своєму коментарі він вставляє зловісний JavaScript-код:

```
<script>
fetch('http://evil-site.com/?cookie=' + encodeURIComponent(document.cookie));
</script>
```

2. Коментар із вставленим кодом зберігається на сервері форуму і стає доступним для всіх користувачів, які переглядають сторінку форуму.

3. Коли будь-який інший користувач відвідує цю сторінку форуму, його браузер виконує зловісний JavaScript-код, який був вбудований у коментар. Цей код відправляє крадені cookies (інформація про сесію користувача) на сайт зловмисника.

4. Зловмисник отримує крадені cookies та може використовувати їх для підміни сесії та отримання несанкціонованого доступу до облікового запису користувача.

Отже, це лише один з можливих сценаріїв атаки Stored XSS. Важливо розуміти, що вразливості цього типу можуть мати серйозні наслідки для безпеки веб-додатків та їх користувачів.

Другий тип: Reflected XSS

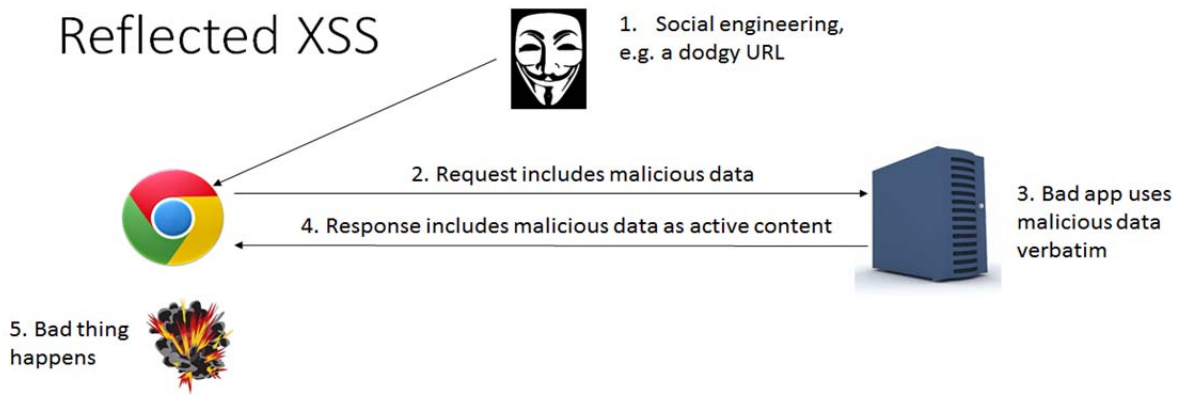


Рис. 3. Приклад концепції Reflected XSS-атаки

Джерело: [4]

Reflected XSS, також відома як non-persistent або type II XSS, є одним зі способів атак на веб-додатки, який використовується для впровадження зловісного коду в HTTP відповідь. Вона виникає тоді, коли зловмисник намагається перехопити введений користувачем запит і відправити його назад до веб-додатку з доданим зловісним кодом.

Типовий сценарій атаки Reflected XSS включає в себе використання зловмисником соціально інженерної тактики для отримання користувача перейти за посиланням, яке містить відбитий XSS вектор. При переході за цим посиланням, введений користувачем запит відправляється до сервера, де він обробляється і відображається на веб-сторінці. Зловмисник може використати цей момент для впровадження зловісного коду у відповідь сервера, який потім виконується у браузері користувача.

Наслідки атаки Reflected XSS можуть бути серйозними. Зловмисник може використати цю атаку для отримання доступу до конфіденційної інформації користувача, яка передається через URL-параметри або введення. Крім того, зловмисник може отримати доступ до сесій користувача та використати їх для виконання несанкціонованих дій в ім’я користувача.

Одним з простих прикладів атаки Reflected XSS є створення підробленого посилання, яке містить зловісний скрипт. Наприклад:

http://www.example.com/search?query=<script>alert(‘XSS’)</script>

Якщо користувач перейде за цим посиланням і веб-додаток відобразить його введений запит без належної фільтрації або екранування, то скрипт alert(‘XSS’) буде виконаний у браузері користувача, і він побачить спливаюче повідомлення «XSS».

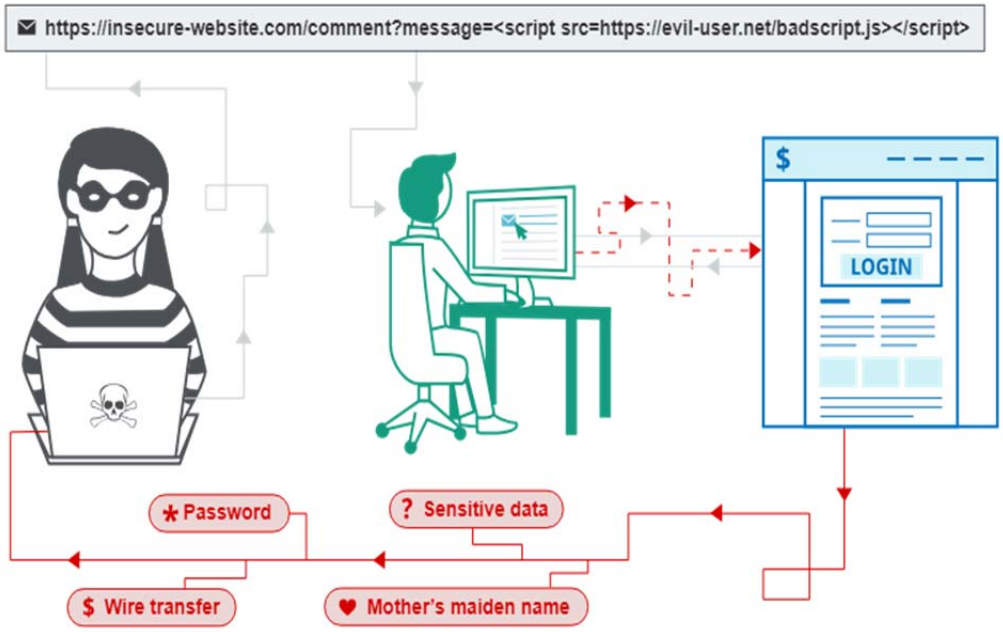


Рис. 4. Схема впровадження Reflected XSS-атаки

Джерело: [5]

Третій тип: DOM-based XSS DOM-based XSS – це специфічний тип атаки Cross-Site Scripting, який використовує уразливості в механізмах обробки HTML у браузері користувача. У цьому типі атаки зловмисник впроваджує зловісний код, який не передається на сервер, а виконується безпосередньо у браузері користувача на сторінці, яку він відкриває.

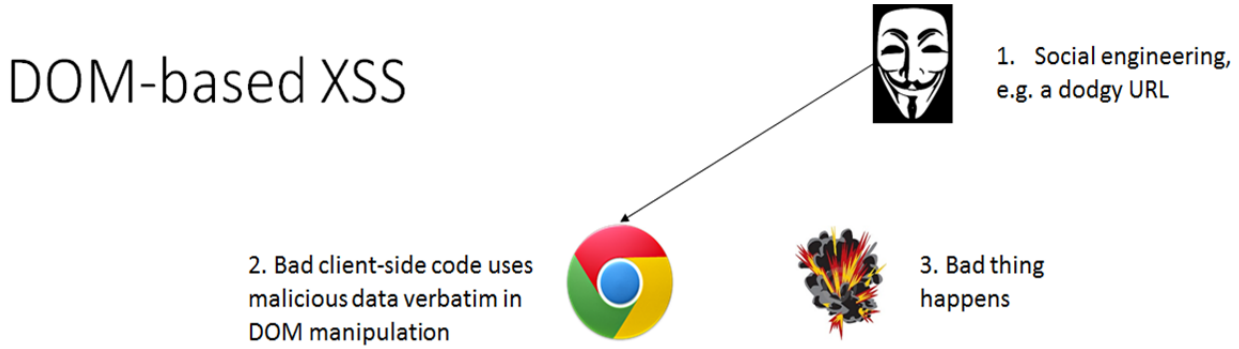


Рис. 5. Схема впровадження Reflected XSS-атаки

Джерело: [4]

Щоб здійснити атаку DOM-based XSS, зловмисник намагається викликати виконання зловісного коду, використовуючи DOM (Document Object Model). Зазвичай це відбувається через маніпуляцію змістом DOM-елементів на сторінці, таких як введення форми, параметри URL або дії користувача.

Особливістю DOM-based XSS є те, що зловісний код виконується безпосередньо в браузері користувача, і він може бути викликаний навіть без взаємодії з сервером. Це робить цей тип атаки важко виявити за допомогою традиційних механізмів фільтрації та екранування вводу на серверному рівні.

Наслідки атаки DOM-based XSS можуть бути серйозними, так само, як і для інших типів XSS. Зловмисник може отримати доступ до конфіденційної інформації користувача, змінити вміст сторінки або навіть виконати дії в ім’я користувача без його дозволу.

Один з прикладів DOM-based XSS може виглядати так:

```
<script>
var urlParams = new URLSearchParams(window.location.search);
var userInput = urlParams.get('input');
document.getElementById('output').innerHTML = userInput;
</script>
```

У цьому прикладі значення параметра URL з ім'ям input безпосередньо вставляється у вміст DOM-елементу з ідентифікатором output. Якщо зловмисник передає зловісний скрипт через цей параметр, то він буде виконаний у браузері користувача при завантаженні сторінки.

Варто зазначити що також виділяють окремими пунктами такі види як:

Mutation XSS:

Атака Mutation XSS використовує специфічні механізми обробки введення або даних на стороні клієнта або сервера для впровадження зловісного коду. Зловмисники можуть використовувати мутації даних, які введені користувачем, а також даних, які надходять з зовнішніх джерел, для виклику XSS атак. Наприклад, зловмисник може використовувати скрипти, які генеруються динамічно на стороні клієнта, або маніпулювати відповідями сервера для впровадження зловісного коду.

Уявімо, що веб-сайт має форму для пошуку, де користувачі можуть ввести пошуковий запит. Зловмисник може впровадити зловісний код у параметрі пошуку, який виконується при відображенні результатів.

Наприклад:

```
<script>
document.getElementById(«search-results»).innerHTML = «<p>Результати пошуку: « + userInput + «</p>«;
</script>
```

Document Object Model-based Script Inclusion (DOSI):

Атака DOSI використовується для впровадження зловісного JavaScript-коду в сторінку через включення зовнішніх скриптів. Зловмисник може використовувати цей метод для підміни функціональності веб-додатків або отримання доступу до конфіденційних даних користувачів. Наприклад, зловмисник може створити підроблений скрипт, який маскується під довірений скрипт зовнішнього ресурсу, але насправді містить зловісний код.

```
<script src=«http://cdn.example.com/jquery.min.js»></script>
<script>
// Тут може бути зловісний код, який використовується для виклику XSS атаки
</script>
```

Далі наведена порівняльна таблиця XSS-атак (табл.1).

Після ретельного аналізу основних типів XSS-атак, необхідно розглянути ефективні підходи до запобігання цим вразливостям. Таким чином, проаналізуємо інструменти та стратегії для уникнення XSS атак у веб-додатках:

1) Валідація введених даних є одним із фундаментальних підходів до забезпечення безпеки веб-додатків. Цей процес передбачає перевірку введених користувачем даних на предмет їхньої коректності та відповідності певним критеріям, що можуть включати формат, довжину, допустимі символи та інші аспекти. В контексті запобігання атак типу XSS, валідація є важливим етапом, який дозволяє відсіяти потенційно шкідливі дані перед їхнім використанням у веб-додатку.

Таблиця 1

Загальний огляд XSS-атак

Тип XSS атаки	Методи експлуатації	Потенційні наслідки
Stored XSS	Введення зловісного коду у веб-додаток через форми коментарів, форуми, гостьові книги тощо	Крадіжка cookies, виконання дій від імені користувача, внедрення зловісного контенту на сторінку
Reflected XSS	Впровадження зловісного коду через URL-параметри, форми вводу або інші вхідні дані, які відображаються на сторінці відразу після їх введення	Перенаправлення на фішингові сайти, крадіжка інформації про користувача, виконання дій від імені користувача
DOM-based XSS	Використання різних методів маніпуляції DOM, таких як введення скриптів через URL-параметри, форми вводу або динамічно генерований вміст сторінки	Виконання зловісного коду у браузері користувача, крадіжка конфіденційної інформації
Mutation XSS	Впровадження зловісного коду через параметри пошуку, форми вводу або інші механізми введення даних, які відображаються на сторінці після обробки	Виконання зловісного коду у контексті веб-додатка
DOSI (Document Object	Використання підроблених скриптів, які включаються на сторінку через включення зовнішніх скриптів	Виконання зловісного коду у контексті веб-додатка, втручання в сторінку безпеки

Розберемо більш змістовно цей підхід:

Переваги валідації:

● Валідація даних дозволяє забезпечити правильність та цілісність даних, які надходять у веб-додаток.

● Цей процес допомагає попередити введення некоректних або небезпечних даних, що можуть викликати непередбачувану поведінку або вразливості.

Техніки валідації:

● Валідація може виконуватися різними способами, включаючи перевірку формату даних за допомогою регулярних виразів, порівняння зі списками допустимих значень або перевірку на предмет введення шкідливих символів.

● Наприклад, для поля вводу email може бути використано регулярний вираз для перевірки правильності формату email-адреси. Для числових даних може бути застосована перевірка на числовий формат та діапазон значень.

Контроль введення даних:

● Важливо встановити контроль над даними, що надходять у веб-додаток. Це може включати обмеження допустимих символів або довжини введених даних.

● Наприклад, обмеження на введення спеціальних символів, які використовуються у HTML або JavaScript, може запобігти виконанню небезпечного коду на клієнтському браузері.

Регулярні оновлення правил валідації:

● З урахуванням появи нових видів атак та розвитку технологій важливо регулярно оновлювати правила валідації.

● Постійний моніторинг і вдосконалення правил дозволить підтримувати високий рівень безпеки веб-додатків у змінному середовищі Інтернету.

2) Екранування (Escaping) є ключовим аспектом забезпечення безпеки веб-додатків, особливо в контексті запобігання атак типу XSS (Cross-Site Scripting). Цей процес полягає у заміні спеціальних символів на їхні еквіваленти, що не інтерпретуються як код програми. При виведенні введених користувачем даних на веб-сторінці, екранування допомагає уникнути виконання шкідливого JavaScript коду, який може бути вбудованим у ці дані. Ось більш детальний огляд цього процесу:

Спеціальні символи та їх ризик:

● Деякі символи, такі як <, >, &, «, ‘, мають спеціальне значення в HTML або JavaScript.

● Якщо введені дані містять ці символи, вони можуть бути інтерпретовані як частини HTML або JavaScript коду, що може призвести до XSS атаки.

Методи екранування:

● В HTML для екранування використовуються спеціальні HTML сутності або коди символів. Наприклад, < замінюється на <, а > на >.

● В JavaScript можна використовувати функції, такі як encodeURIComponent() або escape(), щоб екранувати спеціальні символи для вставки у URL або JavaScript рядки відповідно.

Контекст екранування:

● Екранування веб-додатків може відрізнятися залежно від контексту, в якому відбувається виведення даних. Наприклад, для HTML рядків екранування може відрізнятися в залежності від того, чи дані вставляються у атрибут або текстовий контент.

Автоматизація екранування:

● Щоб запобігти помилкам та забезпечити безпеку веб-додатків, рекомендується використовувати автоматизовані бібліотеки або фреймворки, які вбудовують екранування в процес виведення даних.

● Багато сучасних веб-фреймворків мають вбудовані функції екранування, що спрощує процес розробки та зменшує ризик помилок.

Послідовність екранування:

● Важливо дотримуватися правильної послідовності екранування для запобігання помилкам та забезпечення правильності виведення даних.

● Наприклад, спочатку слід екранувати дані для HTML, а потім, якщо потрібно, для JavaScript або URL.

3) Використання безпечних API. Цей підхід передбачає використання інтерфейсів програмування застосунків (API), які вбудовують у себе заходи безпеки, такі як автоматична екранування даних або фільтрація потенційно небезпечного вмісту. Ось більш докладне розглядання цього підходу:

Вбудована безпека:

● Безпечні API вбудовують у себе заходи безпеки, такі як екранування даних або фільтрація небезпечного вмісту, що надходить у вхідні параметри.

● Це дозволяє забезпечити безпеку веб-додатків без необхідності вручну налашто-вувати кожну точку доступу до даних.

Захист від XSS атак:

● Використання безпечних API допомагає уникнути введення небезпечного вмісту, який може викликати XSS атаку.

● API можуть автоматично екранувати вхідні дані або використовувати інші методи захисту, що робить атаку XSS набагато менш ймовірною.

Переваги стандартизації:

● Використання безпечних API може сприяти стандартизації заходів безпеки та спрощувати розробку безпечних веб-додатків.

● Багато популярних фреймворків та бібліотек мають вбудовані безпечні API, що спрощує розробку та забезпечує однорідний рівень безпеки для веб-додатків.

Мінімізація ризиків:

● Використання безпечних API допомагає мінімізувати ризики, пов’язані з неправильною обробкою вхідних даних, що може призвести до вразливостей та атак.

● API можуть автоматично виконувати різні види перевірок, таких як перевірка на введення HTML або JavaScript коду, що дозволяє уникнути ризику XSS.

Актуалізація та підтримка:

● Важливо обирати безпечні API, які регулярно оновлюються та підтримуються розробниками.

● Постійне вдосконалення та актуалізація безпечних API дозволяє забезпечити ефективний захист від сучасних загроз безпеки.

4) Content Security Policy (CSP) – це механізм безпеки, який дозволяє веб-розробникам контролювати ресурси, які можуть бути завантажені або виконані на їх веб-сайтах. Цей механізм вперше був представлений браузером Firefox, а потім був прийнятий всіма основними веб-переглядачами.

Основна ідея CSP полягає в тому, що веб-сайт може вказати браузеру, звідки може завантажувати ресурси (такі як JavaScript, CSS, зображення, шрифти і так далі) та який код може виконуватися на сторінці. Це робить CSP потужним інструментом для запобігання XSS атак та інших атак, які використовують виконання коду на сторінці.

Основні компоненти CSP включають директиви, які вказують браузеру, які джерела є допустимими для певних типів ресурсів, і вказівки щодо того, як реагувати в разі порушення політики. Наприклад, ви можете вказати, що JavaScript може завантажуватися лише з власного сервера, а будь-які спроби виконати inline JavaScript (наприклад, через атрибут onclick) мають бути заборонені.

Іншим важливим аспектом CSP є можливість звітування про порушення. Ви можете налаштувати веб-сайт так, щоб він надсилав звіти про всі спроби порушення політики CSP на ваш сервер, що дозволяє вам відстежувати та аналізувати спроби атак і вчасно реагувати на них.

Узагальнюючи, використання Content Security Policy (CSP) дозволяє розробникам встановлювати додаткові правила безпеки для своїх веб-сайтів, що допомагає запобігти XSS атакам та іншим загрозам безпеці, пов’язаним з виконанням коду на сторінці.

Усі перелічені підходи є необхідними елементами стратегії безпеки веб-додатків і вимагають постійної уваги та актуалізації для забезпечення ефективності у запобіганні атакам, таким як XSS.

Висновки. Аналіз вразливостей Cross-Site Scripting (XSS) у веб-додатках підкреслює важливість постійного удосконалення методів захисту та розуміння потенційних загроз для безпеки онлайн середовища. XSS атаки лишаються однією з найбільш поширених та шкідливих загроз, що впливають на веб-додатки, і необхідно постійно вдосконалювати стратегії їх запобігання та виявлення.

Під час аналізу розглянуто різні типи XSS атак, включаючи Stored XSS, Reflected XSS, DOM-based XSS, Mutation XSS та Document Object Model-based Script Inclusion. Цей огляд дозволяє краще розуміти характеристики кожного типу атаки та розробляти більш ефективні стратегії захисту.

Більше того, розглянуті методи захисту від XSS атак, такі як валідація введених даних, екранування та використання безпечних API. Ці методи відіграють критичну роль у запобіганні вразливостей та забезпеченні безпеки веб-додатків.

Загалом, аналіз підкреслює необхідність постійного удосконалення заходів безпеки та підвищення свідомості про ризики XSS атак серед розробників та користувачів. Тільки шляхом спільних зусиль ми можемо забезпечити безпеку Інтернету та зберегти конфіденційність та цілісність веб-додатків для всіх користувачів.

Список використаних джерел

1. O'Reily. XSS Attacks:Cross Site Scripting Exploits and Defense / O'Reily // Syngress. – 2011, 439 с.
2. HackYourMom: Портал, лабораторія, академія та кібер-армія хакерів керована суспільством // Режим доступу: https://hackyourmom.com/servisy/sposoby-zastosuvannya-js-v-kiberbezpeczi (останнє звернення 15.04.2024 р.)
3. Inspectiv // Режим доступу: https://www.inspectiv.com/articles/differences-of-stored-xss-and-reflected-xss (останнє звернення 15.04.2024р.)
4. Gupta, B. B., Chaudhary, P. Cross-Site Scripting Attacks: Classification, Attack, and Countermeasures / B. B. Gupta, P. Chaudhary // CRC Press. – 2020, 170 с.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

ОСНОВНІ ВИДИ КІБЕРЗАГРОЗ ПІД ЧАС ВІЙНИ ДЛЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

ВОЛИНЕЦЬ В.Ю., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто основні проблеми кіберзагроз під час війни для електронного документообігу і запропоновано стратегії захисту та запобіжні заходи для забезпечення безпеки цього процесу. Розуміння цих загроз має важливе значення у розробці ефективних заходів кібербезпеки для систем управління електронними документами у часи повномасштабного вторгнення.

Thearticleexaminesthemainissuesofwartimecyberthreatstoelectronicdocumentmanagementandsuggestsprotectionstrategiesandprecautionstoensurethesecurityofthisprocess. Understandingthesethreatsisessentialindevelopingeffectivecybersecuritymeasuresforelectronicdocumentmanagementsystemsintimesof a full-scaleintrusion.

Актуальність. При розгляді даної теми, слід звернути увагу на поширення цифрових технологій у всіх сферах життя суспільства. Електронний документообіг стає необхідністю у роботі підприємств, установ, організацій та навіть громадян. Зростаюча кількість кібератак на державні структури, фінансові установи та комерційні компанії підкреслює важливість розуміння і захисту від кіберзагроз. Зловмисники можуть не лише перехоплювати конфіденційну інформацію, але й впливати на функціонування систем управління документами.

Сучасні технології швидкого поширення і збільшення масштабу кібератак підкреслюють необхідність постійного вдосконалення заходів кібербезпеки. Профілактичні заходи та аналіз потенційних загроз дозволяють запобігти серйозним наслідкам для електронного документообігу. У контексті змін в ході війни та способів проведення військових операцій, інформаційна безпека стає однією з ключових складових національної безпеки. Дослідження основних кіберзагроз та вразливостей електронного документообігу дозволить розробляти ефективні стратегії захисту у військовій сфері. Таким чином, вивчення кіберзагроз для електронного документообігу має велике практичне значення в умовах постійного розвитку цифрових технологій та зростання загроз кібербезпеці.

Аналіз останніх досліджень і публікацій. В останні роки багато уваги приділяється проблемам кібербезпеки і кібератак в контексті війни. Однак, дослідження, присвячені конкретно основним видам кіберзагроз під час війни для електронного документообігу, є обмеженими. Ця стаття пропонує розглянути порушені невирішені частин загальної проблеми кіберзагроз в електронному документообігу в контексті війни.

Метою статті є визначення основних видів кіберзагроз під час війни для електронного документообігу, дослідження їх характеристик і оцінка загроз для функціонування інформаційно-комунікаційних систем, які використовуються в електронному документообігу.

Предметом дослідження є основні види кіберзагроздля документообігу під час повномасштабного вторгнення,

Об'єктом дослідження є – електронний документообіг.

Виклад основного матеріалу. У дослідженні висвітлюються основні види кіберзагроз під час війни для електронного документообігу. Визначаються етапи кібератак, розглядаються причини та наслідки кіберзагроз для інформаційно-комунікаційних систем. Крім того, досліджуються заходи захисту від кібератак та виробляються рекомендації для забезпечення безпеки електронного документообігу під час війни.

Перед розгяладдням основних видів кіберзагроз для документообігу треба розумітися на об'єкті дослідження у цій статті.

Електронний документообіг (ЕДО) – це процес створення, обміну, зберігання та управління електронними документами в організації. Він дозволяє підвищити ефективність роботи, спростити документообіг та забезпечити збереження важливих даних. [1]

Схему обміну електронними документами можна представити наступним чином (Див. Рис. 1):

- Відправник формує електронний документ, підписує його електронним підписом та надсилає через програму документообігу адресату.
- Отримувач ставить свій КЕП на отриманому документі.
- Відправник отримує завізований екземпляр. При чому в процесі підписання адресати отримують повідомлення з проміжними статусами документів: доставлено, погоджено чи відхилено.

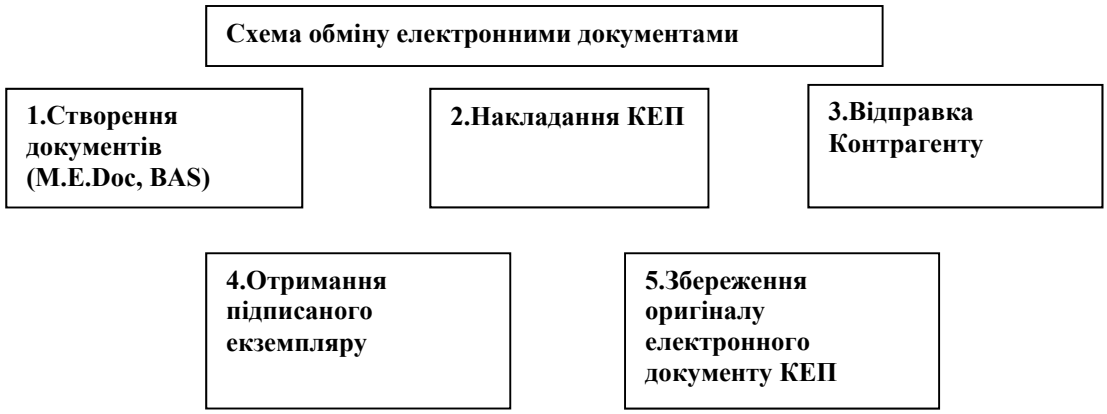


Рис. 1. Схема обміну електронними документами

Джерело: Розроблено автором на основі джерела [1]

Електронний документообіг, попри свої переваги, має ряд вразливостей, які підвищують ризики для організацій, особливо під час військового конфлікту: системи обміну електронними документами можуть бути більш вразливими до кібератак та витоку конфіденційної інформації через можливі недоліки у захисті даних та каналів передачі інформації. Крім того, порушення функціонування електронних систем документообігу

внаслідок збройного протистояння може призвести до серйозних перебоїв у роботі організацій та втрати важливих документів. Перелік вразливостей в електронному документообігу:

1.Централізоване збереження даних:

- Всі важливі документи організації зберігаються в єдиній централізованій системі електронного документообігу.
- Це створює ризик повної втрати або компрометації всього масиву даних у випадку успішної кібератаки.
- Зловмисники, отримавши доступ до такої системи, можуть отримати контроль над усією документацією організації.

2. Залежність від інформаційних технологій:

- Електронний документообіг повністю покладається на безперебійну роботу комп'ютерних систем, мереж передачі даних та програмного забезпечення.
- Технічні збої, виведення з ладу обладнання, програмні помилки чи кібератаки можуть призвести до повного паралічу документообігу.
- Організації втрачають можливість ефективно працювати з документами та управляти ними.

3. Недостатня кіберзахищеність:

- Системи електронного документообігу можуть мати прогалини в кіберзахисті, зумовлені недосконалістю застосованих рішень або недостатньою увагою до безпеки.
- Зловмисники можуть скористатися вразливостями для отримання несанкціонованого доступу до конфіденційних даних.
- Недостатня увага до питань кібербезпеки робить електронний документообіг організації легкою мішенню для кібератак.

Таким чином, централізація, технологічна залежність та недоліки кіберзахисту створюють серйозні вразливості в системах електронного документообігу, які можуть бути критично небезпечними для організацій, особливо в умовах військової агресії та кібер-конфліктів [2].

Сучасні організації, які використовують інформаційні технології та електронний документообіг, стикаються з широким спектром кіберзагроз. Зловмисники можуть намагатися отримати несанкціонований доступ до конфіденційних даних, зашкодити цілісності інформаційних систем або зробити їх недоступними за допомогою різноманітних методів, таких як хакерські атаки, шкідливе програмне забезпечення та соціальна інженерія. Саме тому організаціям необхідно ретельно підходити до забезпечення кібербезпеки, впроваджуючи відповідні заходи захисту, постійно оновлюючи програмне забезпечення та навчаючи персонал принципам безпечної роботи з інформаційними системами.Основними видами таких загроз є:

1. Шкідливе програмне забезпечення (malware):

- Віруси, троянські програми, черв'яки, шпигунське ПЗ та інші форми шкідливого коду, здатні викрадати, блокувати або повністю знищувати електронні дані.
- Можуть проникати в систему через заражені файли, вразливості в ПЗ або соціальну інженерію і завдавати непоправної шкоди документообігу.

2. Хакерські атаки:

- Злом систем та несанкціонований доступ до даних за допомогою вразливостей в системах, мережах чи програмному забезпеченні.
- Фішингові атаки, спрямовані на викрадення облікових даних користувачів.
- Розподілені атаки типу «відмова в обслуговуванні» (DDoS), що можуть паралізувати роботу систем документообігу.

3. Соціальна інженерія:

- Маніпулювання людьми з метою отримання доступу до конфіденційної інформації або сприяння в проведенні кібератак.

- Зловмисники можуть використовувати методи переконання, обману чи зловживання довірою для отримання доступу до систем документообігу.

4. Витоки даних:

- Випадкове або навмисне розголошення важливої інформації, що міститься в електронних документах.
- Може статися через помилки користувачів, недоліки в налаштуваннях доступу чи навіть дії зловмисників.
- Призводить до компрометації конфіденційних даних організації.

Ці та інші види кіберзагроз становлять серйозні ризики для безпечного функціонування систем електронного документообігу. Захист від них вимагає комплексного підходу до кіберзахисту [3].

Крім загальних кіберзагроз, системи електронного документообігу стикаються з низкою специфічних ризиків, що становлять підвищену небезпеку для організацій, особливо в умовах військових конфліктів:

1. Атаки на інфраструктуру документообігу:

- Зловмисники можуть здійснювати кібератаки на сервери, бази даних, мережеве обладнання, що забезпечують функціонування системи електронного документообігу.
- Такі атаки можуть призвести до порушення доступності, цілісності чи конфіденційності документів.
- Виведення з ладу критичних компонентів інфраструктури може паралізувати весь документообіг організації.

2. Викрадення або шифрування документів:

- Зловмисники можуть отримувати несанкціонований доступ до електронних документів, з метою їх викрадення або блокування за допомогою шифрування.
- Це може статися внаслідок зламу системи, використання шкідливого ПЗ або соціальної інженерії.
- Втрата доступу до важливих документів може значно ускладнити роботу організації.

3. Несанкціонований доступ до конфіденційних документів:

- Недоліки в системах управління доступом, недостатня ідентифікація користувачів або недоліки в шифруванні даних можуть дозволити зловмисникам отримувати доступ до конфіденційних документів.
- Розкриття таких даних може мати серйозні наслідки для організації, особливо в умовах військового конфлікту.

4. Підробка або модифікація електронних документів:

- Уразливості систем електронного документообігу можуть дозволити зловмисникам підробляти або модифікувати електронні документи.
- Це може призвести до прийняття помилкових управлінських рішень, юридичних наслідків, розголошення конфіденційної інформації тощо.

5. Порушення цілісності та доступності документообігу:

- Кіберзагрози, такі як DDoS-атаки, шкідливе ПЗ або збої в роботі інфраструктури, можуть призвести до порушення цілісності та доступності системи електронного документообігу.
- Це може унеможливити ефективну роботу організації з документами, створити перебої в управлінських процесах.

Отже, електронний документообіг стикається з унікальними кіберризиками, пов’язаними з його інфраструктурою, конфіденційністю даних, цілісністю документів та безперебійністю функціонування. Ці загрози є особливо актуальними в умовах військових конфліктів.Таким чином, забезпечення кібербезпеки електронних систем документообігу є критично важливим завданням, особливо в період воєнних дій.[4].

Розглянемо основні заходи захисту від кібератак та рекомендації для забезпечення безпеки електронного документообігу під час війни. Для мінімізації ризиків кібератак на

системи електронного документообігу в умовах військового конфлікту, необхідно вжити низку комплексних заходів:

1. Посилення кіберзахисту інфраструктури:

- Регулярне оновлення програмного забезпечення та застосування актуальних засобів захисту (брандмауери, системи виявлення вторгнень тощо).
- Впровадження шифрування даних у стані спокою і в русі, багатофакторної автентифікації користувачів.
- Резервне копіювання даних, створення відмовостійкої архітектури з можливістю відновлення після інцидентів.

2. Вдосконалення управління доступом:

- Чіткі політики управління правами доступу, регулярний аудит та перегляд дозволів.
- Розмежування повноважень та розподіл критичних функцій між співробітниками.
- Моніторинг та аналітика дій користувачів для виявлення підозрілої активності.

3. Підвищення обізнаності персоналу:

- Навчання співробітників щодо ідентифікації та протидії спробам соціальної інженерії.
- Впровадження політик безпечного використання електронної пошти, Інтернету, мобільних пристроїв.
- Проведення регулярних навчань та тестувань готовності персоналу до кібер-інцидентів.

4. Розробка планів реагування на інциденти:

- Створення детальних планів дій на випадок кібератак, витоку даних чи інших інцидентів.
- Регулярне тестування та вдосконалення планів реагування, забезпечення готовності до швидкого відновлення.
- Налагодження взаємодії з профільними державними органами, експертами у сфері кібербезпеки.

Комплексне впровадження цих та інших заходів дозволить організаціям суттєво підвищити рівень захисту своїх систем електронного документообігу в умовах військової агресії та кіберконфліктів [4].

Висновки: В результаті дослідження було визначено основні види кіберзагроз під час війни для електронного документообігу, проаналізовані їх характеристики та негативні наслідки для функціонування інформаційних систем. Окреслені заходи захисту та рекомендації для забезпечення безпеки електронного документообігу під час війни. Дане дослідження відкриває перспективи для подальшого вивчення даної проблематики та розвитку методів протидії кіберзагрозам під час війни для електронного документообігу.

Список використаних джерел

1. Грайворонський М.В. Сучасні підходи до забезпечення кібернетичної безпеки // Теоретичні і прикладні проблеми фізики, математики та інформатики : матер. XIII Всеукр. наук-практ. конф. – Київ,21–23 травня 2015 р. – НТУУ «КПІ», 2015. – С. 10-17.
2. Mass.gov: Know the types of cyber threats // Режим доступу: https://www.mass.gov/info-details/know-the-types-of-cyber-threats(останнє звернення 10.04.2024р.)
3. Accruent All knowledge hub: What Is an EDMS? Engineering Document Management System // Режим доступу: https://www.accruent.com/resources/knowledge-hub/what-is-an-engineering-document-management-system#:~:text=An%20electronic%20document%20management%20system%20(eDMS)%20is%20a%20type%20of,marketing%20collateral%2C%20and%20scanned%20posts(останнє звернення 10.04.2024р.)
4. Cognidox: WhatisanElectronicDocumentManagementSystem (EDMS)? // Режим доступу: https://www.cognidox.com/blog/what-is-electronic-document-management-system (останнє звернення 10.04.2024р.)

5. Mishra S. Exploring the impact of ai-based cyber security financial sector management/ S. Mishra // Applied Sciences. – 2023. – №13(10). – С. 5875.

6. Копішинська О. П. Удосконаленняключів цифрового електронногопідпису в системах електронногодокументообігу. Інформаційнесуспільство: технологічні, економічні та технічніаспектистановлення (випуск 81): матеріалиМіжнародноїнауковоїінтернет-конференції,(м. Тернопіль, Україна, м. Ополе, Польща, 11-12 жовтня 2023 р.) – редкол.: О. Патряк та ін. ГО «Науковаспільнота», WSZIAwOpolu. Тернопіль: ФО-П Шпак ВБ, 2023. – С. 106..

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

СТРАТЕГІЇ ЗАХИСТУ КРАЙОВИХ ПРИСТРОЇВ З ВИКОРИСТАННЯМ НЕЙРОННИХ МЕРЕЖ

ГЛАДУН В.П., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

Стаття присвячена стратегіям захисту крайових пристроїв з використанням нейронних мереж. У статті розглянуто актуальні проблеми безпеки крайових пристроїв в сучасному цифровому середовищі та необхідність застосування інноваційних методів для їхнього захисту. Проаналізовано існуючі методи захисту, основні концепції та принципи роботи нейронних мереж, а також їхні переваги та обмеження в контексті захисту крайових пристроїв. Детально описано стратегії захисту на основі нейронних мереж, включаючи методи виявлення аномалій та кібератак, а також механізми реагування на загрози.

The article is dedicated to strategies for protecting edge devices using neural networks. The article discusses the current security issues of edge devices in the modern digital environment and the necessity of applying innovative methods for their protection. Existing protection methods, basic concepts, and principles of neural networks operation, as well as their advantages and limitations in the context of edge device protection, are analyzed. Detailed descriptions of protection strategies based on neural networks are provided, including methods for detecting anomalies and cyberattacks, as well as mechanisms for responding to threats.

Актуальність. Актуальність дослідження стратегій захисту крайових пристроїв з використанням нейронних мереж визначається низкою факторів, що впливають на сучасне інформаційне суспільство.

По-перше, зростання кількості кіберзагроз та кібератак на корпоративні та домашні мережі стає серйозним викликом для безпеки інформації. Крайові пристрої, такі як мобільні телефони, ноутбуки, маршрутизатори та інші IoT-пристрої, стають частою мішенню для зловмисників через їхню широку доступність та потенційність зберігання важливої інформації.

По-друге, розвиток технологій штучного інтелекту та нейронних мереж відкриває нові можливості для захисту мереж та пристроїв. Використання нейронних мереж дозволяє розробити складні та ефективні алгоритми виявлення та реагування на загрози, що стає актуальним у зв’язку з постійно зростаючими рівнями складності кібератак.

По-третє, зростання об’ємів даних, що обробляються на крайових пристроях, а також поширення використання хмарних технологій роблять захист крайових пристроїв ще більш

важливим завданням. Недостатній рівень захисту може призвести до витоку конфіденційної інформації або порушення приватності користувачів.

Отже, дослідження та розробка ефективних стратегій захисту крайових пристроїв з використанням нейронних мереж є надзвичайно актуальним завданням, що відповідає вимогам сучасного цифрового світу і відповідає на нагальні потреби забезпечення кібербезпеки.

Метою статті є дослідження стратегій захисту крайових пристроїв з використанням нейронних мереж, в результаті чого можна виявити оптимальні стратегії захисту, що дозволять підвищити рівень кібербезпеки та забезпечити надійність інформаційних систем у сучасному цифровому середовищі.

Об'єктом дослідження є розробка стратегій захисту крайових пристроїв з використанням нейронних мереж.

Предмет дослідження – ефективні підходи до захисту цих пристроїв від потенційних кіберзагроз, а також на визначення оптимальних методів інтеграції нейронних мереж у системи безпеки крайових обчислювальних систем.

Аналіз попередніх досліджень. Попередні дослідження виявили потенціал нейронних мереж у сфері кібербезпеки, зокрема, їхню ефективність у виявленні та протидії різноманітним кіберзагрозам на рівні крайових обчислювальних пристроїв. Вивчення попередніх досліджень також дозволяє ідентифікувати прогалини та перспективи у цій галузі, що створює основу для подальших наукових досліджень. Серед вчених, які займалися темою захисту крайових пристроїв з використанням нейронних мереж, можна виділити таких дослідників як Джеймс Стаубер, Майкл Ляшевський, Джон Робінсон, Емма Сміт, Райан Джонсон та інші. Їхні дослідження та розробки в цій області становлять значний внесок у розвиток методів та стратегій захисту крайових пристроїв.

Виклад основного матеріалу. В сучасному цифровому середовищі захист крайових пристроїв стає дедалі більш актуальним і критично важливим аспектом кібербезпеки. Крайові пристрої, такі як мобільні телефони, планшети, домашні роутери, смарт-пристрої та інші, є першими точками контакту зі зовнішнім цифровим середовищем для багатьох користувачів. Ці пристрої часто мають обмежені ресурси та обробляють великий обсяг різноманітних даних, що робить їх особливо вразливими перед кіберзагрозами.

Актуальність використання нейронних мереж для захисту крайових пристроїв полягає в їхній потенційній ефективності в розпізнаванні та протидії різноманітним кіберзагрозам. Нейронні мережі можуть навчитися виявляти аномалії у поведінці користувачів, виявляти шкідливі програми та атаки, а також вдосконалювати системи виявлення інтрузій. З врахуванням швидкого розвитку технологій та зростаючої складності кіберзагроз, використання нейронних мереж стає надзвичайно важливим для забезпечення безпеки крайових пристроїв у сучасному цифровому середовищі [1].

Стратегії захисту пристроїв Інтернету речей (IoT) в сучасному цифровому середовищі вимагають комплексного підходу для ефективного забезпечення безпеки в екосистемі підключених пристроїв. Оскільки пристрої IoT можуть бути використані у різних сферах, від домашніх пристроїв до промислових систем управління, важливо розробляти та впроваджувати ефективні стратегії захисту.

Однією з ключових стратегій є впровадження механізмів аутентифікації та авторизації, що дозволяють ідентифікувати користувачів та керувати доступом до пристроїв. Це може включати в себе використання паролів, біометричних методів аутентифікації та токенів доступу. Ще однією важливою стратегією є шифрування даних, яке забезпечує конфіденційність інформації, що передається між пристроями IoT та іншими системами. Зашифровані дані недоступні для несанкціонованого доступу, забезпечуючи високий рівень безпеки. Регулярні оновлення програмного забезпечення є також важливою складовою стратегії захисту. Виробники пристроїв IoT повинні випускати оновлення, щоб виправляти виявлені уразливості та підвищувати рівень безпеки пристроїв.

Для ефективного виявлення та реагування на загрози використовують системи моніторингу та виявлення вторгнень. Ці системи допомагають вчасно виявляти аномальну активність та потенційні загрози, забезпечуючи оперативне реагування. Фізична безпека також грає важливу роль у захисті пристроїв IoT. Заходи, такі як захист від несанкціонованого доступу та захист від втручання в пристрої, допомагають уникнути фізичних атак. Налагодження привілеїв доступу є іншою важливою стратегією захисту, яка передбачає обмеження доступу до функцій та даних лише на необхідний мінімум. Це допомагає уникнути несанкціонованого доступу та зберегти конфіденційність даних. Впровадження цих стратегій захисту сприяє підвищенню рівня безпеки пристроїв Інтернету речей у різних сферах застосування [1-2].

Аналіз існуючих методів захисту пристроїв Інтернету речей (IoT) виявляє як переваги, так і обмеження цих методів. Одним з найпоширеніших методів є шифрування даних, яке забезпечує конфіденційність і цілісність передачі інформації між пристроями. Шифрування може забезпечити захист від прослуховування та модифікації даних, що передаються між IoT-пристроями та серверами. Іншим поширеним методом є аутентифікація, яка дозволяє перевіряти ідентичність пристроїв та користувачів перед наданням доступу до системи. Це допомагає запобігти несанкціонованому доступу та забезпечити захист від атак зламу аутентифікації.

Однак існують обмеження використання цих методів. Наприклад, шифрування може збільшувати обчислювальні витрати та затримки у передачі даних, особливо на пристроях з обмеженими ресурсами. Крім того, низька потужність обчислень та обмежені можливості пристроїв IoT можуть ускладнювати реалізацію сильних методів шифрування та аутентифікації. Деякі методи захисту, такі як використання паролів або ключів доступу, також можуть бути вразливими до атак перехоплення або перебору паролів. Крім того, велика кількість пристроїв IoT може зробити управління аутентифікацією складним завданням.

Таким чином, ефективний захист пристроїв Інтернету речей вимагає комплексного підходу, який поєднує різні методи захисту та враховує обмеження та потреби конкретного пристрою та його використання.

Використання нейронних мереж для захисту крайових пристроїв є актуальною та перспективною галуззю досліджень в області кібербезпеки. Нейронні мережі є складною системою обчислень, інспірованою структурою та функціонуванням нервової системи людини, і вони здатні до вирішення різноманітних завдань, включаючи виявлення та прогнозування аномальної поведінки, виявлення вторгнень та реагування на кіберзагрози [2].

Нейронні мережі – це математичні моделі, які імітують роботу людського мозку і використовуються для вирішення різних завдань у сфері штучного інтелекту. Основна ідея нейронних мереж полягає в тому, щоб навчити модель відтворювати певний патерн або робити прогнози на основі вхідних даних. Принцип роботи нейронних мереж ґрунтується на використанні штучних нейронів, які збирають та обробляють інформацію. Кожен нейрон отримує сигнали від інших нейронів, обробляє їх за допомогою ваг, а потім видає вихідний сигнал. Така взаємодія між нейронами в нейронних мережах дозволяє моделі вирішувати складні завдання. Основні концепції нейронних мереж включають штучний нейрон (перцептрон), структуру мережі, функцію активації та зв’язки та ваги. Принципи роботи нейронних мереж базуються на алгоритмах навчання, таких як зворотнє поширення помилки (backpropagation) або метод градієнтного спуску, які дозволяють моделі підлаштовувати ваги нейронів для досягнення бажаного результату. Нейронні мережі застосовуються у багатьох галузях, включаючи розпізнавання образів, обробку природної мови, прогнозування та, зокрема, у сфері кібербезпеки для виявлення аномалій та запобігання кібератакам [3].

Основні концепції та принципи роботи нейронних мереж для захисту крайових пристроїв базуються на математичних моделях, які моделюють структуру та функціонування нервової системи людини. Ці мережі складаються з штучних нейронів, які співповідають біологічним нейронам та здатні обробляти вхідні дані та генерувати вихідні сигнали.

Центральним елементом нейронних мереж є штучний нейрон, який отримує вхідні сигнали, обробляє їх за допомогою ваг, використовує функцію активації та генерує вихідний сигнал. Структура мережі може бути різноманітною, включаючи одношарові, багатошарові та зворотні мережі, залежно від конкретної задачі та характеристик даних. Функція активації визначає вихідний сигнал нейрона на основі вхідних даних та ваг. Це математична функція, яка може бути сигмоїдальною, ReLU (Rectified Linear Unit), tanh (гіперболічний тангенс) або іншою. Зв'язки між нейронами визначаються вагами, які відповідають силі зв'язку між ними. Ці ваги налаштовуються в процесі навчання нейронної мережі, яка здійснюється шляхом корекції параметрів мережі на основі навчальних даних.

Принцип роботи нейронних мереж для захисту крайових пристроїв полягає у використанні цих концепцій та принципів для аналізу та класифікації вхідних даних, виявлення аномалій та виявлення загроз. Велика кількість даних, що генерується крайовими пристроями, може бути оброблена та аналізована за допомогою нейронних мереж для виявлення незвичайної або підозрілої активності, що може вказувати на потенційні кіберзагрози.

Огляд основних концепцій та принципів роботи нейронних мереж важливий для зрозуміння їхньої застосовності в області кібербезпеки. Нейронні мережі складаються зі штучних нейронів, які зв'язані між собою і формують глибокі мережі, здатні до автоматичного виявлення складних залежностей у вхідних даних. Принцип роботи нейронних мереж полягає в навчанні моделі на основі великої кількості вхідних прикладів та відповідних вихідних маркерів. Після навчання модель може використовуватися для класифікації нових даних та прийняття відповідних рішень.

Переваги використання нейронних мереж у сфері захисту крайових пристроїв включають їхню здатність до автоматизації процесів виявлення та реагування на кіберзагрози, а також здатність до адаптації до нових типів атак. Нейронні мережі можуть ефективно виявляти аномальну поведінку та вчасно реагувати на потенційні загрози, забезпечуючи надійний рівень захисту для крайових пристроїв. Проте використання нейронних мереж у сфері захисту крайових пристроїв має і свої обмеження. Одним з таких обмежень є потреба великої кількості даних для навчання моделі, що може бути складним у випадку обмежених ресурсів крайових пристроїв. Крім того, навчання нейронних мереж може вимагати значних обчислювальних ресурсів та часу, що може бути недоцільним для крайових пристроїв з обмеженими можливостями.

Таким чином, хоча використання нейронних мереж у сфері захисту крайових пристроїв має великий потенціал для покращення кібербезпеки, важливо враховувати як їхні переваги, так і обмеження при розробці та впровадженні відповідних рішень [3].

Методи виявлення аномалій та кібератак з використанням нейронних мереж є важливими складовими в сучасних системах кібербезпеки, оскільки вони дозволяють автоматизувати процес виявлення та реагування на потенційні загрози. Нейронні мережі можуть бути успішно використані для виявлення аномалій в мережевому трафіку та виявлення надзвичайних змін у звичайних патернах поведінки пристроїв. Одним з методів виявлення аномалій є використання звичайних нейронних мереж для класифікації вхідних даних як «нормальних» або «аномальних» на основі попередньої навчальної вибірки. Під час навчання моделі нейронної мережі використовуються типові патерни поведінки пристроїв та користувачів для створення бази даних, а після цього модель може виявляти аномальні або незвичайні відхилення в реальному часі. Ще одним методом є використання рекурентних нейронних мереж (RNN), які здатні виявляти аномалії в послідовностях даних, таких як часові ряди. RNN здатні виявляти аномальні зміни у звичайних патернах даних та сповіщати про них операторів безпеки. Також застосовуються глибокі згорткові нейронні мережі (CNN), які можуть аналізувати великі обсяги даних та виявляти складні патерни аномальної поведінки в мережевому трафіку.

Мережа Коско, вперше запропонована Бартом Коско, є однією з класичних нейронних мереж, яка знайшла широке застосування в різних областях, включаючи обробку сигналів,

керування системами та аналіз даних. У стратегії захисту крайових пристроїв з використанням нейронних мереж мережа Коско може використовуватися для виявлення аномалій та підозрілої активності. Мережа Коско має особливу структуру, в якій кожний нейрон з'єднаний з усіма нейронами на попередньому та наступному рівнях. Це означає, що вся мережа утворює повнозв'язну структуру, що дозволяє ефективно аналізувати складні зв'язки у вхідних даних.

У контексті захисту крайових пристроїв, мережа Коско може бути навчена на нормальному функціонуванні системи, включаючи типові патерни та нормальні вхідні сигнали. Після навчання мережі вона може виявляти аномалії та підозрілі дії, які відхиляються від звичайних патернів. Це може включати незвичайний обсяг даних, підозрілі запити або непередбачувані зміни в системі. Використання мережі Коско в стратегії захисту крайових пристроїв дозволяє ефективно виявляти потенційні загрози та вчасно реагувати на них, забезпечуючи високий рівень безпеки для системи (Рис. 1) [3].

Мережа Коско використовується в стратегії захисту крайових пристроїв через свою здатність до виявлення аномалій та підозрілої активності. Вона має таку структуру: вхідний, схований та вихідний шари. Вхідний шар розподіляє інформацію між нейронами схованого шару, а схований шар відображає вхідний вектор. Кожен нейрон схованого шару з'єднаний з кожним нейроном вихідного шару. Зв'язки між нейронами в середині шару відсутні, але нейрон сполучений з самим собою, що дозволяє відрізняти діагональні елементи матриці міжнейронних зв'язків від 0.

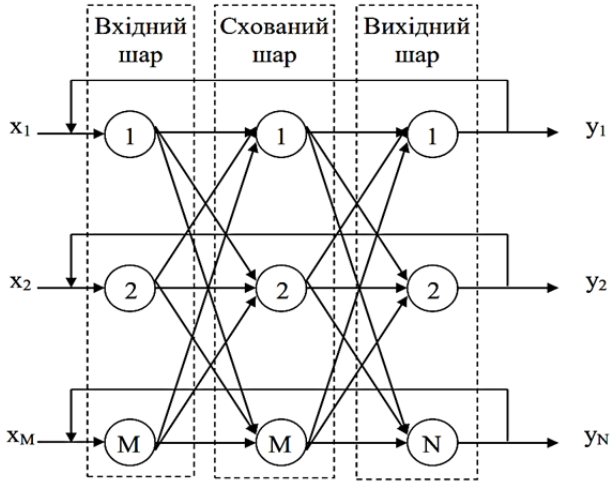


Рис. 1. Структура класичної мережі Коско

Джерело: агреговано на основі [3]

У дослідженнях найбільш дослідженими є дискретні гомогенні бінарні мережі Коско, де стани нейронів змінюються дискретно, що дозволяє ефективно виявляти аномалії. Мережа Коско використовує сигмоїдальну або порогову функції активації для нейронів схованого та вихідного шарів, і навчання відбувається за допомогою правила Хеба. Під час навчання вагові коефіцієнти прямих та зворотніх зв'язків між нейронами схованого та вихідного шарів розраховуються з метою визначення асоціацій між вхідними та вихідними векторами. Стратегія захисту крайових пристроїв з використанням мережі Коско базується на тому, що мережа спочатку навчається на нормальному функціонуванні системи, а потім виявляє аномалії та підозрілу активність. Цей підхід дозволяє системі ефективно виявляти потенційні загрози та вчасно реагувати на них, забезпечуючи високий рівень безпеки. Перевагою такої стратегії є можливість адаптуватися до змінних умов та швидко реагувати на нові види загроз. Крім того, вона дозволяє уникати фальшивих спрацювань і забезпечує ефективне функціонування системи безпеки.

Перевагами використання нейронних мереж для виявлення аномалій є їхня здатність до автоматичного навчання на великих обсягах даних, висока швидкодія та здатність до адаптації до нових типів загроз. Однак недоліками можуть бути складність в навчанні моделі та потреба великої кількості даних для досягнення високої точності виявлення аномалій.

Механізми виявлення та відповіді на загрози за допомогою нейронних мереж є ключовими складовими в сучасних системах кібербезпеки. Нейронні мережі можуть бути ефективно використані для автоматизації процесу виявлення та реагування на потенційні загрози в реальному часі. Основні механізми виявлення та відповіді на загрози за допомогою нейронних мереж включають моніторинг мережевого трафіку, аналіз системних журналів, виявлення аномальних патернів поведінки та реакцію на загрози.

Моніторинг мережевого трафіку дозволяє нейронним мережам аналізувати пакети даних, що пересилаються через мережу, для виявлення підозрілих або незвичайних активностей. Цей процес включає аналіз патернів передачі даних та ідентифікацію відхилень від звичайних. Аналіз системних журналів полягає у використанні нейронних мереж для аналізу журналів подій оперативної системи та програмного забезпечення для виявлення незвичайних дій, таких як спроби неуспішного входу в систему або незвичайні запити до системних ресурсів.

Виявлення аномальних патернів поведінки дозволяє нейронним мережам розпізнавати аномальні дії користувачів або пристроїв у мережі, що може свідчити про потенційні загрози. Наприклад, вони можуть виявляти незвичайну активність, таку як надмірний обсяг запитів до сервера або зміни у звичайних зв’язках між пристроями. Після виявлення потенційної загрози нейронні мережі можуть автоматично ініціювати відповідні заходи безпеки, такі як блокування підозрілих IP-адрес або призупинення доступу до певних ресурсів. Також може бути запущено інші процедури безпеки, наприклад, сповіщення адміністраторів системи або запуск процесів відновлення після інциденту. Ці механізми дозволяють створити ефективні системи кібербезпеки, які можуть швидко реагувати на змінюються умови та нові типи загроз.

Використання нейронних мереж для захисту крайових пристроїв дозволяє автоматизувати процес виявлення та реагування на загрози, що збільшує швидкість реакції та знижує ризик людських помилок. Крім того, нейронні мережі можуть адаптуватися до нових типів загроз та вчитися з досвіду, що робить їх більш ефективними у виявленні навіть раніше невідомих атак. Проте, необхідно враховувати, що ефективність захисту за допомогою нейронних мереж може бути обмеженою в разі недостатньої кількості даних для навчання моделі або в разі недостатньої налаштованості системи. Крім того, нейронні мережі можуть бути вразливі до атак, спрямованих на їхню обхідну або маніпуляцію [1, 3].

Висновки щодо ефективності та перспектив використання нейронних мереж для захисту крайових пристроїв залежать від ретельного аналізу результатів експериментів та практичного застосування. Хоча нейронні мережі показують значний потенціал у виявленні та реагуванні на кіберзагрози, їхнє використання повинно бути відповідно обґрунтоване і належним чином налаштоване для конкретного контексту застосування.

Висновки. Підсумки дослідження вказують на потенціал нейронних мереж у сфері захисту крайових пристроїв. Результати досліджень підтверджують, що використання нейронних мереж може значно підвищити рівень безпеки мережевих інфраструктур шляхом виявлення аномалій та кібератак на ранніх етапах. Значення цього дослідження для практики полягає в тому, що воно надає основу для розробки та впровадження нових систем захисту, які базуються на нейронних мережах. Рекомендації, що випливають з цього дослідження, можуть бути корисними для організацій і підприємств, які прагнуть підвищити рівень безпеки своїх мереж та захистити їх від потенційних кіберзагроз.

Щодо подальших напрямків досліджень у сфері захисту крайових пристроїв з використанням нейронних мереж, рекомендується зосередитися на вдосконаленні алгоритмів виявлення аномалій та адаптації моделей до нових типів загроз. Також важливо досліджувати можливості використання комбінованих підходів, які поєднують нейронні мережі з іншими методами захисту, щоб забезпечити максимальний рівень безпеки мережевих інфраструктур.

Список використаних джерел

1. Gibert D, Mateu C, Planes J, Vicens R. Using convolutional neural networks for classification of malware represented as images. Journal of Computer Virology and Hacking Techniques. 2019 March;15(1):15-28.

2. Мороз А. С. Засоби захисту інформації на основі нейронних мереж / А. С. Мороз, О. Є. Петренко // Проблеми інформатизації : тези доповідей восьмої міжнародної науково-технічної конференції, 26-27.11.2020. – Черкаси: ЧДТУ; Х.: НТУ «ХПІ»; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; ДП «ПД ПКНДІ АП», 2020, Т. 1: секції 1-3. – С. 97.

3. Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації: монографія. К.: Поліграф Консалтинг. 2007. 209 с.

Робота виконана під науковим керівництвом старшого викладача
ШЕСТАКА Я.І.

ВРАЗЛИВІСТЬ ІНФОРМАЦІЇ У СУЧАСНОМУ СВІТІ ТА МЕТОДИ ЇЇ ЗАХИСТУ

ГОНЧАРОВ Д.В., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто та досліджено загрози які ставлять під загрозу безпеку та конфіденційність інформації у сучасному цифровому середовищі. Детально проаналізовано п'ять основних видів загроз у сфері інформаційної безпеки та запропоновано ефективні рекомендації щодо запобігання цим ризикам.

The article examines and investigates threats that endanger the security and confidentiality of information in the modern digital environment. Five main types of threats in the field of information security are analyzed in detail and effective recommendations for preventing these risks are offered in the article.

Актуальність. В умовах сучасності та швидкого розвитку технологій виникає все більше загроз щодо безпеки цілісності та конфіденційності інформації. Значне зростання кількості кібератак, масштабних витоків даних та поширення фейкових новин ставлять під загрозу як особисту, так і корпоративну конфіденційність. Враховуючи усі представлені проблеми, стає очевидним те, що питання захисту інформації стає все більше актуальнішим з кожним днем. Безумовно, водночас з підвищенням кібератак, зростає й інтерес до розвитку технологій по захисту інформації, визначаються вразливості та застосовуються ефективні методи захисту.

Цифрова інформація стає об'єктом для кіберзлочинців, які активно використовують різноманітні способи та техніки для її крадіжки, витоку або зміни за для особистої вигоди чи завдання шкоди. У зв'язку з цим, розвиток методів захисту інформації є критично важливим завданням для забезпечення конфіденційності, цілісності та доступності даних у цифровому середовищі. Аналіз та вирішення цих проблем має стратегічне значення не лише для індивідуальних користувачів, а й для величезних компаній, установ та організацій, тобто місць, які працюють з чималим обсягом інформації.

Метою статті є дослідження та всебічний аналіз вразливостей інформації у сучасному світі з метою підвищення ефективності захисту інформації від витоку, крадіжки та атак у різноманітних сферах діяльності.

Об'єктом дослідження є розробка та впровадження методів захисту інформації у сучасному світі.

Предмет дослідження є вразливість інформація у різноманітних сферах діяльності.

Виклад основного матеріалу. У сучасному світі поява та розвиток новітніх технологій супроводжуються різноманітними наслідками, як позитивного, так і негативного характеру. Хоч впроваджені новації й значно полегшують життя людей, вони також приносять значні ризики та підвищують загрозу кібератак. Поширення інформаційних технологій призвело до збільшення вразливості інформації у інтернет середовищі перед кібер загрозами. Проте, варто зазначити, що інформація у фізичному середовищі також залишається дуже актуальною на сьогодняшній день, як і її вразливість та проблеми з захистом.

Безпосередньо перед аналізом вразливостей та впровадження рекомендацій, треба вміти класифікувати інформацію за видами та різними ознаками:

Рис. 1. Класифікація інформації

Джерело:[1] Інформаційні системи в сучасному суспільстві

Візьмемо по одному пункту з кожної колонки таблиці та розглянемо вразливість інформації на прикладі. Уявімо, що існує компанія «G-Teamer» в офісі якої відбувається дуже важлива нарада з обговоренням рішень, які б допомогли компанії значно вийти вперед на ринку та обігнати своїх конкурентів. За призначенням ця інформація є спеціальною, за способом сприйняття – слуховою, а за формою подання – звуковою. З часом виявляється що конкуренти прослуховували цю розмову. Враховуючи, що приміщення було нове та камери ще не встигли встановити, а деякі співробіники були на розмові у онлайн режимі та спілкувалися за допомогою додатку, компанія так і не змогла виявити зловмисника. Фірма понесла величезні втрати та не змогла виявити як саме відбувся виток інформації.

На даний момент існує 5 основник видів загроз у сфері інформаційної безпеки, які й будуть розглянуті у цій статті:

Рис. 2. Топ-5 загроз у сфері інформаційної безпеки

Джерело:[2] Топ-5 загроз у сфері інформаційної безпеки

1. *Фішинг*. Фішинг – це один з найпопулярніших видів інтернет-шахрайства, який полягає в крадіжці конфіденційних даних користувачів. Фішингові атаки здійснюють зловмисники, які маскуються під надійні джерела, щоб отримати легкий доступ до будь-якого типу делікатних даних: номерів телефонів, номерів та секретних кодів банківських карт, логіни та паролі електронної пошти та облікових записів в соціальних мережах.

Фішинг поділяється на декілька типів: «Фішинг в електронних листах», « Фішинг за допомогою зловмисних програм», « Цільовий фішинг», « Полювання на велику здобич», « Смсшинг» та « Вішинг».

Фішинг в електронних листах – це метод шахрайства, коли зловмисники відправляють підроблені електронні листи, які схожі на листи від легітимних організацій (друзів, знайомих і т.д.), з метою отримання конфіденційної інформації або фінансових даних. За для захисту від фішингу в електронних листах треба завжди перевіряти адресу відправника, уникати переходи на посилання або вкладення в сумнівних листах, і використовувати програмне забезпечення антивірусного захисту та фільтрації спаму.

Фішинг за допомогою зловмисних програм – це метод атаки, коли зловмисники використовують шкідливі програми для отримання конфіденційної інформації або доступу до особистих даних користувачів. Ці програми можуть бути розповсюджені через електронну пошту, соціальні мережі, фейки популярних сайтів або інші канали комунікації. Для захисту від такого виду фішингу важливо використовувати актуальне антивірусне програмне забезпечення, оновлювати програми та операційну систему, уникати переходу на невідомі джерела, а також регулярно робити резервне копіювання даних.

Цільовий фішинг – вид атаки, при якому зловмисники спеціально спрямовують свої напади на конкретні об’єкти або суб’єкти, використовуючи персоналізовані листи або повідомлення. Ціллю є отримання конфіденційної інформації, доступ до систем або здійснення фінансових маніпуляцій. Щоб захиститися від цільового фішингу варто як і у «Фішинг в електронних листах» перевіряти дані відправника та важливі реквізити, бути уважним щодо невідомих повідомлень та перевіряти їх на правдоподібність.

Полювання на велику здобич – такий вид атаки, коли хакери використовують вразливості в системі для отримання доступу до важливих даних або ресурсів організації. Це може бути спрямовано на великі компанії, урядові установи або інші цілі. При таких атаках також варто регулярно оновлювати програмне забезпечення та оперативну систему, використовувати сильні та бажано різні паролі та двофакторну аутентифікацію, встановлювати програми для виявлення та захисту від вразливостей, а також надавати доступ до даних лише необхідним користувачам.

Смсшинг – це метод атаки, коли зловмисники надсилають шкідливі текстові повідомлення на мобільні пристрої з метою шахрайства або крадіжки особистої інформації. Діяти при «Смсшинг» треба як і при «Фішинг в електронних листах».

Вішинг – метод соціальної інженерії, коли зловмисники використовують підроблені веб-сайти або телефонні дзвінки, щоб викликати довіру та виключити особисту чи фінансову інформацію від потенційних жертв. Щоб запобігти «Вішингу» варто перевіряти автентичність веб-сайтів та не вказувати особисту інформацію або фінансові дані через ненадійні джерела.

Великої популярності фішингові атаки набули під час війни. Цим видом шахрайства окупанти намагаються дізнатися важливу інформацію щодо військових об’єктів, лікарень, розташування ППО і т.д. Тому сучасним українським інтернет-користувачам особливо важливо бути ознайомленими із вище перерахованими видами фішингу та методами захисту від нього.

2. *DDos-атаки*. Від початку повномасштабної війни росії проти України DDoS-атаки (distributed denial-of-service) залишаються серед найпоширеніших видів кібератак, до яких вдаються ворожі хакери. DDoS-атака – це атака на комп’ютерні системи органу, організації, установи з метою порушення доступності атакованих вебресурсів. Простими словами, під час атаки одночасно створюється така величезна кількість зовнішніх запитів (рахунок може

йти на мільйони), що атакована система не в змозі їх обробити. Як наслідок – виникають збої в її роботі або вона взагалі перестає повноцінно працювати. DDoS-атака, на відміну від DoS-атаки, здійснюється з кількох джерел, а не з одного. Також варто зазначити, що на окремих громадян такі види атак здебільшого не спрямовуються. Проте кінцева мета зловмисників – позбавити саме громадян доступу до важливих послуг, сервісів, до правдивої інформації.

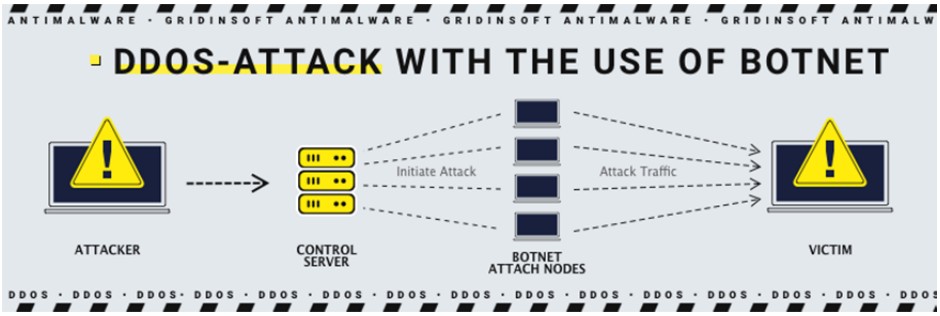


Рис. 3. Схема DDoS-атаки

Джерело: [2] Що таке атаки типу «відмова в обслуговуванні» (DDoS)?

Зловмисники, які запускають DDoS-атаки, використовують мережі розподілених скомпрометованих пристроїв, щоб порушити роботу системи, націлюючись на один або кілька компонентів, необхідних для встановлення з'єднання з мережевим ресурсом. Зазвичай DDoS-атаки здійснюють із метою поширення паніки та дестабілізації. Іноді використовують для приховування деструктивних дій, тобто коли DDoS-атака слугує прикриттям атаки іншого виду. Проте самі DDoS-атаки загрози для персональних даних громадян не становлять. Варто знати, що для проведення DDoS-атак хакери часто використовують зламані пристрої людей. Тому важливо дотримуватися основних правил кібергігієни, користуватися антивірусами, оновлювати вчасно програмне забезпечення, застосовування фільтрацію трафіку і т.д.

3. *Крадіжка або незаконне використання даних*. Крадіжка інформації може бути здійснена як у інтернет, так і у фізичному середовищі. Викрадення даних є злочином, під час якого зловмисник використовує шахрайство або обман для отримання конфіденційної інформації жертви та використовує її в зловмисних цілях від імені жертви. Як правило, такі крадіжки здійснюються заради економічної виоди.

За для забезпечення захисту особистих даних варто використовувати безпечне з'єднання: якщо ви збираєтеся використовувати вашу особисту інформацію в Інтернеті, переконайтеся, що з'єднання безпечне. Бажано використовувати домашню, корпоративну мережу або мобільний зв'язок. Уникати публічних Wi-Fi, не захищених паролем. У крайніх випадках користуватися віртуальною приватною мережею (VPN), яка дозволяє зашифровувати всі повідомлення та таким чином уникнути проблеми викрадення даних. Також необхідно мати надійне багаторівневе рішення для захисту пристроїв від шкідливого програмного забезпечення та несанкціонованого доступу зловмисників.

4. Вразливості в ОС та мережевих пристроях. Щороку виявляються тисячі нових вразливостей, що вимагає від компаній виправлення операційних систем (ОС) і додатків, а також переналаштування параметрів безпеки у всій своєму мережевому середовищі. Для попереджувального усунення вразливостей до того, як вони будуть використані для кібератаки, організації, серйозно ставляться до безпеки свого середовища, проводять управління вразливостями, щоб забезпечити максимально можливий рівень безпеки. Вразливістю вважаються будь-які засоби, за допомогою яких зовнішній зловмисник може отримати неавторизований доступ або привілейований контроль над додатком, службою, кінцевою точкою або сервером. Відчутні приклади включають порти зв'язку, відкриті для Інтернету, небезпечні конфігурації програмного забезпечення або ОС, методи, за допомогою

яких можна отримати привілейований доступ через схвалену взаємодію з даним додатком або ОС, а також вразливість, яка дозволяє шкідливим програмам заразити систему. Кожна нова вразливість становить ризик для компанії. Таким чином, повинен часто використовуватися певний процес, щоб надати компанії спосіб швидко і постійно виявляти і усувати вразливості. Високий рівень управління вразливостями передбачає 6 процесів, при цьому кожен з процесів включає в себе підпроцеси і задачі: виявлення, розстановка пріоритетів, оцінка, визначення засобу усунення, перевірка та звіт.

5. *Людський фактор*. Безпека будь-якої системи визначається надійністю її найслабшої ланки. Найбільш складним і одночасно найбільш уразливим ланкою будь-якої системи є людина. Негативний вплив людини на безпеку позначають поняттям «людський фактор», тобто сукупність соціальноекономічних здібностей людини, ступінь реалізації яких обумовлена мотивацією і ставленням людини до процесу трудової діяльності, його моральної і матеріальної зацікавленістю в високопродуктивному працю. Основними проявами людського фактора є наступні: людина в процесі своєї діяльності з тих чи інших причин може допускати помилки різного характеру (відповідно до законів Парето 20% працівників створюють 80% проблем). Властивість людини-оператора безпомилково виконувати свої функції при заданих умовах професійної діяльності в часі описується його надійністю, яка є однією зі складових професійної придатності. Необхідно також враховувати, що в процесі життєдіяльності людина може опинитися в екстремальній ситуації, коли фізичні і психологічні навантаження досягають таких рівнів, при яких індивідуум втрачає здатність до раціональних дій і рішень, адекватним ситуації, що склалася. Особливе значення у вирішенні даної проблеми має навчання і подальша атестація працівників, зокрема, в галузі управління ризиками. Сучасна система навчання передбачає моніторинг росту кваліфікації персоналу, розробку методів оцінки кваліфікації, застосування сучасних освітніх технологій і методик.

Висновки. Вразливість інформації у сучасному світі є однією з найбільших загроз для організацій та індивідів. Проте застосування ефективних методів захисту, таких як шифрування, аутентифікація та захист мережі, може значно знизити ризик втрати конфіденційності, цілісності та доступності інформації. Дуже важливо враховувати актуальність існуючих вразливостей та підвищувати рівень захисту за допомогою запропонованих або пошуку нових методів її захисту.

Список використаних джерел

1. Інформаційні системи в сучасному суспільстві. // Режим доступу: https://www.miyklas.com.ua/p/informatica/10-klas/informatciini-tekhnologiyi-v-suspilstvi-322205/informatciini-sistemi-v-suchasnomu-suspilstvi-318282/re-8a0f2028-b72b-4703-ac23-ff9b522f327a (останнє звернення 17.03.2024р.)
2. Аудит інформаційної безпеки: що це і навіщо потрібно, коли проводити. // Режим доступу: https://blog.colobridge.net/uk/2023/06/information_security_audit-ua/ (останнє звернення 19.03.2024р.)
3. Що таке фішинг? // Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing (останнє звернення 25.03.2024р.)
4. Що таке DDoS-атака? // Режим доступу: https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka (останнє звернення 26.03.2024р.)
5. Що таке атаки типу «відмова в обслуговуванні» (DDoS)? // Режим доступу: https://gridinsoft.ua/ddos (останнє звернення 26.03.2024р.)
6. Розподілена атака на відмову в обслуговуванні (DDoS). // Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/distributed-denial-of-service/ (останнє звернення 28.03.2024р.)

7. Що таке вразливості в контексті обробки даних: управління вразливостями? // Режим доступу: https://bsoprivacygroup.com/shcho-take-vrazlyvosti-v-konteksti-obrobky-danykh-upravlinnia-vrazlyvostiamy/ (останнє звернення 29.03.2024р.)
8. Людський фактор в проблемі безпеки. // Режим доступу: http://rua.pp.ua/91chelovecheskiy-faktor-probleme-24159.html (останнє звернення 31.03.2024р.)

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ ЯК КЛЮЧ ДО ЗАХИСТУ ОНЛАЙН-АККАУНТІВ

ГОРЮК В.С., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто основні принципи двофакторної аутентифікації. Підкреслена значущість використання двофакторної аутентифікації як ключового елемента в забезпеченні безпеки онлайн-акаунтів. Досліджено важливість використання двофакторної аутентифікації в сьогоденні. Запропоновано програму для двофакторної аутентифікації «Google Authenticator» для забезпечення захисту онлайн-акаунтів.

The article discusses the basic principles of two-factor authentication. The importance of using two-factor authentication as a key element in ensuring the security of online accounts is emphasized. The importance of using two-factor authentication in the present day is investigated. A program for two-factor authentication «Google Authenticator» is proposed to ensure the protection of online accounts.

Актуальність. Актуальність теми двофакторної автентифікації як ключ до захисту онлайн-акаунтів полягає в важливості забезпечення безпеки онлайн-акаунтів та особистих даних в умовах зростаючої загрози кібератак та крадіжок. Сучасне онлайн-середовище навіть із своїми перевагами надає масивну площину для зловмисників, які постійно вдосконалюють свої техніки, щоб проникнути в системи. Традиційні методи аутентифікації, такі як паролі, перестають бути надійними, оскільки їх легко можна вгадати або зламати. Застосування двофакторної автентифікації значно підвищує рівень безпеки онлайн-акаунтів, оскільки вона вимагає додаткового підтвердження, крім самого пароля. Цей додатковий шар захисту може включати в себе коди, відправлені на мобільний телефон, використання біометричних даних або фізичні об’єкти, такі як ключі або картки. Такий підхід робить аккаунти більш стійкими до зломів та зловживань. Враховуючи, що багато людей використовують онлайн-послуги для фінансових операцій, покупок та обміну конфіденційною інформацією, забезпечення безпеки стає ще більш критичним завданням. Двофакторна автентифікація допомагає захистити ці аккаунти від крадіжки та шахрайства, роблячи онлайн-середовище більш безпечним для всіх користувачів. Паролі, як відомо, мають свої обмеження, оскільки їх можна вгадати або вкрасти. Фішингові атаки, що вимагають розкриття паролів, стають все поширенішими. У таких умовах важливо мати механізми, які роблять аутентифікацію більш складною для зловмисників. І саме тут двофакторна автентифікація виступає на перший план, додаючи додатковий рівень захисту. Отже, з урахуванням усіх цих факторів, стає очевидним, що двофакторна автентифікація є критично важливою для захисту онлайн-аккаунтів та особистих даних у сучасному цифровому світі.

Метою статті є дослідження та аналіз двофакторної аутентифікації, її принципів роботи, переваг та методів для забезпечення захисту персональних даних.

Об'єктом дослідження є розробка методів захисту онлайн-акаунтів.

Предметом дослідження є ефективність використання засобів двофакторної аутентифікації для забезпечення захисту онлайн-акаунтів.

Аналіз попередніх досліджень. Досліджено системи захисту даних від несанкціонованого доступу, розвиток технології двофакторної автентифікації. Її визначення структури, основних характерних рис присвячені праці вітчизняних та закордонних науковців: Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П., Kevin Curran, Thomas L. Norman та ін.

Виклад основного матеріалу. У сучасному світі, де все більше аспектів нашого життя переноситься в онлайн, захист наших персональних даних і конфіденційної інформації стає дедалі важливішим. Зростаюча кількість кіберзлочинів і крадіжок особистих даних свідчить про те, що традиційні методи автентифікації, такі як паролі, вже не забезпечують достатнього рівня безпеки. Зловмисники постійно вдосконалюють свої методи злому, і прості паролі легко піддаються атакам грубої сили та фішинговим атакам. Такі атаки можуть легко зламати пароль і отримати доступ до особистої інформації користувача. У таких умовах стає очевидною необхідність використання більш надійних методів автентифікації, таких як двофакторна аутентифікація, щоб забезпечити високий рівень безпеки для наших онлайн-акаунтів і особистих даних.

Двофакторна автентифікація (2FA) – це засіб додаткової безпеки, який вимагає двох форм ідентифікації для доступу до облікового запису (Рис. 1)[2]. 2FA вимагає від користувача пройти два етапи перевірки особистості під час входу в систему, що значно ускладнює несанкціонований доступ. Зазвичай першою формою ідентифікації є пароль, а другою формою може бути відбиток пальця, код, надісланий на ваш телефон, або токен безпеки [2].

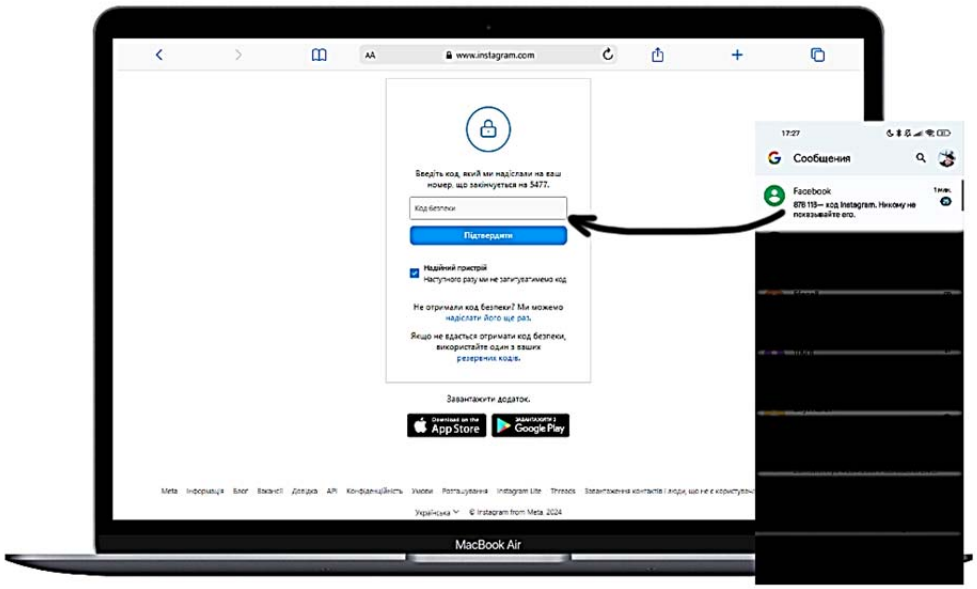


Рис. 1. Використання двофакторної аутентифікації при авторизації

Джерело: розроблено автором в середовищі Adobe Photoshop (знімок з екрану)

Однією з ключових областей розвитку технології 2FA є вдосконалення методів біометричної аутентифікації. Розпізнавання обличчя, відбитків пальців та інші біометричні дані можуть стати ще більш точними та надійними, забезпечуючи високий рівень безпеки.

Крім того, дослідження в галузі квантового шифрування може вивести захист інформації на новий рівень. Використання квантових властивостей для передачі ключів та

захисту інформації може розширити можливості 2FA та зробити її ще більш відповідною вимогам сучасного цифрового світу. 2FA має величезний вплив на користувачів та організації. З одного боку, це забезпечує високий рівень безпеки та захисту від несанкціонованого доступу. З іншого боку, воно може викликати деякі труднощі для користувачів, які можуть вважати процес аутентифікації занадто складним або часом затратним. Для організацій важливо забезпечити ефективне впровадження та навчання персоналу щодо використання 2FA. Крім того, важливо регулярно перевіряти системи та вдосконалювати їх, щоб уникнути можливих вразливостей та забезпечити стійкий захист [1-2].

Всього існує два основних типи шифрування, що використовуються у двофакторній аутентифікації (2FA). Одним з них є використання одноразових паролів (OTP). OTP – це тимчасові паролі, які дійсні лише протягом короткого періоду часу, зазвичай 30 – 60 секунд. Ці паролі можуть генеруватися спеціальними додатками на телефоні користувача або надсилатися у вигляді повідомлень. Вони забезпечують високий рівень безпеки, оскільки навіть якщо зловмисник дізнається ваш пароль, він не зможе отримати доступ до OTP, що генерується на вашому пристрої. Ще одним типом є використання push-повідомлень. Під час використання цього методу на телефон користувача надсилається запит на підтвердження входу. Для цього користувачу достатньо натиснути кнопку в push-повідомленні. Цей метод зручний у використанні, оскільки не вимагає від користувача вводити додаткові коди [3-4].

Крім цього, існують інші методи, що використовуються у 2FA. Наприклад, компанії можуть використовувати апаратні маркери, які генерують нові коди кожні кілька секунд або хвилин. Також використовується голосова автентифікація, аналогічна push-повідомленням, але з використанням автоматизованої системи для підтвердження особистості. Фізичні ключі, як USB-ключі чи смарт-картки, також використовуються як додатковий рівень безпеки окрім пароля. Найбільш продвинутий метод – біометрична автентифікація. Вона використовує унікальні фізичні характеристики користувача, такі як розпізнавання обличчя, сканування райдужної оболонки ока або відбитки пальців. Цей метод є зручним та безпечним, оскільки біометричні дані неможливо забути або вкрасти [1-4].

Розглянемо класичну блок-схему двофакторної автентифікації (Рис. 2).

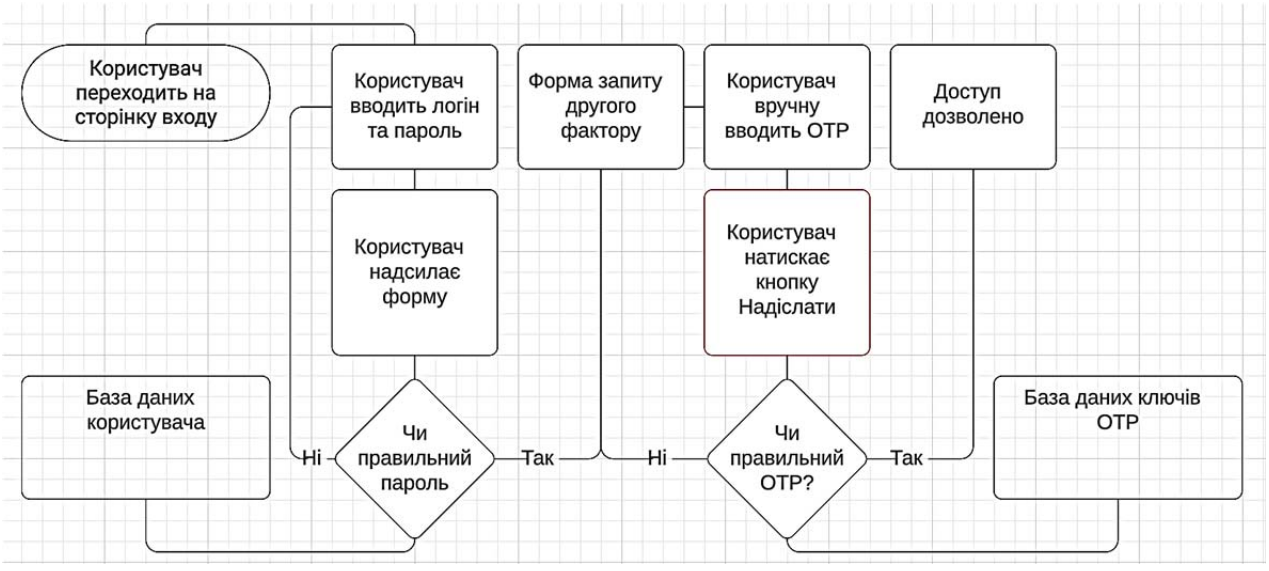


Рис. 2. Класична блок-схема двофакторної автентифікації

Джерело: розроблено автором в середовищі lucid *(знімок з екрану)*

У 2019 році за даними статистики, лише 53% користувачів заявили, що використовували двофакторну автентифікацію (2FA). Серед них найпоширенішим методом був SMS з використанням коду (72%), за яким йшла електронна пошта (за допомогою посилання або коду) із показником 67%. У 2020 році використання двофакторної автентифікації (2FA)

продовжило зростати, наближаючись до 69% користувачів, які повідомили, що використовували її. SMS залишався найпопулярнішим методом з використанням 2FA, з 78% використанням, тоді як електронна пошта залишалася на другому місці з 72%. Статистика 2FA показує, що 79% користувачів повідомили, що використовували 2FA у 2021 році, порівняно з 53% у 2019 році та 28% у 2017 році [5]. SMS (85%) залишається найпоширенішим методом використання 2FA, що трохи більше, ніж у 2019 році (72%). Електронна пошта є другим найпоширенішим другим фактором (74%) (Рис. 3). У 2022 році тренд зростання використання двофакторної автентифікації (2FA) продовжився, з 83% користувачів, які повідомили, що використовували її. SMS залишався найпопулярнішим методом з використанням 2FA, але його використання зросло до 88%, тоді як електронна пошта залишалася на другому місці з 77%. У 2023 році тренд зростання використання двофакторної автентифікації (2FA) продовжився, з 86% користувачів, які повідомили, що використовували її. SMS залишався найпопулярнішим методом з використанням 2FA, з 87% використанням, тоді як електронна пошта залишалася на другому місці з 78%. За інформацією на початок 2024 року, використання двофакторної автентифікації (2FA) продовжило зростати. Це підтверджується тим, що вже 86% користувачів повідомили, що використовували її. Що стосується методів, то SMS залишається досить популярним, з 85% використанням. Електронна пошта також залишається популярним методом, проте її використання трохи знизилося до 74%. Таким чином, можна зробити висновок, що за останні п’ять років використання двофакторної автентифікації зросло значно, що свідчить про зростаючу увагу до кібербезпеки та захисту особистої інформації в онлайн середовищі [4-5].

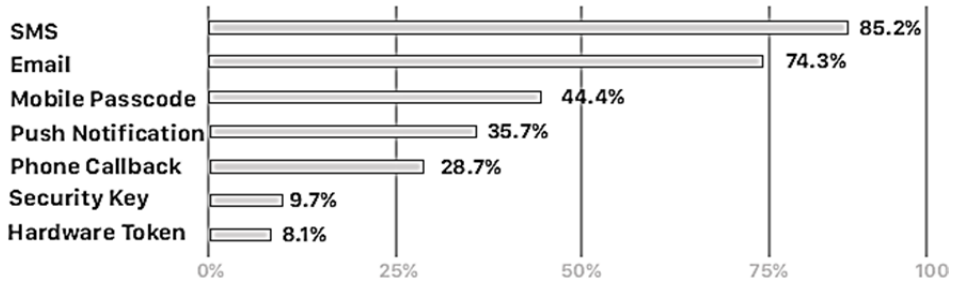


Рис. 3. Статистика використання методів двофакторної автентифікації

Джерело: розроблено автором в середовищі Adobe Photoshop *(знімок з екрану)*

2FA значно підвищує рівень безпеки онлайн-акаунтів, роблячи їх більш стійкими до зломів. Ця система може допомогти захиститися від фішингових атак, оскільки зловмисник, навіть отримавши ваші облікові дані, не зможе пройти другий етап аутентифікації. Також вона ускладнює атаки грубої сили, тому що зловмисникові необхідно не тільки підібрати ваш пароль, а й отримати доступ до вашого другого фактору аутентифікації. 2FA використовується у соціальних мережах, таких як Facebook, Twitter, Instagram, Google, а також у поштових сервісах, наприклад, Gmail та Outlook, і в онлайн-банкінгу, наприклад, PayPal, Payoneer та ін.

При виборі застосунку для 2FA важливо звернути увагу на розробника та функціональність. Додаток повинен бути від надійного розробника з хорошою репутацією і підтримувати різні методи генерації OTP, такі як push-повідомлення, SMS-повідомлення або коди з Google Authenticator. Також важливо, щоб додаток був простим і зручним у використанні. Для максимального захисту аккаунтів варто використовувати надійні паролі для додатків 2FA, регулярно робити резервні копії та використовувати різні методи 2FA для різних акаунтів. Незважаючи на переваги, 2FA може бути трохи незручною у використанні, особливо через додатковий крок під час входу в систему. Втрата доступу до другого фактору аутентифікації може також стати проблемою. Деякі веб-сайти та служби не підтримують 2FA, а деякі методи 2FA можуть бути вразливими для атак [1-3, 5].

Для забезпечення максимального захисту доступу до аккаунту, рекомендується використовувати додаток, такий як Google Authenticator. Цей додаток надає користувачам надійний та швидкий спосіб підтвердження своєї ідентичності за допомогою технології одноразових паролів (OTP). Google Authenticator володіє інтуїтивно зрозумілим і простим інтерфейсом, що робить його легким у використанні. Це особливо важливо, оскільки високий рівень безпеки повинен поєднуватися із зручністю та легкістю в обслуговуванні для підтримки позитивного користувацького досвіду.

Google Authenticator для входу на сайт або службу, де реалізовано підтримку 2FA, треба використовувати наступним чином:

1. Встановити Google Authenticator на пристрій користувача. Додаток можна встановити на Android або IOS.
2. Увімкнути 2FA в обліковому записі на веб-ресурсі. Користувачу буде надано вибір де він може обрати QR-код або ключ налаштування.
3. Відкрити Google Authenticator на мобільному пристрої та натиснути знак плюс у нижньому правому куті, щоб додати сайт або службу (Рис. 4.).

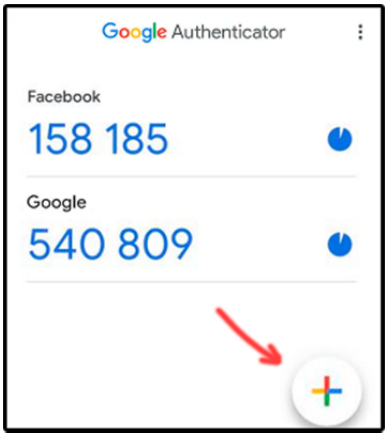


Рис. 4. Додавання нового ключа в застосунку «Google Authenticator»

Джерело: розроблено автором в середовищі Adobe Photoshop *(знімок з екрану)*

Користувачеві пропонуються два варіанти. Перший варіант – відсканувати код швидкої відповіді (QR-код). Якщо обрати цей варіант, то користувачу потрібно буде навести пристрій на QR-код, щоб захопити його зображення. Далі потрібно ввести ключ налаштування. Вибравши цей варіант – користувачу потрібно буде ввести ім'я для входу, ключ налаштування та тип ключа. Google Authenticator створить логін і відобразить його одноразовий ключ. Для завершення потрібно повернутись на сайт або службу та завершити процес налаштування 2FA. Щоб завершити процес налаштування 2FA на сайті – користувачеві потрібно буде ввести пароль, створений у додатку.

Після успішного налаштування входу в Google Authenticator, користувач може використовувати цей автентифікатор для отримання одноразового пароля при кожному вході на сайт чи в службу. Google Authenticator грунтується на алгоритмі TOTP на основі часу, який визначений у RFC 6238 від Internet Engineering Task Force (IETF) [3]. Алгоритм TOTP (Time-based One-Time Password) генерує шестизначний пароль, що враховує поточний час доби, для забезпечення унікальності кожного пароля. Коди доступу періодично змінюються згідно з RFC, де рекомендований інтервал за замовчуванням становить 30 секунд. Традиційні методи двофакторної аутентифікації (2FA), такі як Google Authenticator або SMS-повідомлення, пропонують один і той же рівень захисту для всіх користувачів. Це може бути незручно для користувачів, які здебільшого входять в систему з низькоризикованих пристроїв і мереж.

Модель 2FA на основі ризиків вирішує проблему балансу між безпекою та зручністю для користувачів, динамічно адаптуючи рівень аутентифікації під ризик атаки. Це робить систему більш зручною для користувачів, не жертвуючи при цьому безпекою. Однак, варто враховувати, що впровадження цієї моделі вимагає певних зусиль та ресурсів. Процес роботи моделі 2FA на основі ризиків полягає в наступному: спочатку збираються дані про користувача, такі як його IP-адреса, тип пристрою, геолокація та історія входів. Далі ці дані аналізуються за допомогою алгоритму машинного навчання для оцінки ризику атаки. На основі цього аналізу рівень аутентифікації динамічно підлаштовується під рівень ризику.

Однією з ключових переваг цієї моделі є її здатність адаптуватися до конкретного контексту та рівня ризику. Наприклад, коли користувач виконує вхід з незвичного місця або пристрою, система може автоматично запропонувати додаткові шаги аутентифікації для підвищення безпеки. Це дозволяє забезпечити високий рівень захисту без надмірного обмеження зручності для користувачів.

Наприклад, користувачам з високим ризиком можуть бути запропоновані додаткові фактори аутентифікації, такі як біометрія або push-повідомлення, тоді як для користувачів з низьким ризиком може бути достатньо пароля. Серед переваг моделі 2FA на основі ризиків можна виділити зниження навантаження на користувачів шляхом зменшення потреби в 2FA для низькоризикованих входів, підвищення безпеки за рахунок надання додаткового захисту для користувачів з високим ризиком та збільшення гнучкості, дозволяючи використовувати різні методи аутентифікації. Проте модель 2FA на основі ризиків має свої недоліки, серед яких складність реалізації та налаштування, можливість помилок при оцінці ризику, а також необхідність постійного навчання та оновлення алгоритму машинного навчання. Усупереч цим недолікам, модель 2FA на основі ризиків є перспективним напрямком розвитку 2FA, що пропонує кращий баланс між безпекою та зручністю для користувачів.

Також, окрім Google Authenticator, існує другий додаток для генерування кодів доступу для забезпечення двофакторної автентифікації під назвою Microsoft Authenticator. Microsoft Authenticator та Google Authenticator є двома найбільш популярними варіантами. Одним з ключових відмінностей між Microsoft Authenticator та Google Authenticator є підтримка різних функцій. Microsoft Authenticator пропонує зручний варіант підтвердження входу за допомогою push-повідомлень, що може бути швидшим та зручнішим, ніж введення вручну OTP, особливо якщо ви часто входите в систему з одного пристрою. З іншого боку, Google Authenticator сконцентрований виключно на 2FA і не має такої функціональності. Крім того, Microsoft Authenticator пропонує додаткові функції, такі як вбудований менеджер паролів для зберігання облікових даних у безпечному місці, а також генерація кодів для сервісів, сумісних із TOTP (Time-based One-Time Password), навіть якщо вони не інтегровані безпосередньо з програмою. Google Authenticator зосереджений лише на 2FA і не має таких додаткових можливостей. Обидва додатки є надійними варіантами для захисту ваших онлайн-акаунтів за допомогою 2FA. Вибір між ними залежить від ваших конкретних потреб та уподобань. Для зручності використання та додаткових функцій можна вибрати Microsoft Authenticator, тоді як для простоти та мінімалізму – Google Authenticator. Обрати Microsoft Authenticator можливо у разі, якщо потрібна зручність push-повідомлень для підтвердження входу, або якщо потрібен вбудований менеджер паролів для зберігання облікових даних. Також його можна обрати у разі не потреби у генерації кодів для TOTP-сервісів. Обрати Google Authenticator можливо у разі, якщо ви віддаєте перевагу простоті та мінімалізму, і вам не потрібні push-повідомлення або додаткові функції, або якщо ви вже використовуєте окремий менеджер паролів.

Висновки. Двофакторна автентифікація є ефективним інструментом для захисту особистих даних та конфіденційної інформації в онлайн-світі. Рекомендується

використовувати 2FA для всіх онлайн-акаунтів, які підтримують цю можливість, з огляду на постійний розвиток технологій та необхідність посилення кібербезпеки. Аналізуючи принципи, переваги та різноманітні методи застосування двофакторної автентифікації, можна зрозуміти, що цей засіб є ефективним інструментом для захисту особистих даних та конфіденційної інформації. З урахуванням постійного розвитку технологій та необхідності посилення кібербезпеки, 2FA залишається ключовим елементом в цьому контексті.

Було запропоновано використовувати додаток «Google Authenticator» для забезпечення захисту аккаунтів. Використання додатку «Google Authenticator» для захисту аккаунтів є одним із найефективніших та надійних методів реалізації двофакторної автентифікації. Цей додаток генерує одноразові коди, які потрібно ввести після введення основного пароля для підтвердження особистості користувача. Основні переваги використання «Google Authenticator» включають високий рівень безпеки завдяки тому, що коди генеруються безпосередньо на пристрої користувача і не передаються через Інтернет, що робить їх важкими для перехоплення зловмисниками. Крім того, додаток забезпечує зручність використання, оскільки може бути встановлений на смартфон або планшет, що робить процес аутентифікації швидким і зручним для користувача. Загалом, використання «Google Authenticator» є рекомендованим методом для забезпечення безпеки онлайн-акаунтів, оскільки він поєднує в собі надійність, зручність та ефективність в одному інструменті.

Список використаних джерел

1. Що таке двохфакторна автентифікація // Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-two-factor-authentication-2fa (останнє звернення 23.02.2024р.)
2. Що таке двофакторна автентифікація на iPhone та Android, як вона працює? // https://expertonline.com.ua/blog/scho-take-dvofaktorna-avtentifikatsiya : (останнє звернення 28.02.2024р.)
3. Налаштування двофакторної аутонтифікації ssh за допомогою google authenticator // https://freehost.com.ua/ukr/faq/articles/nalashtuvannja-dvofaktornoji-autontifikatsiji-ssh-za-dopomogoju-google-authenticator/ : (останнє звернення 28.02.2024р.)
4. What Is Two-Factor Authentication (2FA)? // https://authy.com/what-is-2fa/ : (останнє звернення 28.02.2024р.)
5. 2FA Statistics: 2FA Climbs, While Password Managers and Biometrics Trend // https://duo.com/blog/the-2021-state-of-the-auth-report-2fa-climbs-password-managers-biometrics-trend : (останнє звернення 28.02.2024р.)

Робота виконана під науковим керівництвом PhD, старшого викладача
КОСТЮК Ю.В.

ВИМОГИ ДО ЗАХИСТУ МИТНОЇ ІНФОРМАЦІЇ

ГРИНЮК В.Є., 1 курс 6мз група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто класифікацію митної інформації та досліджено основні вимоги до захисту митної інформації, побудови та функціонування системи захисту митної інформації. Зазначено, що принципи інформаційної безпеки включають забезпечення цілісності, конфіденційності, а також одночасну доступність інформації для всіх авторизованих користувачів. Проаналізовано чинне Законодавство України щодо захисту інформації в інформаційно-комунікаційних системах. Зазначено важливість класифікації інформації та критерії класифікації. У роботі аналізуються основні види захисту інформації (етичний, правовий, адміністративний (організаційний), технічний (фізичний) та програмний).

This article examines the classification of customs information and investigates the basic requirements for the protection of customs information, the construction and operation of the customs information protection system. It is stated that the principles of information security include ensuring the integrity, confidentiality, and at the same time availability of information to all authorized users. The current legislation of Ukraine on information security in information and communication systems is analyzed. The importance of information classification and classification criteria are emphasized. The work analyzes the main types of information protection (ethical, legal, administrative (organizational), technical (physical), software).

Актуальність. Специфіка роботи митної служби передбачає роботу з інформацією що надходить з різних джерел та має різний рівень агрегації та конфіденційності. Саме забезпечення для цій інформації необхідної цілісності, належного рівня конфіденційності та легкої доступності є запорукою ефективності функціонування всієї митної системи в Україні.

В контексті військової агресії з боку російської федерації значення захисту інформації стає запорукою національної безпеки, а також ефективного функціонування державних органів в цілому, а також митної служби зокрема. Вимоги до захисту інформації уможливлюють протидію кібератакам країни агресора і мають бути у стані постійного удосконалення як на технічному, так і на законодавчому рівні.

Мета статті є дослідження вимог до захисту митної інформації в Державній митній службі України з метою підвищення ефективності їх впровадження та використання. Опис вимог до захисту митної інформації.

Об'єктом дослідження є вимоги до захисту митної інформації.

Предмет дослідження – є захист та безпека митної інформації.

Аналіз попередніх досліджень. Дослідження класифікацій та вимог до захисту митної інформації, визначення структури та основних характеристик *присвячені численним законам України, наказам і постановам, а також працям вітчизняних та зарубіжних вчених*: *Бабалик Є.П., Федоришина Л.М.*

Виклад основного матеріалу. Забезпечення економічної безпеки держави являє собою визначення умов системи, відповідних критеріїв, основних характеристик, певних організаційних форм та чітких механізмів для захисту національної економіки від різних загроз комплексу національних інтересів. На даний момент Україна стикається з певними складними обставинами, які, на жаль, можна вважати безпрецедентними за часів незалежності – повномасштабна військова агресія російської федерації, яка лише поглиблює нестабільність економіки, яка вже була нерівноважною через пандемію COVID-19 та карантинні обмеження.

Наразі для забезпечення формування успішного майбутнього України варто зосередитись на посиленні євроінтеграційного вектору, але за умови утримання від зниження

захисту національного ринку та виробників важливим є зосередження уваги інституцій державного управління на регулюванні процесів переміщення товарів через митні кордони, оптимізації дій учасників зовнішньоекономічної діяльності з метою максимального їх захисту.

Першим етапом в процесі захисту інформації є її класифікація. Класифікація даних, або інформації, це процес систематизації інформації за важливими категоріями з метою забезпечення безпеки критично важливих даних. Наприклад, фінансові файли в організації не мають зберігатися разом із документами відділу зв'язків з громадськістю. Замість цього, вони повинні знаходитися у відокремлених папках, доступ до яких мають лише особи, які мають право працювати з кожним типом інформації. Таким чином, збережена інформація зберігається в безпеці та може бути легко доступна за необхідності [12].

В митній службі щодня обробляють величезну кількість даних – інформацію про клієнтів (суб'єктів зовнішньо-економічного розвитку тощо), записи рахунків-фактур, історію замовлень, списки розсилки, дані користувачів у програмному забезпеченні – цей список можна продовжувати. Однак не всі дані однаково важливі, і деякі елементи вимагають більшого захисту, ніж інші. Таку конфіденційну та важливу інформацію потрібно захищати від вразливості до загроз безпеки. Ось чому так важливо класифікувати інформацію. Це допомагає визначити, яка інформація потребує особливого захисту та як визначити та класифікувати дані, що потребують захисту.

Правильна класифікація інформації є основою для того, щоб інформаційні дані були впорядкованими, доступними та корисними. Класифікувати інформацію за великим обсягом, різноманіттям і релевантністю – це складне, але важливе завдання.

Більшість організацій дотримуються таких кроків, щоб полегшити роботу: Аналіз інформаційних активів та визначення рівня чутливості кожного з них. Першим кроком класифікації інформації є визначення вартості кожного інформаційного активу залежно від ризику втрати чи шкоди в разі розголошення інформації. На основі цього підходу інформація може бути поділена наступним чином (Рисунку 1).

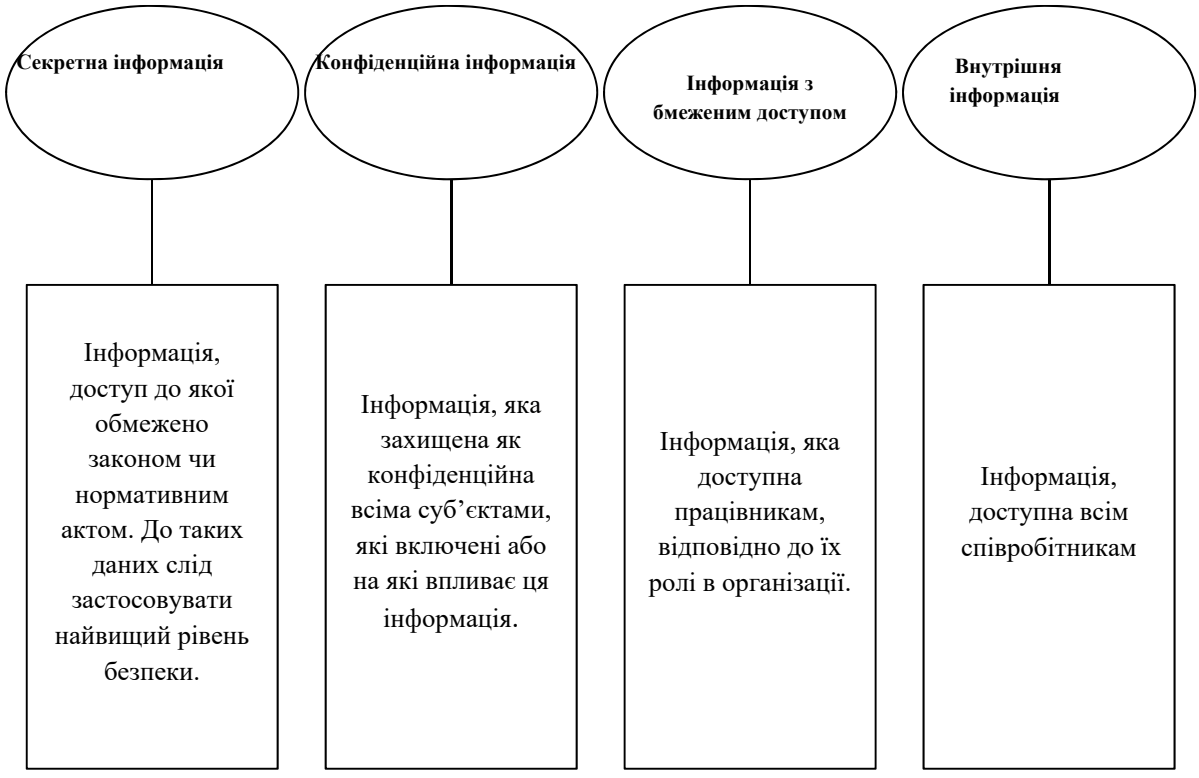


Рис. 1. Класифікація інформації на основі значення

Джерело: розроблено автором

Коли вся інформація класифікується залежно від її цінності, створюється система маркування даних. Відповідна класифікація інформації передбачає просте, зрозуміле та послідовне маркування даних. За результатами проведеної класифікації, визначаються необхідні методи та засоби захисту інформації, на основі системи маркування даних.

Правильно спланована система класифікації даних робить важливу інформацію легкою для роботи та відстеження, а також полегшує пошук даних. Найпоширеніші причини, чому класифікація інформації є особливо важливою, включають:

Ефективність – на базовому рівні, якщо провести класифікацію інформації, то можна ефективніше керувати повсякденною діяльністю. Класифікована і верифікована інформацію набагато простіше шукати, знаходити і отримувати; зміни інформації також швидко простежуються.

Безпека – захист конфіденційної інформації є основною ідеєю класифікації інформації. Здійснення класифікації інформації допомагає впроваджувати інформаційну безпеку. Відповідальність за захист інформації лежить на кожному, хто працює з нею. Система забезпечує те, що співробітники розуміють цінність інформації, з якою вони працюють, і захищають цю інформацію. Корисною тактикою є класифікація інформації для спрямування відповідних заходів безпеки в залежності від типу інформації, яка вилучається, передається або копіюється. Шифрування даних, зберігання даних на безпечних серверах з надійними брандмауерами та відповідність стандартам захисту даних значно допомагають захиститися від зовнішніх загроз. Крім того, можуть існувати внутрішні загрози, які також є небезпечними – наприклад, умисне порушення даних, випадкове порушення даних. Тому важливо обмежувати доступ до інформації та запобігати загрозам.

Відповідність – класифікація інформації у сфері інформаційної безпеки допомагає маркувати інформацію як конфіденційну, захищати її від загроз і дотримуватись регуляторних вимог, таких як GDPR (General Data Protection Regulation). Також можна легко впроваджувати свої власні стандарти з метою проведення класифікації інформації.

Критеріями класифікації інформації можуть бути такі:

Цінність – найчастіше використовуваний критерій для класифікації інформації – це цінність даних. За умови ризиків втрати або розголошення важливої інформації, що може створити значні організаційні, комерційні або репутаційні проблеми, потрібно її зашифрувати.

Вік – за умови що важливість інформації з часом знижується, то секретність інформації можна знизити.

Строк користі – за умови, що потрібно внести необхідні зміни в доступну інформацію, в цьому випадку вона стає «найбільш корисною».

Особиста інформація – якщо інформація, в якій особисті дані осіб або її захист регулюється нормативними документами у сфері захисту конфіденційної інформації, то в такому випадку треба шифрувати таку інформацію.

Беручи до уваги українське законодавство про інформацію можна визначити такі категорії інформації за змістом:

- щодо особи (фізичної, юридичної тощо);
- енциклопедична та довідкова;
- екологічна інформація (щодо стану довкілля тощо);
- щодо робіт та послуг (товарів тощо);
- щодо технічної та наукової;
- щодо податкової;
- щодо правової;
- щодо статистичної;
- щодо соціологічної;
- щодо технологічної (критична тощо) [10].

Схожа система класифікації використовується Державною прикордонною службою України [2].

Якщо проаналізувати запропоновані категорії, то частина з них, наприклад інформація про фізичну особу, буде входити до інформації, з якою працює Державна митна служба України.

В своєму авторефераті дисертації на здобуття наукового ступеня к.ю.н. Бабалик Є. П. дає своє визначення терміну «митної інформації», як офіційної, що збирається, накопичується, використовується та зберігається митними органами під час їх поточної діяльності відповідно до законодавства у процесі здійснення митної справи, та частково поширюється у вигляді знеособлених даних [1].

Проте, як зазначає д-р екон. наук, доцент, Федоришина Л.М. у своїй статті про класифікацію та джерела формування митної інформації, додатково до визначення Бабалика Є.П., вказує на необхідність відповідного захисту митної інформації посадовими особами, яке вона вкладає в своє широке розуміння митної інформації. Крім того, вона надає поняття митної інформації у вузькому розумінні, з акцентом на те, що на підставі сукупності відповідних даних, які подаються декларантом в митний орган, ним здійснюється аналіз ризиків у митній сфері [11].

Офіційна Класифікація митної електронної інформації раніше регламентувалась Наказом Державного Митного комітету України Про електронну інформацію в митній системі України від № 48 від 08.02.96, в якому зазначено, що практично вся митна інформація, яка обробляється в електронній базі митної установи, відноситься до даних з обмеженим доступом, поділяється на три категорії, – згідно ступеня конфіденційності та викладена в Таблиці 1[5].

Таблиця 1

Категорії інформації з обмеженим доступом

Категорія	Вид інформації з обмеженим доступом	Види документів
1	Програмне забезпечення і інформація, які не містять даних, що прямо визначають або безпосередньо визначають митну діяльність	• дані технічного обладнання • документація персоналу • універсальне програмне забезпечення, яке використовується при передачі і для обробки та зберігання митної інформації • вузькоспеціалізоване програмне забезпечення або спеціальне
2	Дані, що забезпечують технологічну роботу митної діяльності	• митні декларації • транзитні документи • протоколи де зазначаються дані про порушені митні правила • протоколи де зазначаються дані про контрабанду • гарантійні листи
	Нормативно-довідкова інформація	• кадрові документи • бухгалтерські документи
3	Службова інформація нормативно-правового спрямування	• документи які регламентують діяльність організації (накази) • службове листування
	Інформація щодо зовнішньоекономічної діяльності	• зовнішньоекономічні договори (контракти) • акти виконаних робіт (наданих послуг) • рахунки (інвойси)
	Інформація щодо групових статистичних баз даних	• статистичні документи

Джерело: розроблено автором, агреговано на основі [5]

Таке твердження Наказу про те що всю інформацію, що оброблена електронними обчислювальними засобами митної служби, класифікується як інформація з обмеженим доступом унеможливлювало функціонування веб застосунків організації. Цей документ втратив чинність 04.04.2006 і не був замінений.

Відповідно з українським законодавством про автоматизовані системи і захист інформації в них, власність або право на інформацію, яка створюється і обробляється в інформаційній автоматизованій системі, належить власнику автоматизованої системи, який здійснює цю обробку, а саме – митній службі України [8].

Державна митна служба України, як власник інформації, має право на юридичний захист від шкоди, завданої навмисним чи ненавмисним втратою, знищенням, фальсифікацією, спотворенням, блокуванням інформації та іншими неправомірними діями.

Про інформацію в Єдиній автоматизованій інформаційній системі, яка проходить етапи зберігання і обробки і розповсюдження, можна охарактеризувати її класифікацію наступним чином відповідно до наказу Державного митного комітету України:

1) Інформація, що створюється і обробляється працівниками митної системи, відноситься до категорії «А». Дотримуючись положень законодавства про авторське право та відповідності правам власності на програмне забезпечення, що створюється власними розробниками або закуповується в інших розробниках, його розповсюдження без відповідного дозволу володільця інформації не допускається.

2) Інформація, що створюється і обробляється працівниками митної системи за розпорядженням керівництва, відноситься до категорії «Б». Обмін цією інформацією з іншими установами митної системи проводиться виключно з дозволу або розпорядження керівництва таких установ. Обмін цією інформацією з установами, органами, структурами і організаціями, які не належать до митної системи України, затверджується керівництвом Державного митного комітету України у кожному випадку передачі.

3) Інформація, що створюється і обробляється виключно персоналом, зі спеціальним дозволом, відноситься до категорії «В». До такої інформації організовують такі заходи з безпеки, як організаційні, так і програмно-апаратні, а зберігають інформацію у закодованому вигляді. Тільки керівництво Державного митного комітету України надає письмовий дозвіл на поширення [5].

Відповідно до нормативних документів у сфері захисту інформації в інформаційних та телекомунікаційних системах [4] існує поділ інформації на такі категорії: Відкрита інформація, конфіденційна інформація, таємна інформація.

Власністю держави являється відкрита інформація, згідно з визначенням українського законодавства про інформацію, це і статистична, правова, соціологічна інформація, так і довідково-енциклопедична інформація. Таку інформацію можна використати з метою підтримки діяльності загальнодержавних або місцевих органів самоврядування. Також інформація, яка висвітлює діяльність цих органів, може розміщуватись в мережі Інтернет, в глобальних інформаційних та комунікаційних мережах і системах або передається комунікаційними мережами.

Конфіденційна інформація є державною власністю або підпадає під вимоги українського законодавства про захист такої інформації, включаючи конфіденційну інформацію про громадян.

Одним з видів конфіденційної інформації є службова інформація. Відповідно до українського законодавства яким регулюється облік, збереження, порядок використання, знищення документів і матеріальних електронних носіїв інформації, вона поділяється на наступні види інформації:

- мобілізаційна «М»;
- криптографічна «К»;
- спеціальна «СІ» [7].

Таємна інформація – до неї належить інформація, що становить державну або іншу передбачену законом таємницю.

Захист інформації у визначенні українського законодавства в сфері захисту інформації в автоматизованих системах – це комплекс організаційних, технічних та правових заходів, спрямованих на запобігання завданню шкоди інтересам власника інформації та

особам, які користуються нею. У нормативних документах можна знайти і такі визначення схожих термінів, такі як «безпека інформації» та «безпека інформаційних технологій»[8].

Складна проблема полягає у забезпеченні безпеки в інформаційних технологіях. Сюди входить напрям правового регулювання використання інформаційних технологій, удосконалення розвитку технологій, еволюцію систем сертифікації та створення для експлуатації відповідних організаційних і технічних умов. Вирішення цієї проблеми достатньо фінансово затратне, тому основним завданням потрібно збалансувати витрати і необхідну безпеку, пов'язаних з її утриманням. Для вирішення цієї задачі необхідно спрогнозувати потенційні загрози, оцінити ймовірність їх виникнення та можливі наслідки, обрати відповідні заходи і в результаті створити безвідмовну систему захисту.

Інформаційна безпека, основна задача якої полягає в тому, щоб забезпечити всім користувачам цілісність, конфіденційність та доступність інформації.

Захист інформації у трактуванні українського законодавства характеризується комплексом певних дій, в результаті яких інформація у системі застрахована від ризиків впливу несанкціонованих дій зловмисників [9].

Згідно з організаційно-розпорядчим документом української митної системи про автоматизовану інформаційну систему митної служби[6], захист інформації в Єдиній автоматизованій інформаційно-аналітичній системі (ЄАІС) Держмитслужби передбачає створення та підтримку такої системи, яка в свою чергу забезпечить надійний захист інформації на технічному (інженерному, програмно-апаратному) та нетехнічному (правовому, організаційному) рівнях. Ці заходи призначені для запобігання або ускладнення можливості втручання в інформаційний потік, а також для зменшення можливих збитків що несе в собі несанкціонований доступ до митної інформації. Основна мета подібних заходів, це створення умов для безпеки митної інформації в автоматизованих інформаційних системах митної служби. Забезпечення захисту митної інформації має бути здійснено на всіх етапах функціонування автоматизованих інформаційних систем митної служби, включаючи всі етапи технологічної обробки даних та у всіх режимах функціонування системи.

Відповідно до Митного кодексу України [3] керівник центрального органу виконавчої влади, що відповідає за реалізацію державної митної політики, несе відповідальність згідно із законом, якщо електронні інформаційні ресурси у митних органах експлуатуються без застосування комплексної системи захисту інформації або системи управління інформаційною безпекою, що відповідає вимогам законодавства з питань захисту інформації в інформаційно-комунікаційних системах та кібербезпеки.

Захист митної інформації в напрямку запобігання виникнення ризику можливих порушень в роботі автоматизованих митних інформаційних систем та можливих загроз несанкціонованого доступу до митної інформації, доцільно віднести до наступних груп:

- морально-етична;
- правова;
- адміністративна (організаційна);
- технічна (фізична);
- програмна.

Все ж таки потрібно зазначити наступне, що такий розподіл є в певній мірі умовним. При тому, що поєднання програмного та апаратного забезпечення захисту, це сучасний тренд розвитку технологій.

Морально-етичні засоби – ця група включає норми поведінки, які традиційно сформувалися або формуються з поширенням комп'ютерів, мереж і т. д. Ці норми в основному не є обов'язковими і не затверджені законодавчим шляхом, але їх невиконання часто призводить до падіння авторитету та репутації людини, групи осіб, організації або країни. Морально-етичні норми бувають неписаними, так і формалізованими у певному статуті. Прикладом є етичний Кодекс професійної поведінки членів Міжнародного консорціуму з сертифікації в галузі безпеки інформаційних систем – (ISC)2 (The International Information System Security Certification Consortium).

Правові засоби – до цієї групи відносять чинні нормативно-правові акти, де регламентуються правила використання митної інформації та встановлюється відповідальність при порушенні, захищають авторські права та упорядковують інші питання, пов'язані з застосуванням інформаційних технологій в митній системі.

В суспільстві, де значну роль відіграє електронна інформація, вкрай важливо постійно вдосконалювати національне законодавство з метою боротьби з кіберзлочинами в судовому, кримінальному і цивільному напрямах. Вже сьогодні за участю міжнародних організацій ухвалене спеціалізоване законодавство в багатьох країнах світу і постійно ведеться робота з його актуалізації. Такі нормативно-правові документи не варто порівняти між собою, оскільки кожен нормативно-правовий документ доцільно розглядати у контексті всієї правової системи. Наприклад, закони про конфіденційність мають вплив на нормативно-правові акти в галузі процесуального, кримінального і судового законодавства, про електронну та іншу інформацію і адміністративне регулювання.

Однією з головних законодавчих ініціатив є Будапешська конвенція – це рамкова угода, яка дозволяє сотням фахівців-практиків з країн підписантів обмінюватися досвідом і налагоджувати відносини, що сприяють співпраці в конкретних випадках, включаючи і надзвичайні ситуації, які виходять за рамки конкретних положень, передбачених цією Конвенцією [14]. Конвенція про кіберзлочинність («Будапештська конвенція») вважається найбільш всеосяжною і послідовною міжнародною угодою про кіберзлочинність та електронні докази на сьогоднішній день. Вона слугує орієнтиром для будь-якої країни при розробці національного законодавства у сфері кіберзлочинності, а також основою для міжнародного співробітництва між державами-учасницями Конвенції.

Будапештська конвенція передбачає криміналізацію поведінки – від незаконного доступу, втручання в дані та системи до шахрайства, пов'язаного з комп'ютерним втручанням в роботу систем до комп'ютерного шахрайства та дитячої порнографії; процесуальні повноваження для розслідування кіберзлочинів та захисту електронних доказів; кіберзлочинності та захисту електронних доказів будь-якого скоєного злочину, а також ефективну міжнародну співпрацю. Договір відкритий для приєднання будь-якої країни [13].

Адміністративні або організаційні засоби – нормують такі процеси як функціонування, так і використання технічних ресурсів та діяльність особового складу. Регулювання порядку поводження користувачів в інформаційних системах відбувається у такий спосіб, щоб надати змогу розтягнути його в часі і максимально ускладнити, або запобігти порушенням безпеки в максимально можливому обсязі.

Вони включають в себе:

- Заходи, передбачені при проектуванні, будівництві та облаштуванні об'єктів безпеки (врахування природних впливів, протипожежна безпека, захист приміщень, контроль доступу, прихований моніторинг працівників тощо);
- Розробку, ремонт і модифікацію спеціалізованих програмного забезпечення та сертифікованих пристроїв, а саме: сувора ідентифікація, сертифікація програмного і технічного інструментарію та актуалізація за погодженими змінами;
- Вчинення відповідних дій, необхідних для проведення відбору та навчання потенційних користувачів (визначення кандидатів у співробітники з підвищеним рівнем довіри, доведення до них необхідних процедур при обробці конфіденційної інформації, та відповідальності за її порушення). Найважливішим при цьому є – створення умов, які унеможливлюють здійснення зловживань або роблять їх невигідними;
- Затвердження положень про використання і збереження інформації та визначення концепції її захисту, – з метою доведення до користувачів необхідних вимог щодо організації обліку, зберігання, використання та знищення документів і носіїв конфіденційної інформації; обмеження доступу за допомогою паролів, застосування авторизації допуску. При цьому важливо також передбачити систему покарань та адміністративних норм – за їх порушення.

Слід зауважити, що адміністративні засоби – це важлива частина інформаційного захисту, і їх значення неможливо переоцінити. Воно полягає в їх доступності та здатності

доповнювати нормативно-правові вимоги, необхідні для дотримання. Їх особливість полягає в тому, що вони застосовують інші види технічного і програмного захисту, – для оптимізації його рівня. Але при цьому не слід надмірно обтяжувати працівників великою кількістю адміністративних правил, оскільки це фактично зменшує надійність захисту інформації (інструкції можуть просто не виконуватися).

Інженерно-технічний захист направлений на використання технічних, інженерних та програмних засад – з метою унеможливлення витоків, знищення і блокування інформації, запобігання порушенню цілісності і режимів допуску до захищених ресурсів [9].

До захисту інформації фізичними (технічними) засобами використовуються необхідні електричні, механічні та електронно-механічні пристрої. Конструктивне поєднання цих пристроїв вкупі з відповідними захисними спеціалізованими матеріалами дає можливість посилити захист інформації від несанкціонованого доступу і викрадень, запобігти її втратам у разі хакерських атак, диверсій, саботажу, стихійних лих та техногенних аварій, або внаслідок несправності складових конструкції.

До вказаних пристроїв (засобів) відносяться:

Засоби захисту для кабельних систем. З метою зменшення ризиків відмови кабельних систем оптимальний варіант – побудувати структуровану кабельну систему (СКС), яка використовує ідентичні кабелі для організації передачі даних, сигналів від датчиків пожежної безпеки, відеоінформації від систем безпеки, а також місцевої телефонної мережі. Поняття «структурованість» означає, що кабельна система будинку розподіляється на кілька рівнів залежно від її призначення та розташування. З метою організації ефективної і надійної СКС потрібно дотримуватися вимог міжнародних стандартів.

Засоби захисту системи електроживлення. Одним з надійних способів запобігти втраті інформації під час тимчасових відключень електроенергії або стрибків напруги в електричній мережі – це встановлення джерел безперебійного живлення. Різноманітні технічні та експлуатаційні характеристики дозволяють вибрати засіб, який відповідає вимогам. За умов підвищених вимог до надійності можуть використовуватися аварійні генератори електричного струму або резервні лінії електропостачання, підключені до різних підстанцій;

Засоби архівації та дублювання даних. При роботі з великими обсягами інформації рекомендується організувати окремий спеціалізований сервер для архівації даних. Якщо архівна інформація має велику цінність, її слід зберігати в спеціально облаштованому приміщенні. У випадку пожежі або природних катастроф дублікати найцінніших архівів варто зберігати в іншому приміщенні (можливо, в іншій будівлі, в іншому районі міста або в іншому місті);

Засоби захисту від впливу інформації через різноманітні фізичні поля, що виникають під час роботи технічних пристроїв, включають засоби виявлення прослуховувального обладнання, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням генераторів шуму широкого спектру тощо. Матеріали, що забезпечують недоторканість, можливість транспортування засобів зберігання інформації та захист їх від копіювання, також належать до цієї групи. Це переважно спеціальні тонкоплівкові матеріали зі змінним колірним спектром або голографічні мітки, нанесені на документи та об’єкти (включаючи комп’ютерну техніку), які дозволяють перевірити автентичність об’єкта та контролювати доступ до нього. Як зазначалося раніше, технічні засоби захисту найчастіше реалізуються в поєднанні з програмним забезпеченням.

Щоб відповідати вимогам щодо захисту митної електронної інформації, слід зазначити наступне:

● Митна інформація про суб’єкти зовнішньоекономічної діяльності, товари, комерційні транспортні засоби збирається на митному кордоні України, накопичується у відповідних форматах для внесення до баз даних, і є інформацією з обмеженим доступом. Зокрема, обробка частина цієї інформації, що містить персональні дані осіб, здійснюється без їх згоди;

● Митна інформація, отримана митними органами, може використовуватися виключно для митних цілей. Заборонено оприлюднення та передачу її третій стороні без дозволу суб'єкта (фізичних осіб, органу тощо), який надає таку інформацію;

● За розголошення митної інформації винні у порушенні конфіденційності посадові особи підпадають під відповідальність згідно до законодавства України.

Щодо захисту митної електронної інформації варто відмітити наступне:

● Захист електронної інформації в системах, здійснюється в порядку, визначеному законодавством України.

● Обробка інформації в інформаційних системах митних органів здійснюється відповідно до вимог КСЗІ (комплексна система захисту інформації).

В той же час, у разі виконання певних умов відповідного законодавства в сфері захисту інформації допускається обробка інформації в базах митних даних без застосування КСЗІ, але все ж таки з дотриманням вимог кібербезпеки [3].

Висновки. Першим етапом в процесі захисту інформації є її класифікація. Класифікація даних, або інформації, це процес систематизації інформації за категоріями з метою забезпечення безпеки критично важливих даних. Правильно спланована система класифікації даних робить інформацію легкою для роботи та відстеження, окрім того, полегшує пошук даних. Найпоширенішими причинами, чому класифікація інформації є особливо важливою, є ефективність, безпека, відповідність. Найбільш часто використовуваним критерієм для класифікації інформації є цінність даних.

Базовими принципами безпеки для митної інформації є забезпечення її цілісності, конфіденційності і водночас доступності для всіх авторизованих користувачів. Належний рівень захисту митної інформації може бути досягнутий лише комбінацією різних методів: морально-етичних, правових, адміністративних (організаційних), технічних (фізичних), програмних).

Список використаних джерел

1. Бабалик Є.П. Адміністративно-правові основи інформаційного забезпечення митних органів в Україні: автореф. дис. … канд. юрид. наук: 12.00.07/ Кормич Борис Анатолійович, Одеська національна юридична академія, – Одеса, 2010. –18 с.

2. Види інформації [Електронний ресурс] // Державна прикордонна служба України. – Режим доступу: https://dpsu.gov.ua/ua/vidi-informacii/ (дата звернення: 10.04.2024). – Назва з екрана.

3. Митний кодекс України [Електронний ресурс]: Закон України від 13.03.2012 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/4495-17#Text (дата звернення: 30.03.2024).

4. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] : Кабінет Міністрів України. – Режим доступу: https://www.kmu.gov.ua/npas/32791826 (дата звернення: 10.04.2024).

5. Про електронну інформацію в митній системі України [Електронний ресурс] : Наказ Державного Митного комітету України від N 48 від 08.02.96. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0083-96#Text (дата звернення: 30.03.2024).

6. Про Єдину автоматизовану інформаційну систему Державної митної служби України [Електронний ресурс]: Наказ Міністерства Фінансів України 04.11.2010 № 1341. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1132-23#Text (дата звернення: 30.03.2024).

7. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію [Електронний ресурс] : Постанова Кабінету Міністрів України № 736

від 19.10.2016. – Режим доступу: https://www.kmu.gov.ua/npas/249419755 (дата звернення: 30.03.2024).

8. Про захист інформації в автоматизованих системах [Електронний ресурс] : Закон України №80/94-ВР. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 30.03.2024).

9. Про захист інформації в інформаційно-комунікаційних системах [Електронний ресурс] : Закон України № 3549-IX. – Режим доступу:https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text] (дата звернення: 30.03.2024)

10. Про інформацію [Електронний ресурс]: Закон України від 02.10.1992 р. № 2657-XII (зі змінами). – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 30.03.2024).

11. Федоришина Л.М. Митна інформація: класифікація та джерела її формування / Л.М. Федоришина // Інноваційна Економіка. Науково-виробничий журнал. Серія: Економіка та інноваційний розвиток національного господарства. – 2020, с. 5-12.

12. Information Classification in Information Security [Електронний ресурс] // SimpliLearn. – Режим доступу: https://www.simplilearn.com/information-classification-article (дата звернення: 10.04.2024). – Назва з екрана.

13. Joining the Convention on Cybercrime: Benefits [Електронний ресурс] // Cybercrime. – Режим доступу: https://rm.coe.int/cyber-buda-benefits-8-february-2024-en-2776-0534- 0937-v-1/1680ae70ee (дата звернення: 10.04.2024). – Назва з екрана.

14. The Budapest Convention (ETS No. 185) and its Protocols [Електронний ресурс] // Cybercrime. – Режим доступу: https://www.coe.int/en/web/cybercrime/the-budapest -convention (дата звернення: 10.04.2024). – Назва з екрана.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

ЕФЕКТИВНІСТЬ ТЕХНОЛОГІЇ ВІРТУАЛЬНОЇ ПРИВАТНОЇ МЕРЕЖІ (VPN) У ЗАХИСТІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ В УМОВАХ ЗРОСТАЮЧОЇ ЗАГРОЗИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ

ГУРТОВЕНКО А.А., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто основні засади побудови та функціонування віртуальної приватної мережі між структурованими структурами. Зазначено переваги застосування віртуальної приватної мережі у використанні повсякденних потребах бізнесу. Розглянуто як зразок підхід до реалізації корпоративної віртуальної приватної мережі –»OpenVPN Access Server».

The article discusses the basic principles of building and operating a virtual private network between structured entities. The advantages of using a virtual private network in everyday business needs are noted. An approach to the implementation of a corporate virtual private network – «OpenVPN Access Server» – is considered as an example.

Актуальність. У сучасному цифровому світі, де електронні комунікації відіграють найважливішу роль, постає питання в захисті приватності та безпеки даних. У захисті даних потребують як персональні користувачі так і організації.

Існує багато ефективних інструментів для забезпечення захисту даних, кожен з них вузько направлений і використовується в своїй окремій галузі. Та саме віртуальна приватна мережа стає все популярнішою з кожним роком. Популяризації віртуальної приватної мережі посприяло саме її легкодоступність та умовна безкоштовність.

Незважаючи на те, що віртуальна приватна мережа є давно розробленою технологією, в наші дні – є інструментом для вирішення багатьох проблем, пов'язаних з несанкціонованим доступом. Завдяки різним реалізаціям віртуальної приватної мережі можна обрати найбільш потрібний метод реалізації для вирішення проблем з безпекою. Завдяки чому, при використанні віртуальної приватної мережі, створюється зашифрований тунель, який пов'язується між ресурсами організації та кінцевими мережами та користувачами, що надає захист від зовнішнього доступу і втручання.

Метою статті є дослідження побудови та функціонування реалізації корпоративної віртуальної приватної мережі «OpenVPN Access Server» та її застосування в захисті від несанкціонованого доступу.

Об'єктом дослідження є віртуальна приватна мережа « OpenVPN Access Server « в умовах захисту від несанкціонованого доступу.

Предмет дослідження технологія реалізації віртуальної приватної мережі «OpenVPN Access Server»

Аналіз попередніх досліджень. Дослідженню вибору технології віддаленого доступу для ефективної організації захисту мережевих з'єднань присвячені праці Українських та закордонних науковців: І.Я. Тишик, А.Ф. Джентиле, Д.Ю. Кириченко, Д.С. Комін, Д.В. Конов, Є. Антонюк та ін.

Виклад основного матеріалу. Популярність використання віртуальних приватних мереж зростає в попиті з кожним роком. Адже це не тільки безкоштовно і практично, але й зручно в налаштуванні та використанні. В умовах сьогодення людство використовує віртуальні приватні мережі в різних цілях, що можна спостерігати згідно статистики (Рис.1).

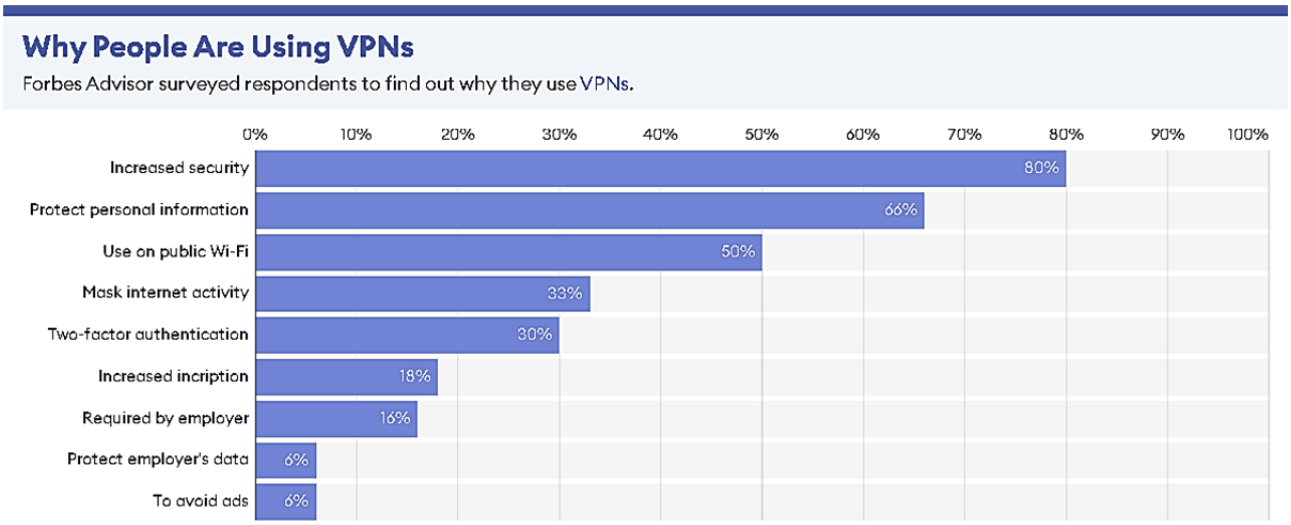


Рис. 1. Чому люди використовують VPN?

Джерело: [1]

Якщо розглядати мотиви використання віртуальної приватної мережі, то найпоширенішими є підвищення безпеки, захист персональних даних та респонденти, які використовують VPN у публічних Wi-Fi мережах. З огляду на це, можна зробити висновок, що актуалізація віртуальної приватної мережі набуває все більшої популярності.

Також неможливо не виділити таку актуальність віртуальної приватної мережі як обходження цензури та обмежень в Інтернеті. Згідно з оцінкою VPN-провайдера Surfshark приблизна кількість користувачів віртуальних приватних мереж становить 1,6 мільярда

людей, з поправкою на те, що Surfshark не враховував користувачів у країнах з проникненням на ринок менше 10%. Якщо ж брати доцільно, то кількість користувачів по всьому світі перевищує 1,6 мільярда людей.

Найбільшого визнання віртуальні приватні мережі зазнали в країнах Близького Сходу, де VPN є практичним способом обходу інтернет-цензури та обмежень. Згідно статистики, наданої компанією «AtlasVPN» (Рис.2), найбільше завантажень віртуальних приватних мереж у Катарі (69,87%), Об'єднаних Арабських Еміратах (61,7%) та Сінгапурі (53,71%), а найменш популярним даний сервіс у Південній Африці (1,44%), Японії (1,83%) та Кенії (1,92%). Україна посідає в цьому списку 33 місце і, посилаючись на цю статистику можна побачити, що попит на віртуальні приватні мережі у 2023 році (9,09%) значно знизився в порівнянні з 2022 роком (17,18%).

Pos.	Country	Downloads				Population	VPN adoption index			
		2023	2022	2021	2020		2023	2022	2021	2020
1	Qatar	2 012 318	1 129 081	2 007 756	1 528 763	2.88M	69.87%	39.2%	69.69%	53.06%
2	United Arab Emirates	6 101 770	4 270 047	5 886 566	6 093 301	9.89M	61.7%	43.18%	59.52%	61.61%
3	Singapore	3 142 042	2 170 865	2 874 601	945 425	5.85M	53.71%	37.11%	49.14%	16.16%
4	Oman	1 986 271	1 356 303	1 718 353	1 805 478	5.11M	38.87%	26.54%	33.65%	35.36%
5	Netherlands	5 032 830	4 093 890	2 801 098	1 639 583	17.13M	29.38%	23.9%	16.35%	9.57%
6	Saudi Arabia	10 044 842	9 419 488	12 760 979	10 081 329	34.81M	28.86%	27.06%	36.65%	28.96%
7	Kuwait	1 075 914	818 069	1 265 560	933 664	4.27M	25.2%	19.16%	29.63%	21.86%
8	Turkey	14 398 181	12 390 300	19 020 753	9 449 156	84.34M	17.07%	14.69%	22.55%	11.2%
9	France	10 534 433	8 907 640	6 017 733	3 425 823	65.27M	16.14%	13.65%	9.22%	5.25%
10	Australia	3 988 989	2 581 455	2 503 351	2 498 393	25.50M	15.64%	10.12%	9.82%	9.8%

Рис. 2. Глобальний індекс впровадження VPN

Джерело: [2]

Незважаючи на корисність такого інструменту як віртуальна приватна мережа в Єгипті, Туреччині, Китаї, Індії, діють обмеження на використання сервісів, які надають послуги віртуальних приватних мереж. Що порушує права людини, оскільки це відбирання права на конфіденційність та безпеку персональних даних.

Віртуальна приватна мережа створює безпечне з'єднання, яке також є зашифрованим між пристроєм користувача та сервером провайдера VPN. Таке з'єднання дозволяє приховати свою реальну IP-адресу, замінюючи її на адресу сервера віртуальної приватної мережі, забезпечуючи цим анонімність у мережі, такої як публічні Wi-Fi мережі. Під час використання віртуальної приватної мережі користувач приєднується до сервера VPN, за допомогою якого весь трафік маршрутизується через нього, що надає змогу користувачеві з'являтися в мережі Інтернет з місцезнаходження сервера віртуальної приватної мережі, а не фізичного місцезнаходження.

Базуючись на цьому, можна стверджувати, що віртуальна приватна мережа надає користувачам цілком приватне та безпечне з'єднання, надаючи перелік переваг в безпечному користуванні мережею Інтернет:

- захист трафіку користувача: користувачі передають, зберігають дані в мережі Інтернет, та якщо не шифрувати ці дані вони стають вразливими для кіберзлочинців, саме тому використання віртуальної приватної мережі є корисним, адже вона надає це шифрування.
- надання конфіденційності в Інтернеті: коли ви використовуєте мережа Інтернет всі збирають ваші дії в мережі, починаючи від інтернет-провайдера закінчуючи інтернет-магазином. Збираючи ці дані, вони мають повноцінне право на передачу даної інформації

органам державного контролю. Саме тому використання віртуальної приватної мережі надає конфіденційність в мережі Інтернет шифруючи трафік, тим самим – маскуючи дії користувача.

- зміна IP-адреси: як було розглянуто вище, влада багатьох країн обмежує довільне використання інтернет-ресурсами, вводячи інтернет-цензуру та обмеження на деякий контент, який вони вважають не доцільним в своїй країні. Саме використання віртуальної приватної мережі вирішує цю проблему шляхом заміни вашої IP-адреси на адресу серверу віртуальної приватної мережі.
- запобігання обмеженню пропускної здатності: деякі інтернет-провайдери вдаються до регулювання пропускної здатності, тим самим обмежуючи комфортне використання послуги з високим споживанням трафіку. Віртуальна приватна мережа вдало справляються і з цією проблемою, адже вона шифрує трафік, тим самим інтернет-провайдер не зможе обмежити вам трафік, бо гадки не зможе відслідковувати дії.
- безпечне середовище під час роботи дистанційно та передачі даних: в останній час набуває популярності як робота дистанційно, саме тому багато компаній потребують в захисті даних при передачі їх між робітниками що працюють дистанційно та між іншими мережами власником якої є дана компанія. Тому використання віртуальної приватної мережі вирішує всі проблеми компаній в забезпеченні захисту інформації під час обміну чи роботі з інформацією в мережі Інтернет.
- кращий онлайн-геймінг: з розвитком онлайн-ігор також виникла проблема від захисту ігрових мереж від DDoS-атак та потреба уникнути несправедливих блокувань IP – адрес, саме тому віртуальна приватна мережа є гарним рішенням цих проблем.

З огляду на вище зазначене можна дійти висновку, що віртуальна приватна мережа є найпотрібнішим інструментом кожного користувача мережі Інтернет. Віртуальні приватні мережі поділяються також за принципом роботи:

- бізнес VPN: поєднує в собі характеристики подібні до VPN типу «мережа мережа», який за своїми властивостями поєднує декілька мереж в єдину мереж, що зручно для корпоративних мереж, при цьому маршрутизатор, який є одиницею, що об’єднується в цій мережі, – має можливість працювати як сервер, і як клієнт. Також бізнес VPN поєднує в собі таку характерність як VPN з віддаленим доступом, що надає змогу користувачам отримувати безпечний віддалений доступ до кооперативної мережі, що є зручним для працівників, які працюють дистанційно.
- персональний VPN: тип віртуальної приватної мережі, який має призначення для персонального використання. Працює за принципом створювання безпечного зв’язоку між користувачем та мережею Інтернет.

Віртуальні приватні мережі мають безліч різновидностей між собою, починаючи з технічної реалізації (працюють на рівні маршрутизатора та провайдери віртуальних приватних мереж), протоколом роботи (OpenVPN, IPSec, PPTP) закінчуючи їх фінансовою доступністю.

Найзатребуванішим серед віртуальних приватних мереж за принципом роботи є бізнес-VPN: він вимагає посиленого ставлення до безпеки та захисту даних від несанкціонованого доступу, адже недбале ставлення до забезпечення кібербезпеки в межах кооперативної мережі може стати як фінансовою проблемою, так і привести до втрати конфіденційності даних, що є порушенням законодавства про захист персональних даних та збитків у репутації організації.

Існує багато представників, які надають різні технології віртуальних приватних мереж: Cisco, Fortinet, Microsoft, Palo Alto Networks, але найбільш комплексне та функціональне рішення надає компанія OpenVPN. Їх комерційний продукт OpenVPN Access Server надає цілий перелік функціоналу, який є спроможний втримувати їх послуги серед

лідерних позицій на конкурентній арені. Простий в встановленні та налаштуванні, масштабованість, підтримка на різних платформах, розширені можливості щодо конфігурації – все це стосується даного продукту, де вони зазнали визначних досягнень.

Access Server підтримує два типи VPN-з'єднань: remote access та site-to-site.

Remote access VPN надає можливість робітникам організації віддалений доступ до мережі організації. Цей тип з'єднання шифрує весь отриманий та відісланий трафік робітника, який працює дистанційно. Саме за допомогою цього з'єднання працівники можуть безпечно використовувати дані, інструменти та ресурси, які знаходяться в штаб-квартирі. Проте віддалений доступ віртуальної приватної мережі має також свої недоліки, а саме зі зростанням робітників, які працюють віддалено, втрачається оптимізація в роботі з хмарними технологіями. Проблема в тому, що віддалений доступ VPN реалізується за допомогою архітектури «Hub-and-Spoke» (Рис. 3), що має ваду – чим далі користувач знаходить від центру обробки даних, тим більше погіршується продуктивність та проблеми з затримкою. Для покращення та оптимізації цього процесу, як варіант, є належна архітектура мережевої безпеки та рішення проблем з оптимізацією доступу до внутрішнього центру обробки даних.

Якщо віртуальна приватна мережа з віддаленим доступом мала свої недоліки, то тип з'єднання Site-to-Site їх принаймні не має. Site-to-Site VPN – це з'єднання, яке поєднує в собі декілька мереж, наприклад, локальну мережу головного офісу та локальну мережу філії даної організації (Рис. 4). Більшість організації обирають саме Site-to-Site замість приватних каналів багатопротокольної комутації міток (Multiprotocol Label Switch), тому що з'єднання віртуальної приватної мережі надає можливість використовувати інтернет-з'єднання для приватного трафіку. Також зручність цього типу з'єднання полягає в незалежності від географічного розташування двох мереж, які поєднуються.

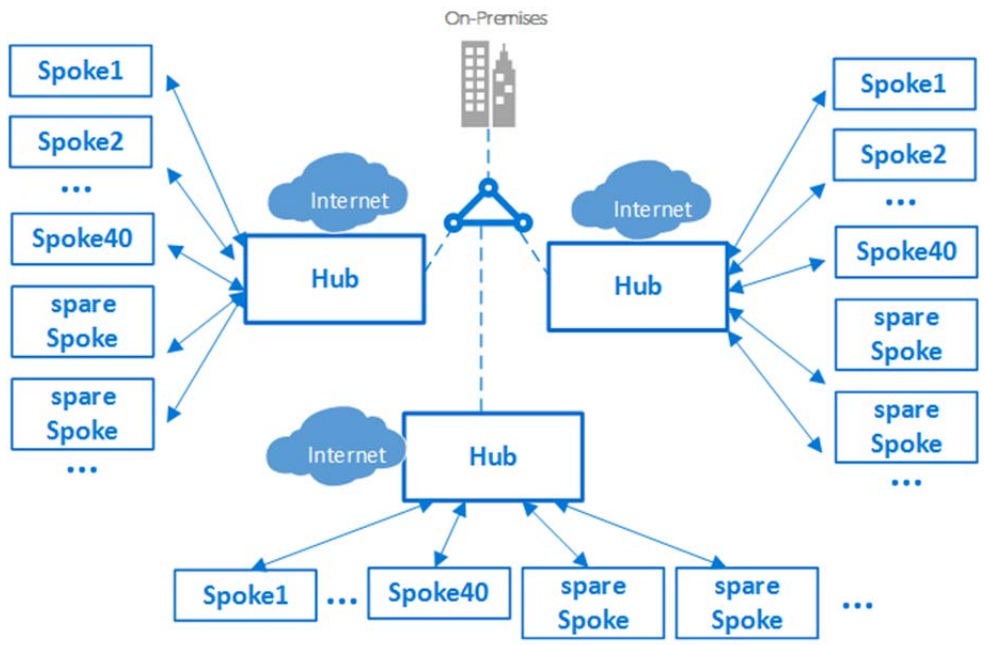


Рис. 3. Реалізація мережевої топології «Hub-and-Spoke»

Джерело:[3]

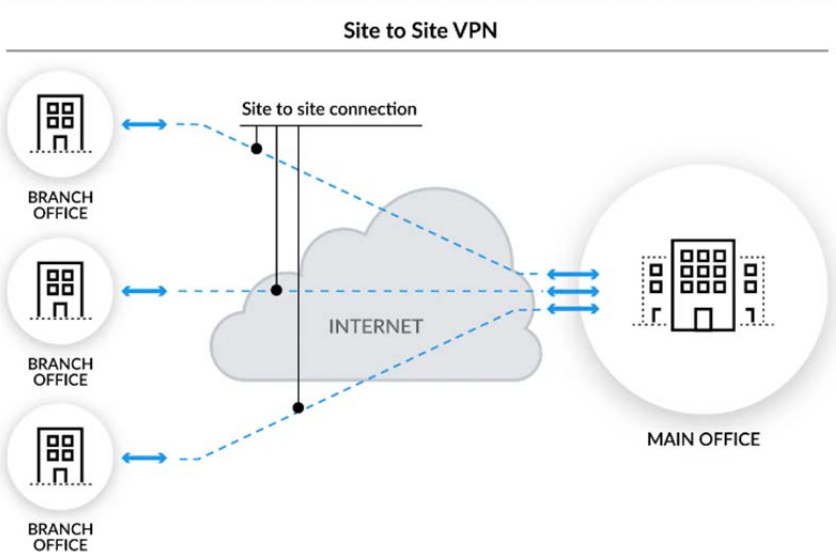


Рис. 4. Тип з'єднання «Site-to-Site VPN»

Джерело: [4]

Access Server забезпечує віртуальну приватну мережу 3 рівня (L3VPN) з використання поширеного протоколу OpenVPN. Даний протокол шифрування входить у трійку кращих протоколів, завдяки тому, що має відкритий вихідний код, який, в свою чергу, має гнучке налаштування, що дає змогу налаштовувати його під конкретні потреби. Також даний протокол використовує UDP, який забезпечує більш швидку передачу даних, але з втратою стабільності підключення; а також – TCP, який забезпечує стабільне підключення, але з втратою швидкості передачі даних.

OpenVPN використовує різні методи забезпечення цілісності, доступності та конфіденційності даних. Даний протокол використовує поширений метод шифрування даних AES (Advanced Encryption Standard) з різними довжинами ключа 192-біт, 256-біт. Даний метод шифрування є найефективнішим та безпечним серед алгоритмів шифрування. Невід'ємною частиною даного протоколу є механізм ключування: використовує обмін ключами Diffie-Hellman, який встановлює безпечний зв'язок між клієнтом та мережею чи сервером. Саме така процедура надає змогу обмінюватися сеансовими ключами лише між сторонами, які поєднані. Не обійшлося без використання протоколу з'єднання TLS/SSL: OpenVPN використовує один з цих протоколів для безпечного транспортування даних по мережі.

Незважаючи на всі переваги, віртуальні приватні мережі мають також і недоліки. Найпоширеніші з них є висока вартість бізнес-VPN, складність в налаштуванні та управлінні, пропускна здатність та проблеми зі швидкістю, а також найголовніше – це безпека і конфіденційність даних.

Беручи до уваги всі вище перераховані складові продукту OpenVPN Access Server, він має переваги у всіх недоліках, починаючи з високої захищеності даних та закінчуючи невисокою вартістю за надання послуг.

Віртуальна приватна мережа є ефективною в захисті від несанкціонованого доступу. З огляду на шифрування трафіку при передачі між вузлами мережі, що створює складнощі для перехоплення його злочинцями, захист від витоку фізичною IP-адреси заміною її на адресу VPN серверу, базовий компонент для використання організаціями, адже він створює захищений канал між локальними мережами, обхід географічних обмежень, які накладають деякі веб-сайти та сервіси, тим самим надаючи доступ користувачам до заблокованого контенту, та не менш важливе мережеве фільтрування, яке ефективне в кооперативних мережах, адже воно блокує небажаний контент або з'єднання.

Висновки. Використання віртуальної приватної мережі у захисті електронних комунікацій є дієвим інструментом проти несанкціонованого доступу. Оцінюючи популяризацію віртуальної приватної мережі, можна дійти висновку, що користувачі мережі Інтернет все більше замислюються над своєю приватністю та безпекою персональних даних. Саме цей інструмент надає можливість створювати захищений та зашифрований зв'язок користувача з мережею, що на даному цифровому етапі є важливим компонентом в захисті даних. Проте, не зважаючи на успіхи віртуальної приватної мережі, варто враховувати, що вона не є захистом від усіх кіберзагроз. Тому важливо створювати комбінований захист з різних інструментів захисту від кіберзагроз, таких як: антивірусне програмне забезпечення, файервол та інші заходи щодо створення комплексного захисту від кіберзагроз.

Список використаних джерел

1. VPN Statistics And Trends In 2024 // Режим доступу: https://www.forbes.com/advisor/business/vpn-statistics/ (останнє звернення 20.03.2024р.)
2. Global VPN Adoption Index // Режим доступу: https://atlasvpn.com/vpn-adoption-index (останнє звернення 20.03.2024р.)
3. Hub-and-Spoke network topology // Режим доступу: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/hub-spoke-network-topology (останнє звернення 21.03.2024р.)
4. What is a Site-to-Site VPN? // Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn (останнє звернення 21.03.2024р.)

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д.О.

METHODS FOR IDENTIFYING CYBER-OFFENDERS IN INDUSTRIAL ENTERPRISE COMMUNICATIONS

ДАНИЛОВ С.О., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглядаються методології, що використовуються для виявлення порушників в електронних комунікаціях промислового підприємства. Вона підкреслює критично важливу роль точної ідентифікації порушників для підтримки безпеки та захисту інформаційних активів підприємства. У цьому контексті в статті обговорюються різні технологічні стратегії та алгоритмічні рішення, призначені для ефективного виявлення та ретельного вивчення протиправної діяльності. Основна увага приділяється застосуванню передових аналітичних методів, які допомагають в інтерпретації шаблонів даних і поведінки, що свідчать про порушення безпеки, тим самим сприяючи швидкому і точному виявленню потенційних загроз цілісності інформації.

The article delves into the methodologies utilized for pinpointing offenders within the electronic communications of an industrial enterprise. It highlights the critical role of accurately identifying culprits to maintain the security and protection of an enterprise's informational assets. In this context, the paper discusses various technological strategies and algorithmic solutions designed to detect and scrutinize unlawful activities effectively. The focus is on the application of advanced analytical techniques that assist in the interpretation of data patterns and behaviors indicative of security breaches, thereby aiding in the prompt and precise identification of potential threats to information integrity.

Relevance. The modern industrial landscape is undergoing a profound digital transformation, with enterprises becoming increasingly reliant on electronic communications to orchestrate production processes, monitor equipment status, and facilitate data exchange. While this technological shift unlocks immense opportunities for optimizing operations and boosting efficiency, it also exposes organizations to emerging cybersecurity threats.

The proliferation of the Internet of Things (IoT), cloud computing services, and other cutting-edge technologies has amplified the risk of cyberattacks targeting industrial facilities. Inadequate security measures guarding electronic communications can culminate in grave consequences, such as disruptions to production workflows, breaches of confidential information, compromises to employee and environmental safety protocols, and substantial financial losses.

Industrial enterprises, owing to their pivotal role in the manufacturing of goods and provision of essential services, warrant heightened vigilance. A failure to implement robust cybersecurity measures can precipitate significant material losses, irreparable reputational damage, and even jeopardize the organization's very existence.

Consequently, addressing the pressing challenge of identifying cyberoffenders in the realm of industrial enterprise communications has emerged as an imperative task. Effective identification strategies are crucial for safeguarding the sustainability and reliability of production processes, protecting sensitive information, and pre-empting potential cyberattacks. This article delves into the multifaceted methods and approaches tailored to unmask and attribute malicious activities within the digital communication channels of industrial organizations.

The aim of this article is to explore various methods for identifying cyberoffenders who illicitly access or compromise the electronic communications within an industrial enterprise setting. This examination is undertaken with the overarching goal of fortifying the security posture and safeguarding the organization's invaluable information assets.

The research object encompasses the intricate realm of electronic communications within an industrial enterprise, encompassing communication systems, data networks, and the software infrastructure that underpins these digital channels.

The research subject lies in the identification of unauthorized intruders who infiltrate the electronic communications infrastructure of an industrial enterprise, posing potential threats to the confidentiality, integrity, and availability of sensitive information and operational data.

Analysis of previous studies. The existing literature offers a comprehensive examination of threat identification and countermeasures within the business cybersecurity landscape. For instance, Jamal et al. highlight the vulnerability of industrial networks to high-impact cyberattacks, leading to the implementation of reactive security systems focused on threat detection rather than prevention. They propose a hybrid model that combines convolutional neural networks (CNN) and deep belief networks (DBN) to enhance intrusion detection [1, pp. 13842-13843]. Further, Tsiknas et al. discuss the vulnerabilities in the Industrial Internet of Things (IIoT) due to the interconnectivity and heterogeneity of systems in Industry 4.0 standards. They emphasize the necessity for multilevel security approaches that extend beyond traditional encryption, due to increased complexities and the sophistication of potential cyber threats [2, pp. 181-182]. Both sets of researchers recognize the pressing need for improved cybersecurity measures but note a gap in the current literature concerning the identification of offenders behind cyberattacks. While the importance of safeguarding industrial systems and detecting anomalies is well acknowledged, the methods for tracing the origins of these attacks and identifying the perpetrators are not sufficiently covered. This gap underlines the need for research into forensic techniques and offender attribution methods to enhance the security and resilience of industrial enterprise communications against cyber threats.

Presentation of the main material. Table 1 overviews key threats to industrial enterprise communications, identifies the potential cyber-offenders associated with each threat, and proposes viable counter-measures to address and mitigate these threats.

Table 1

Threats to industrial enterprise communications

#	Threats	Cyber-Offender	Counter-measures
1	Phishing attacks	Hackers impersonating employees	Implement advanced email filtering and staff training
2	Malware distribution	External attackers	Deploy antivirus solutions and regular system updates
3	Insider threats	Disgruntled or negligent employees	Enforce strict access controls and monitor user activity
4	Ransomware attacks	Cybercriminal groups	Backup data regularly and educate on ransomware tactics
5	Denial of Service (DoS) attacks	Competitors or hacktivists	Increase bandwidth and deploy DoS protection systems
6	Data interception and eavesdropping	Industrial spies	Use encryption for data in transit and at rest
7	Unauthorized access through weak authentication	Opportunistic hackers	Implement multi-factor authentication
8	SQL injection attacks on databases	Skilled hackers	Use prepared statements and validate all inputs
9	Zero-day exploits	Advanced persistent threats (APT)	Keep all systems patched and use intrusion detection
10	Manipulation of operational technology	State-sponsored actors	Segregate networks and monitor physical and network access

Source: elaborated by the author

Phishing remains a predominant threat, exploiting human vulnerabilities to gain unauthorized access to sensitive data. Typically executed through deceptive emails that mimic legitimate communications, attackers trick employees into divulging confidential information. The potential cyber-offenders in this scenario are often hackers impersonating employees or trusted partners. To counter this, enterprises should implement advanced email filtering technologies that can detect and block phishing attempts and conduct regular staff training to raise awareness about identifying such deceptive tactics.

Malware, including viruses, worms, and trojans, can disrupt operations, steal sensitive data, or gain unauthorized access to network systems. External attackers, such as cybercriminals looking for financial gain or espionage, often deploy malware. The recommended counter-measure is to deploy robust antivirus solutions across all endpoints and maintain regular updates to system and application software to protect against known vulnerabilities.

Not all threats originate from outside; some are the work of disgruntled or negligent employees within the organization. These insiders can misuse their access to leak or sabotage information. Mitigating such risks requires enforcing strict access controls to limit information access based on roles and continuously monitoring user activity to detect and respond to irregular behavior patterns.

Ransomware encrypts an organization’s data until a ransom is paid. Cybercriminal groups, attracted by financial incentives, commonly perpetrate these attacks. Organizations can counteract these threats by regularly backing up data and ensuring it can be restored quickly and by educating employees on how to recognize and avoid ransomware tactics.

DoS attacks aim to overwhelm systems with traffic, rendering them inoperable and disrupting business operations. Competitors or hacktivists may launch such attacks to damage a business’s reputation or advance a political agenda. Increasing network bandwidth, coupled with the deployment of specialized DoS protection systems, can help mitigate these attacks.

Industrial espionage is a significant threat in competitive sectors, where rivals or spies might intercept communications to gain a competitive advantage. The use of encryption for all data transmitted across networks and stored on devices is crucial for protecting against eavesdropping.

Weak authentication processes allow opportunistic hackers easy access to internal networks. Strengthening security measures through the implementation of multi-factor authentication (MFA) significantly reduces the risk of unauthorized access.

Some attacks involve inserting malicious SQL queries into input fields to manipulate or access the database. Skilled hackers can exploit these vulnerabilities to extract confidential information. Counter-measures include using prepared statements in database queries and validating all user inputs to prevent unauthorized commands from executing.

Zero-day exploits are previously unknown vulnerabilities that hackers exploit before developers have a chance to issue patches. Advanced persistent threats (APTs), which are continuous, stealthy, and sophisticated hacking processes, often use zero-day exploits. Regularly updating and patching systems and employing advanced intrusion detection systems are crucial to defend against such attacks.

Manipulation of operational technology in industries where operational technology (OT) is integrated with IT systems, such as in manufacturing or utilities, the stakes are exceptionally high. State-sponsored actors or highly organized criminal groups may target these systems to disrupt operations or cause physical damage. Segregating networks and monitoring both physical and network access can help protect against these threats.

Table 2 outlines various methods for identifying cyber-offenders in industrial enterprise communications, along with their respective strengths and weaknesses.

Table 2

Methods for identifying cyber-offenders in industrial enterprise communications

#	Method	Strengths	Weaknesses
1	Network Monitoring	Provides real-time analysis and alerts for unusual activities.	Requires significant resources to monitor and manage effectively.
2	Event Log Analysis	Enables detailed tracking of all network activities.	Time-consuming; can be overwhelming due to data volume.
3	Anomaly Detection in User Behavior	Utilizes machine learning to spot deviations from normal behavior.	May generate false positives if not properly tuned.
4	Use of Advanced Protective Systems (Firewalls, IDS)	Offers robust protection against various types of cyber threats.	High setup and maintenance costs.
5	Application of AI and Machine Learning	Can predict and prevent attacks by learning from past data.	Requires extensive training data and computational power.
6	Content Analysis (Textual, Keyword, Image)	Helps identify threatening or suspicious communications.	Context and nuances may be missed, leading to errors.
7	Blockchain Technology	Provides tamper-proof records of transactions and data flows.	Complex to implement and manage; scalability issues.
8	Traffic Monitoring and Analysis	Identifies unusual patterns of data flow and resource use.	Can be invasive and raise privacy concerns.
9	Access Control Systems	Prevents unauthorized access through intelligent authentication.	Can be bypassed if security protocols are not regularly updated.
10	Continuous Technology Improvement	Adapts to evolving cyber threats and incorporates latest defenses.	Ongoing process that requires constant investment and training.

Source: elaborated by the author

Network monitoring stands as a critical first line of defense, offering real-time analysis and alerts to identify unusual activities that may indicate a security breach. The strength of this approach lies in its ability to provide immediate notifications about potential threats, enabling quick responses that could mitigate or prevent damage. However, this method demands substantial resources for effective monitoring and management, including the need for continuous updates and oversight, which can strain organizational resources.

Event log analysis allows organizations to maintain detailed records of all network activities, which are crucial for forensic analysis following a security incident and for preventing future occurrences. The voluminous data generated can be overwhelming and analyzing these logs thoroughly is a time-consuming process that requires specialized skills.

Leveraging machine learning algorithms to detect deviations from normal user behaviors, effectively identifying potential threats from within the organization. Its strength lies in its proactive nature, spotting potential issues before they escalate into serious breaches. However, without precise tuning, this system can generate false positives that may lead to unnecessary alarms and could potentially divert attention from genuine threats.

Implementing advanced protective systems such as firewalls and intrusion detection systems (IDS) provides robust defense mechanisms against a variety of cyber threats. These systems are designed to block unauthorized access and attacks, serving as a sturdy barrier against cyber infiltration. However, they come with high setup and maintenance costs, making them a significant investment.

Artificial intelligence and machine learning are at the forefront of cybersecurity, with the ability to analyze past incidents and predict future threats based on that data. This predictive capability can help prevent attacks before they happen. However, these technologies require substantial training data and significant computational power, which may be beyond the reach of smaller enterprises.

Content analysis involves scrutinizing communications to detect any threatening or suspicious elements. This method is particularly useful in intercepting malicious communications that could lead to data breaches or other security incidents. Its limitation, however, is that it might miss subtleties and contextual nuances, potentially leading to misinterpretations or oversights.

Blockchain offers a secure method of recording transactions and data flows, creating tamper-proof logs that enhance security. Its decentralized nature makes it less susceptible to traditional forms of cyberattacks. Despite these advantages, blockchain technology is complex to implement and can face scalability issues as the network grows.

The monitoring of data flow and resource usage to identify patterns that deviate from the norm, which could indicate cyber threats. While effective, it raises privacy concerns due to its invasive nature, as it involves deep scrutiny of all network traffic, possibly affecting user privacy.

Access control systems prevent unauthorized access through mechanisms that require proper authentication before allowing entry to secure areas of the network. While effective in controlling access, these systems are not infallible; they need constant updates to guard against evolving hacking techniques that might otherwise bypass older security protocols.

Lastly, the continuous improvement of technology is essential in adapting to the rapidly evolving landscape of cyber threats. This method involves regular updates and training, ensuring that the organization’s defenses keep pace with the latest hacking tactics. The primary challenge here is the ongoing commitment of time and resources required to stay current.

Conclusions. Our investigation into the methods for identifying cyber-offenders in the electronic communications of industrial enterprises underscores the critical importance of this domain within modern cybersecurity. As we delved into both existing research and the latest advancements in technology, it became evident that the landscape of cybersecurity is evolving, with the detection and protection against cyber threats presenting increasing challenges. The integration of machine learning techniques, biometric technologies, and user behavior analytics has shown significant potential in enhancing the robustness of cybersecurity measures. These technologies not only aid in the detection of intrusions but also bolster preventive strategies to safeguard against potential cyberattacks.

Список використаних джерел

1. Jamal, M.H., Khan, M.A., Ullah, S., Alshehri, M.S., Almakdi, S., Rashid, U., Alazeb, A., Ahmad, J. (2023). MULTI-STEP ATTACK DETECTION IN INDUSTRIAL NETWORKS

USING A HYBRID DEEP LEARNING ARCHITECTURE. *Mathematical Biosciences and Engineering*, Vol. 20 (8), pp. 13824-13848, doi: https://doi.org/10.3934/mbe.2023615

2. Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. (2021). CYBER THREATS TO INDUSTRIAL IOT: A SURVEY ON ATTACKS AND COUNTERMEASURES. *IoT*, Vol. 2, pp. 163-186, doi: https://doi.org/10.3390/iot2010009

Робота виконана під науковим керівництвом д-ра екон. наук, професора
ТОКАРЯ В.В.

РОЛЬ ТА ЕФЕКТИВНІСТЬ МЕТОДУ ШИФРУВАННЯ AES ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

ЗАДОРОЖНІЙ О.В., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

Стаття вивчає методи шифрування файлів та їх значення в контексті забезпечення безпеки інформації. У ній розкриваються основні принципи шифрування файлів і проводиться дослідження переваг використання програмних рішень для захисту і передачі конфіденційної інформації. Розглядаються найпоширеніші типи методів шифрування, кожен з яких аналізується. Дослідження містить порівняльний аналіз типів шифрування для вибору найбільш ефективного, зокрема, методу шифрування AES (Advanced Encryption Standard) для забезпечення безпеки інформації. Була розроблена та впроваджена модель захисту, заснована на методі шифрування AES (Advanced Encryption Standard), яка є ефективним та надійним засобом захисту конфіденційності даних. Крім того, модель враховує процес генерації та управління ключами, а також обмін ключами між учасниками комунікації з метою забезпечення конфіденційності та цілісності даних.

The article examines file encryption methods and their importance in the context of information security. It reveals the basic principles of file encryption and examines the advantages of using software solutions to protect and transmit confidential information. The most common types of encryption methods are considered, each of which is analyzed. The *study contains a comparative analysis of encryption types to select the most effective one, in particular, the AES (Advanced Encryption Standard*) *encryption method* to *ensure information security*. *A protection model based on the AES (Advanced Encryption Standard*) *encryption method was developed and implemented*, *which is an effective and reliable means of protecting data confidentiality*. *In addition, the model takes into account the process of key generation and management, as well as the exchange of keys between communication participants to ensure the confidentiality and integrity of data.*

Актуальність проблеми. Проблема забезпечення безпеки інформаційних систем є надзвичайно актуальною в сучасному цифровому світі. З поширенням інтернету та зростанням кількості цифрових даних значно збільшилася загроза кібератак і порушення конфіденційності даних. У зв'язку з цим, виникає необхідність в застосуванні надійних методів шифрування для захисту інформації від несанкціонованого доступу.

Роль методу шифрування Advanced Encryption Standard (AES) в цьому контексті вельми важлива. AES є одним із найефективніших і надійних алгоритмів шифрування, що забезпечує високий рівень захисту конфіденційної інформації. Ефективність AES полягає в його складній математичній структурі та стійкості до криптоаналітичних атак. Використання

AES дозволяє ефективно захищати дані на різних рівнях, від персональних комп'ютерів до корпоративних серверів. Одним з ключових аспектів ефективності AES є його широке використання у різних галузях індустрії, включаючи фінанси, медицину, військовість та комерційний сектор. Це свідчить про високу довіру до цього методу шифрування і підкреслює його значення для захисту інформації в сучасному світі.

Отже, метод шифрування AES відіграє важливу роль у забезпеченні безпеки та захисту інформаційних систем, надійно захищаючи конфіденційні дані від потенційних загроз.

Актуальність проблеми шифрування методом AES очевидна в контексті нашої сучасної інформаційної епохи. Зі зростанням обсягу та важливості цифрових даних, які зберігаються та обмінюються, постає серйозна загроза їхньої безпеки. Хакери, кіберзлочинці, шпигуни та інші зловмисники постійно намагаються незаконно отримати доступ до конфіденційної інформації для своїх цілей. Шифрування методом AES, хоч і має свої недоліки, є сильним і надійним алгоритмом, який рекомендований Національним інститутом стандартів і технологій США (NIST). Його високий рівень безпеки робить його ефективним інструментом для захисту конфіденційної інформації від несанкціонованого доступу. Однак потребується постійне вдосконалення та вдосконалення, щоб забезпечити максимальний рівень захисту в умовах постійно зростаючих загроз кібербезпеці.

Актуальність проблеми шифрування файлів стає дедалі важливішою у сучасному цифровому світі. Зі зростанням обсягу та значення цифрових даних постійно зростає ймовірність кібератак та прослуховування, які загрожують конфіденційності та безпеці інформації. Попередні дослідження яскраво демонструють ефективність шифрування файлів як засобу захисту конфіденційної інформації. Область досліджень включає в себе різні аспекти шифрування, такі як методи, алгоритми та програмні продукти, спрямовані на захист даних. Зростаючий обсяг цифрової інформації, що зберігається та обмінюється, робить шифрування файлів критично важливим для забезпечення конфіденційності та безпеки. Навіть при фізичному доступі до пристроїв чи файлів, шифрування забезпечує надійний захист, оскільки дані перетворюються у нерозбірливу форму за допомогою спеціального ключа. Таким чином, шифрування файлів відіграє ключову роль у забезпеченні конфіденційності та безпеки даних у сучасному цифровому середовищі, де захист від несанкціонованого доступу є критично важливим аспектом інформаційної безпеки.

Метою дослідження є аналіз ролі та ефективності методу шифрування AES (Advanced Encryption Standard) у забезпеченні безпеки та захисту інформаційних систем, а також оцінка його впливу на загальний рівень захищеності інформаційних систем.

Предмет дослідження – шифрування методом AES, спрямоване на розробку та оцінку ефективності застосування цього алгоритму в системах зберігання та передачі конфіденційної інформації.

Об'єктом дослідження – методи шифрування, зокрема метод шифрування AES, та їх роль та ефективність у забезпеченні безпеки та захисту інформаційних систем.

Аналіз попередніх досліджень. Досліджено методи шифрування, зокрема їхню ефективність для застосування забезпечення захисту. У своїх роботах науковці вивчили різні варіанти шифрування, враховуючи ключові аспекти, такі як швидкодія, стійкість до злому, доступність, а також відповідність стандартам безпеки. На основі аналізу результатів дослідження виявлено, що метод шифрування AES (Advanced Encryption Standard) видається найбільш підходящим для забезпечення безпеки на підприємстві. Великий внесок в розвиток області шифрування зробили вчені як з України, так і з інших країн. Серед вітчизняних науковців, які присвятили свої дослідження цій темі, варто зазначити Г. Головка, який активно досліджує проблеми кібербезпеки та розробляє нові методи шифрування. Також важливий внесок у цю галузь вніс М. Толочин, який спеціалізується на криптографії та застосуванні сучасних алгоритмів шифрування для захисту інформації. Серед закордонних вчених, які активно досліджували роль та ефективність методу шифрування AES для забезпечення безпеки та захисту інформаційних систем, можна відзначити таких науковців,

як Джоан Дейз, яка є одним із авторів оригінального алгоритму AES, та Вінсент Рід, який працював над дослідженням та покращенням алгоритму. Їхні внески в область криптографії та кібербезпеки виявилися вельми значущими, сприяючи розвитку ефективних методів шифрування та підвищенню рівня захисту інформаційних систем.

Виклад основного матеріалу. Роль та ефективність методу шифрування AES для забезпечення безпеки та захисту інформаційних систем є надзвичайно важливими у сучасному цифровому світі. Advanced Encryption Standard (AES) є одним із найбільш широко використовуваних методів шифрування, що забезпечує високий рівень безпеки для конфіденційної інформації. Роль AES полягає у забезпеченні конфіденційності, цілісності та доступності даних у системах зберігання та передачі інформації. Використання AES дозволяє захистити дані від несанкціонованого доступу та забезпечити їхню цілісність під час передачі через мережі.

Ефективність методу шифрування AES виявляється у його високій стійкості до криптоаналітичних атак, швидкості обробки даних та ефективності ресурсів обчислювальних систем. AES вже довгий час використовується у багатьох сферах, включаючи фінансові установи, урядові організації, медичні системи та комерційні платформи, що свідчить про його успішність та надійність. Таким чином, AES відіграє ключову роль у забезпеченні безпеки та захисту інформаційних систем, і його ефективність переконливо доведена у практиці.

Криптографія – це наука, що вивчає засоби захисту інформації вже понад чотири тисячі років – одночасно з розвитком писемності люди шукали способи зашифрувати написане, приховавши його суть від сторонніх очей. Історії відомо про різні види шифрування ще з античних часів, наприклад, моноалфавітний шифр Цезаря, який використовував принцип зсуву літерних позицій в алфавіті [1].

Аналіз ефективності та застосування типів методу шифрування для забезпечення безпеки інформаційних систем. Оскільки під час шифрування файлів інформація перетворюється на секретний код за допомогою спеціальних методів і унікального ключа, це забезпечує збереження конфіденційних даних. Це як замок на дверях, що захищає те, що знаходиться всередині. Найкращі системи шифрування файлів ще більше ускладнюють доступ до них сторонніх людей. Існують різні способи такого шифрування, що дають змогу забезпечити безпеку ваших важливих речей.

Симетричне шифрування – найпростіший тип шифрування, де для шифрування і розшифрування повідомлення використовується лише один ключ. Це означає, що як відправник, так і отримувач інформації, яку зашифровано симетричним методом, використовують той самий ключ. У відміну від симетричного шифрування, асиметричне шифрування використовує два ключі: ключ шифрування та ключ дешифрування. Це гарантує, що для розшифрування зашифрованих даних відправника потрібно використовувати обидва ключі. Гібридне шифрування комбінує переваги симетричних і асиметричних методів з метою підвищення безпеки та ефективності процесу. У цьому методі дані спочатку шифруються швидким і ефективним симетричним шифруванням. Після цього шифрований текст додатково захищається асиметричним шифруванням перед його відправленням. Хешування – це техніка, яка використовує математичну функцію для перетворення вхідних даних будь–якого розміру на значення фіксованої довжини. Важливо відзначити, що хешування відрізняється від шифрування. У хешуванні відсутній ключ, тому неможливо забезпечити повну конфіденційність. Крім того, хеш можна відтворити. Зазвичай хешування використовується як метод зберігання та пошуку даних разом із криптографією. Воно часто використовується для перевірки документів, цифрових підписів та контролю цілісності даних. Blowfish – це симетричний алгоритм шифрування, спочатку розроблений як альтернатива стандарту шифрування даних (DES). Метод шифрування Blowfish використовує блоки розміром 64 біти і шифрує їх окремо. Цей алгоритм відомий своєю гнучкістю, швидкістю і стійкістю. Крім того, він широко доступний і є суспільним надбанням, що підвищує його привабливість [2].

Порівнюючи Advanced Encryption Standard (AES) з іншими відомими методами шифрування, можна виділити декілька ключових відмінностей. AES відомий своєю високою стійкістю до криптоаналітичних атак, що робить його популярним використанням у багатьох сферах, включаючи фінанси, урядові установи та технологічні компанії. Його ефективність базується на використанні заміни та зсуву байтів, додаткових раундів і підключених ключів. У порівнянні з DES (Data Encryption Standard), AES має значно більшу довжину ключа, що робить його відчутно більш стійким до атак перебору. Також AES ефективніший у використанні обчислювальних ресурсів, що дозволяє йому працювати швидше та ефективніше на сучасних пристроях. У порівнянні з RSA (Rivest-Shamir-Adleman), який базується на асиметричному шифруванні, AES є симетричним шифром, що забезпечує більшу швидкодію та ефективність при шифруванні великих обсягів даних. В цілому, AES відзначається високою швидкодією, стійкістю та ефективністю, що робить його одним з найбільш вживаних методів шифрування в сучасному світі.

Для захисту організації вкрай важливо шифрувати файли, щоб запобігти несанкціонованому доступу до них. Основні причини для цього:

- Захист даних: шифрування гарантує, що конфіденційна інформація залишається конфіденційною та захищеною від несанкціонованого доступу.
- Безпечна комунікація: шифрування дозволяє безпечно обмінюватися конфіденційними даними через мережі та електронну пошту.
- Відповідність: шифрування полегшує дотримання правил конфіденційності, кодуючи та безпечно зберігаючи конфіденційні дані.
- Безпечне зберігання: шифрування запобігає несанкціонованому доступу до даних, що зберігаються на портативних носіях і хмарних платформах.

Щоб забезпечити надійний захист файлів від несанкціонованого доступу, важливо використовувати ефективне програмне забезпечення для шифрування. Перш ніж почати процес шифрування, необхідно обрати файли, які підлягатимуть шифруванню, і встановити відповідні параметри шифрування, такі як алгоритм і довжина ключа. Ключ шифрування є критично важливою складовою у процесі захисту. Важливо створити надійний і складний ключ, а потім зберегти його в безпечному місці, недоступному для несанкціонованих осіб. Регулярне оновлення заходів безпеки, таких як зміна ключа і вдосконалення алгоритмів шифрування, допомагає забезпечити постійний захист ваших даних.

Шифрування дозволяє зберегти конфіденційність і цілісність ваших даних, запобігаючи їхньому несанкціонованому розкриттю або зміні. Правильно налаштовані параметри шифрування дозволяють ефективно захистити важливу інформацію від потенційних загроз та зберегти спокій і впевненість у безпеці даних. Значення AES вивчення ефективності та застосування методів шифрування для забезпечення безпеки файлів у різних галузях AES – це симетричний алгоритм шифрування, що використовується для захисту даних від несанкціонованого доступу. Він був визнаний Національним інститутом стандартів і технологій (NIST) США як стандарт шифрування даних у 2001 році. AES використовується в широкому спектрі галузей для забезпечення безпеки файлів: урядові та військові організації, захисту секретної інформації, такої як військові таємниці або дипломатичні переговори, для захисту фінансових даних, таких як номери кредитних карток або банківські реквізити, захисту пацієнтських даних, таких як записи про історію хвороби або результати тестів, конфіденційної інформації. Важливо постійно вивчати та вдосконалювати методи шифрування, щоб йти в ногу з еволюцією криптоаналітичних атак [3].

Алгоритм шифрування Advanced Encryption Standard (AES) включає в себе послідовність кроків, які детально визначаються та виконуються під час процесу шифрування. Ця послідовність кроків включає в себе такі операції, як SubBytes, ShiftRows, MixColumns та AddRoundKey. Кожен крок має свою важливу роль у забезпеченні надійності та стійкості шифрування, а також впливає на кінцевий результат захищеної інформації.

Операція SubBytes включає заміну кожного байта в блоку на відповідний байт з таблиці заміни (S-box), що додає різноманітність і запобігає простим шаблонним атакам.

ShiftRows виконує циклічний зсув байтів у рядках, що допомагає розподілити дані по блоку більш рівномірно. Операція MixColumns змішує стовпці блоку за допомогою матричного множення, що сприяє додатковому перетворенню даних. Нарешті, AddRoundKey включає додавання ключа раунду до блоку даних, що забезпечує кінцеве шифрування.

Останній раунд виконується окремо і включає лише додавання ключа раунду до даних. Цей процес забезпечує надійний рівень захисту даних, але для ефективного використання алгоритму необхідно правильно керувати ключем шифрування та враховувати потенційні криптоаналітичні атаки.

Крім того, вчені постійно працюють над розробкою нових алгоритмів шифрування, які є ще більш стійкими до різних видів криптоаналітичних атак. Вони вдосконалюють існуючі методи та створюють нові шифри з урахуванням сучасних вимог до безпеки. Провідні дослідники інформаційної безпеки постійно аналізують потенційні вразливості і пропонують вдосконалення, щоб забезпечити надійний захист від потенційних загроз.

Принцип роботи алгоритму AES (Рис. 1) включає в себе здійснення цих кроків відповідно до заданих параметрів шифрування. Кожен крок обробки даних має свою унікальну функцію та сприяє створенню надійного криптографічного захисту.

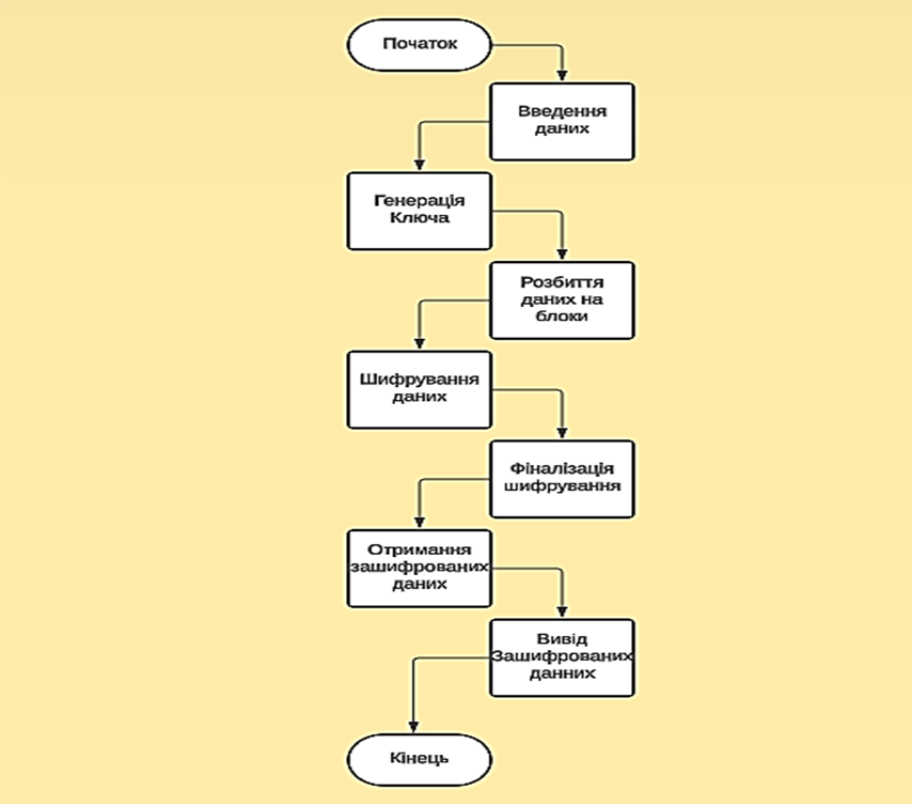


Рис. 1. Принцип виконання алгоритму шифрування AES

Джерело: розроблено автором в середовищі lucid (знімок з екрану)

Як наслідок, загрози безпеці даних відносно швидко зросли, а підприємства стали основними мішенями. Це створює прецедент для балансу між доступністю, простотою використання та безпекою даних, що дозволяє їм здійснювати щоденні операції, забезпечуючи при цьому конфіденційність чутливих даних. Компанії повинні забезпечити безперебійне виконання своїх щоденних операцій, гарантуючи при цьому конфіденційність даних. Для вирішення цього завдання був розроблений Advanced Encryption Standard (AES) – алгоритм шифрування, який став стандартом де–факто для захисту електронних даних [4].

Для поліпшення ефективності та продуктивності шифру AES розглядалися та висунулися пропозиції: використання апаратного шифрування може значно підвищити

ефективність методу AES за рахунок оптимізації обчислювальних операцій, що виконуються на апаратному рівні. Це досягається за допомогою спеціалізованих пристроїв, таких як шифрувальні прискорювачі або спеціалізовані чіпи, які здатні виконувати операції шифрування та дешифрування набагато швидше, ніж загальнопризначені процесори. Це особливо важливо для сучасних систем, які вимагають високої швидкодії та ефективності обробки даних в реальному часі. Режими шифрування, такі як CBC (Cipher Block Chaining), CTR (Counter), GCM (Galois/Counter Mode) та інші, визначають спосіб, яким вхідні дані поділяються на блоки та як кожен блок обробляється. Кожен режим має свої особливості та переваги. Наприклад, режим CBC використовує попередній блок шифротексту як частину вхідних даних для шифрування наступного блоку, що робить його вразливим до атак на зміну даних. У той же час, режим CTR використовує лічильник для створення унікального шифротексту для кожного блоку, що робить його менш вразливим до певних видів атак. Вибір оптимального режиму шифрування залежить від конкретних вимог до безпеки та функціональності системи.

Модель захисту шифрування AES включає в себе вибір ключа шифрування, процес шифрування та розшифрування даних, керування доступом, моніторинг та аудит безпеки, а також застосування шифрування на різних рівнях системи. Ця модель спрямована на забезпечення безпеки та конфіденційності даних шляхом застосування алгоритму AES. Основною метою моделі є захист конфіденційної інформації від несанкціонованого доступу та забезпечення безпеки інформаційних систем. Це досягається шляхом встановлення механізмів керування доступом, вибору відповідного ключа шифрування, а також застосування процедур моніторингу та аудиту безпеки. Такий підхід дозволяє ефективно захищати конфіденційні дані та забезпечувати їхню цілісність в сучасних інформаційних системах.

Для більш детального розуміння як має працювати метод шифрування AES, було розроблено модель (Рис.2.).

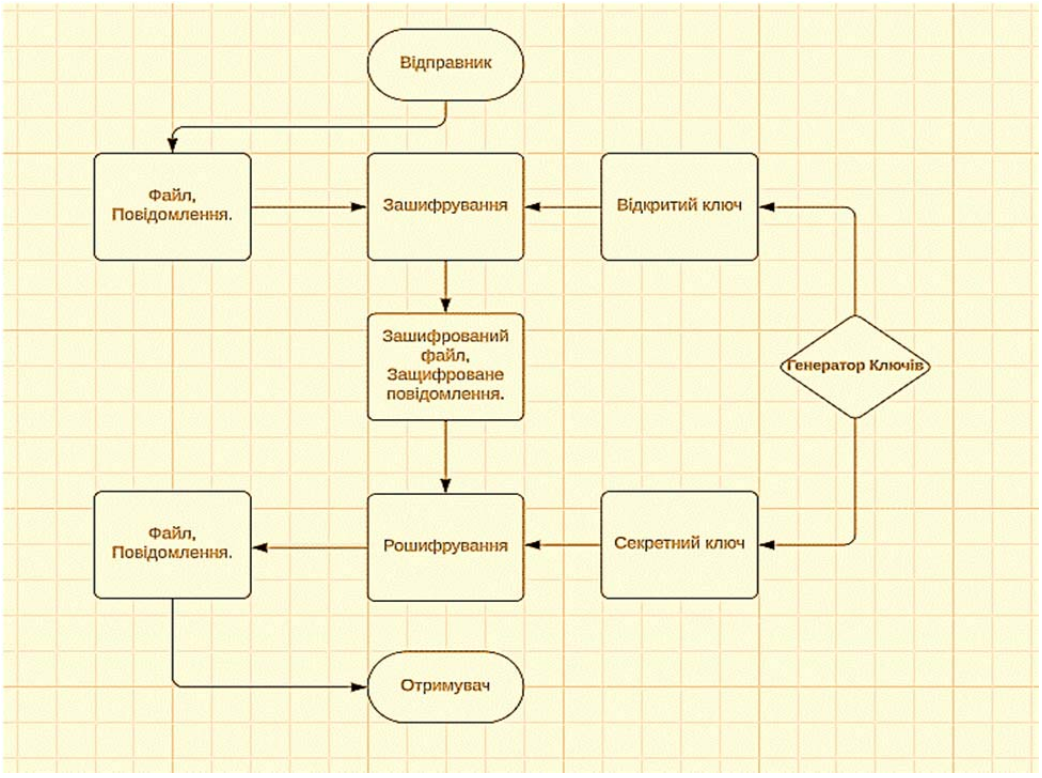


Рис. 2. Модель захисту шифрування AES

Джерело: розроблено автором в середовищі lucid (знімок з екрану)

Як наведено на рисунку одним з ключових факторів який повинна мати програмна розробка для шифрування та дешифрування є – генератор ключів. Генератор ключів – це інструмент, що використовується для створення криптографічних ключів, які використовуються при шифруванні та дешифруванні даних. Криптографічні ключі визначаються як випадкові або псевдовипадкові послідовності бітів і використовуються для захисту конфіденційності, цілісності та автентичності даних. Завдяки цьому відправник вибирає файл який хоче зашифрувати копіює повний шлях до файлу та вставляє його в командний рядок з допомогою аргумента. Повний шлях та вся назва разом з форматом файлу це той необхідний мінімум. Після цього відбувається шифрування. Користувач який не знає секретний ключ не зможе отримати данні які були зашифровані, через те, що процес шифрування перетворює звичайний текст зрозумілий для людини, в незрозумілий для читача шифротекст.

Однак, шифрування – це не тільки про перетворення даних у незрозумілу форму, але також і про забезпечення захищеності цієї інформації від несанкціонованого доступу. Ключ визначає, як саме дані будуть перетворені під час шифрування і яким чином вони можуть бути відновлені під час дешифрування. Тому без ключа неможливо відновити початковий текст і зрозуміти зашифровану інформацію. Для дешифрування файлу потрібно мати доступ до правильного ключа або пароля, який був використаний для його шифрування. Вказати файл, який потрібно розшифрувати, у програмі для дешифрування. Під час процесу дешифрування потрібно буде вказати ключ або пароль, який був використаний для зашифрування файлу. Ввести ключ чи пароль у відповідне поле. Якщо ж пароль правильний то почнеться дешифровка файлу чи тексту, якщо ж не правильний програма чи командний рядок покаже помилку що пароль був введено не коректно. Важливою частиною є правильність введеного ключа або пароля [5].

Висновки. Метод шифрування Advanced Encryption Standard (AES) відіграє ключову роль у забезпеченні безпеки інформаційних систем шляхом застосування симетричного блочного шифрування. Ефективність AES базується на його надійності та стійкості, що дозволяє ефективно захищати конфіденційні дані від несанкціонованого доступу. Завдяки використанню складних математичних операцій і правильному використанню ключів шифрування, AES став одним із найпопулярніших і найбільш безпечних методів шифрування у світі.

Принцип роботи алгоритму AES полягає в поділі вхідних даних на фіксовані блоки та їх подальшому обробленні у послідовності шифрувальних раундів. Кожен раунд включає такі операції, як SubBytes (заміна байтів), ShiftRows (циклічний зсув байтів у рядках), MixColumns (змішування стовпців) та AddRoundKey (додавання ключа раунду). Останній раунд виконується окремо і включає лише додавання ключа раунду до даних.

У зв’язку з постійним розвитком кіберзагроз та криптографічних атак, вчені постійно вдосконалюють алгоритми шифрування. Зокрема, проводяться дослідження з метою розробки нових алгоритмів, які були більш стійкими до атак і забезпечували б вищий рівень безпеки. Однак на сьогоднішній день AES залишається одним з найефективніших і надійних методів шифрування, який широко використовується у різних галузях, включаючи фінанси, медицину, військовість та комерційний сектор.

Підсумовуючи, метод шифрування AES відіграє важливу роль у забезпеченні безпеки інформаційних систем, надійно захищаючи конфіденційні дані від несанкціонованого доступу. Його ефективність та стійкість роблять його найкращим вибором для захисту інформації у цифровому світі.

Список використаних джерел

4. Матеріали Української софтверної IT компанія «SIM–NETWORKS» // Режим доступу: https://www.sim–networks.com/ukr/blog/data–encryption–best–practices (останнє звернення 27.03.2024р.)

5. Шифрування: типи і алгоритми. https://hostpro.ua/wiki/ua/security/encryption–types–algorithms (останнє звернення 27.03.2024р.)
6. Матеріали IT компанія «KINGSTON» // Режим доступу: https://www.kingston.com/ua/blog/data–security/what–is–encryption (останнє звернення 27.03.2024р.)
7. У чому особливості AES? // Режим доступу: https://nordlayer.com/blog/aes–encryption (останнє звернення 31.03.2024р.)
8. ПРАКТИЧНЕ ЗАСТОСУВАННЯ МЕТОДА ШИФРУВАННЯ AES // Режим доступу: https://journals.nupp.edu.ua/sunz/article/view/2756?articlesBySameAuthorPage=2 (останнє звернення 29.03.2024р.)

Робота виконана під науковим керівництвом PhD, старшого викладача
КОСТЮК Ю.В.

АНАЛІЗ ТА ОЦІНКА МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

ЗБІЦЬКА К.О., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто основні засади та функціонування методів криптографічного захисту електронного голосування. Визначено переваги та недоліки описаних методів шифрування. Описано актуальність та новизна запропонованих методів шифрування електронного голосування.

The article examines the basic principles and functioning of methods of cryptographic protection of electronic voting. The advantages and disadvantages of the described encryption methods are determined. The relevance and novelty of the proposed methods of spreading electronic voting are described.

Актуальність: Голосування є важливим атрибутом волевиявлення народу в демократичній державі, що також відіграє ключову роль у формуванні та функціонуванні суспільства. За останні роки збільшилося використання дистанційних технологій. Це стосується і впровадження «електронної демократії» та «електронного врядування». Для того, щоб у виборців була можливість віддалено голосувати, маючи сучасні інформаційні технології, необхідно забезпечити захист голосів при «електронному голосуванні», що останнім часом набирає все більше популярності.

Електроне голосування може охоплювати в собі декілька варіантів голосування, серед яких є безпосереднє голосування за допомогою електронних пристроїв, а також можливість застосування технічних засобів для автоматичного підрахунку голосів, що дозволяє набагато швидше ввести підрахунок голосів, знижуючи ризик впливу людського фактору.

Електронне голосування стає все більш популярним, оскільки допомагає уникнути різних видів шахрайства, таких як підробка голосів, маніпулювання результатами голосування та інших видів атак на систему очного голосування. Крім того, можливість електронного голосування надає шанс будь-кому, хто на момент голосування досяг віку вісімнадцяти років, віддати свій голос у прийняті важливих для населення рішень, таких як вплив на політичні та суспільні рішення за рахунок вибору представників та підтримка або відхилення конкретних ініціатив.

Метою статті є аналіз та порівняння криптографічних методів шифрування електронного голосування з метою покращення їхнього захисту.

Об'єктом дослідження статті є сам процес електронного голосування, його системи та протоколи, що використовуються, а також криптографічні алгоритми та методи, призначені для забезпечення безпеки та конфіденційності голосів та даних в електронному голосуванні.

Предметом дослідження статті є методи криптографічного захисту електронного голосування.

Аналіз попередніх досліджень. Досліджено та проаналізовано роботи видатного криптографа Девіда Чаума (що розробив протоколи електронного голосування, зокрема, «Direct Recording Electronic» (DRE) та «End-to-End Verifiable Voting Systems», що забезпечують високий рівень безпеки та конфіденційності в електронному голосуванні), а також роботи Рональда Ріверса (що вніс свій вклад в розробку алгоритм RSA для шифрування та підпису даних, а також досліджував питання криптографічного захисту електронного голосування).

Виклад основного матеріалу. Забезпечення цілісності та конфіденційності голосів при голосуванні є запорукою захищеності та довіри громадян. Захист голосів при електронному голосуванні вимагає більшої надійності, оскільки при неправильному захисті може бути порушена система голосування, а також підрахунку голосів. Вони можуть буть підроблені, викрадені, видалені, що призведе до неправильного оприлюднення результатів і як наслідки – буде прийнято неправильне рішення.

В першу чергу, для захисту кожної електронної структури необхідно використовувати шифрування даних. Таким чином, можна забезпечити конфіденційність даних, проте, кожне таке шифрування вимагає необхідного дешифрування. Серед існуючих методів електронного шифрування можна провести аналіз гомоморфного шифрування, що являє собою криптографічний метод, який дозволяє виконувати обчислення із зашифрованими даними без необхідності дешифрування [1]. Для електронного голосування це може означати, що усі дані, які будуть внесені в систему, не потребують розшифрування в кінці, наприклад, при підрахунку голосів, тим самим забезпечуючи їх надійність при зберіганні та прозорість і безпеку при самому голосуванні.

Додаткову безпеку в цьому методі може забезпечити залучення алгоритмів штучного інтелекту (ШІ), як показано на рисунку 1. Ця гарантована конфіденційність даних може надати великій групі людей впевненість і безпеку, що необхідні для обміну своїми даними з проектами штучного інтелекту, надаючи величезні обсяги необроблених даних, необхідних для запуску алгоритмів ШІ, які мають вплив у реальному світі [1].

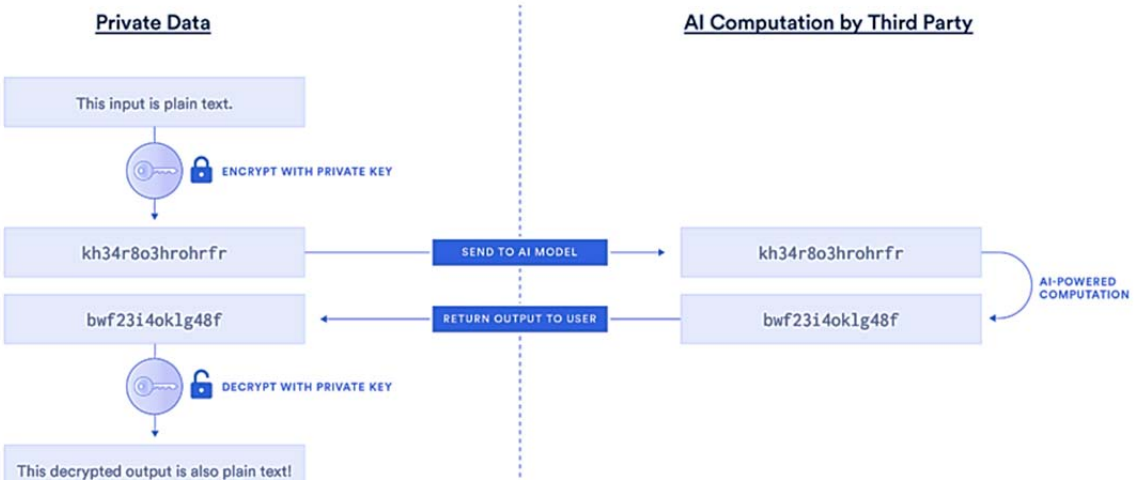


Рис. 1. Обчислення алгоритмів ШІ з використанням гомоморфного шифрування

Джерело: [2]

Говорячи про алгоритми криптографічного захисту електронного голосування, можна виділити алгоритм Zero-Knowledge Proof, що перекладається як доведення з нульовим розголошенням.

Доведення з нульовим розголошенням (ZKP) – це криптографічна технологія, що дозволяє перевіряти достовірність частини інформації без розкриття самої інформації [2]. Така технологія займає особливе місце у криптографії та blockchain для підвищення конфіденційності та безпеки.

Довіра з нульовим розголошенням має містити в собі три основні критерія – обґрунтованість, статистична повнота та нульове розголошення. В реалізації такого методу до електронного голосування це можна інтерпретувати таким чином, що обґрунтованість може бути досягнута, наприклад, шляхом представлення доказу про право виборців голосувати без розкриття своїх особистих даних або що голосування було виконано правильно, тобто голос був зарахований до відповідного кандидата, і це підтверджується без розкриття самого голосу. Другий критерій відповідає за повноту наданої інформації, що може бути досягнуто через використання великої кількості тестових ситуацій або голосів для перевірки правильності роботи системи. За допомогою ZKP можна перевірити, чи зараховані голоси відповідають очікуваній статистичній моделі без розголошення інформації про окремі голоси або виборців. Останній третій критерій відповідає за нульове розголошення, тобто, де можна довести достовірність голосування без розкриття інформації про те, за кого або як саме голосували окремі виборці [3].

Оскільки результатом голосування є великі обсяги даних, то їх можна зобразити за допомогою дерева Меркла. Воно створено для того, щоб організувати та структурувати великі обсяги даних та полегшити роботу системи. Деревоподібна структура Меркла забезпечує доступний запис транзакцій у блоці, таким чином, дуже просто перевірити, чи були дані в блоці змінені або підроблені. Це працює саме так, тому що будь-яка зміна транзакції (або будь-яких інших пов’язаних даних) у дереві Меркла призведе до іншого відповідного кореня Меркла [4].

Ефективність використання дерева Меркла пояснюється при аналізі зображень на рисунку 2. Ціль такого методу полягає в тому, щоб за допомогою хешування, що являє собою перетворення даних довільної форми та розміру в один рядок, можна зменшити об’єм використаного місця. Дані об’єднуються в хеші, два отримані результати об’єднуються і знову хешуються. Цей цикл повторюється до тих пір, доки не залишиться лише один рядок. Такий метод дозволить довести, що голос певного виборця був внесений до великого обсягу даних.

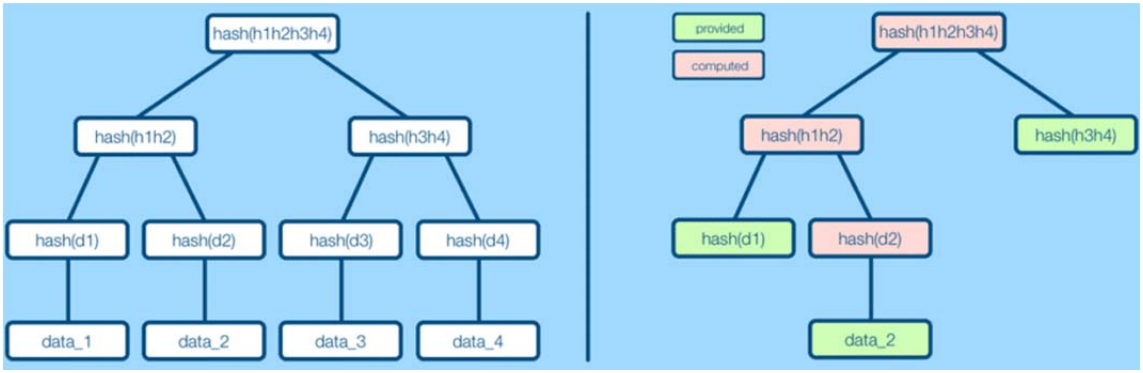


Рис. 2. Дерево Меркла

Джерело: Розроблено автором (знімок з екрану)

Додатковим методом захисту електронних голосів може стати метод MixNet. MixNet – це скорочення від Mix Network, технології, яка допомагає зберігати конфіденційність і безпеку інформації, що надсилається через Інтернет. Це робиться шляхом змішування даних з різних джерел перед тим, як відправити їх до місця призначення, що ускладнює пошук джерела та призначення даних стороннім особам [5].

Використання такого методу може визначати наступні переваги:

- конфіденційність;
- анонімність;
- спільний доступ;
- операції.

MixNet застосовує протоколи, які змішують і перемішують дані з різних джерел, надсилаючи їх через мережу взаємопов'язаних вузлів. Він поєднує такі метадані, як географічне розташування, IP-адреси відправника та отримувача, розмір повідомлення та час надсилання та отримання. Через це стороннім особам важко отримати будь-яку значущу інформацію, яка могла б допомогти розкрити особи користувачів або передбачити вміст даних [5].

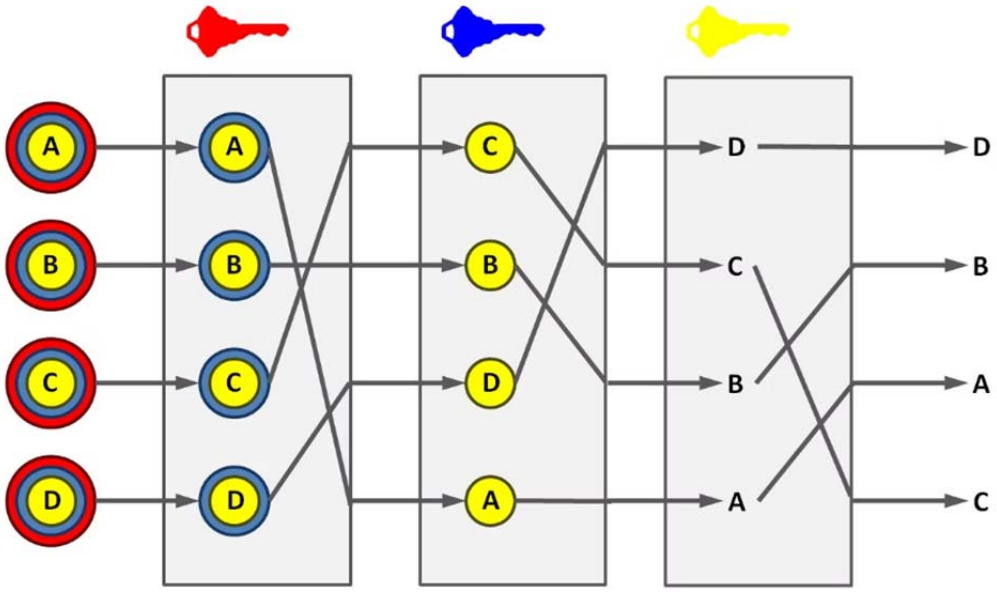


Рис. 3. Алгоритм використання методу MixNet

Джерело: [5]

Застосування методу blockchain ще не набуло великої популярності в електронному голосуванні, але такі перспективи можуть бути значущі в забезпеченні цілісності та конфіденційності голосів виборців.

Перевагами використання технології blockchain є те, що вона являє собою ланцюг пов'язаних боків, кожен з яких містить в собі інформацію та час, коли вона була додана або змінена, що робить її прозорою до всіх змін, в тому числі і до несанкціонованих.

Структура методу blockchain можна зобразити за схемою, що зображено на рисунку 4.

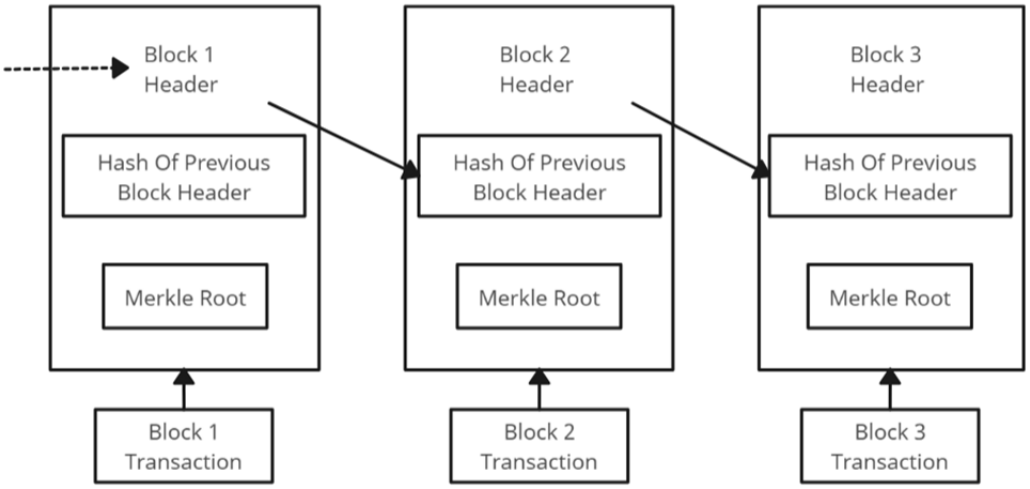


Рис. 4. Структура методу blockchain

Джерело: Створено автором (знімок з екрану)

Але якщо все ж таки виникла така ситуація, що при перевірці голосів було виявлено про стороннє вторгнення та зміну блоків, для подальшого запобігання подібних ситуацій можна використати алгоритми proof-of-work, proof-of-stake та proof-of-elapsed-time, які дозволяють обмежити неконтрольований випуск та підробку блоків (за умови що більш ніж половина мережі утворена доброчесними вузлами), що значно ускладнює проведення атак на сховище такого типу [6].

Порівняльна характеристика та оцінка методів криптографічного захисту, їх переваги та недоліки зазначені в Таблиці 1 та Таблиці 2.

Таблиця 1

Переваги та недоліки криптографічних методів захисту в електронному голосуванні

№	Назва методу	Переваги	Недоліки
1	Гомоморфне шифрування	• Інтегрітет голосів; • конфіденційність; • довіра до системи.	• Вразливість до атак; • велика обчислювальна потужність; • складність реалізації.
2	Zero-Knowledge Proof	• Конфіденційність; • захист від фальсифікації; • простота використання.	• Складність реалізації; • обчислювальні витрати; • можливість неправильної інтерпретації.
3	Mix Network	• Конфіденційність; • відсутність централізованого контролю.	• Високі витрати; • передача даних затримок; • можливість атак.
4	Blockchain технологія	• Довіра та прозорість; • зниження витрат і часу; • можливість голосувати з будь-якого місця.	• Технічні проблеми; • можливість атак; • важкість впровадження.

Таблиця 2

Порівняння та оцінка методів криптографічного захисту в електронному голосуванні

№	Назва методу	Ефективність	Безпека	Масштабованість	Витрати на реалізацію
1	Гомоморфне шифрування	Висока	Висока	Середня	Високі
2	Zero-Knowledge Proof	Висока	Висока	Середня	Висока
3	Mix Network	Середня	Висока	Середня	Висока
4	Blockchain технологія	Висока	Висока	Висока	Середня

В результаті аналізу даних з таблиць можна зробити висновок, що кожен з цих методів забезпечує надійність голосів виборців та збереження даних, але вони також вразливі до різних типів атак. Проте, blockchain має найвищі показники серед описаних методів, що забезпечує надійність, ефективність та доцільно для роботи з великою кількістю даних, також, на відміну від інших методів, blockchain технологія відносно не затратна у реалізації.

Враховуючи вищевикладене, можна зробити висновок, що використання кожного з цих методів окремо не гарантує стовідсоткової надійності, тому доцільно поєднати декілька методів, наприклад, використання технології blockchain та гомоморфного шифрування, оскільки їх показники є найвищими, крім того, ці методи взаємодоповнюють та компенсують можливості один одного. Такий варіант захисту може забезпечити додаткову надійність тим, що голоси виборців будуть зашифровані до моменту оприлюднення голосів і розташовуватися у блоках, які пов'язані один з одним, що робить втручання неавторизованих користувачів в систему помітним і тим самим попереджає витік конфіденційної інформації до третіх осіб.

Висновки. Впровадження системи електронного голосування являє собою новий напрямок в електронних технологіях, оскільки в реаліях сьогодення не кожна людина може самостійно бути присутня на голосуванні очно. Саме голосування є важливим етапом при волевиявленні виборців, оскільки це допомагає кожній особі, що на момент голосування досягла вісімнадцятирічного віку, зробити свій внесок в прийняті важливих рішень та впроваджень для народу та країни в цілому.

Кожен внесений голос має бути анонімним та захищеним, особливо, коли це стосується голосування в електронному середовищі. Захищати також треба не тільки голоси, а ще й дані користувачів, при авторизації в системі.

Серед методів криптографічного захисту електронного захисту показали ефективність застосування гомоморфне шифрування голосів виборців, використання алгоритму доведення з нульовим розголошенням, застосування технології MixNet, що забезпечує додаткову надійність голосів за рахунок шифрування та перемішування.

Одним з методів криптографічного захисту, що ще не здобув значного визнання, але має високі переваги у використанні є залучення технології blockchain. Головна особливість цього методу є те, що кожен голос, внесений користувачем, записаний в спеціальний блок, що пов'язаний з усіма попередніми та майбутніми блоками і кожна несанкціонована зміна не буде непоміченою.

Неможливо надати гарантію стовідсоткового захисту для голосів в електронному голосуванні, але краще подбати про захист завчасно, проаналізувавши усі можливі варіанти шахрайських дій, та надати якомога більшу гарантію захисту.

Список використаних джерел

1. Homomorphic Encryption. – URL: https://chain.link/education-hub/homomorphic-encryption
2. Все про технологію доведення з нульовим розголошенням і її вплив на блокчейн. – URL: https://academy.binance.com/uk/articles/what-is-zero-knowledge-proof-and-how-does-it-impact-blockchain
3. Доведення з нульовим розголошенням (ZKP): як це працює і чому це важливо. – URL: https://medium.com/@kyivskiicryptan/BE-1581b67634e9
4. Дерево Меркла. – URL: https://academy.binance.com/uk/glossary/merkle-tree
5. What Is a MixNet and How Does It Work? – URL: https://www.makeuseof.com/what-is-a-mixnet
6. Burmaka Ivan, et al. Proof of Stake for Blockchain Based Distributed Intrusion Detecting System. In: International scientific-practical conference. Springer, Cham, 2020. P. 237–247.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т.В.

АНАЛІЗ МЕТОДІВ І СТРАТЕГІЙ ЗАХИСТУ ГЕЙМЕРСЬКИХ ОБЛІКОВИХ ЗАПИСІВ ТА ІГРОВИХ ДАНИХ У ВЕБЗАСТОСУНКАХ ОНЛАЙН-ГРИ

КІР'ЯКОВ Г.Д., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто різноманітні методи та стратегії захисту геймерських облікових записів та ігрових даних у веб-застосунках онлайн-гри. Розглянуті підходи до захисту, включаючи використання паролів, двофакторної автентифікації, шифрування даних та інші методи, спрямовані на забезпечення безпеки та конфіденційності користувачів у віртуальному ігровому середовищі.

The article discusses various methods and strategies for protecting gamer accounts and game data in online game web applications. Various security approaches are considered, including the use of passwords, two-factor authentication, data encryption, and other methods aimed at ensuring the safety and privacy of users in a virtual gaming environment.

Актуальність: Віртуальні ігри стають все більш популярними на теперішній час, залучаючи мільйони користувачів по всьому світу. Разом з цим зростає інтерес до захисту геймерських облікових записів та ігрових даних у веб-застосунках онлайн-гри.

Геймерські облікові записи часто містять значну кількість особистої інформації, такої як ім'я, адреса електронної пошти, платіжні дані та інше, і вони стають предметом інтересу для кіберзлочинців, які можуть намагатися використовувати ці дані для своїх цілей. Тому забезпечення безпеки цих облікових записів стає вельми важливим завданням для розробників і операторів ігрових платформ. Отже, на сьогоднішній день існує велика потреба у вивченні та розробці ефективних стратегій, які забезпечать надійний захист геймерських облікових записів та особистих даних гравців.

Забезпечення безпеки геймерських облікових записів та ігрових даних є важливою задачею для розробників веб-застосунків онлайн-гри та операторів ігрових платформ. У зв'язку з цим виникає необхідність у вивченні та аналізі різних методів та стратегій, які дозволять ефективно захистити користувачів від потенційних кіберзагроз.

У роботі розглянуто різноманітні підходи до захисту геймерських облікових записів та ігрових даних у веб-застосунках онлайн-гри. Зокрема, акцентується увага на таких аспектах, як використання паролів, двофакторна автентифікація, моніторинг активності користувачів, шифрування даних та інші методи, спрямовані на забезпечення безпеки та конфіденційності віртуальних гравців.

Метою статті є аналіз методів і стратегій захисту геймерських облікових записів та ігрових даних у веб-застосунках онлайн-гри з метою виявлення ефективних підходів до захисту цих даних від несанкціонованого доступу, крадіжок та інших кіберзагроз.

Об'єктом дослідження статті є геймерські облікові записи та ігрові дані у веб-застосунках онлайн-гри. Це включає в себе не лише облікові записи користувачів та їхні дані, а й інші важливі елементи інфраструктури онлайн-ігор, такі як сервери гри, бази даних і тому подібне.

Предметом дослідження статті є методи і стратегії захисту геймерських облікових записів та ігрових даних у веб-застосунках онлайн-гри. Це включає в себе розгляд різних аспектів захисту, таких як використання паролів, двофакторної автентифікації, шифрування даних, моніторинг активності користувачів та інші техніки та підходи до забезпечення безпеки в онлайн-іграх.

Аналіз попередніх досліджень. Дослідження з теми захисту геймерських облікових записів та ігрових даних у веб-застосунках онлайн-гри виявляють значний інтерес до цієї проблематики в кількох наукових галузях, таких як кібербезпека, інформаційна безпека та інформаційні технології. Дослідження проводилися як університетами, так і приватними компаніями, зокрема, виробниками ігрових платформ та іншими зацікавленими сторонами. Серед робіт та науковців, які можна виокремити, слід звернути увагу на роботу Майкла Девіса «Підвищення безпеки онлайн-ігор за допомогою двофакторної аутентифікації», а також на роботу Алана Джексона «Захист приватності для онлайн-гравців: комплексний підхід». Ці та інші науковці зробили значний внесок у розвиток наукового дослідження з питань кібербезпеки та захисту особистих даних у веб-застосунках онлайн-гри.

Виклад основного матеріалу. Аналіз методів і стратегій захисту геймерських облікових записів та ігрових даних у веб-застосунках онлайн-гри виявляє важливість та актуальність цієї проблематики в сучасному цифровому світі. Оскільки онлайн-ігри зростають у популярності, захист особистих даних гравців та їхніх облікових записів стає надзвичайно важливим завданням для розробників веб-застосунків та операторів ігрових платформ.

Одним із важливих та ключових методів захисту є використання сильних паролів та механізмів аутентифікації, таких як двофакторна аутентифікація. Якщо брати до уваги ці методи в більш детальному плані, то головними аспектами при створені сильного пароля для захисту геймерських облікових записів та ігрових даних у веб-застосунках онлайн-гри є:

- Довжина та складність. Рекомендується використовувати комбінацію великих та малих літер, цифр та спеціальних символів. Чим більше символів та різноманітніший їхній набір, тим складніше пароль для вгадування.
- Унікальність. Важливо, щоб пароль був унікальним для кожного облікового запису. Використання одного й того ж паролю для кількох сервісів збільшує ризик компрометації даних, оскільки вразливість у одному сервісі може призвести до доступу до інших.
- Автоматизовані інструменти. Для створення та керування сильними паролями можна скористатися спеціальними програмами або вбудованими менеджерами паролів, які генерують та зберігають паролі в зашифрованому вигляді.

На рисунку 1 наведено необхідний час для зламу зловмисником паролю в залежності від його складності та довжини.

кількість символів	містить тільки цифри	малі літери	великі і малі літери	цифри, великі і малі літери	цифри, великі і малі літери, символи
4	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
5	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
6	Миттєво	Миттєво	Миттєво	1 сек	5 сек
7	Миттєво	Миттєво	25 сек	1 хвилина	6 хвилин
8	Миттєво	5 сек	22 хвилини	1 година	8 годин
9	Миттєво	2 хвилини	19 годин	3 дні	3 тижні
10	Миттєво	58 хвилин	1 місяць	7 місяців	5 років
11	2 сек	1 день	5 років	41 рік	400 років
12	25 сек	3 тижні	300 років	2л років	34к років
13	4 хвилини	1 рік	16к років	100к років	2млн років
14	41 хвилина	51 рік	800к років	9млн років	200млн років
15	6 годин	1к років	43млн років	600млн років	15млрд років
16	2 дні	34к років	2млрд років	37млрд років	1трлн років
17	4 тижні	800к років	100млрд років	2трлн років	93трлн років
18	9 місяців	23млн років	6трлн років	100трлн років	7квадрильйонів

Рис. 1. Час зламу пароля

Джерело: [1]

У випадку двофакторної аутентифікації додаткового захисту можна досягти, використовуючи методи, що описані нижче:

- Другий рівень захисту. 2FA вимагає введення додаткового коду або підтвердження через інший канал після введення паролю. Це додає додатковий шар безпеки, оскільки крім чого, що знає користувач (пароль), він також повинен мати доступ до чогось, що він має (наприклад, мобільний телефон або ключ безпеки).
- Використання мобільних додатків або SMS. Зазвичай 2FA здійснюється через мобільний додаток аутентифікації або через SMS-повідомлення з одноразовим кодом. Користувач вводить цей код після введення паролю для підтвердження своєї особи.
- Фізичні пристрої аутентифікації. Деякі сервіси пропонують використання фізичних пристроїв, таких як ключі безпеки або апаратні аутентифікатори, які генерують унікальні коди аутентифікації.

Іншим важливим аспектом є моніторинг активності користувачів та виявлення підозрілих дій. Система моніторингу геймерських облікових записів та ігрових даних відіграє ключову роль у забезпеченні безпеки та захисту інформації у світі онлайн-ігор. Основна мета цієї системи полягає у виявленні можливих загроз безпеці та запобіганні їх негативним наслідкам.

Однією з основних її функцій є виявлення несправностей та аномалій у поведінці облікових записів та ігрових активностей. Це включає виявлення несподіваних дій, таких як доступ до облікового запису з незвичних місць або пристроїв, а також раптові зміни у поведінці гравців.

Крім того, система проводить аналіз поведінки користувачів з метою виявлення змін, які можуть свідчити про можливі порушення безпеки або несанкціонований доступ. Це допомагає вчасно реагувати на потенційні загрози та запобігати можливим атакам. Вона також відповідає за виявлення спроб шахраїв та атак. Система моніторить активність гравців і виявляє будь-які спроби використання недозволених програм або порушень правил гри, що може завдати шкоди ігровому середовищу та досвіду користувачів.

Нарешті, завдяки моніторингу активності користувачів забезпечується аудит та звітність, створюючи детальні звіти про активність облікових записів та ігрових даних. Це дозволяє проводити аналіз і вдосконалювати систему безпеки для забезпечення ще більш ефективного захисту в майбутньому.

Зважаючи на потребу моніторингу активності користувачів у веб-грі, кілька інструментів можуть бути використані для цієї мети. Один із таких інструментів – Google Analytics (рис. 2), що відомий своєю широкою функціональністю та можливістю надавати докладну аналітику взаємодії користувачів з грою. За допомогою інструментів аналітики можна виявити зміни у поведінці користувачів, які можуть свідчити про можливі проблеми безпеки, такі як спроби вторгнення або шахрайство.

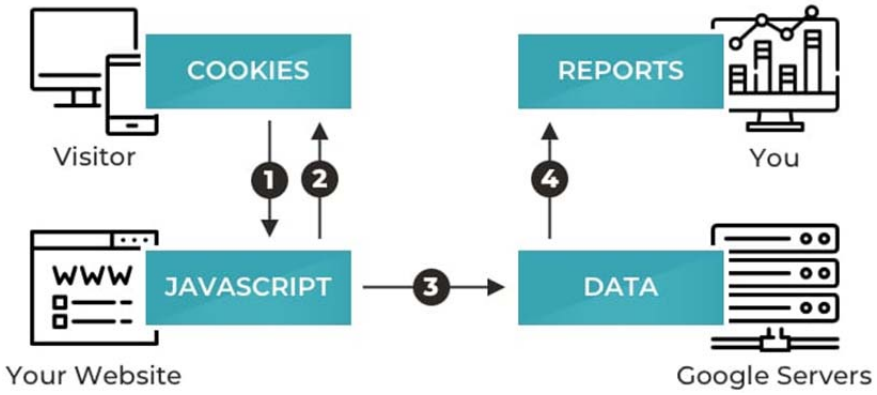


Рис. 2. Принцип роботи Google Analytics

Джерело: [3]

Ключовим елементом забезпечення безпеки захисту геймерських облікових записів та ігрових даних у веб-застосунках онлайн-гри є також обізнаність гравців про кібербезпеку та правила безпеки в Інтернеті. Популяризація правильних практик створення паролів, усвідомлення ризиків та використання доступних інструментів захисту може значно зменшити ризики для геймерів у веб-застосунках онлайн-гри.

Обізнаність гравців про соціальну інженерію та фішинг, а також навчання їх правильним практикам створення сильних та унікальних паролів може допомогти у зменшенні ризиків несанкціонованого доступу до їх облікових записів. Важливо також розуміти, як уникати шахрайства та шкідливих програм, оновлювати програмне забезпечення та використовувати антивірусні програми для захисту від кіберзагроз. Додатково гравцям слід навчатися правильно здійснювати покупки та платежі в Інтернеті, уникати надання особистої інформації через ненадійні канали та перевіряти безпеку сайтів перед виконанням транзакцій. Розуміння та дотримання цих правил може значно зменшити ризики для гравців у веб-застосунках онлайн-гри та забезпечити їхню онлайн безпеку.

Для прикладу того, як важлива кібергігієна, було проведено наукове дослідження фахівцем одного з провідних вендорів Verizon на тему «The 2021 Data Breach Investigations Report», де ключовими висновками стали такі моменти [2]:

- Фішинг (phishing) у 2021 р., як і раніше, був найпопулярнішою тактикою порушення безпеки даних. Порівняно з попереднім 2020 р. кількість інцидентів із застосуванням фішингу зросла ще на 11% та досягла 36% їх загальної кількості. Велику роль відіграло поширення COVID-19, що спричинило збільшення комунікацій та замовлень онлайн і дало зловмисникам нову тему для маніпуляцій.
- Друге місце посіла компрометація корпоративних електронних адрес (Business Email Compromises – BECs). 2021 р. кількість випадків уведення в оману (misrepresentation) користувачів виявилася в 15 разів більшою проти попереднього року.

• Удвічі частіше (у 10% випадків), як порівняти з 2020 р., застосували програми-вимагачі (ransomware), що 2021 р. опинилися на третьому місці. Таке зростання зумовлено новими зловмисними тактиками, зокрема, викрадення даних під час їх шифрування.

Знання та вчасне реагування на підозрілі ситуації може зберегти понад 98% кібератак.

Крім того, використання шифрування даних відіграє ключову роль у захисті ігрових даних. Шифрування в ігровій індустрії використовує різні криптографічні алгоритми для захисту різних типів даних, від особистих облікових записів гравців до ігрової статистики та інтелектуальної власності розробників. Так, AES є одним з найпоширеніших симетричних алгоритмів шифрування і часто використовується для захисту особистих облікових записів гравців та фінансових даних. Він володіє високою ефективністю та надійним рівнем захисту. В свою чергу, RSA є асиметричним алгоритмом шифрування, який часто використовується для захисту ключів шифрування та підписів даних. Він дозволяє безпечно обмінюватися ключами між клієнтом та сервером без необхідності в обміні секретними ключами. SHA є алгоритмом хешування, який використовується для створення унікального хешу з вихідних даних. Він широко використовується для захисту паролів користувачів шляхом збереження хешованих значень у базі даних. А ECC, що є асиметричним алгоритмом, використовується для шифрування та підпису даних з меншою довжиною ключа порівняно з RSA, що корисно використовувати в обмежених просторах.

PGP є програмним засобом для шифрування та підпису електронної пошти та файлів. Він забезпечує надійний захист конфіденційної інформації і може бути використаний для захисту інтелектуальної власності розробників.

Оцінювання та аналіз описаних алгоритмів шифрування для ігрових даних інформації зведено в Таблицю 1, що відтворює ефективність, рівень захисту та уразливість до різних типів атак.

Таблиця 1

Аналіз криптографічних методів захисту для геймерських облікових записів та ігрових даних у веб-застосунках онлайн-гри

№	Назва шифрування	Ефективність	Рівень захисту	Уразливість до атак
1	AES	Висока	Високий	Криптоаналіз, Brute Force
2	RSA	Висока	Високий	Факторизація, Криптоаналіз
3	SHA	Висока	Високий	Колізії хеш-функцій, Preimage attack
4	ECC	Висока	Високий	Криптоаналіз, Витік приватного ключа

Джерело: розроблено автором

З таблиці видно, що кожен криптографічний алгоритм має високий рівень захисту, проте, вони можуть бути уразливі до різних типів атак. Шифрування AES та RSA виявилися найефективнішими та надійнішими у захисті ігрових даних, але потребують обережності в управлінні ключами та захисту від відомих атак. SHA та ECC також є ефективними, але можуть бути вразливими до деяких видів криптоаналізу. PGP, хоча і надає високий рівень захисту, може бути піддано атакам на підписи та іншим видам криптоаналізу.

Висновки. В цілому, аналіз методів і стратегій захисту геймерських облікових записів та ігрових даних підкреслює необхідність комплексного підходу до цієї проблеми, включаючи технологічні та організаційні заходи, які спрямовані на забезпечення максимальної безпеки та конфіденційності гравців. Використання унікальних та складних паролів, які важко підібрати, додає додатковий шар захисту для облікових записів гравців. Двофакторна аутентифікація дозволяє гравцям підтверджувати свою особу за допомогою додаткового коду або пристрою, що забезпечує вищий рівень безпеки. Моніторинг активності користувачів є важливим елементом захисту геймерських облікових записів та

ігрових даних, оскільки дозволяє швидко виявляти та реагувати на потенційно небезпечну або шкідливу активність. Також важливу роль відіграє освіта користувачів щодо кібербезпеки та правил безпеки в Інтернеті, критично знати для запобігання можливих шахрайських дій. Шифрування допомагає захищати особисті дані гравців та іншу конфіденційну інформацію від несанкціонованого доступу, забезпечуючи конфіденційність та цілісність даних.

У цілому, аналіз методів і стратегій захисту геймерських облікових записів та ігрових даних підкреслює необхідність комплексного підходу до цієї проблеми, включаючи технологічні та організаційні заходи, які спрямовані на забезпечення максимальної безпеки та конфіденційності гравців.

Список використаних джерел

1. Георгієнко В. Скільки часу потрібно для зламу вашого паролю? – URL: https://www.prostir.ua/?blogs=skilky-chasu-potribno-dlya-zlamu-vashoho-parolyu

2. Дослідження щодо безпеки даних від Verizon: головні висновки – URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/doslidzhennya-shchodo-bezpeky-danykh-vid-verizon-holovni-vysnovky

3. How to Set Up Google Analytics: The Complete Guide (with video) – URL: https://www.orbitmedia.com/blog/how-to-setup-google-analytics/

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т.В.

ПРОЄКТУВАННЯ СИСТЕМИ МОНІТОРИНГУ ТА ЗАХИСТУ ВЕБСЕРВІСІВ У РЕАЛЬНОМУ ЧАСІ ВІД КІБЕРАТАК

КЛІМАРЧУК Т.П., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто актуальність застосування систем моніторингу та захисту веб-сервісів в реальному часі від кібератак. Зазначено підходи до забезпечення моніторингу та захисту інформації в веб-сервісах з детальним описом архітектури систем, та перспективи покращення.

The article considers the relevance of using monitoring systems and protecting web services in real time from cyberattacks. Approaches to ensuring monitoring and protection of information in web services with a detailed description of system architecture and prospects for improvement are indicated.

*Актуальність.*У сучасному цифровому світі веб-сервіси відіграють важливу роль у різноманітних сферах, починаючи від електронної комерції та закінчуючи фінансовими операціями та комунікаціями. Однак, разом із зростанням використання веб-сервісів, збільшується і загроза їх безпеці з боку кіберзлочинців. Кібератаки стають все більш складними та розповсюдженими, використовуючи різноманітні техніки та методи, щоб завдати шкоди веб-сервісам, їх користувачам та власникам.

Проблема безпеки веб-сервісів стає особливо актуальною через високий ризик фінансових втрат, порушення конфіденційності даних користувачів та пошкодження

репутації компанії. Тому розробка ефективної системи моніторингу та захисту веб-сервісів в реальному часі є критичною для забезпечення безпеки та стійкості цих сервісів.

Останні дослідження та публікації в області проєктування систем моніторингу та захисту веб-сервісів в реальному часі від кібератак відображають широкий спектр підходів та методів для розв'язання цієї проблеми. Деякі з них акцентують увагу на розвитку алгоритмів машинного навчання для виявлення аномального поведінки в мережевому трафіку, інші дослідження досліджують можливості використання блокчейн-технологій для забезпечення недоступності даних та автентифікації користувачів.

1. Машинне навчання для виявлення аномалій:дослідження в цьому напрямку акцентує увагу на розвитку алгоритмів машинного навчання, таких як нейронні мережі, дерева рішень та методи кластеризації, для виявлення аномальних паттернів у мережевому трафіку. Ці дослідження намагаються покращити точність та швидкодію систем виявлення атак, зменшуючи при цьому кількість фальшивих позитивів.

2. Блокчейн-технології для забезпечення безпеки: досліджують можливості використання технологій блокчейн для забезпечення недоступності даних та автентифікації користувачів. Вони пропонують рішення, що базується на розподіленому зберіганні даних та створенні непереборної системи ідентифікації та авторизації.

3. Комбіновані підходи:такі дослідження об'єднують різноманітні підходи та техніки, такі як машинне навчання, блокчейн та аналіз журналів подій, для створення комплексних систем моніторингу та захисту веб-сервісів.

Однак, не зважаючи на ці досягнення, існують певні невирішені аспекти, такі як необхідність розробки системи, яка забезпечує комплексний моніторинг та захист в реальному часі, інтегруючи різноманітні методи та техніки для ефективного виявлення та відвертання кібератак. Означена стаття спрямована на вирішення цієї проблеми та пропонує новий підхід до проєктування системи моніторингу та захисту веб-сервісів, яка забезпечує високий рівень безпеки та стійкості у реальному часі.

*Метою статті*є проєктування та імплементація ефективної системи моніторингу та захисту веб-сервісів в реальному часі з метою запобігання кібератакам та забезпечення безпеки та стабільності роботи цих сервісів.

*Об'єктом дослідження*є процес розробки та реалізації системи моніторингу та захисту веб-сервісів в реальному часі з використанням сучасних методів.

Предмет дослідження – є веб-сервіси та їх інфраструктура, що піддаються потенційним кібератакам.

*Виклад основного матеріалу.*В епоху цифровізації та глобалізації інформаційних процесів, кібербезпека веб-сервісів набуває все більшої актуальності. Зростання залежності суспільства від інформаційних технологій породжує нові виклики у забезпеченні надійного захисту даних та інформаційних ресурсів від зловмисників. Цифрова епоха інформаційного суспільства привнесла з собою не тільки позитивні трансформації. Основними недоліками стали ризики кіберінцидентів, які набувають все більших масштабів. Так, за один день, в будь якій корпоративній інформаційно-телекомунікаційній системі виникає велика кількість подій, частина з яких є кіберінцидентами. Наявність кіберінцидентів в інформаційно телекомунікаційній системі свідчить про розвиток кібератак або вже їх здійснення. Наслідки цих атак можуть призвести до несанкціонованого доступу до інформації, яка циркулює в мережі, або ж до позбавлення її працездатності. Проте є низка заходів та технологій, які вже сьогодні можуть використовуватись для запобігання, виявлення кібератак та зменшення їх впливу на мережу. Саме огляду цих технологій й присвячений даний посібник.

Враховуючи це, розробка ефективних систем моніторингу та захисту веб-сервісів в реальному часі від кібератак стає не тільки актуальною, але й нагальною потребою. Дане дослідження має на меті проєктування такої системи, яка здатна ідентифікувати та нейтралізувати потенційні загрози в реальному часі, тим самим значно підвищуючи рівень безпеки веб-сервісів.

Практична значимість отриманих у ході дослідження результатів полягає у можливості їх застосування для захисту веб-сервісів різноманітних організацій, від малого бізнесу до великих корпорацій, а також державних установ. Розроблена система сприятиме підвищенню рівня кібербезпеки, зниженню ризиків втрати або пошкодження даних через кібератаки, а також забезпечить високий рівень довіри користувачів до веб-сервісів.

В цілому, дане дослідження спрямоване на розвиток сучасних підходів до забезпечення кібербезпеки веб-сервісів і представляє собою важливий крок у формуванні більш безпечного цифрового простору.

Незважаючи на всю популярність сучасних веб-сервісів, і на те, що вони приносять значущу вигоду для усіх видів бізнесу, можна спостерігати негативний тренд у якості безпеки цих самих сервісів. Через те, що зараз більшість маленьких та середніх бізнесів концентруються на отриманні як можна швидшого і більшого прибутку, вони не приділяють увазі безпеці у своїх веб-додатках.

Така тенденція сама по собі наражає на небезпеку не лише конфіденційні дані користувачів, які у більшості випадків неминуче будуть зберігатися у сервсі, але ще і репутацію самої компанії, яка зобов’язана відповідати за безпеку даних, які були довірені їй користувачами.

З рис. 1 можна побачити, що кількість компаній, які зазнали хоч б одну атаку є майже половина. Запропонований підхід для забезпечення моніторингу та захисту інформації надає таким компаніям перевагу в досягненні безпеки з мінімальними зусиллями, адже підхід покриває максимум відомих атак і не потребує окремого реагування на кожну з них. Це дозволяє підприємствам ефективно впроваджувати інтегровані заходи захисту, які реагують на широкий спектр загроз, забезпечуючи високий рівень безпеки при оптимальному використанні ресурсів.

Існує два підходи для забезпечення моніторингу та захисту інформації в веб-сервісах: «фрагментарний» і «комплексний».

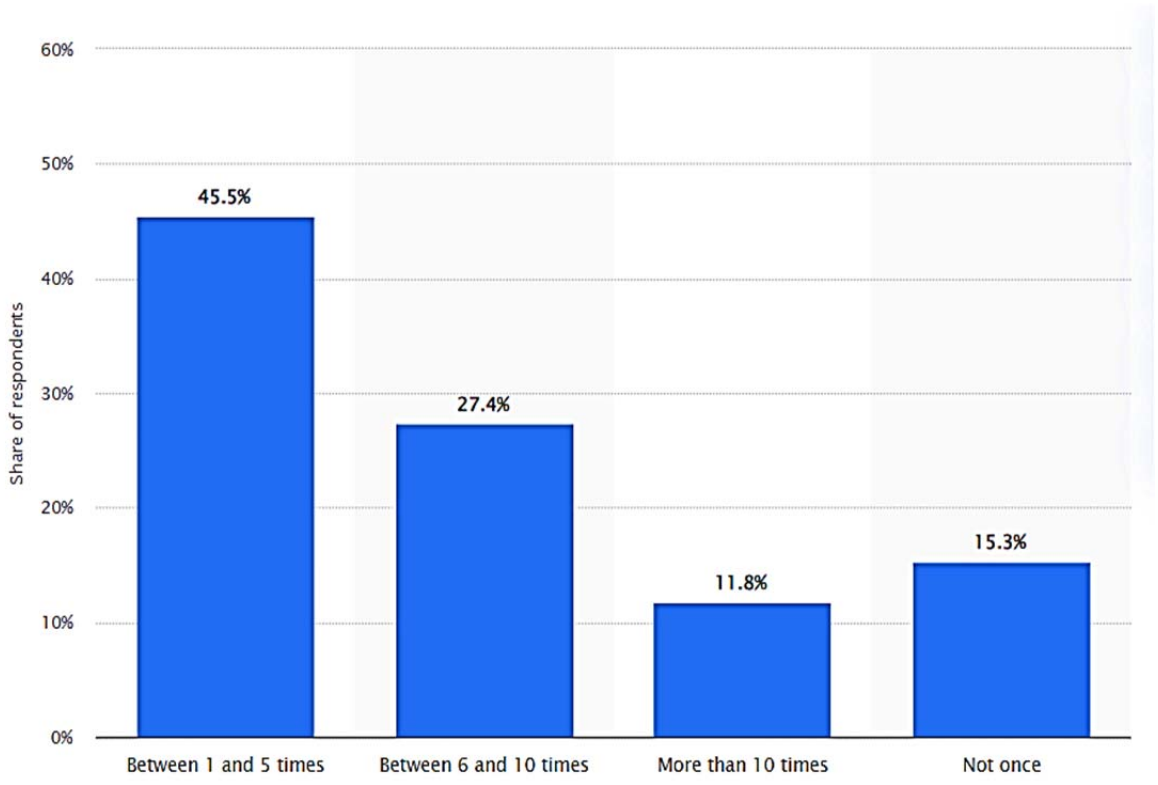


Рис. 1. Частота успішних кібератак проти організацій у всьому світі у 2022 році

Джерело: StatistaResearchDepartment

«Фрагментарний» підхід до захисту інформації в веб-сервісах спрямований на протидію конкретним, чітко визначеним загрозам, що можуть виникнути в заданих умовах експлуатації. Прикладами реалізації цього підходу є застосування окремих засобів управління доступом, таких як ролева модель доступу або двофакторнааутентифікація, для обмеження доступу до конкретних ресурсів. Також до таких заходів відносяться автономні засоби шифрування, які дозволяють захищати конфіденційні дані на рівні файлів або папок, а також спеціалізовані антивірусні програми для виявлення та нейтралізації конкретних видів загроз. Однією з переваг цього підходу є його вибірковість до конкретних загроз, що дозволяє точно адаптувати заходи захисту до потреб системи. Однак істотним недоліком фрагментарного підходу є відсутність цілісного середовища обробки інформації, що може призвести до неспроможності виявлення та вирішення комплексних загроз. Навіть невеликі зміни у загрозі можуть призвести до втрати ефективності захисту, оскільки фрагментарні заходи захисту спрямовані тільки на вирішення конкретних аспектів безпеки.

«Комплексний» підхід до захисту інформації орієнтований на створення цілісного, всебічного середовища обробки інформації, що об’єднує різнорідні заходи протидії різноманітним загрозам. Цей підхід передбачає впровадження комплексу заходів безпеки, таких як мережеві брандмауери, системи виявлення вторгнень, системи моніторингу активності користувачів та шифрування на різних рівнях інфраструктури. Організація захищеного середовища обробки інформації дозволяє забезпечити певний рівень безпеки, що є безперечною перевагою комплексного підходу. Однак до недоліків цього підходу відносяться обмеження на свободу дій користувачів, які можуть відчувати ускладнення при доступі до ресурсів через високий рівень захисту. Крім того, чутливість до помилок встановлення та налаштування засобів захисту може призвести до вразливостей у системі. Складність управління цією системою також може бути значним фактором ускладнення її впровадження та експлуатації.

Для забезпечення повного моніторингу і захисту інформації в веб-сервісах використано комплексний підхід для забезпечення повноти безпеки від різних видів атак.

Архітектура системи заснована на принципах мікросервісної архітектури, забезпечуючи високу масштабованість, гнучкість та надійність. Вона включає наступні ключові компоненти:

- Модуль збору даних: здійснює неперервний моніторинг вхідного та вихідного трафіку веб-сервісу, фіксуючи всі запити та відповіді. Даний модуль використовує сучасні технології захоплення пакетів та аналізу трафіку для збору максимально повної інформації.
- Модуль аналізу даних: інтегрує алгоритми машинного навчання та штучного інтелекту для аналізу зібраних даних, виявлення аномалій та шаблонів поведінки, характерних для кібератак. Використання глибинного навчання та нейронних мереж дозволяє ідентифікувати складні та приховані загрози.
- Модуль реагування на інциденти: відповідає за автоматичну реакцію на виявлені загрози, включаючи блокування зловмисного трафіку, ізоляцію потенційно інфікованих систем та повідомлення адміністраторів. Також включає засоби для ручного втручання та подальшого аналізу інцидентів.
- Інтерфейс користувача(UI): забезпечує інтуїтивно зрозуміле середовище для моніторингу стану системи, перегляду звітів про інциденти та управління налаштуваннями захисту. UI розроблений таким чином, щоб максимально спростити роботу з системою для адміністраторів веб-сервісів.

Аналіз отриманих результатів здійснюється на основі порівняння ефективності системи до та після її впровадження, а також за допомогою порівняльного аналізу з іншими існуючими рішеннями. Основні критерії оцінки включають:

- Точність виявлення атак: відсоток правильно ідентифікованих загроз серед загальної кількості атак.
- Час виявлення та реакції на інциденти: час від моменту початку атаки до її ідентифікації та блокування.

- Мінімізація помилкових спрацьовувань: важливо, щоб система з мінімальною кількістю помилок визначала легітимний трафік.

Науковий внесок дослідження полягає в розробці новітніх методів аналізу даних та машинного навчання, що дозволяють значно підвищити ефективність захисту веб-сервісів від кібератак. Результати дослідження можуть бути застосовані для подальшого розвитку та вдосконалення систем кібербезпеки в різних областях.

Розширений аналіз методів захисту та використання технологій:

- Захист з використанням штучного інтелекту

Використання алгоритмів штучного інтелекту (ШІ) та машинного навчання (МН) дозволяє системі не тільки виявляти відомі типи атак, а й адаптуватися до нових загроз, які постійно еволюціонують. ШІ може аналізувати великі обсяги даних в реальному часі, визначаючи складні взаємозв'язки та шаблони, недоступні для традиційних методів аналізу. Такий підхід забезпечує високу точність ідентифікації загроз із зниженням кількості помилкових спрацьовувань.

- Глибинний аналіз трафіку та поведінкові моделі

Глибинний аналіз трафіку (Deep Packet Inspection, DPI) та аналіз поведінкових моделей є ключовими елементами системи, що дозволяють детально вивчати кожен пакет даних, проходячи через мережу, і визначати аномальну поведінку, типову для кібератак. DPI забезпечує можливість глибокого аналізу вмісту пакетів на предмет наявності зловмисного коду або спроб експлойта, тоді як аналіз поведінкових моделей допомагає виявити неправильні або підозрілі дії користувачів або програм.

- Контекстний аналіз доступу

Використання контекстного аналізу доступу дозволяє системі враховувати різноманітні фактори, такі як час, місцезнаходження, тип пристрою та ідентифікаційні дані користувача, при визначенні рівня доступу до ресурсів. Це допомагає уникнути несанкціонованого доступу до конфіденційної інформації та зменшити ризик інцидентів безпеки.Контекстний аналіз також сприяє дозволяючи реагувати на зміну умов та надавати гнучкий контроль над доступом до ресурсів у реальному часі.

- Автоматизація реагування на інциденти

Автоматичне реагування на інциденти є критично важливим для забезпечення швидкої відповіді на кібератаки, мінімізуючи потенційні збитки. Система використовує передбачувальні алгоритми для прогнозування потенційних загроз та автоматично застосовує заходи щодо їх нейтралізації, такі як ізоляція інфікованих систем, блокування зловмисного трафіку або автоматичне оновлення правил фаєрволу.

Впровадження та тестування системи.

Ефективність системи повинна бути підтверджена серією випробувань на реальних веб-сервісах. Тестування включало сценарії з відомими типами атак, такими як DDoS, SQL ін'єкції, XSS-атаки, а також симуляції новітніх і складних атак, щоб перевірити здатність системи адаптуватися до нових загроз.

Результатом тестування повинна бути здатною ефективно ідентифікувати та блокувати понад кібератака з мінімальним часом відгуку, значно підвищуючи рівень безпеки веб-сервісів. Крім того, система має продемонструвати високу адаптивність, успішно виявляюти та реагуючи на нові та невідомі до цього часу типи атак.

Майбутні напрямки досліджень.

На основі отриманих результатів, дослідження може бути розширене для розробки спеціалізованих алгоритмів для захисту від конкретних типів кібератак, таких як AI-підсилені атаки або атаки на IoT-пристрої. Також перспективним є вивчення можливостей інтеграції системи з іншими інструментами кібербезпеки для створення єдиної, більш комплексної системи захисту. Крім того, дослідження може включати вивчення методів атак та захисту в контексті віртуальної та розподіленої реальності, оскільки ці технології набувають все більшого поширення та стають об'єктом інтересу для кіберзлочинців.

Висновки. Розроблена система моніторингу та захисту веб-сервісів в реальному часі від кібератак є важливим кроком вперед у забезпеченні кібербезпеки. Її висока ефективність, адаптивність та автоматизація реагування на інциденти забезпечує значний захист від різноманітних кібератак. Проте, враховуючи постійний розвиток кіберзагроз та швидку зміну тактик атак, необхідно постійно вдосконалювати систему, розширювати її можливості та адаптувати до нових викликів. Майбутні напрямки досліджень включають розробку спеціалізованих алгоритмів захисту, інтеграцію з іншими системами кібербезпеки та пошук нових методів виявлення та реагування на загрози. Розроблена система відображає високий рівень інженерного та наукового досвіду у галузі кібербезпеки, але подальші зусилля у напрямку її удосконалення та розвитку залишаються невід'ємною частиною боротьби з кіберзагрозами у цифровому світі.

Список використаних джерел

1. Частота успішних кібератак проти організацій у всьому світі у 2022 році//Режим доступу: https://www.statista.com/statistics/221394/successful-cyber-attacks-launched-against-businesses-worldwide (останнє звернення 08.04.2024р.)

2. Підходи для забезпечення моніторингу та захисту інформації //Режим доступу: https://pmf.uad.lviv.ua/storage/uploads/лекція%202%20інформаційна%20безпека.pdf

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

ВИДИ ЗАГРОЗ У КІБЕРФІЗИЧНИХ СИСТЕМАХ

КОПИЛ Д.О., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

Проаналізовано різновиди атак та властивості безпечності у кіберфізичних системах. Для забезпечення збереження конфіденційності та захисту цілісності інформації розглянуто вимоги щодо криптографічних засобів захисту інформації у складі КФС.

In the paper types of attacks and security properties of cyber-physical systems analysed. Requirements to cryptographical units for data security in cyber-physical system are reviewed to ensure the confidentiality and integrity of information.

Вступ. Інформаційна безпека завжди викликала занепокоєння, і сьогодні, коли комп'ютерні технології використовуються в більшості сфер нашого життя, безпека важлива як ніколи.

Термін «кіберфізичні системи» визначає системи, які забезпечують взаємодія між фізичним світом та IT-системами. Основним призначенням кіберфізичних систем є керування поведінкою фізичних об'єктів, частиною яких вони є. CFC не є традиційними системами реального часу, вони надають додаткові властивості класичним системам. Їх кібернетичний і фізичний компоненти інтегровані для навчання та адаптації, самоорганізації та продуктивності.

Актуальність. На даний момент основною проблемою є надійна взаємодія систем керування з фізичними системами [1]. Інформаційні системи з кожним днем ускладнюються, а тому навіть найменший протік інформації може мати катастрофічні наслідки [9]. У цьому

напрямі сучасні дослідження спрямовані на створення систем, здатних збалансувати поєднання фізичних і обчислювальних елементів [4]. Такі системи називаються кібер-фізичними системами (КФС) [2].

Загалом відомо багато методів забезпечення безпеки (аутентифікація, контроль доступу, цілісність повідомлень) [3]. Однак вони спрямовані на захист інформації, а не фізичних систем [5]. На практиці ці методи можуть бути зруйновані через людські помилки, неточності програмного забезпечення, збої в конфігурації пристрою [7]. В результаті зловмисники можуть успішно атакувати КФС [8]. Захист даних за допомогою шифрування є одним з можливих рішень проблеми безпеки [6]. Зашифрований текст буде доступний лише тому, хто знає секретний ключ [10]. Цим питанням займається криптографія [11]. Чітких вимог до криптографічного захисту інформації досі немає, тому в статті будуть сформульовані властивості, якими повинна володіти КФС, щоб бути надійною [12].

Метою статті є узагальнення видів атак та загроз у кіберфізичних системах, а також формулювання криптографічних вимог до КФС.

Предметом дослідження є види загроз у кіберфізичних система.

Об'єктом дослідження є кіберфізичні системи.

Характеристики КФС. Основним завданням кібернетико-фізичних систем є управління поведінкою фізичного об'єкта, частиною якого вони є, а також можливість зміни поведінки системи при необхідності.

Кіберфізичні системи використовуються в багатьох сферах, таких як управління охороною здоров'я, управління автомобілями, електромережі, фізична інфраструктура (дороги, мости).

Незалежно від сфери застосування КФС має такі основні властивості [2]:

– Залежність від середовища виконання.

КФС дуже тісно пов'язані з середовищем, в якому вони працюють (фізичними об'єктами). Будь-яка зміна поведінки навколишнього середовища призводить до зміни поведінки кіберфізичної системи.

– Чітко визначені навички.

КФС, як правило, складаються з кількох компонентів, які мають різні характеристики. Датчики, що вбудовані у фізичні пристрої для моніторингу, мають обмежені можливості, але програмне забезпечення, яке керує цими датчиками, потужніше.

– Мережевість.

КФС, на відміну від традиційних автономних вбудованих систем, потребує мережевого зв'язку між компонентами для надання своїх послуг.

Принцип роботи КФС. Роботу кібернетично-фізичних систем можна розділити на три етапи [3]:

1. Моніторинг

Це найважливіший етап роботи КФС, який полягає у спостереженні за змінами середовища, в якому працює КФС. Він також використовується для отримання відгуків про будь-яку минулу діяльність із КФС. Для запобігання можливих проблем з системою у майбутньому, це є необхідною процедурою..

2. Обробка даних

Це стосується аналізу даних, зібраних під час моніторингу, щоб визначити, чи відповідає фізичний процес заздалегідь визначеним критеріям. Якщо критерії не відповідають, коригувальні дії будуть визначені відповідно до інших критеріїв.

3. Виконання

На цьому етапі виконуються дії, визначені на етапі обробки даних. При цьому можна повністю змінити поведінку КФС. Будь-яка кіберфізична система може перебувати в одному з трьох можливих режимів: пасивному, пасивно-активному та активному.

Пасивний режим – у цьому режимі кіберфізична система не виконує жодних дій, окрім збору інформації та контролю середовища (наприклад, медичних пристроїв).

Пасивно-активний режим – у цьому режимі кіберфізична система контролює своє середовище.

Якщо певна дія виконується неправильно, то відбувається непряме виконання зі зміною поведінки системи. Наприклад: центри обробки даних здійснюють інтелектуальне планування для зниження температури в певних місцях.

Активний режим – в цьому режимі кіберфізична система, як і в пасивно-активному режимі, контролює своє оточення. Однак, коли певна діяльність виконується неправильно, то відбувається пряме втручання зі зміною фізичного середовища. Наприклад: системи вентиляції приміщень.

Різновиди атак у КФС. Атака – це будь-яка спроба знищити, вимкнути, здобути несанкціонований доступ до системи або викрадення даних з неї. [3].

Атаки у КФС (рис. 1) можна класифікувати так [4]:

1. A1 і A2 являють собою обманні атаки, при яких зловмисник надсилає фальшиве повідомлення від датчика або контролера. Неправдива інформація може включати неточні вимірювання, час або інформацію про відправника. У будь-який момент атаки система не знає про шахрайство та припускає, що всі дані та послуги, отримані від зловмисника, вважаються законними. У цьому типі атаки зловмисник може перехопити будь-яку інформацію, що передається в системі. Такі атаки здійснюються за наявності секретного ключа або шляхом злому датчиків (A1) чи контролерів (A3).

2. A2 і A4 відображають DoS-атаки. Зловмисник перешкоджає контролеру отримати інформацію від фізичної системи. У цьому випадку канали зв'язку проникають і зловмисник може не тільки отримати доступ до інформації, але й змінити або видалити її. Це також може призвести до неправильного виконання та затримок ініціалізації певних служб.

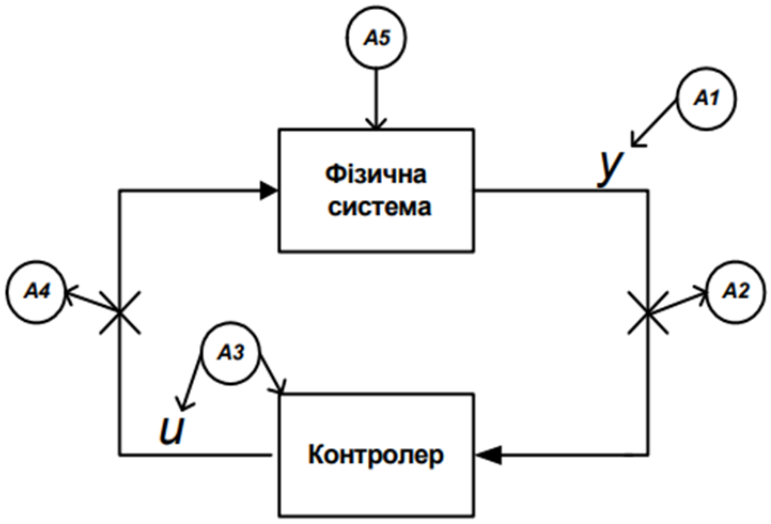


Рис. 1. КФ Атаки

Джерело: Розроблено автором

3. A5 – пряма атака на КФС. З алгоритмічної точки зору неможливо забезпечити відбиття цих атак (крім їх виявлення). Тому значні зусилля слід зосередити на запобіганні прямим атакам на фізичні системи.

Хоча атаки A5 є найбільш руйнівними, вони трапляються рідко, тому при розробці систем захисту інформації слід враховувати атаки A1-A4.

Загрози у кіберфізичній безпеці. Щоб гарантувати безпеку в кіберфізичних системах, необхідно уникати багатьох загроз, основними з яких є:

Нечітка модель загроз (змінена модель загроз) – це традиційна модель загроз для комп'ютерних систем, зосереджена лише на програмних загрозах. Більшість кіберфізичних

систем також залежать від середовища виконання. Під час атаки зловмисники не обов'язково спотворюють поведінку фізичної системи, іноді процес зчитування інформації може призвести до збою кіберфізичної системи.

Специфіка вимог до безпеки для певних систем (вимоги до безпеки для конкретних програм) – традиційні вимоги до безпеки можуть бути недостатніми для певних кіберфізичних систем. Тому кожна функція кіберфізичної системи має власний набір заходів безпеки. Наприклад, авторизація в медичній кіберфізичній системі може означати дозвіл на отримання певних ліків, тоді як авторизація в інтелектуальній кіберфізичній системі може просто надавати доступ до певних програм.

Безпека, орієнтована на користувача – використання кіберфізичних систем не обмежується спеціалізованими системами. Багато кіберфізичних програм є повсякденними системами, користувачі яких зазвичай не мають технічного досвіду. Це системи медичного моніторингу, інтелектуальна інфраструктура тощо. Таким чином, рішення безпеки для кіберфізичних систем мають бути простими у використанні (функція plug-n-play, прозорість безпеки).

Вимоги щодо безпеки у КФС. Щоб запобігти атаці на систему, необхідно дотримуватися наступних вимог безпеки.

Конфіденційність – означає можливість приховати дані [5]. Зазвичай це досягається за допомогою криптосистем. Криптосистема – це математична функція, яка перетворює (шифрує) вхідне повідомлення в зашифрований текст. Зашифрований текст можна перетворити у вихідний стан лише за наявності зворотної функції. Процеси шифрування та дешифрування можуть відбуватися лише за допомогою криптографічного ключа. Розшифрувати повідомлення практично неможливо, не знаючи точного значення ключа. Існує два типи криптографічних систем, які можна використовувати для забезпечення конфіденційності: симетричні та асиметричні криптосистеми.

Симетричні криптосистеми – це криптосистеми, в яких для шифрування і дешифрування використовується один і той же ключ [6]. Недоліком цих систем є те, що в разі втрати або крадіжки ключа втрачається конфіденційність системи. Серед відомих алгоритмів, які використовують симетричний ключ, є AES [7] і RC5 [8].

В асиметричних криптосистемах для шифрування і дешифрування використовуються різні ключі, які пов'язані між собою певною залежністю [9]. У той же час обчислювально дуже важко встановити один ключ для розпізнавання іншого. Один із ключів (наприклад, ключ шифрування) може бути загальнодоступним, і в цьому випадку проблема отримання загального секретного ключа не виникає. Відомі такі асиметричні алгоритми: RSA, Diffie–Hellman.

Цілісність

Для забезпечення цілісності даних необхідно враховувати можливість виявлення будь-яких змін, внесених у передане повідомлення. Зазвичай це робиться за допомогою хеш-функції.

Функція хешування приймає як вхідні дані, цілісність яких повинна бути забезпечена, і як вихід випадкове значення фіксованої довжини, яке називається колекцією [9]. Оскільки ця функція є односторонньою, результат буде іншим при найменшій зміні вхідних даних. Для асиметричних сценаріїв хеш-функція використовується для отримання даних, зашифрованих за допомогою закритого ключа – цифрового підпису. Під час перевірки цілісності даних за допомогою відкритого ключа обчислюється хеш-функція, а потім розшифрований текст порівнюється з існуючим текстом. Відомі такі алгоритми: MD5 [10], SHA [11].

Аутентифікація

Автентифікація створює рівень довіри між системами, який потім формує основу всього подальшого спілкування. В інтерактивних системах аутентифікація забезпечує розпізнавання системи. Деякі відомі методи – це цифрові сертифікати, біометрія, взаємодія запит-відповідь.

Авторизація

Враховуючи ідентичність суб'єкта, який взаємодіє з системою, авторизація ідентифікує системні дані та керує ними за допомогою моделі контролю доступу. У своїй основній формі це працює так:

1. Особа, яка хоче використовувати об'єкт у системі, робить запит.

2. Модель управління доступом приймає запит й ідентифікує особу, після чого надає їй певні

привілеї на основі чітко визначених правил.

3. Якщо запит відповідає привілеям, тоді доступ дозволений.

Криптографічні вимоги у КФС. Зі сказаного вище можна зробити висновок, що для збереження конфіденційності та захисту цілісності інформації основною вимогою є використання криптографічних методів.

Процес криптографічного закриття даних може здійснюватися як програмним, так і апаратним забезпеченням. Апаратна реалізація значно дорожча, але вона також має переваги: висока продуктивність, простота, безпека. Програмна реалізація більш практична і забезпечує більшу гнучкість у використанні.

Незалежно від способу реалізації, до сучасних систем криптографічного захисту інформації висуваються такі вимоги [6, 12]:

– Знання алгоритму шифрування не повинно зменшувати надійність шифрування. Ця вимога була сформульована ще в 19 ст. Керкгофф; криптосистеми поділяються на два види: загального користування (алгоритм доступний потенційному порушнику) і обмеженого користування (алгоритм секретний).

– Вибір криптографічної технології повинен відповідати вимогам надійності.

– Зашифроване повідомлення має бути прочитано лише за наявності ключа.

– Шифр має бути надійним, навіть якщо зловмисник знає достатню кількість вхідних даних і відповідних зашифрованих даних.

– Невелика зміна ключа або вихідного повідомлення має призвести до суттєвої зміни зовнішнього вигляду зашифрованого тексту.

– Структурні елементи алгоритму шифрування мають бути незмінними.

– Довжина зашифрованого повідомлення має дорівнювати довжині вихідного повідомлення.

– Додаткові біти, вставлені в повідомлення під час процесу шифрування, повинні бути повністю та надійно приховані в зашифрованому повідомленні.

– Будь-який ключ із набору можливих повинен забезпечувати однакову крипто-стійкість.

– Не повинно бути простих і легких для створення залежностей між ключами, які постійно використовуються в процесі шифрування

– Кількість операцій, необхідних для розшифровки інформації в пошуках можливих ключів, повинна бути явно нижчою за оцінками і повинна перевищувати можливості сучасних комп'ютерів або вимагати використання дорогих обчислювальних систем.

Висновки. У роботі представлено основні характеристики кіберфізичних систем, а саме: залежність від середовища виконання, чітко визначені можливості та мережевість. Описано наступні види атак: атаки підробки, атаки DoS, прямі атаки на КФС. Розглянуто особливості безпеки в КФС (конфіденційність, цілісність, автентифікація, авторизація) та основні загрози кіберфізичної безпеки (нечітка модель загроз, специфіка вимог безпеки окремих систем, орієнтована на користувача безпека). Сформульовано основні крипто-графічні вимоги до КФС.

Список використаних джерел

1. Мельник А. О., Кіберфізичні системи: проблеми створення та напрями розвитку. – Львів: Видавництво Львівської політехніки. – 2014. – С. 154–161.

2. Laura Vegh, Liviu Miclea. Securing Communication in Cyber-Physical Systems using Steganography and Cryptography / Technical University of Cluj-Napoca, Faculty of Automation and Computer Science, Romania, June 2014.

3. Krishna Kumar. Venkatasubramanian, Security solutions for cyber-physical systems, Arizona State University, December 2009.

4. Alvaro A. Cardenas Saurabh Amin, Shankar Sastry, Secure Control: Towards Survivable CyberPhysical Systems, University of California, Berkeley, August 2013.

5. Saddek Bensalem, Roberto Passerone,Alberto Sangiovanni-Vincentelli,CPS Methods and Techniques,Project co-funded by the European Union's Seventh Framework Programme,July 2013.

6. Elliptic Curve Cryptographic Co-Processor Components for Security On medical Embedded Systems.

7. Daemen J. and Rijmen V. The Design of Rijndael: AES – The Advanced Encryption Standard. Springer Verlag, 2002.

8. Rivest R. L. The RC5 encryption algorithm. – 1995. – P. 86–96. Workshop on Fast Software Encryption.

9. Buchanan W. Cryptography. River Publishers, 2022. – 175 с.

10. Rivest R. L. The md5 message-digest algorithm (rfc 1321), 1992.

11. Diffie W. and Hellman M. E. New directions in cryptography. ieee transactions on information theory // IEEE Transactions on Information Theory, 22(6):644–654, 1976.

12. Swapna Iyer,Cyber Security for Smart Grid, Cryptography, and Privacy, Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616-3793, USA, July 2011.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

АКТУАЛЬНІСТЬ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ТА ЇЇ ЗНАЧЕННЯ ДЛЯ СУЧАСНОГО СВІТУ ТЕХНОЛОГІЙ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

КОРЧАГІНА М.О., 1 курс 6мз група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

Ця наукова стаття досліджує значення та ефективність методів біометричної автентифікації у сфері захисту сучасних цифрових інфраструктур від несанкціонованого доступу та кіберзагроз. Шляхом всебічного аналізу різних видів біометричної ідентифікації, таких як розпізнавання відбитків пальців, геометрії обличчя, сканування райдужної оболонки ока, розпізнавання голосу та аналізу почерку. Дослідження оцінює актуальність даних методів ідентифікації, їхні переваги, недоліки, обмеження а також сфери та методи практичного застосування.

This article explores the significance and effectiveness of biometric authentication methods in protecting modern digital infrastructures from unauthorized access and cyber threats. Through comprehensive analysis of various types of biometric identification, such as fingerprint recognition, facial geometry, iris scanning, voice recognition, and handwriting analysis, the study evaluates the relevance of these identification methods, their advantages, disadvantages, limitations, as well as practical application areas and methods.

Актуальність проблеми. В сучасну епоху стрімкого розвитку цифрових технологій та зростаючої залежності суспільства від інформаційних систем, захист конфіденційних даних та забезпечення інформаційної безпеки набувають критичного значення. Із появою нових методів захисту, з'являються і нові методи його подолання. Рівень кіберзлочинів невпинно зростає з кожним роком, а фінансові втрати від витоку даних та несанкціонованого доступу вимірюються мільярдами доларів.

Традиційні методи автентифікації, такі як паролі та захисні коди, все частіше виявляються недостатньо надійними через можливість їх підбору або крадіжки. Тому постає гостра потреба у впровадженні ефективніших засобів ідентифікації користувачів, які б забезпечували високий рівень безпеки та захисту інформації.

Біометрична автентифікація, яка базується на унікальних фізичних або поведінкових характеристиках людини, стає все більш затребуваною в різних сферах – від банківської справи та електронної комерції до державних і військових установ. Ця технологія дозволяє точно встановити особу та унеможливлює підробку ідентифікаційних даних. На відміну від традиційних методів, біометричні ознаки людини, такі як відбитки пальців, геометрія обличчя, малюнок райдужної оболонки ока чи голос, є незмінними та унікальними для кожної особи.

Підвищений інтерес до біометричних систем автентифікації зумовлений низкою переваг, які вони надають: підвищений рівень безпеки, зручність використання, неможливість втратити або передати іншій особі біометричні дані. Проте разом із перевагами існують і певні недоліки, наприклад: забезпечення конфіденційності біометричних даних, вартість впровадження систем, правові аспекти тощо.

Таким чином, актуальність дослідження біометричних методів автентифікації та їх ролі в забезпеченні інформаційної безпеки обумовлена нагальною потребою захистити конфіденційні дані та критично важливі інформаційні активи від несанкціонованого доступу та кіберзагроз в сучасному технологічному світі.

Метою даної роботи є дослідження принципів роботи біометричних систем автентифікації, аналіз переваг та недоліків їх використання, визначення ролі та значення біометрії в сучасних технологіях забезпечення інформаційної безпеки.

Об'єктом дослідження є процес автентифікації користувачів в інформаційних системах із застосуванням біометричних характеристик.

Предметом дослідження є біометричні системи автентифікації, їх види, принципи роботи, переваги і недоліки, а також роль у забезпеченні інформаційної безпеки.

Аналіз попередніх досліджень. Питання біометричної автентифікації та її застосування в сучасних інформаційних системах і технологіях активно досліджуються багатьма науковцями. Фундаментальні основи біометричних методів ідентифікації розглядаються в роботах А. Дж. Росса, А. К. Джейна, Д. Мальтоні та інших. Велику увагу приділено вивченню різних біометричних характеристик, методів їх вимірювання та опрацювання.

В. О. Хорошко аналізує проблеми забезпечення інформаційної безпеки з використанням біометричних технологій. Автор розглядає принципи роботи різних біометричних систем, їх переваги та недоліки, а також тенденції розвитку цієї галузі.

О. Г. Корченко аналізує проблеми та перспективи використання біометричних систем у державних інформаційних системах, а також визначає шляхи підвищення їх ефективності.

Виклад основного матеріалу.

Принципи роботи біометричних систем автентифікації.

Біометричні системи працюють за наступним загальним принципом:

1) Запис та реєстрація біометричних зразків користувачів у базі даних (відбитки пальців, зображення райдужної оболонки ока, зразки голосу та інші дані).

2) Під час автентифікації відбувається захоплення біометричних даних користувача за допомогою спеціальних датчиків та сенсорів.

3) Отримані біометричні дані користувача порівнюються з раніше записаними шаблонами у базі даних.

4) На основі результатів порівняння визначається ступінь схожості та проводиться ідентифікація або верифікація користувача.

Залежно від використовуваних біометричних характеристик розрізняють такі основні типи біометричних систем:

- Системи розпізнавання відбитків пальців. Це один з найпоширеніших та перевірених методів, заснований на аналізі унікального малюнка папілярних візерунків.

- Системи розпізнавання геометрії долоні, які вимірюють характеристики форми долоні, відстань між опорними точками тощо.

- Системи розпізнавання малюнка вен, які фіксують візерунок розгалуженої мережі вен на тильній стороні долоні або пальців.

- Системи розпізнавання райдужної оболонки ока, що працюють з унікальним рисунком радіальних кілець райдужки.

- Системи розпізнавання обличчя, які ідентифікують особу за характеристиками рис обличчя.

- Системи розпізнавання голосу, що аналізують звукові хвилі мови людини.

- Системи динаміки почерку, що фіксують особливості рухів під час підпису або рукописного введення.

Крім автоматичних біометричних систем існують також змішані системи, що поєднують біометричну автентифікацію з традиційними методами (паролі, картки, ключі тощо) для підвищення рівня безпеки.

Біометричні характеристики оцінюються за низкою критеріїв, серед яких головні: унікальність, стійкість, визначеність, легкість збору та обробки даних. Найбільш перспективними вважаються мультимодальні системи, що використовують поєднання кількох біометричних ознак.

Існуючі алгоритми і методи біометричного розпізнавання можна поділити на дві основні групи: статичні та динамічні (Рис. 1.)

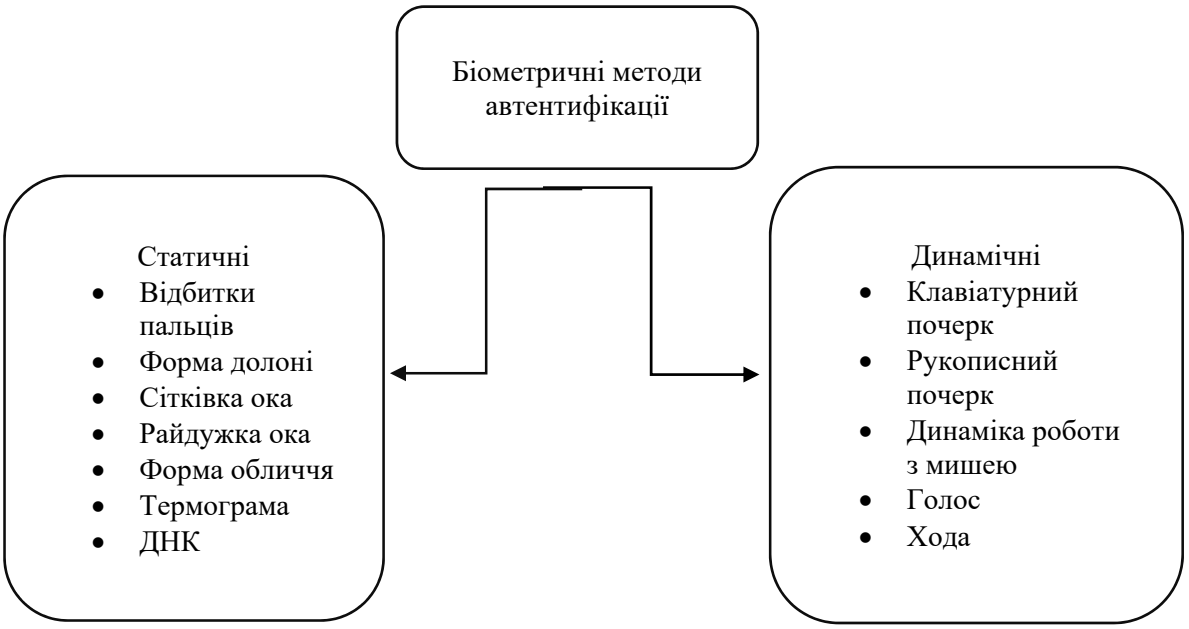


Рис. 1. Біометричні методи автентифікації

Джерело: Розроблено автором

Статичні методи ґрунтуються на унікальних фізіологічних характеристиках людини, які вона має з народження і не може їх змінити, такі як дактилоскопія, васкулярна автентифікація, розпізнавання за райдужною оболонкою ока, сітківка ока, геометрія руки, обличчя та термограма. Динамічні методи базуються на характеристиках поведінки людини, таких як розпізнавання голосу та динаміка підпису.

Для порівняння цих методів автентифікації розглядалися такі показники як визнання користувачами (згода людей на збір даних, час взаємодії з пристроєм, психологічний комфорт), вартість, простота використання, стійкість до підробок та атак, частота відмов в обслуговуванні (FRR), частота помилкових спрацювань (FAR), час розпізнавання об'єкту, розмір шаблону та стабільність роботи за нестандартних умов (при хворобах та старінні).

Таблиця 1

Порівняльний аналіз показників біометричних методів автентифікації

	Визначення користувача	Стійкість до підробок	Вартість	Простота використання	FRR	FAR	Час розпізнавання об'єкту	Розмір шаблону	Стабільність роботи за нестандартних умов
Відбиток пальця	5	5	7	8	5	5	6	5	9
Геометрія руки	5	6	4	8	5	5	8	9	4
Геометрія обличчя	9	3	7	9	1	6	8	5	3
Райдужна оболонка	4	6	5	6	7	7	7	7	8
Динаміка підпису	7	4	6	8	8	7	9	7	6
Голос	9	1	9	9	3	5	6	2	3

Джерело: [1]

Для визначення найбільш ефективного методу автентифікації використовувався метод власних векторів, відомий як метод Сааті. Цей метод дозволив побудувати матриці порівнянь для кожного критерію, розрахувати коефіцієнти пріоритету альтернатив та обчислити усереднені значення пріоритетності методів біометричної автентифікації з урахуванням всіх критеріїв. Мета полягала в тому, щоб визначити найкращий метод на основі багато-критеріального аналізу.

Результати оцінки свідчать про те, що найвищий пріоритет отримала біометрична технологія розпізнавання підпису. Крім того, методи ідентифікації особистості за райдужною оболонкою ока та відбитком пальця також показали себе дуже ефективними. У той самий час, розпізнавання за голосом виявилося найменш ефективним. Оскільки різні характеристики методів мають різне значення для користувачів, були введені вагові коефіцієнти для кожного критерію з метою визначення оптимального методу автентифікації, враховуючи їхню важливість.

У ході дослідження було встановлено, що людину можна ідентифікувати за допомогою різноманітних фізіологічних ознак, які є унікальними для кожної особи. До таких ознак можна віднести геометрію руки, відбитки пальців, особливості сітківки та райдужної оболонки ока, а також портретні дані, такі як інфрачервона карта людини. Також до цього переліку входять характеристики мови, рукописний почерк, а також унікальні риси клавіатурного та комп'ютерного почерку, а також інші фізіологічні особливості, що роблять кожну особу унікальною.

Біометрична ідентифікація базується на винятковості цих параметрів. Ймовірність того, що дві людини матимуть однакові ознаки, є дуже низькою (наприклад, ймовірність того, що в двох різних людей відбитки пальців на однакових пальцях однієї руки будуть ідентичними, становить 1 до 24 мільйонів, практично зводячи ймовірність до нуля). Основні характеристики наведених вище методів біометричної ідентифікації представлені в таблиці.

Таблиця 2

Характеристики методів біометричної автентифікації

Методи	Вірогідність відмови у доступі %	Вірогідність помилкової ідентифікації %	Збереження конфіденційності	Вартість реалізації, у.о.
Геометрична будова руки	0,2-4	0,2-1	Неможливо приховати	600-3000
Відбитки пальців	2-6	0,0001	Неможливо приховати	60-600
Особливості сітківки ока	0,4	6-10	Неможливо приховати	4000
Райдужна оболонка	0,2-2	0,0001	Неможливо приховати	500-6000
Портрет обличчя	1-9	----------	Неможливо приховати	55000
Рукописний почерк	0,5-5	0,5-5	8-10	----------
Клавіатурний почерк	3-9	3-9	6-10	----------

Джерело:[2]

Ідентифікація за відбитками пальців є однією з найпопулярніших систем біометричної ідентифікації. Відбитки пальців використовуються для ідентифікації вже більше століття через їхню унікальність та стійкість до змін з часом. Останнім часом такі системи стають автоматизованими завдяки розвитку обчислювальних можливостей. Їх популярність зумовлена простотою отримання та доступністю для збору.

Використання відбитків пальців як методу ідентифікації було почато наприкінці 19-го століття, коли Френсіс Галтон виявив певні характеристики, що можна було використовувати для ідентифікації відбитків пальців. Розроблені ним «точки Галтона» стали основою для подальшого розвитку цієї системи ідентифікації. Перехід до автоматизації ідентифікації відбитків пальців розпочався на початку другої половини 20-го століття з появою комп'ютерної технології. Для отримання цифрового зображення відбитків пальців використовуються різні типи датчиків, такі як оптичні, ємнісні, ультразвукові та теплові. Оптичні датчики є найпоширенішими на сьогоднішній день..

На простому технічному рівні, якщо роздільна здатність отриманого зі сканеру зображення складає 300 – 500 dpi, можна виділити значну кількість малих деталей на поверхні пальця, які можна класифікувати. Однак у системах ідентифікації зазвичай використовують лише два типи особливих точок відбитка пальця:

- Кінцеві точки – точки, де папілярні лінії «виразно» закінчуються.
- Точки розгалуження – точки, де папілярні лінії роблять розгалуження.

Рис. 2. Скан відбитку пальця з відміченими порами, точками розгалуження і кінцевими точками

Джерело: Розроблено автором на основі зображення з мережі інтернет

Використовуючи скановане зображення відбитку пальця з роздільною здатністю близько 900 dpi можна роздивитися деталі будови папілярних ліній та розпізнати пори потових залоз (див. Рис. 2, де жовті кола позначають пори, а червоні кола і лінії – кінцеві точки та точки розгалуження). Всі ці деталі використовують для ідентифікації. Не дивлячись на наглядну простоту, цей метод не є широко застосовним через складність отримання зображень такої якості поза лабораторією.

У випадку автоматизованого розпізнавання відбитків пальців, на відміну від звичної дактилоскопії, стається не так багато проблем і помилок, котрі пов'язані із зовнішніми чинниками, котрі мають змогу впливати на процес розпізнавання. Проте, при використанні фарбового методу отримання відбитків пальців стає складніше уникнути зсуву або повороту пальця, змін тиску, або зміни якості поверхні шкіри. В свою чергу, електронні сканери, що не використовують фарбу, дозволяють отримувати зображення відбитків пальців з якістю, достатньою для подальшої обробки. Якість зображення папілярного візерунку пальця, отриманого зі сканера є одним з основних критеріїв, який впливає на вибір алгоритму обробки відбитку пальця і, в підсумку, ідентифікації особи.

Вищеописаний метод автентифікації має такі переваги:

- надійність
- зручність
- безвідмовність
- легкість у застосуванні
- не потребує зображення високої роздільної здатності

Недоліками же є наступні фактори:

- через маленький розмір пальців у дітей, ускладняється їх ідентифікація
- можливі відмови через пошкодження шкіряного покрову на пальці
- неможливість ідентифікації при повній втраті пальця.

Розпізнавання за сітківкою ока здійснюється за допомогою інфрачервоного світла низької інтенсивності, яке проходить через зіницю і визначає кровоносні судини на задній стінці ока.

При скануванні сітківки ока людини відображаються її унікальні візерунки. За наявності відповідного освітлення, кровоносні судини ідентифікувати легше, ніж навколишні тканини, через їх властивість легше поглинати світло. Приклад візерунку кровоносних судин сітківки ока продемонстрований на Рис.3.

Рис. 3. Кровоносні судини сітківки ока, що використовуються для ідентифікації

Джерело:[3]

Ймовірність непропуску авторизованого користувача (помилка першого роду) в цьому методі становить лише 0,0001%. Проте ймовірність помилки другого роду складає близько 0,1%, що є досить високим показником. Пов'язано це з тим, що в першу чергу дані системи були розроблені для потреб військових, де вимоги до уникнення помилок першого роду є найвищими. У зв'язку з цим передбачається, що користувач може повторювати процедуру проходження автентифікації кілька разів поспіль.

Говорячи про автентифікацію за райдужною оболонкою ока, цей метод ґрунтується на тому, що при виділенні частотної або будь-якої іншої інформації про структуру райдужної оболонки а також її збереженні у вигляді спеціальних кодів, наприклад, у системі Дагмана цей код називається райдужним кодом (Iriscode). Зберігаються ці коди у базі даних для подальшого порівняння. Процес побудови коду складається з трьох етапів: виділення зображення райдужної оболонки, обробка зображення (включаючи усунення шуму, поліпшення зображення та інші операції) та формування коду. Коди зазвичай представлені у вигляді послідовності з бітів, а критерієм при їх порівнянні виступає код Геммінга. В своїй більшості такі методи не працюють з кольоровою інформацією.

Меланін райдужної оболонки, також відомий як хромофор, головним чином складається з двох відмінних гетерогенних макромолекул, які називаються еумеланіном (коричнево-чорним) і феомеланіном (жовто-рудим), чиє поглинання при довших довжинах хвиль у ближній інфрачервоній області спектра є незначним. Однак при коротких довжинах хвиль у видимій області спектра ці хромофори збуджуються і можуть утворювати різноманітні зразки. Кожна райдужна оболонка має свій унікальний візерунок, він є неповторним для кожної людини і не змінюється протягом життя. На Рис.4. наведено приклад вигляду візерунка райдужної оболонки ока, який використовується для ідентифікації.

Розпізнавання голосу або мовця – це здатність пристрою або програми отримувати та інтерпретувати диктоване або розуміти та виконувати усні команди. Розпізнавання голосу набуло популярності та використання зі зростанням штучного інтелекту (ШІ) та розумних асистентів, таких як Alexa від Amazon та Siri від Apple.

Системи розпізнавання голосу дозволяють споживачам взаємодіяти з пристроєм чи програмою, просто говорячи до неї, що дозволяє виконувати запити без дотику.

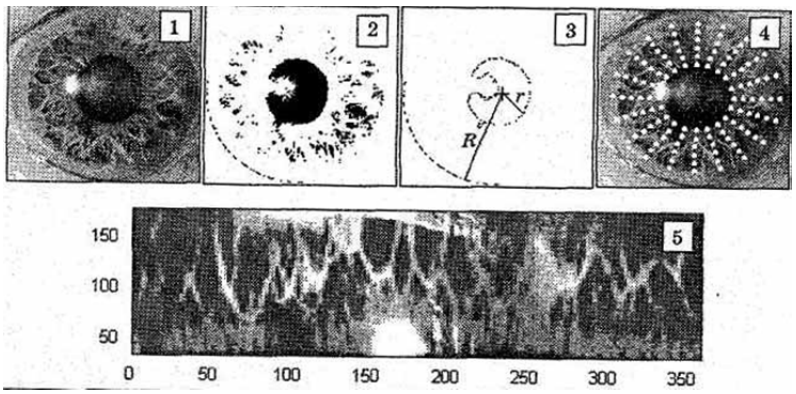


Рис. 4. Візерунок райдужної оболонки ока

Джерело:[4]

Системи розпізнавання голосу можуть ідентифікувати та розрізняти голоси, використовуючи програми автоматичного розпізнавання мови (АРМ). Деякі програми АРМ вимагають від користувачів спочатку навчання програми розпізнавати їх голос для більш точного перетворення мовлення на текст. Системи розпізнавання голосу оцінюють частоту, акцент та стиль мовлення.

Хоча розпізнавання голосу та розпізнавання мовлення іноді використовуються разом, вони не є взаємозамінними. Розпізнавання голосу ідентифікує мовця, тоді як розпізнавання мовлення оцінює, що було сказано.

Існують два основні застосування технологій та методик розпізнавання мовця. Якщо мовець стверджує, що являється певною особою, і його голос використовується для перевірки цього твердження, це називається верифікацією або автентифікацією. З іншого боку, ідентифікація – це завдання визначення ідентичності невідомого мовця. У певному сенсі верифікація мовця – це відповідність 1:1, де голос одного мовця порівнюється з певним шаблоном, тоді як ідентифікація спікера – це відповідність 1:N, де голос порівнюється з кількома шаблонами.

З точки зору безпеки, ідентифікація відрізняється від верифікації. Зазвичай розпізнавання мовця використовується як «сторож» для надання доступу до системи. Ці системи працюють з відома користувачів і, як правило, потребують їх співпраці. Системи ідентифікації мовця також можуть бути впроваджені таємно без відома користувача для ідентифікації мовців у дискусії, сповіщення автоматизованих систем про зміни мовця, перевірки, чи користувач вже зареєстрований у системі та інше.

У судових дослідженнях зазвичай спочатку виконують процес ідентифікації мовця для створення списку «найкращих відповідностей», а потім проводять серію процесів перевірки для встановлення кінцевої відповідності. Робота зі зразками від мовця для порівняння зі списком найкращих відповідностей допомагає з’ясувати, чи це та сама особа на основі кількості схожостей чи відмінностей. Це використовується обвинуваченням та захистом як доказ того, чи дійсно підозрюваний є злочинцем.

Розпізнавання за підписом, також відоме як верифікація підпису, є біометричною технологією, яка використовує унікальний підпис особи для підтвердження її ідентичності. Процес включає захоплення підпису особи за допомогою цифрового пристрою, такого як планшет або смартфон, та аналіз його за допомогою вдосконалених алгоритмів для вилучення унікальних характеристик, таких як форма, розмір, швидкість і натискання при підписі.

Розпізнавання підпису може бути використане для різних цілей, включаючи автентифікацію документів, контроль доступу та фінансові транзакції. Воно широко використовується в банках та інших фінансових установах для перевірки ідентичності клієнтів, які підписують чеки, авторизують зняття грошей або здійснюють інші транзакції.

Однією з переваг технології розпізнавання підпису є її простота використання, оскільки більшість людей звикли підписувати своє ім'я і не потребують ніякої спеціальної підготовки чи обладнання. Однак на точність розпізнавання підпису можуть впливати такі фактори, як вік, стан здоров'я та емоційний стан.

Необхідно забезпечити належні заходи захисту та регулювання, щоб забезпечити відповідальне використання технології розпізнавання підпису та захист приватності та безпеки осіб. Крім того, важливо забезпечити, щоб технологія не використовувалася для дискримінації осіб на підставі їхнього підпису або інших особистих характеристик.

Розпізнавання за підписом може здійснювати і людина, але спеціальні пристрої мають значно більше інформації в порівнянні з експертом-людиною. Такі системи ідентифікації зазвичай статистично кращі за експертів.

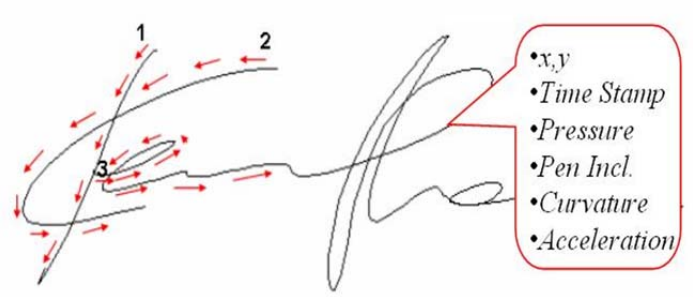


Рис. 5. Аналіз підпису

Джерело: [5]

У випадку проілюстрованому на Рис.5. перевіряється відхилення підпису по осям «х» та «у», швидкості написання, нажиму на перо, типу чорнил, викривлення та в який момент відбувалося прискорення і уповільнення написання.

Висновок. Біометричні системи автентифікації набувають все більшого поширення в різноманітних сферах людської діяльності завдяки своїм значним перевагам над традиційними методами ідентифікації. Використання унікальних біометричних характеристик людини забезпечує високий ступінь захисту інформації та інформаційних ресурсів від несанкціонованого доступу.

Серед ключових переваг біометричної автентифікації слід відзначити підвищену безпеку, надійність, зручність використання, неможливість передачі доступу іншим особам. Біометрія допомагає реалізувати концепцію нульових довірчих систем шляхом суворої перевірки особистості користувача.

Поряд із перевагами, біометричні системи мають певні недоліки та ризики, пов'язані із вартістю впровадження, загрозами компрометації даних, проблемами приватності й помилками розпізнавання. Для протидії цим ризикам необхідно дотримуватись комплексу заходів кібербезпеки, зокрема, криптографічного захисту, багаторівневої автентифікації, обмеження доступу тощо.

Після детального аналізу біометричних методів ідентифікації було встановлено, що найбільший потенціал для подальших досліджень мають динамічні методи, які базуються на аналізі особливостей підсвідомих рухів. Особливо це стосується методів, що аналізують характеристики інформаційного (комп'ютерного) почерку. Це стає особливо актуальним в ситуаціях, коли майже кожне робоче місце обов'язково має персональний комп'ютер.

Однією з ключових переваг динамічних біометричних методів, зокрема, ідентифікації за динамікою інформаційного почерку, є їхня доступність і простота реалізації. Для їхнього впровадження не потрібне дороге спеціалізоване обладнання, як у випадку сканування сітківки ока. Такі системи можуть забезпечувати постійний контроль за доступом до конфіденційної інформації та ефективно боротися з інформаційним шпигунством і витоком даних, проте, вони можуть виявитися менш точними.

Ефективність захисту найкраще досягається за допомогою систем, що комбінують біометричні методи з іншими апаратними засобами аутентифікації або з різними видами біометричних ідентифікацій. Поєднуючи різні підходи, можна створити надійну систему захисту, що здобуває великий інтерес провідних виробників програмного забезпечення.

Отже, в подальших дослідженнях важливо зосередитися на підвищенні якості ідентифікації за допомогою динамічних біометричних методів, використовуючи сучасні статистичні та ймовірнісні методи моделювання.

Список використаних джерел

1. Ukrainian Scientific Journal of Information Security, 2013, vol. 19, issue 2
2. Automatic signature verification and writer identification – the state of the art. Pattern Recognition, Volume 22, Issue 2
3. 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities by Anil Kumar Jain, Karthik Nandakumar, Arun Ross // Режим доступу: https://www.researchgate.net/publication/290509735_50_Years_of_Biometric_Research_Accomplishments_Challenges_and_Opportunities
4. Biometric template selection and update: a case study in fingerprints // Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0031320304000081
5. https://biometrics.sabanciuniv.edu/signature.html
6. Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 27 жовтня 2022 року)
7. Encyclopedia of Cryptography and Security // Режим доступу: https://link.springer.com/referencework/10.1007/978-1-4419-5906-5

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ DOM-BASED XSS

КОТЕНКО Ю.В., 1 курс 6мз група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто основні типи XSS та їх місце в загальному пулі сучасних вразливостей, що впливають на безпеку вебсайтів. Детально охарактеризовано DOM Based XSS в контексті інших типів XSS. Розглянуто приклад DOM Based XSS, а також *методи виявлення та запобігання* DOM Based XSS.

The article discusses the main types of XSS and their place in the general pool of modern vulnerabilities affecting the security of websites. DOM Based XSS is thoroughly characterized in the context of other types of XSS. An example of DOM Based XSS is considered, as well as methods for detecting and preventing DOM Based XSS.

Актуальність. XSS є однією з найпоширеніших вразливостей безпеки, що впливають на вебдодатки по всьому світу. Універсальний характер цієї загрози вимагає постійних досліджень для розуміння її еволюції та розробки ефективних заходів протидії. Атаки XSS можуть призвести до несанкціонованого доступу до особистих даних, маніпуляцій з

вебсторінками та переадресації на шкідливі сайти, що безпосередньо впливає на довіру та безпеку користувачів. З розвитком вебтехнологій з'являються нові фактори, що потенційно можуть спричиняти нові вразливості XSS. Зі зростанням регуляторного контролю щодо захистом даних, таких як GDPR та CCPA, організації повинні забезпечити безпеку своїх вебдодатків від атак XSS для відповідності юридичним нормам. Порушення безпеки, включаючи ті, що спричинені XSS, можуть призвести до значних економічних втрат через крадіжку даних, простої систем та втрати бізнес-репутації.

Метою статті є дослідження особливостей DOM Based XSS та методів, що використовуються для їх запобігання.

Об'єктом дослідження є розробка системи запобігання DOM Based XSS.

Предмет дослідження – DOM Based XSS.

Аналіз попередніх досліджень. У ході дослідження проаналізовано низку робіт вітчизняних та закордонних науковців [2-7].

У статті «Захист від передових кіберзагроз: всеосяжний посібник із захисту від фішингу, XSS та SQL-ін'єкцій» [2]. Наір С. зазначає, що атаки типу XSS є серйозною загрозою для вебдодатків. Нижче представлено основні аспекти XSS, описані в статті та наведено рис.1., який демонструє компоненти і методи атак.

Існує декілька видів XSS-атак, включаючи відображені XSS, збережені XSS і DOM-based XSS. Відображені XSS використовують динамічно сформовані вебсторінки, щоб виконувати скрипти в контексті жертви. Збережені XSS можуть бути більш небезпечними, оскільки їхні шкідливі скрипти зберігаються на сервері, а DOM-based XSS працюють безпосередньо з об'єктною моделлю документа.

Ці атаки можуть використовуватися для викрадення особистих даних, підробки сесій користувачів, а також для обману користувачів на виконання шкідливих дій. Атаки можуть завдати серйозної шкоди вебдодаткам та їхнім користувачам.

Важливі аспекти захисту включають безпечні методи програмування, такі як: верифікація введення, експортування контенту, політика безпеки контенту, регулярні перевірки.

Верифікація введення – це перевірка даних, які вводяться користувачами, щоб переконатися в їхній відповідності очікуваним параметрам.

Експортування контенту – це переконання, що будь-які дані, які відображаються у браузері, безпечні та не містять шкідливих сценаріїв.

Політика безпеки контенту дозволяє вебдодаткам контролювати джерела скриптів, щоб зменшити ризик XSS.

Регулярні перевірки, або періодичні перевірки безпеки та аудити коду допомагають виявляти та виправляти вразливості, пов'язані з XSS атаками.

Коваленко А. [3] у своїй статті «Технології тестування DOM XSS вразливостей» обрав метод GERT (Graphical Evaluation and Review Technique) для аналізу вразливостей XSS, оскільки цей метод ефективно дозволяє моделювати та аналізувати стохастичні мережі. Ця методологія використовує підхід мережевого синтезу GERT для побудови математичних моделей процесу тестування. Розроблені математичні моделі дозволяють оцінити тимчасові затрати тестування DOM XSS уразливості, враховуючи виконання або аналіз структури DOM. Розроблена технологія може бути використана для тестування веб-додатків на предмет DOM XSS уразливості, що дозволить розробникам знаходити та усувати ці вразливості, забезпечуючи безпеку веб-додатків.

Автори статті «Аналіз безпеки вебсерверів проти атак типу XSS за допомогою тестування на проникнення» [4] зазначають, що різні вебдодатки, які використовуються в інтернеті, можуть стати об'єктом атак, особливо якщо вони не проходили тестування на безпеку. Тому важливо провести тестування для виявлення можливих вразливостей. Для тестування безпеки вебсерверів проти атак XSS автори рекомендують використовувати інструменти Zap і Acunetix.

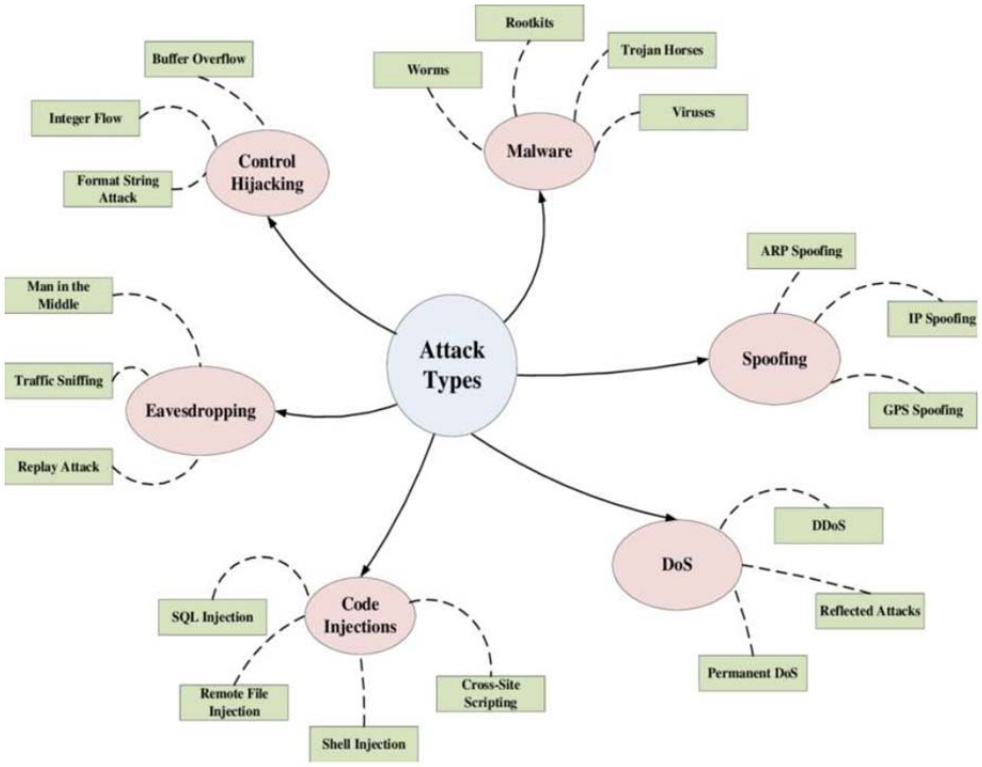


Рис. 1. Компоненти і методи атак

Джерело: [2]

У статті «До полегшеного гібридного підходу для виявлення вразливостей DOM XSS за допомогою машинного навчання» [5] зазначено, що вразливості DOM XSS є одним із видів атак на вебдодатки. Ці атаки виникають через помилки у JavaScript-коді, і їх важко виявити та запобігти. У цій статті також представлено дослідження, де використовувалися методи машинного навчання для аналізу великого масиву даних, зібраних під час сканування веб-сайтів. Це дало змогу зібрати 18 мільярдів функцій JavaScript та виявити понад 180 000 потенційно уразливих функцій. Автори статті пропонують використовувати машинне навчання у поєднанні з існуючими підходами відстеження для виявлення уразливостей DOM XSS. Було виявлено, що поєднання глибоких нейронних мереж (DNN) і методів відстеження здатне ефективніше ідентифікувати уразливості у великих масивах даних. Встановлено, що поєднання машинного навчання та методів відстеження зменшило вартість аналізу окремих функцій JavaScript у 3,43 рази, виявивши при цьому 94,5% унікальних уразливостей. Запропонований підхід є досить ефективним для використання у різних сферах, зокрема для аналізу великих кодових баз, а також для захисту браузерів у режимі реального часу.

Виклад основного матеріалу.

Cross-Site Scripting (XSS) на сьогодні є однією з найпоширеніших загроз у сфері веббезпеки, що впливає на мільйони вебсайтів та ставить під загрозу безпеку користувачів. Зароджуючись у ранні дні інтернету, XSS значно еволюціонував, відображаючи складність сучасних вебдодатків. По мірі розвитку вебтехнологій вдосконалювались також методології та інструменти, призначені для захисту вебсервісів від різноманітних кіберзагроз, включно з XSS. Технології, такі як брандмауери вебдодатків (WAFs), міцні політики безпеки контенту та рішення для моніторингу в реальному часі, відіграють ключову роль у захисті проти цих атак. Додатково, сучасні рамки розробки та платформи все частіше включають вбудовані функції безпеки, які допомагають знижувати вразливості з самого початку. Ця стаття має на меті розкласти на складові природу атак XSS, надаючи чітке розуміння їх механізмів, залучених ризиків та найкращих практик для їх зменшення. Досліджуючи історичні та сучасні випадки, ми ілюструємо серйозний вплив вразливостей XSS та підкреслюємо

важливість проактивних заходів безпеки в умовах все більш взаємопов'язаного цифрового світу.

Cross-Site Scripting – це тип ін'єкцій, під час яких шкідливі сценарії впроваджуються на безпечні та надійні вебсайти. XSS-атаки відбуваються, коли зловмисник використовує вебпрограму для надсилання шкідливого коду, як правило, у формі сценарію на стороні браузера, іншому кінцевому користувачеві. Недоліки, які дозволяють цим атакам бути успішними, досить широко поширені та виникають у будь-якому місці, де вебдодаток використовує вхідні дані від користувача в межах вихідних даних, які він генерує, без їх перевірки чи кодування.

Зловмисник може використовувати XSS, щоб надіслати шкідливий сценарій нічого не підозрюючому користувачеві. Браузер кінцевого користувача не може дізнатися, що сценарію не можна довіряти, і виконає сценарій. Оскільки він вважає, що сценарій надійшов із надійного джерела, зловмисний сценарій може отримати доступ до будь-яких файлів cookie, маркерів сеансу чи іншої конфіденційної інформації, яка зберігається вебпереглядачем і використовується на цьому сайті. Ці сценарії можуть навіть переписати вміст сторінки HTML [1].

Виділяють три типи або категорій XSS: Reflected XSS, Stored XSS, DOM Based XSS. Розглянемо більш детально кожну з них ґрунтуючись на інформації представленій в The Open Worldwide Application Security Project [1].

Reflected XSS (відображений XSS, непостійний або тип I) виникає, коли вебдодаток негайно повертає користувацьке введення в повідомленні про помилку, результатах пошуку або будь-якій іншій відповіді, що включає частину або всі дані, надані користувачем як частину запиту, без того, щоб ці дані були безпечно відображені в браузері, і без постійного зберігання введених користувачем даних. У деяких випадках ці дані можуть навіть не залишати браузер.

Stored XSS (збережений XSS, стійкий або тип II) зазвичай виникає, коли дані, введені користувачем, зберігаються на цільовому сервері, наприклад у базі даних, на форумі, у журналі відвідувачів, у полі коментарів тощо. Потім жертва може отримати ці збережені дані з вебзастосунку, якщо ці дані не було належним чином підготовлено для відображення у браузері. З появою HTML5 та інших браузерних технологій можна уявити сценарій, коли шкідливий код залишається назавжди в браузері жертви, наприклад, у базі даних HTML5, і навіть не надсилається на сервер.

DOM Based XSS (XSS на основі DOM або тип 0) – це XSS-атака, при якій шкідливий код виконується внаслідок модифікації DOM-»середовища» у браузері жертви, що використовується оригінальним скриптом на стороні клієнта, через що клієнтський код працює «неочікуваним» чином. Тобто сама сторінка (HTTP-відповідь) не змінюється, але код на стороні клієнта, який міститься на сторінці, виконується по-іншому через шкідливі зміни, які відбулися у DOM-середовищі. Тобто DOM Based XSS суттєво відрізняється від інших XSS-атак, де шкідливий код розміщено в HTTP-відповіді через уразливість на сервері.

Зосередимо увагу на DOM Based XSS та на методах запобігання цим атакам адже наслідки DOM Based XSS можуть бути серйозними, оскільки такі атаки обходять захист на серверному рівні та виконуються безпосередньо у браузері жертви. Розглянемо декілька можливих наслідків:

- Викрадення даних. Зловмисник може отримати доступ до конфіденційної інформації, такої як куки, сесійні ідентифікатори або інша приватна інформація, що дозволить йому виконувати дії від імені жертви.
- Зміна сторінки. Зловмисник може змінювати DOM-структуру сторінки, впливаючи на те, як вона відображається та як взаємодіє з користувачем. Це може включати додавання підроблених форм для фішингу або зміну вмісту сторінки.
- Підробка дій. Зловмисник може змусити жертву виконати небажані дії, такі як відправка форм або кліки по посиланнях, що можуть призвести до виконання шкідливого коду або завантаження небезпечних файлів.

- Поширення шкідливого коду. Зловмисник може впроваджувати шкідливий код, який поширюється до інших користувачів або систем, що взаємодіють з цим зараженим додатком.

- Зловживання ресурсами. Використовуючи DOM Based XSS, зловмисник може використовувати ресурси жертви, наприклад, для виконання DDoS-атак або майнінгу криптовалют.

Розглянемо приклад [8], який демонструє суть DOM Based XSS.

Припустимо, є код, який створює форму, що дозволяє користувачеві обрати бажану мову, яка також задається через параметр «default»:

Select your language:

<select><script>

document.write(«<OPTION value=1>«+decodeURIComponent(document.location.href.substring(document.location.href.indexOf(«default=«)+8))+»</OPTION><«);

document.write(«<OPTION value=2>English</OPTION><«);

</script></select>

…

Якщо сторінку викликають з такою URL-адресою:

http://www.some.site/page.html?default=French

Атака DOM Based XSS можлива, якщо відправити жертві наступне посилання:

http://www.some.site/page.html?default=<script>alert(document.cookie)</script>

Коли жертва натискає на це посилання, браузер надсилає запит на:

/page.html?default=<script>alert(document.cookie)</script>

на www.some.site. Сервер відповідає сторінкою, що містить наведений вище код Javascript. Браузер створює об’єкт DOM для сторінки, у якому об’єкт document.location містить рядок:

http://www.some.site/page.html?default=<script>alert(document.cookie)</script>

Оригінальний код Javascript на сторінці не очікує, що параметр за замовчуванням міститиме розмітку HTML, і тому він просто декодує та відтворює її на сторінці (DOM) під час виконання. Потім браузер відтворює отриману сторінку та виконує сценарій зловмисника:

alert(document.cookie)

Варто зазначити, що відповідь HTTP, надіслана з сервера, не містить корисного навантаження зловмисника. Це корисне навантаження проявляється в сценарії на стороні клієнта під час виконання, коли помилковий сценарій отримує доступ до змінної DOM document.location і припускає, що він не є шкідливим. Крім того, URL-адреси більшості веб-переглядачів за замовчуванням кодують document.location, що зменшує вплив або можливість багатьох атак DOM XSS.

У цьому прикладі шкідливий код не знаходиться в HTTP-відповіді, але все одно відправляється на сервер як частина HTTP-запиту, тож його можна виявити на стороні сервера. Однак існують техніки, що дозволяють приховати шкідливий код від сервера, наприклад, використовуючи фрагменти URI (частину після символу «#»), які не передаються на сервер. Тоді атака відбувається повністю на клієнтській стороні.

На основі «DOM Based XSS Prevention Cheat Sheet» [9] опишемо методи захисту DOM Based XSS.

1. HTML-екранування, а потім JavaScript-екранування перед вставкою ненадійних даних у підконтекст HTML у контексті виконання.

Методи і атрибути JavaScript, які рендерять HTML, можуть створювати вразливості DOM Based XSS, щоб цьому запобігти необхідно спочатку використати HTML-кодування, щоб уникнути розбірливого виконання HTML, а потім використати JavaScript-екранування, щоб уникнути маніпуляції зі шкідливим JavaScript.

2. JavaScript-екранування перед вставленням ненадійних даних у підконтекст атрибутів HTML у контексті виконання.

Підконтекст атрибута HTML у контексті виконання відрізняється від стандартних правил кодування. Це пояснюється тим, що правило кодування атрибутів HTML у контексті відтворення атрибутів HTML необхідне для пом'якшення атак, які намагаються вийти з атрибутів HTML або намагаються додати додаткові атрибути, які можуть призвести до XSS.

В контексті виконання DOM, потрібно лише закодувати атрибути HTML у JavaScript, які не виконують код (атрибути, окрім атрибутів обробки подій, CSS і URL-адреси). Використання JavaScript-екранування для значень атрибутів, які не виконують код, допомагає запобігти введенню шкідливих даних. Для забезпечення безпеки дані повинні бути правильно закодовані, щоб не дозволити маніпуляції із шкідливим кодом.

3. Обережно вставляйте ненадійні дані у підконтекст обробника подій та коду JavaScript у контексті виконання.

Розміщення динамічних даних у коді JavaScript особливо небезпечно, оскільки кодування JavaScript має іншу семантику для даних, закодованих у JavaScript, порівняно з іншими кодуваннями. У багатьох випадках кодування JavaScript не зупиняє атаки в контексті виконання. Наприклад, рядок, закодований у JavaScript, виконуватиметься, навіть якщо він закодований у JavaScript. Тому JavaScript, вставлений у обробник подій або безпосередньо у код JavaScript, може бути виконаний навіть після екранування. Потрібно уникати використання setAttribute або схожих методів для вставки JavaScript-коду, та використовувати прямі прив'язки обробників подій, де це можливо.

4. JavaScript-екранування перед вставленням ненадійних даних у підконтекст атрибута CSS у контексті виконання

Зазвичай виконання JavaScript із контексту CSS вимагає або переходу javascript:attackCode() до методу CSS url(), або виклику методу CSS, expression() який передає код JavaScript для безпосереднього виконання.

Вклик expression() функції з контексту виконання (JavaScript) було вимкнено. Щоб пом'якшити вплив url() методу CSS, варто переконатися, що здійснюється кодування URL-адреси даних, які передаються в url() метод CSS.

5. URL-екранування, а потім JavaScript-екранування перед вставленням ненадійних даних у підконтекст атрибута URL у контексті виконання

Логіка, яка аналізує URL-адреси як у контексті виконання, так і в контексті візуалізації, виглядає однаковою. Тому правила кодування для атрибутів URL-адреси в контексті виконання (DOM) мало змінені. Якщо використовувати повні URL-адреси, це розірве посилання, оскільки двокрапка в ідентифікаторі протоколу (http: або javascript:) буде закодовано URL-адресою, що запобігатиме виклику протоколів httpi.javascript

6. Наповнюйте DOM за допомогою безпечних функцій або властивостей JavaScript

Найфундаментальнішим безпечним способом заповнення DOM ненадійними даними є використання властивості безпечного призначення textContent.

7. Виправлення вразливостей міжсайтового сценарію DOM.

Найкращий спосіб виправити міжсайтовий сценарій на основі DOM – це використовувати правильний метод виведення (приймач). Наприклад, щоб використовувати введення користувача для запису в div tageлемент, не потрібно використовувати innerHtml, натомість бажано використовувати innerTextабо textContent. Це вирішить проблему, і це правильний спосіб повторно усунути вразливості XSS на основі DOM.

Завжди погана ідея використовувати керований користувачем вхід у небезпечних джерелах, таких як eval. У 99% випадків це вказує на погане чи ліниве програмування, тому просто не робіть цього замість того, щоб намагатися очистити вхідні дані.

Висновки. DOM Based XSS представляють критичну підгрупу вразливостей XSS, які вимагають спеціальної уваги в протоколах веббезпеки. Завдяки всебічному розумінню їх механізмів та наслідків, розробники та фахівці з безпеки можуть зміцнити свої захисні заходи проти цієї поширеної загрози. Завдяки впровадженню стратегій проактивного виявлення та пом'якшення, веб-екосистема може зменшити ризики, пов'язані з DOM Based XSS, та зберегти цілісність онлайн-взаємодій.

Список використаних джерел

1. Cross site scripting (XSS) | OWASP foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-community/attacks/xss/ (дата звернення: 16.04.2024).
2. Nair S. S. Securing against advanced cyber threats: A comprehensive guide to phishing, XSS, and SQL injection defense. Journal of computer science and technology studies. 2024. Т. 6, № 1. С. 76–93. URL: https://doi.org/10.32996/jcsts.2024.6.1.9 (дата звернення: 14.04.2024).
3. Коваленко А. В. DOM XSS vulnerability testing technology. Ukrainian scientific journal of information security. 2017. Т. 23, № 2. URL: https://doi.org/10.18372/2225-5036.23.11821 (дата звернення: 03.05.2024).
4. Mungfaridah R., Riadi I. Web server security analysis against cross site scripting (XSS) attacks using penetration testing. International journal of computer applications. 2022. Т. 184, № 30. С. 45–52. URL: https://doi.org/10.5120/ijca2022922370 (дата звернення: 03.05.2024).
5. Towards a lightweight, hybrid approach for detecting DOM XSS vulnerabilities with machine learning / W. Melicher та ін. WWW '21: the web conference 2021, м. Ljubljana Slovenia. New York, NY, USA, 2021. URL: https://doi.org/10.1145/3442381.3450062 (дата звернення: 03.05.2024).
6. Weamie S. J. Y. Cross-Site scripting attacks and defensive techniques: a comprehensive survey. International journal of communications, network and system sciences. 2022. Т. 15, № 08. С. 126–148. URL: https://doi.org/10.4236/ijcns.2022.158010 (дата звернення: 01.05.2024).
7. Demhi D., Batmetan J. R., Liando O. E. S. Cross-site scripting reflected as A risk high-level attack on university website. International journal of information technology and education. 2022. Т. 1, № 3. С. 103–111. URL: https://doi.org/10.62711/ijite.v1i3.65 (дата звернення: 01.05.2024).
8. DOM based XSS | OWASP foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-community/attacks/DOM_Based_XSS (дата звернення: 03.05.2024).
9. DOM based XSS | OWASP foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-community/attacks/DOM_Based_XSS (дата звернення: 03.05.2024).

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

СТВОРЕННЯ МОДЕЛІ РОЗРОБКИ БЕЗПЕЧНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

ЛЄЩЕНКО Т.І., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

Наукова стаття робить практичний розбір деяких вразливостей програмного забезпечення, що найчастіше зустрічаються в реальному світі і негативно впливають на найбільшу кількість продуктів, і приводить найефективніше рішення для усунення кожної з них. Також робота дає визначення, що таке пропозиція по написанню безпечного коду, і надає деякі приклади. Разом з методами мінімізації вразливостей програмного забезпечення вони формують модель розробки, обґрунтування і характеристики якої описуються в основному тексті.

The article conducts a practical investigation of some of the most frequently exploitable software vulnerabilities that affect the largest share of the information technology market. The author suggests solutions to avoid these vulnerabilities. The work explains what are recommendations for writing secure code and provides some definitive examples. In the ending part, there is a unique secure software development model, which is based on smaller cybersecurity principles, and whose essence is given detailed information about.

Актуальність. Більшість вразливостей програмного забезпечення виникають по вині розробників. Це пов'язано з різноманітністю і складністю технологій розробки, вивчення яких забирає майже весь час програмістів, не залишаючи вікна для навчання безпечному кодуванню. Саме тому важливо доповнювати комп'ютерні науки новими надбаннями в сфері стандартизації розробки безпечного ПЗ (програмного забезпечення), які плавно інтегруватимуться з основними процедурами реалізації проектів на кожному етапі життєвого циклу.

Вразливості програмного забезпечення наносять компаніям щорічно величезні збитки [1, 8, 9]. На їх усунення витрачаються цінні ресурси організації, включаючи робочий час спеціалістів, і вони можуть призводити до негативних наслідків різної природи: порушення конфіденційності клієнтської інформації, витік даних про нові розробки компанії, зупинка бізнес-процесів через відключення підтримуючої IT-інфраструктури (information technology).

Щоб пояснити призначення створеної моделі, потрібно подивитися на програмне забезпечення, як на продукт. У разі використання зловмисниками вразливостей, всі питання, що виникають, в тому числі відшкодування завданих збитків, регулюються ліцензійною угодою між користувачем і розробником. Обов'язок випуску латок, що усувають вразливості, авжеж, у повному обсязі покладається на розробника. Кожна сторона відчуває наслідки. Модель покликана мінімізувати вірогідність появи в програмі вразливостей нульового дня (zero-day vulnerability) і їх ризики інформаційної безпеки шляхом недопущення найпоширеніших слабкостей програмного забезпечення на кожному з етапів розробки: проектування, реалізації і конфігурації (кількість етапів обрано з точки зору кібербезпеки, а не менеджменту проектам). Результат застосування – збільшення прибутку компаній, що постачають продукт, через збільшення довіри клієнтів, а користувачам гарантується безпека їх інформаційних ресурсів.

Метою наукової статті є створення моделі для безпечної розробки, основаної на аналізі методів мінімізації вразливостей програмного забезпечення та власних пропозицій автора.

Об'єкт. Вразливості програмного забезпечення.

Предмет. Способи усунення вразливостей програмного забезпечення.

Аналіз попередніх досліджень. Дослідженню проблем безпечного програмування, зменшення ризиків інформаційної безпеки, що несуть шкідливі програми, оцінки

ефективності засобів захисту від шкідливого ПЗ, сучасних кіберзагроз, побудови систем захисту з гарантією безпеки конфіденційної інформації, протидії неавторизованому доступу до даних призначені праці зарубіжних науковців: M. Tim Jones, David A. Wheeler, Michael Howard, David LeBlanc, John Viega, H. Saltzer та Michael D. Schroeder та ін [4, 5, 6, 7].

Виклад основного матеріалу. Методи мінімізації вразливостей програмного забезпечення, як говорилося раніше, є складовою моделі безпечної розробки і відіграють в ній найважливішу роль. По суті, це конкретні засоби усунення вразливостей, кожен призначений для свого типу і обмежений напрямками застосування. Розглянемо декілька методів для найпоширеніших вразливостей.

Переповнення буфера – це вразливість програмного забезпечення, яка полягає в тому, що програма намагається писати в пам’ять, яка знаходиться поза межами виділеного буфера. Негативні наслідки, до яких може призвести цей тип вразливостей, включають неочікуване завершення роботи програми, створення загрози для інформації, підвищення привілеїв. В 2024 році вразливості переповнення буфера залишаються найнебезпечнішим недоліком програмного забезпечення [3].

Вразливості короткого запису та короткого читання (підтипи переповнення буфера) виникають, коли одна частина програми не погоджується з іншою щодо розміру буфера, що призводить до неправильного виконання і появи загроз інформаційній безпеці.

Короткий запис означає, що після запису в буфер, він був заповнений не повністю. Тобто, в його кінці можуть знаходитися дані попереднього використання. В залежності від природи цих даних, це може призвести, наприклад, до витоку даних при передачі буфера через мережу. Наступний ситуація намагається продемонструвати цю небезпечність.

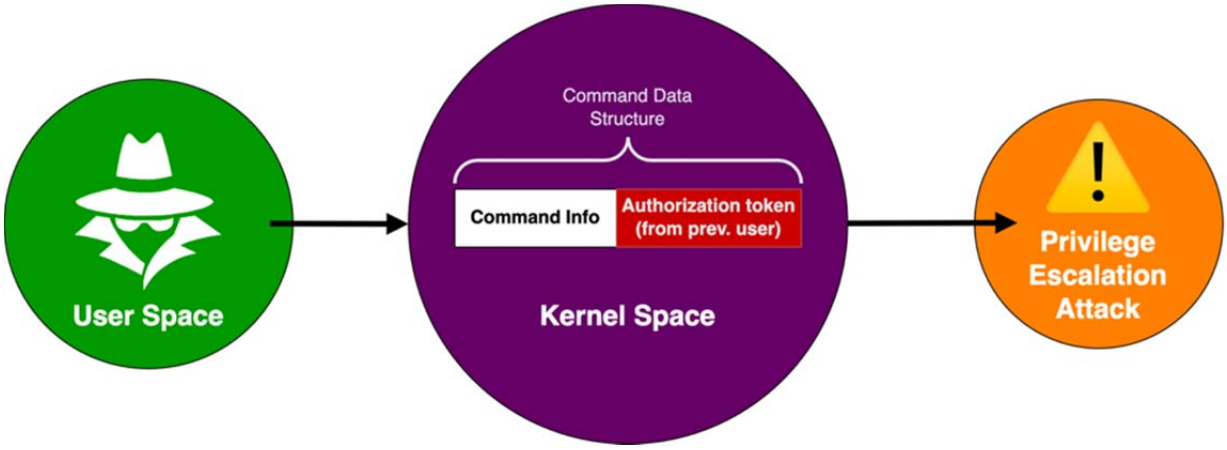


Рис. 1. Вразливість короткого запису на рівні операційної системи

Джерело: розроблено автором

Операційні системи на базі UNIX вимагають командну структуру даних для виконання системного виклику. Існують різні версії цієї структури, які відрізняються довжиною, тому користувач разом із самою структурою передає і її розмір. Скажімо, серед інших даних в кінці структури повинен бути спеціальний токен авторизації, що підтверджує право користувача на виконання того чи іншого системного виклику. Якщо в системі запущений заражений процес, який отримав чергу виконання системного виклику, він може навмисно передати структуру даних меншого розміру, щоб при копіюванні в пам’ять ядра залишився токен авторизації від попереднього користувача. Далі може статися атака підвищення привілеїв, якщо токен мав адміністративні права.

Вразливість короткого читання – це підтип вразливості переповнення буфера, що призводить до невизначеної поведінки програми, якщо дані були прочитані не повністю. Найчастіше виникнення такого типу вразливостей пов’язано з роботою з рядками стилю C. Цей тип даних, на відміну від цілочисельних змінних, має довільну довжину і завжди

закінчується NULL-символом. Високорівневі інтерфейси для взаємодії із рядками, наприклад *string* в C++, навпаки, дозволяють мати NULL-символи і контролюють довжину. Тому при використанні конвертаційних функцій, якщо зчитувати буфер лише до першого NULL-символу, який зустрінеться, ми можемо працювати з неповними даними (коротке читання буфера).

Одним прикладом в реальному житті може бути вразливість верифікації SSL (secure sockets layer) сертифікатів [2].

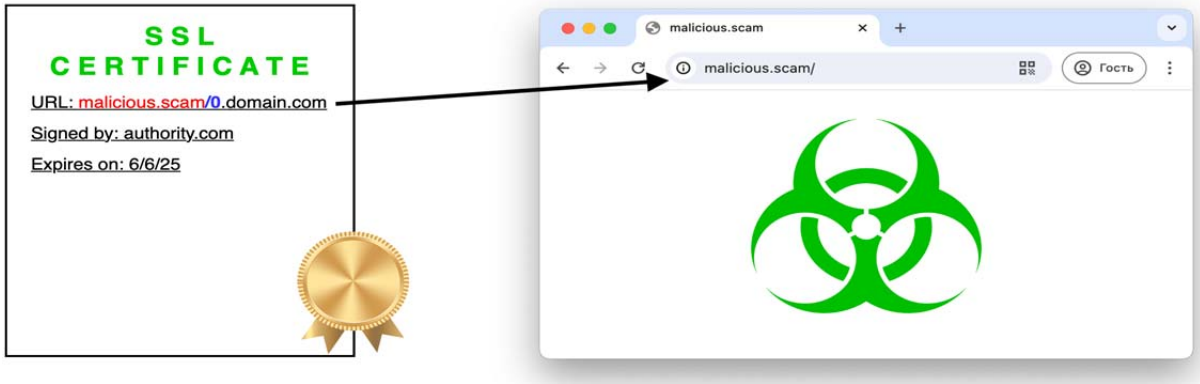


Рис. 2. Вразливість короткого читання в клієнтському SSL-стеку

Джерело: розроблено автором

Якщо у зловмисника є офіційно зареєстрований домен, він може запросити у центра сертифікації CA (certificate authority) підписання сертифікату для обережно створеного піддомену. Запит приймає адресу піддомену в якості Pascal-рядка, і цей тип даних здатен зберігати NULL-символи. Вразливість виявляється тоді, коли стек SSL протоколів у браузері неправильно конвертує Pascal-рядок у рядок стилю C. До поки зустрінеться перший NULL-символ, домен, що браузер в результаті отримав, співпадатиме з адресою шкідливого веб-сайту. Далі це може призвести, наприклад, до XSS (cross-site scripting) атаки і втрати конфіденційних даних.

Щоб уникнути вразливостей короткого читання та короткого запису буфера, потрібно використовувати такі методи в написанні коду:

- Перед повторним використання буфера слід очистити (заповнити NULL-символами) його, так як, на перший погляд, непотрібні дані можуть бути корисні зловмиснику для проведення атаки у майбутньому;
- Бібліотечні функції, що повертають результат операції, наприклад, *write*, необхідно завжди перевіряти на успішність. Полегшити це завдання можуть спеціальні високорівневі інтерфейси або власні написані макроси;
- При використанні функцій зчитування (запису) буфера варто перевіряти повернуту кількість символів, що були зчитані (записані). Якщо значення менше або більше за розмір буфера, програма повинна повідомити користувача;
- При роботі зі структурами даних варіативної довжини завжди треба переконатися, що розмір відповідає очікуваному;
- Уникати конвертацій високорівневих інтерфейсів для взаємодії із рядками у звичайні рядки стилю C. Якщо таке не можливо, додати умову, щоб вихідна довжина відповідала початковій;
- Уникати цілочисельного переповнення.

Друга складова моделі розробки безпечного програмного забезпечення – пропозиції. Пропозиції відрізняються від методів тим, що не усувають якоїсь однієї вразливості, скоріше посилюють загальний захист програмного забезпечення в якійсь мірі (вимірювання буде описано нижче). Іншими словами, вони зменшують ризики інформаційної безпеки одразу всіх типів вразливостей. Кожна пропозиція має свої унікальні переваги для розробки:

Таблиця 1

Пропозиції по розробці безпечного програмного забезпечення

№ пропозиції	Назва пропозиції	Переваги	КПЗ (коефіцієнт посилення захисту) 0-1
1	Автоматичне управління пам'яттю	Коротші терміни випуску програми	0.25
2	Організація коду	1. Легкість додавання нових функцій; 2. Швидкий пошук багів та 3. Збільшення покриття коду	0.75
3	Документація	Делегування обов'язків між розробниками	0.25
4	Підписання коду	1. Цілісність програми та 2. Збільшення довіри користувача	0.50
5	Статичний аналізатор	Виявлення вразливостей ще до першого виконання	0.50

Джерело: розроблено автором

Автоматичне управління пам'яттю передбачає використання спеціальних інструментів обраної мови (мов) програмування або середи виконання, що беруть на себе роботу розробників з динамічного виділення пам'яті та її звільнення після завершення використання. Таким чином вся увага програміста зосереджується на досягненні основних завдань, що однозначно зменшує терміни випуску програми. Додатковою перевагою є зменшення вірогідності появи в програмі багів будь-якого типу.

Організація коду з використанням таких структурних елементів, як функції, структури, класи, домени тощо, дозволить в майбутньому легко додавати нові функції. Організація робить код програми більш універсальним, де відкриваються «гнізда» для швидкого розширення існуючих можливостей. Кінцевий користувач забажає продовжити користування застосунком, якщо буде впевнений, що проект не закинутий. Друга перевага означає, що при спостеріганні неочікуваної поведінки програми розробникам вдасться швидко знайти у вихідному коді джерело вразливості і виправити її, так як структурованість і організація дозволятимуть без перешкод слідувати за потоком керування. Нарешті, збільшення покриття коду. Цей принцип є дуже важливим в тестуванні програмного забезпеченні. Він стверджує, чим більша кількість рядків коду піддалася тестам, тим простішою є організація програми, що, в свою чергу, збільшує рівень захищеності від вразливостей [5]. Можемо бачити, що ця пропозиція дозволяє відокремити (зробити самостійними) одні елементи програми від інших і тестувати кожен з них індивідуально.

Документація взаємопов'язана з попередньою пропозицією, тому що перед тим, як функцію можна буде задокументувати, весь її код має бути ізольованим від решти функціоналу програми (організація). Одна з ситуацій, де документація може стати в нагоді, – зміна команди розробників. Так нові спеціалісти, не витрачаючи зайвого часу, ознайомляться з існуючою базою коду і продовжать розширення можливостей. Але це не єдине застосування пропозиції. Делегація обов'язків означає визначення чіткого інтерфейсу взаємодії розробників, як один має правильно використовувати код іншого. Це надзвичайно важливо, і від цього залежить безпека програмного забезпечення. Уявімо функцію, яка повертає об'єкт. Існує два варіанти розв'язку подій – той, хто отримав об'єкт, або має власність над ним, або не має. Якщо має, то на плечах розробника лежить відповідальність за звільнення області

пам’яті, виділеної під зберігання об’єкта. Документація є єдиним засобом комунікації в таких обставинах, інакше інформація буде не відомою. Якщо не використовувати пропозицію, це може призвести до появи нових вразливостей, наприклад, витоку пам’яті.

Статичні аналізатори допомагають виявити вразливості програмного забезпечення ще до першого виконання. В цій науковій статті досліджувався Xcode static analyzer. Цей інструмент аналізує такі види багів: помилки в логіці програми, наприклад, доступ до неініціалізованих змінних або звертання до NULL-вказівників, витік пам’яті, невикористовувані змінні, непередбачене використання фреймворків третіх сторін.

Програма – теж інформація. Підписання коду гарантує його цілісність, а також є засобом верифікації автентичності скачаного програмного продукт. Використання цієї пропозиції показує клієнту, що розробленому програмному рішенню можна довіряти і надавати чутливі конфіденційні дані.

Відношення методів і пропозиція в моделі можна зобразити наступним чином:
$recommendations = [Recommendation0, Recommendation1, \dots, Recommendation\ n]$
$0 \leq k < n$

$$S(p) = x + \sum_{i=0}^{k} \text{КПЗ}(i),$$

де k – кількість пропозицій, впроваджених в проект;
i – номер пропозиції;
КПЗ(i) – коефіцієнт посилення захисту для пропозиції і (див. Таблицю 1);
x – кількість методів, що використовує програмне забезпечення;
p – об’єкт захисту і
$S(p)$ – оцінка захищеності об’єкта (програмного забезпечення).

Хоча методи мінімізації вразливостей програмного забезпечення і пропозиції мають властивості атомарності, найефективніше їх застосовувати разом. В будь-якому випадку, одне одному вони однозначно не перешкоджатимуть. Середа, де методи і пропозиції можна легко застосовувати з найбільшою гарантією безпеки, – це проект, реалізований по моделі розробки безпечного програмного забезпечення:

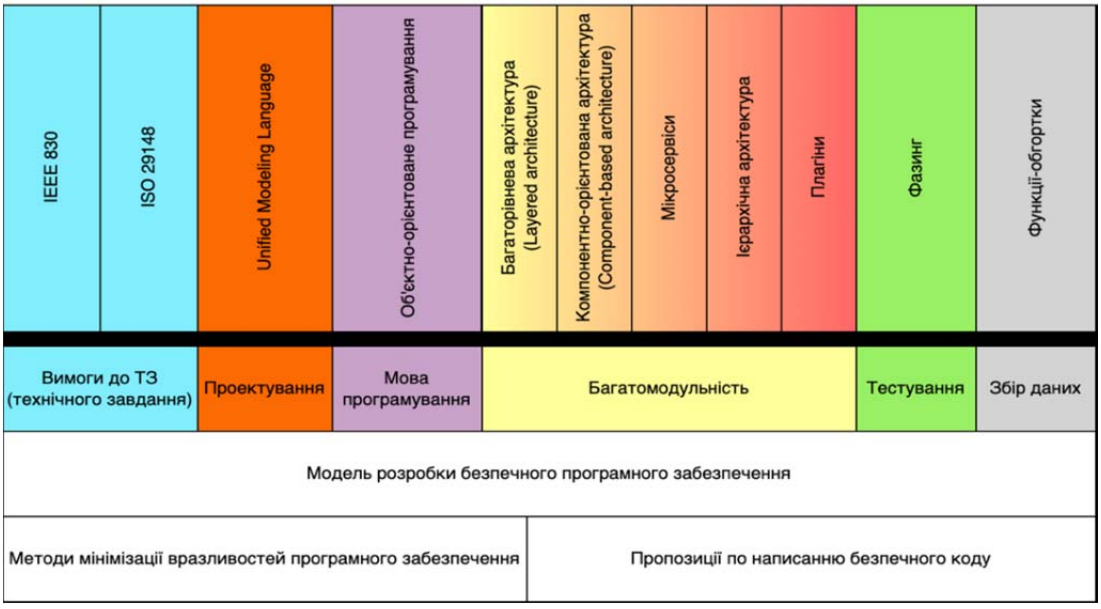


Рис. 3. Модель розробки безпечного програмного забезпечення

Джерело: розроблено автором

Модель має сім атрибутів. Коротко опишемо кожен з них.

Проектування безпечного програмного забезпечення починається з формулювання чітких вимог до функцій захисту. Без них складно буде оцінити ефективність функцій. При створені ТЗ слід опиратися на існуючі стандарти в даній сфері. Наукова робота пропонує використовувати або IEEE 830 (Institute of Electrical and Electronics Engineers), або ISO 29148 (International Organization for Standardization).

Для самого проектування пропонується використовувати UML-діаграми (Unified Modeling Language). Стандарт має багату семантику та розширений синтаксис для впровадження програмних систем зі складною структурою і комплексною поведінкою.

В якості мови програмування для проекту з точки зору кібербезпеки краще обирати ту, яка відноситься об'єктно-орієнтованої парадигми. Сучасні високорівневі мови програмування оснащені захисними механізмами, що дозволяють виявляти вразливості переповнення буфера, використання неперевірених вхідних даних як рядок форматування, помилки в логіці програми, такі як безкінечний цикл, тощо. Об'єкти – це спосіб безперешкодно поєднати основний функціонал із супровідним кодом, який гарантує безпечність виконання, без спотворення API (application programming interface). Наприклад, *NSOutputStream*, клас об'єктно-орієнтованого фреймворку Apple Foundation Framework, звільняє розробника від перевірки кодів помилки при записі даних у файл, мінімізуючи вірогідність виникнення вразливостей.

Багатомодульна архітектура програми має багато переваг, але нас цікавить ізоляція коду, що вимагає підвищених привілеїв для виконання операцій. Майже неможливо написати весь проект абсолютно безпечним, в будь-якому разі знайдеться хоча б декілька вразливостей. Якщо зловмиснику вдасться проникнути в програму, що складається лише з одного модуля, для нього це безпрограшна лотерея з головним призом – повний доступ до функцій ядра операційної системи. Кількість місць, що виконують привілейований код, має бути мінімізовано. Модель пропонує обрати одну з наступних багатомодульних архітектур програмного забезпечення: багаторівнева (layered), компонентно-орієнтована (component-based), мікросервісна, ієрархічна або архітектура на основі плагінів.

Фазинг – це техніка випадкової або вибіркової зміни даних і передачі їх програмі із подальшим спостереженням за поведінкою. Якщо програма аварійно завершує роботу або іншим чином поводиться неправильно, це свідчить про потенційну вразливість, яку можна використати при кібератаці. Фазинг користується популярністю серед шкідливих хакерів, які шукають переповнення буфера та інші типи вразливостей. Оскільки його використовуватимуть хакери проти програми, розробники повинні таким самим шляхом виявити будь-які вразливості раніше за них. Робота розробника набагато легша, ніж робота зловмисника. У той час як другий повинен не тільки знайти місця в програмі зі слабкою перевіркою вхідних даних, але й визначити точну природу вразливості і створити план атаки, яка використовує цю вразливість, першому потрібно лише переглянути вихідний код, щоб визначити, як усунути вразливість. Слід пам'ятати, що усунути вразливість набагато легше, ніж довести, що її неможливо використати. Розробники не мають права гаяти час і повинні бути на декілька кроків попереду шкідливих акторів.

Збір даних надзвичайно важливий для підрахунку витрачених ресурсів системи, таких як оперативна пам'ять, час ЦП (центрального процесора) тощо. Зібрана інформація використовується, щоб оптимізувати програмне забезпечення та створювати логи (logs), які повідомляють про надмірне споживання. Непередбачена поведінка програми може означати або випадкову помилку розробника, або використання зловмисниками вразливості. Тож, щоб захистити продукт, повинен бути впроваджений надійний засіб збору даних. Ця наукова стаття пропонує як рішення функції-обгортки. Вони мають такий самий інтерфейс, що й оригінальна функція, і працюють по дуже простому принципу. Перед і після виклику бекенд-функції виконується спеціальний код, в нашому випадку ведення системного журналу. Уявімо, що клієнтська бібліотека надає користувачу (програмісту) можливість надіслати GET запит віддаленому серверу через функцію *url_get*. Ми можемо декларувати свою

однойменну функцію і за допомогою динамічного компонувальника викликати оригінальну версію. Перед тим, як повернути результат, значення 1 додається до загальної кількості звернень і підраховується довжина відповіді сервера. Таким чином, якщо зловмиснику вдасться підставити шкідливий сервер в якості адреси призначення, ми легко зможемо виявити і усунути джерело вразливості, подивившись в журнал зібраної інформації.

Висновки. Створено модель розробки безпечного програмного забезпечення, що складається із семи атрибутів і побудована на методах мінімізації вразливостей та власних пропозицій автора наукової статті по написанню безпечного коду. Вона є середою, де засоби захисту спрацьовують найефективніше, і яку можна використовувати як шаблон для розробки нових проектів. Позитивним наслідком використання моделі по призначенню для компаній, що займаються продажом програмних продуктів, є збільшення прибутку і довіри клієнтів, а для кінцевих користувачів – гарантія безпеки конфіденційної інформації. Подальші розробки включають застосування моделі розробки безпечного програмного забезпечення на реальних продуктах, щоб оцінити її практичне значення, і як вона протистоїть постійно еволюціонуючим загрозам кіберпростору. Можливо, варто буде відкалібрувати коефіцієнти пропозицій, а, можливо, – розширити модель, додавши нові.

Список використаних джерел

1. Збитки від атаки вірусу Petya.A у світі сягають 8 мільярдів доларів – експерт [Електронний ресурс] / слова експерта. – Київ : УНІАН, 2017. – Режим доступу: https://www.unian.ua/science/2003241-zbitki-vid-ataki-virusu-petyaa-syagayut-8-milyardiv-dolariv-ekspert.html (дата звернення: 20.04.2024).
2. CVE-2009-2408 [Електронний ресурс] / номер вразливості присвоєний компанією Red Hat Inc. – Bedford : MITRE, 2009. – Режим доступу: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2408 (дата звернення: 20.04.2024).
3. CWE Top 25 Most Dangerous Software Weaknesses [Електронний ресурс] / список складений MITRE. – Bedford : MITRE, 2023. – Режим доступу: https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html (дата звернення: 20.04.2024).
4. Secure Programming HOWTO / David A. Wheeler. – Версія 3.72, доданий новий розділ. – [Б. м. : б. в.], 2015. – 194 с.
5. Defensive Programming [Електронний ресурс] / M. Tim Jones. – San Francisco : UBM Technology Group, 2005. – Режим доступу: https://www.drdobbs.com/defensive-programming/184401915 (дата звернення: 20.04.2024).
6. 24 Deadly Sins of Software Security / Michael Howard. – 1-е вид. – New York : McGraw-Hill, 2009. – 432 с. – ISBN-13 978-0071626750
7. The Protection of Information in Computer Systems [Електронний ресурс] / Norman Hardy. – Madison : University of Wisconsin-Madison, 1997. – Режим доступу: https://web.mit.edu/Saltzer/www/publications/protection/ (дата звернення: 20.04.2024).
8. Збиток від вірусу WannaCry оцінили в мільярд доларів [Електронний ресурс] / MediaSapiens. – Київ : ГО «Детектор Медіа», 2017. – Режим доступу: https://ms.detector.media/kiberbezpeka/post/18972/2017-05-25-zbytok-vid-virusu-wannacry-otsinyly-v-milyard-dolariv/ (дата звернення: 20.04.2024).
9. Cybercrime cost world economy $620 billion last year [Електронний ресурс] / David Sun. – Сінгапур : SPH Media Limited, Co., 2017. – Режим доступу: https://web.archive.org/web/20220124010351/https://www.kaplan.com.sg/wp-content/uploads/2017/07/TNP_Cybercrime-cost-world-economy-620-billion-last-year_5-July-2017.pdf (дата звернення: 20.04.2024).

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д.О.

ПРИНЦИПИ БЕЗПЕКИ ОСНОВНИХ МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМ

МАЛООКИЙ О.В., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

Стаття присвячена проблемі захисту конфіденційної інформації, що зберігається на мобільних пристроях. Розглядаються основні тенденції розвитку сфери інформаційних технологій, а також засоби захисту інформації для мобільних пристроїв. Наводиться класифікація сучасних мобільних операційних систем та виявляються вимоги до захищеної мобільної операційної системи. Описано алгоритм машини факторизації для виявлення шкідливих додатків

This article addresses the issue of protecting confidential information stored and processed on mobile devices. The article discusses the main trends in the development of information technology, as well as means of protecting information for mobile devices. It provides a classification of modern mobile operating systems and identifies requirements for a secure mobile operating system. Developed an actorization algorithm for detecting malicious applications.

Актуальність. Однією з основних тенденцій розвитку сфери інформаційних технологій є збільшення частки мобільних пристроїв, таких як смартфони або планшетні персональні комп'ютери, по відношенню до традиційних ПК. Варто зазначити, що за підсумками 2022 року загалом постачання смартфонів у світовому масштабі зменшилося порівняно з 2021-м на 11% – до менш ніж 1,2 млрд одиниць. Лідером з обсягу продажів стала південнокорейська компанія Samsung з часткою 22% проти 20% 2021 року. На другому місці знаходиться Apple: за рік компанія зміцнила позиції з 17% до 19%. Apple стала найбільшим виробником смартфонів у світі в 2023 році – Samsung відстала на 8 млн З 2011 по 2022 роки включно південнокорейської компанії Samsung Electronics вдавалося утримувати статус найбільшого постачальника смартфонів, але за підсумками 2023 року його вдалося отримати Apple, якщо вірити статистиці IDC. Робота даних пристроїв, також як і в персональних комп'ютерах, здійснюється під управлінням операційних систем, які за своїм принципом побудови та роботи багато в чому аналогічні операційної системи для персонального комп'ютера. При цьому смартфони та планшетні ПК зберігають і обробляють дані, які, як правило, представляють для їх користувачів не меншу, а часто й більшу цінність, ніж інформація, що зберігається та обробляється на ПК. До таких даних відносяться списки контактів, приватне листування з використанням сервісу служба коротких повідомлень, нотатки, які користувач робить у спеціальному програмному забезпеченні свого пристрою, списки викликів абонентом з прив'язкою до часу, електронні поштові повідомлення та ін. В даний час існує кілька тенденцій, які роблять актуальним питання забезпечення захисту мобільних операційних систем від атак з боку зловмисників.

Метою статті є аналіз принципів безпеки основних мобільних операційних систем та їх вплив на забезпечення конфіденційності, цілісності та доступності даних користувачів. Ознайомитися з причинами та способами попередження втрати інформації на мобільних телефонах, поняттями мобільного віруса та антивіруса

Об'єктом дослідження є принципи безпеки, реалізовані в основних мобільних операційних системах, які включають, але не обмежуються архітектурою систем, методами аутентифікації, механізмами шифрування даних, контролем доступу, захистом від вірусів та іншими засобами безпеки.

Предмет дослідження є система безпеки, що використовуються в основних мобільних операційних системах, таких як iOS, Android.

Аналіз попередніх досліджень. Дослідження принципів безпеки в основних мобільних операційних системах праці вітчизняних та закордонних науковців В.М Федорченко, І.В. Гензерський, Н.Ю. Шевякова, Є. М. Бровченко, В. П. Самарай, І. П. Даценко, В. І. Павленко, А.В. Середа, Jorja Wright, Maurice E. Dawson Jr, Marwan Omar. Попередні дослідження на цю тему виявили різноманітні аспекти, які варто враховувати при оцінці та вдосконаленні безпеки мобільних операційних систем.

Виклад основного матеріалу. Однією з найбільш помітних тендецій розвитку комп'ютерної техніки останні роки є неухильне зростання обчислювальної потужності мобільних електронних пристроїв: мобільних телефонів, планшетних комп'ютерів, електронних книг тощо. За даними Всесвітнього економічного форуму (ВЕФ), кіберзлочинність стала третьою за величиною економікою світу після США та Китаю. Cybersecurity Ventures прогнозує, що 2024 року це коштуватиме світові $9,5 трлн. Розвиток ШІ сприяє цій тенденції. Наприклад, злочинці вже використовують генеративні моделі для верифікації акаунтів за допомогою фотографій. Наслідок – користувачі втрачають довіру до онлайн-сервісів та мобільних застосунків. Отже, інвестиції у кібербезпеку та захист конфіденційних даних стануть трендом розробки мобільних застосунків. Gartner пропонує системний підхід CTEM (Continuous Threat Exposure Management), який допоможе скоротити кількість несанкціонованого втручання в системи на 60%. Цей фреймворк допоможе правильно оцінювати ризики, пріоритезувати вектори критичних загроз, аналізувати їх з точки зору зловмисника та тестувати ефективність заходів безпеки. Сучасні мобільні пристрої оснащуються повноцінними операційними системами, близькими за своїми можливостями до універсальним операційним системам персональних комп'ютерів. Не дивно що мобільні операційні системи запозичують від універсальних операційних систем як окремі алгоритмічні рішення, а й цілі програмні компоненти. Так найпоширеніша на сьогоднішній день мобільна операційна система Google Android використовує те саме ядро, що й універсальна операційна система Linux, а друга за популярністю мобільна операційна система Apple IOS побудована на основі прикладних інтерфейсів універсальних операційних систем сімейства BsD UNIX.

Типові загрози безпеці операційної системи мобільного пристрою суттєво відрізняються від аналогічних загроз для операційної системи персонального комп'ютера чи мережевого сервера. Деякі загрози, незначні для звичайних комп'ютерів стають дуже небезпечними для мобільних пристроїв, і навпаки. Програмне забезпечення, впроваджена в операційну систему персонального комп'ютера і доступ до електронних банківських рахунків кристувача, зазвичай має дуже обмежені повноваження по несанкціонованому переказу коштів з цих рахунків [1-2]. Але програмна закладка, впроваджена в операційну систему мобільного пристрою, елементарно вирішує це завдання шляхом несанкціонованого замовлення дорогих SMS-послуг з телефонного номера, котрольованого порушником, або (рідше) шляхом імітації голосового дзвінка на платний номер. З іншого боку, загрози, пов'язані з одночасним доступом кількох користувачів до одного екземпляра операційної системи для мобільних операційних систем, як правило, неактуальні.

До найбільш актуальних загроз безпеки мобільних операційних систем зазвичай відносять такі: розкриття конфіденційної інформації внаслідок втрати або крадіжки мобільного пристрою; несанкціоноване замовлення дорогих послуг програмною закладкою, упровадженою в операційну систему мобільного пристрою; розкриття конфіденційної інформації внаслідок перехоплення бездротового мережевого трафіку, що генерується мобільним пристроєм; несанкціонований збір програмною закладкою персональних даних користувача мобільного пристрою; втрата даних, що зберігаються на мобільному пристрої. Одним з найпоширеніших видів атак став також фішинг з використанням URL- адрес, схожих на адреси веб-сайтів податкових служб, подарункових ваучерів, преміальних програм і облікових записів в соціальних мережах [2]. Також потрібно не забувати про те що пошук вразливостей є ще більш загрозливою активністю в мережі. Якщо його проводить неуповноважена або некомпетентна особа, можуть виникнути наслідки, такі як відмова

систем або їх компонентів, втрата або псування інформаційних ресурсів, розголошення конфіденційної інформації. Але ті ж дії у виконанні грамотних адміністраторів є невід'ємною складовою мережевої безпеки. Сканери безпеки бувають комерційні і вільні (безкоштовні). Мабуть, найвідоміший з комерційних сканерів – Internet Scanner, продукт компанії Internet Security Systems [3].

Мобільні віруси – це невеликі програми, призначені для втручання в роботу мобільного телефону, смартфона, комунікатора, які записують, пошкоджують або видаляють дані і поширюються на інші пристрої через SMS та Інтернет. Вперше про мобільних вірусах заговорили ще в 2000 році. Вірусами назвати їх було важко, так як це був набір команд, виконуваний телефоном, який передавався через SMS. Такі повідомлення забивали відповідні комірки пам'яті і при видаленні блокували роботу телефону. Найбільшого поширення набули команди для таких телефонів, як Siemens і Nokia [4]. У недалекому минулому основною платформою, для якої писали віруси, була Symbian. Однак ситуація на ринку мобільних телефонів складається таким чином, що смартфони на Symbian, хоча і вельми популярні, поступаються чималі частини ринку апаратам інших виробників. Наприклад, пристроям на Windows Mobile, це iPhone та інші платформи. Тенденція така, що чим функціональніший телефон, тим до більшої кількості загроз він схильний. Будь-які команди, функції та можливості, що дозволяють створювати програми і програми для мобільних телефонів, можуть стати інструментом для створення вірусів. Основною метою мобільних вірусів, як і у випадку з комп'ютерними вірусами, є отримання персональної інформації, яку можна продати або використати в особистих потребах. До такої інформації можуть відноситися особисті дані власника телефону, дані самого пристрою, приватні повідомлення, інколи номери кредитних карт.

Викрадення даних, що зберігаються у додатках, завжди вважається однією з найбільш критичних загроз безпеці Android. Дослідження показують, що це може статися навіть для додатків, які в принципі не мають вразливостей, але вразливості можуть бути у самій операційній системі, наприклад, спільне використання мережевих даних. Під час атаки шкідливий додаток може функціонувати у фоновому режимі і збирати дані цільового додатку. Багато додатків використовують інформацію, що зберігається в базах даних. Крім того, додаток може взаємодіяти з базами даних іншого додатку, що надає такі функціональні можливості. Вразливий додаток може дозволити шкідливій програмі порушувати цілісність та конфіденційність даних, що зберігаються в базах даних [5]. Така легкість в отриманні несанкціонованого доступу до вмісту файлів спровокувала появу великої кількості спеціальних інструментів, розрахованих на усунення проблеми доступу до коду додатків. Крім того, важливою проблемою залишається можливість аналізу коду додатку за допомогою реверс – інжинірингу. А саме, дослідження коду додатку, а також документації на нього з метою розуміння принципів його роботи, захисних механізмів, зберігання даних тощо для виконання несанціонованої зміни або копіювання, використання додатку чи іншого об'єкта з аналогічними функціями. В даний час для мобільних операційних систем розробляється величезна кількість шкідливого програмного забезпечення. За даними, близько чверті всіх програм, написаних для операційної системи Android, є шкідливими. Кількість шкідливих програм для Android зростає експонеційно, щороку воно збільшується у 2-16 разів. Така велика різниця в цифрах, що даються різними джерелами, пояснюється тим, що межа між множинами шкідливих і неушкоджених мобільних додатків є програми, що дозволяють легальному власнику телефону виявити вкрадений у нього телефон шляхом непомітного перехоплення та доставки на задану адресу електронної пошти інформації про зроблені дзвінки, відправлених та отриманих SMS, географічному розташування тощо. Якщо такий додаток таємно встановлено на мобільному пристрої, що належить чужому людині, воно є шкідливим. Але якщо воно таємно встановлено на телефон, подарований дружині або дитині, питання про шкідливість програми не є очевидним. Інший приклад «прикордонних» додатків – нав'язливі банерні мережі.

Типовими симптомами зараження мобільного пристрою шкідливими програмами є: Незрозуміло швидке зменшення коштів на рахунку; поява нових ярликів у списку встановлених програм; поява незрозумілих записів у папках отриманих та надісланих SMS повідомлень або у списках вхідних та вихідних голосових дзвінків; стрибкоподібне збільшення витрат електроенергії без видимих причин [6].

Не менш серйозною проблемою ніж зловмисне програмне забезпечення, є некоректно працюючі мобільні програми, що завдають шкоди користувачеві ненавмисно в результаті допущених розробниками програмних помилок. Користувачі часто не розуміють, що причина некоректної роботи мобільного пристрою, криється не в пристрої як такому, а в недостатньо налагодженому додатку. В результаті недопрацьовані програми можуть надавати помітний негативний вплив на репутацію розробників операційної системи мобільного пристрою.

Компанія Apple вирішує цю проблему шляхом ретельного тестування всіх мобільних додатків сторонніх виробників, розроблених для iPhone та iPad. Таке тестування може займати кілька тижнів, більше половини додатків у результаті отримують відмову у розміщенні в офіційному онлайн-магазині Apple App Store. За деякими відомостями, причиною відмови часто є недостатньо високе якість програми, а те, що цей додаток може скласти конкуренцію власним розробкам Apple. Крім того, кожен виробник програмного забезпечення для iOS повинен бути попередньо зареєстрований в Apple App Store, що коштує від 100 доларів США на рік. Хоча ця сума і є суто символічною багатьох вірусописачів навіть така сума є неприйнятною [4-5]. Загалом дана стратегія дозволяє радикально скоротити кількість та різноманітність шкідливого програмного забезпечення, що розробляється для операційної системи iOS. Поки відомий лише один шкідливий додаток, що зумів проникнути на Apple App Store і отримати помітне поширення – спам-бот Find and Call. Декілька інших шкідливих програм (у тому числі і знаменитий вірус Ike) небезпечні тільки для тих мобільних пристроїв, на яких зламано програмне блокування, що забороняє встановлення додатків із джерел, відмінних від App Store (тобто виконаний jailbreak). З іншого боку, обмеження доступу сторонніх фірм до ринку додатків для iOS помітно знижує популярність цієї операційної системи серед кінцевих користувачів.

Android Market допускаються всі програми, крім свідомо шкідливих та свідомо непрацездатних. Іноді це призводить до скандальних ситуацій, негативно позначаються на репутації торгової марки Android. Наприклад, Android-версія eMobiStudio MemoryUp, що добре зарекомендував себе на платформах Symbian, BlackBerry та Windows Mobile, несанкціоновано видалила через програмну помилки дані адресних книг кількох тисяч користувачів, які встановили цю програму. Відкритість операційної системи Android не слід перебільшувати. На відміну від більшості розробників універсальних операційних систем Google зберігає за собою контроль над усіма додатками, що працюють на всіх примірниках ОС Android. При необхідності компанія Google так само, як і Apple може одночасно видалити всі екземпляри будь-якої заданої програми, встановлений на всіх мобільних пристроях зі своєю операційною системою.

При цьому розробники мобільних операційних систем широко використовують рішення, випробувані на універсальних операційних системах. Так, у версії 4.2 ОС Android почала підтримуватися функція довіреного підтвердження користувачем потенційно небезпечної дії, дуже схожа на UAC в Windows. Ця функція використовується за умовчанням під час надсилання SMS-повідомлень – до тих пір, поки користувач не підтвердить відправлення повідомлення, воно не буде надіслано, при цьому прикладні програми не мають технічної можливості імітувати це підтвердження. Для попередніх версій Android існують програми третіх фірм (наприклад, LBE Security Master, LBE Privacy Guard), що реалізують аналогічну функціональність. У мобільних операційних системах широко застосовується давно використовується в універсальних операційних системах ідентифікація програмних файлів цифровим підписам. Подібно до того, як користувач Windows може заборонити встановлення на свій комп’ютер драйверів, які не мають цифрового підпису

Microsoft, користувач Android може заборонити встановлення на свій пристрій програмних файли, безпека яких не підтверджена Google.

Як правило, на пристроях, що працюють під керуванням iOS, виконуються тільки довірені додатки, ретельно перевірені та схвалені фахівцями Apple. Тому до системи управління доступом iOS не пред'являється високих вимог. Таким чином, незважаючи на свою крайню примітивність, підсистема управління доступом iOS є цілком задовільною. Принцип мінімізації повноважень дотримується в базових конфігураціях як Android, так і iOS (втім, в останньому випадку не цілком зрозуміло, чи можна коректо говорити про принцип мінімізації повноважень для такої примітивної системи розмежування доступу) – жодна програма не має технічної можливості отримати повноваження суперкористувача root. Однак багато користувачів Android та деякі користувачі iOS відключають цей захист. В результаті програми, в тому числа і шкідливі, отримують більше функціональних можливостей, до яких входять можливості реалізовувати стелс-технології та активно протидіяти засобам адміністрування та антивірусного програмного забезпечення.

Операційна система iOS зберігає всі дані в частині користувача зовнішньої пам'яті у зашифрованому вигляді. Найбільш конфіденційні дані зазнають додаткового шифрування. Ключі, що використовуються при цьому, не надаються користувачем, а зберігаються у внутрішній пам'яті пристрою, тобто захист фактично реалізується тільки від порушника, який намагається прочитати зовнішню пам'ять цього пристрої, використовуючи інший пристрій. В операційній системі Android, на відміну від iOS, шифрування даних практично не застосовується, хоч і підтримується. Практично всі виробники антивірусного програмного забезпечення вже розробили версії своїх програм для операційної системи Android по архітектурі та функціональності мобільні антивірусні комплекси не мають принципових відмінностей від антивірусних комплексів, призначених для застосування на персональних комп'ютерах чи серверах.

Антивірусні програми для мобільних операційних систем часто доповнюються так званою «протиугінною» функціональністю, що дозволяє легальному користувачу пристрою знайти свій пристрій за сигналами GPS, віддалено змусити пристрій видати гучний звуковий сигнал, що привертає увагу оточуючих до злодія, видалено знищити персональні дані, що зберігаються на пристрої. Ефективність такого захисту залишає бажати кращого. Після вимикання та повної перепрошивки вкраденого пристрою весь протиугінний функціонал вимикається. Крім того, навіть протиугінна, що справно працює. програма не завжди дозволяє повернути вкрадений пристрій.

З урахуванням наведеної класифікації загроз захищена мобільна ОС має реалізовувати такі функціональні можливості та компоненти: блокування пристрою у періоди невикористання; шифрування інформації, що захищається, що зберігається на запам'ятовуючих пристроях мобільного терміналу; автентифікація при вході до системи; обмеження доступу програмних засобів сторонніх виробників до функцій пристрою; контроль цілісності спеціального та загальносистемного програмного забезпечення під час завантаження ОС, а також за розкладом; перевірка електронного підпису встановлюваних сторонніх додатків; реєстрація спроб доступу сторонніх програмних до функцій пристрої; видалення даних та/або ключовий інформації у разі виникнення однієї з подій: неправильне введення пароля більше три рази; вихід або потрапляння до територіальної зони, заданої на основі географічних координат; реєстрація спроб аутентифікації користувача у системі; реалізується підтримка технології віртуальної приватної мережі із шифруванням IP-трафіку; зберігання ключової інформації у зашифрованому вигляді.

Для того щоб запобігти зараженню мобільним вірусом, слід пам'ятати про заходи безпеки. Творці шкідливого ПЗ широко використовують засоби соціальної інженерії для розповсюдження своїх програм, часом – досить примітивних, які не вміють розмножуватися самостійно, але вміють робити щось інше [6-8]. Так, наприклад, зловмисник може написати програму, яка таємно відправляє платні SMS з зараженого телефону. Цю програму можуть безкоштовно пропонувати для скачування з Інтернету та встановлення на мобільний

телефон. Як правило, подібні програми мають вельми привабливі назви. У результаті, встановивши своїми руками на свій же телефон шкідливу програму, власник апарату може позбутися засобів на рахунку, а до усього іншого, втрачати їх регулярно.

Основні можливості програм-антивірусів: виявлення вірусів, шпигунських програм та інших загроз; блокування переходів по шкідливим і фішингових посиланнях; фільтрація небажаних дзвінків та SMS; приховування особистих контактів, дзвінків та SMS-повідомлень; можливість віддалено заблокувати смартфон, стерти особисті дані та визначити місцезнаходження пристрою в разі втрати або крадіжки; мінімальне використання ресурсів батареї: Dr.Web Mobile Security Suite підтримується най сучасними операційними системами: Android OS, S60, Symbian, Windows Mobile.

У стандартних моделях нейронних мереж для виявлення шкідливих додатків по вектору характеристик безпеки не враховується так звана «взаємодія» характеристик. Очевидно, якщо в додатку є кілька небезпечних характеристик, об'єднання деяких з них може однозначно вказувати на шкідливість програми – саме в цьому полягає зміст обліку «взаємодії» характеристик безпеки додатків. «Взаємодія» характеристик представлена їх попарним впливом один на одного за принципом кожна з кожною, таким чином формується матриця розміром n^2 де n – кількість характеристик. Оскільки характеристик велика кількість, то тільки зберігання матриці розміром їх кількості в квадраті вимагає великих витрат пам'яті, а враховуючи те, що на кожному кроці навчання мережі елементи матриці повинні змінюватись, тобто відбувається постійне взаємодія з такою великою структурою, навчання вимагатиме не тільки великих витрат пам'яті, а й часу. Машини факторизації були представлені Штеффеном Рендлом 2010 року як клас нових нейромережевих моделей, що поєднують у собі переваги машини опорних векторів та факторизаційних моделей. Машини факторизації можуть виконувати завдання регресії, класифікації та ранжирування. Особливість машин факторизації полягає в обробці будь-яких вхідних векторів, що представляють об'єкти реального світу, та оцінки парних взаємодій їх елементів навіть за сильної розрідженості цих векторів, на відміну від SVM, які не можуть працювати з сильно розрідженими даними, чи можуть, але видають низьку точність. Ще одна перевага машин факторизації – лінійна складність $O(kn)$, де k – гіперпараметр, що визначає розмірність факторизації, а n – кількість ознак описуваного об'єкта (розмір вхідного вектора). Найбільшу популярність машини факторизації набули у рекомендаційних системах, які повинні враховувати парні взаємодії, при цьому маючи сильно розріджені дані. Однак, більшість даних, що описують об'єкти реального світу, є сильно розрідженими в силу наявності множин можливих ознак, але які містять у собі лише малу частина всіх цих ознак. Так само і Android додатки – всі разом мають безліч, залежно від вибору, від десятків до сотень тисяч, характеристик безпеки, але окремі додатки, найчастіше, включають лише кілька характеристик і в рідкісних випадках близько тисячі характеристик, що все одно є малою частиною від їхньої загальної кількості. Математично, ідея взаємодії компонентів x з вагами w записується у вигляді поліноміальної регресії другого порядку:

$$h(x) = w_0 + \sum_{i=1}^{n} w_i x_i + \sum_{i=1}^{n} \sum_{j=i+1}^{n} W_{ij} x_i x_j$$

де W − матриця ваг взаємодії x_i та x_j. Якщо уявити v_i як i − рядка V, нейронна мережа буде тренувати прихований вектор v_i для кожного x_i та ваги моделі парної взаємодії w_{ij} будуть представлені як скалярні твори відповідних прихованих векторів для x_i та x_j:

$$h(x) = w_0 + \sum_{i=1}^{n} w_i x_i + \sum_{i=1}^{n} \sum_{j=i+1}^{n} \langle v_i, v_j \rangle x_i x_j \quad (1),$$

де скалярний добуток векторів v розмірності k вважається за такою формулою:

$$\langle v_i, v_j \rangle = \sum_{m=1}^{k} v_i, m v_j, m.$$

Формула (1) і є математичне уявлення моделі машини факторизації. У моделі машини факторизації параметри w_0, w_i, v_i тренуються та оновлюються із використанням стохастичних методів, які виконують псевдовипадкові зміни величин ваги, зберігаючи ті зміни, які ведуть до поліпшень. На практиці найчастіше застосовується метод градієнтного спуску.

Приховані вектори v_i формуються в процесі навчання мережі та найчастіше їх розмірність k набагато менше n – розміру вхідного вектора x, в силу його розрідженості. Це гарантує те, що не доведеться зберігати велику кількість непотрібних даних і працювати з матрицею розміру $n \times n$. Завдяки цьому уявленню складність методу і знижується з $O(n2)$ до $O(kn)$.

Висновки. Операційні системи продовжують еволюціонувати, включаючи все більше функцій і опцій. З розвитком інтернету ОС почали включати мережеві можливості, підтримку віртуалізації, хмарні технології та багато іншого. Мобільні ОС, такі як Android та iOS, принесли нові тенденції у розвиток, включаючи покращені методи взаємодії з користувачем, ефективне управління енергоспоживанням та інтеграцію з різними видами пристроїв. Історія та еволюція ОС показують динамічний та вражаючий шлях від простих систем управління завданнями до складних та багатофункціональних продуктів. Вони відображають зміни у технологіях та потребах суспільства, а також продовжують формувати основу для майбутніх інновацій в інформаційних технологіях.

Якщо постійно моніторити ринок, використовувати основні способи захисту, встановлювати нові антивіруси та програми захисту, можна захистити свій мобільний телефон на 99,9%. Повного захисту досягти практично неможливо, оскільки випускаються постійно як нові способи захисту, а й нові віруси. Підводячи підсумки, щоб залишатися в безпеці, не варто заходити на сайти, що викликають підозри, не качати ніякі файли з піратських сайтів, і дотримуватися кроків щодо забезпечення безпеки свого мобільного телефону, перелічені в цій статті і тоді ніхто не вкраде пароль від картки або соціальної мережі.

Список використаних джерел

1. Богуш В.М., Кривуца В.Г., Кудін А.М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуці В. Г. Київ. 2004. 508 с.
2. Бровченко, Є. М., Самарай, В. П., Даценко, І. П., Павленко, В. І. (2023). Мобільний пристрій як частина адаптивної кейс-менеджмент системи. Інфокомунікаційні та комп'ютерні технології, 2(04), С. 157–163. https://doi.org/10.36994/2788-5518-2022-02-04-18.
3. Baryshev, Y., Kaplun, V. and Neiyumina, K. «Discretional model and method of distributed information re-sources access control». In Scientific Works of Vinnytsia National Technical University. 2 (Jun. 2017).
4. Богуш В. М., Юдін О. К. «Інформаційна безпека держави». К.: «МКПрес», 2005. 432 с.
5. Вєртузаев М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник/За ред. С.Г. Лаптєва. К.: Видавництво Європейського університету, 2001. 201 с.
6. ДСТУ ISO/IEC 27001: 2015 Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001: 2013, IDT).

7. Лєнков С. В., Перегудов Д.А., Хорошко В. А. Методи та засоби захисту інформації (в 2-ох томах). К: Арий, 2008.

8. Федорченко В.М. Аналіз загроз для мобільних пристроїв та способів їх захисту / В.М. Федорченко, І.В. Гензерський, Н.Ю. Шевякова // Системи обробки інформації. – 2011. – № 7. – С. 68-71.

Робота виконана під науковим керівництвом д-ра екон. наук, професора
ЧУБАЄВСЬКОГО В.І.

БЕЗПЕКА ОБЛІКОВИХ ДАНИХ У ВЕБДОДАТКАХ МЕТОДАМИ ДВОФАКТОРНОЇ АВТОРИЗАЦІЇ

МІЛЕВСЬКИЙ Д.В., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто основні методи побудови систем двофакторної авторизації, оцінюється ризик різних методів онлайн-атак проти систем двофакторної авторизації PassWindow. Проводиться порівняльний аналіз різних систем двофакторної авторизації з системою PassWindow у сфері протидії різним сценаріям атак.

The article considers different ways of two factor authorization systems building, assesses risks of different online attacks against PassWindow two factor authorization systems. A comparative analysis is carried out for different two factor authorization systems using PassWindow in the field of countering various attack scenarios.

Актуальність. Інформація піддається різним видам несанкціонованих дій, таких як витік, отримання користувачем неправомірного доступу та прав до ресурсів. Правильно побудована система керування та управління доступом може значно знизити ризики подібних випадків, що є одним із найважливіших завдань інформаційної безпеки.

Статичні пари ідентифікатору і паролю, що використовуються в більшості існуючих систем, можуть бути скомпрометовані за допомогою різних вид атак, таких як підбір, перехоплення та соціальна інженерія. Такі атаки є можливими завдяки великим інтервалам часу, протягом яких ідентифікатор та пароль залишаються без змін. Адміністратори деяких систем створюють обмеження у вигляді строку, протягом якого пароль може залишатися незмінним. Проте зазвичай цей строк становить тижні або навіть місяці, що дає достатньо часу зловмисникам для проведення атаки.

Рішенням даної проблеми є застосування двофакторної авторизації, коли система окрім ідентифікатора з паролем вимагає від користувача додаткову інформацію (таку як код) або апаратний ідентифікатор, що асоціюється з користувачем.

Метою статті є дослідження основних методів побудови систем двофакторної авторизації.

Об'єктом дослідження є захист облікових даних.

Предмет дослідження – двофакторна авторизація.

Двофакторна система авторизації базується на тому, що окрім паролю до певного імені, користувач також володіє інструментом для отримання відповідного йому ключа доступу. Це може бути збережений електронний сертифікат, отриманий разовий код, біометрія тощо [1].

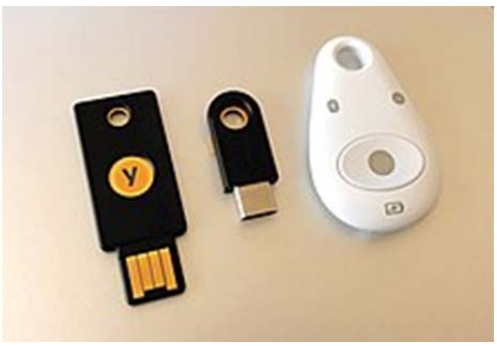


Рис. 1. Апаратні ключі двофакторної авторизації

Джерело: [2]

Основні способи побудови систем двофакторної авторизації [3]:

Програмне забезпечення для ідентифікації конкретного комп'ютера. На комп'ютер встановлюється спеціальна програма, що створює в ньому криптографічний маркер. Так як маркер постійно знаходиться на комп'ютері, користувачу потрібно вводили лише ім'я (логін) та пароль.

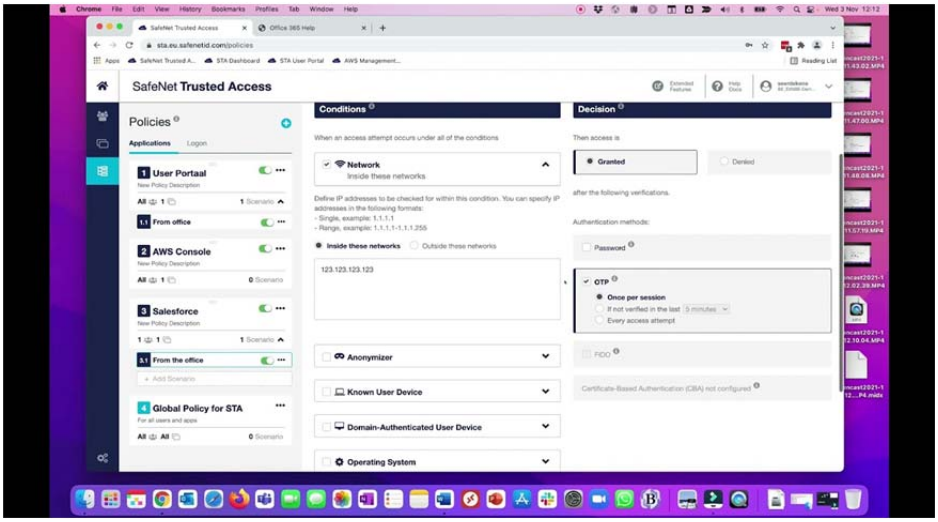


Рис. 2. Thales SafeNet Trusted Access

Джерело: [4]

Біометрія – ідентифікація на основі фізичних характеристик людини, таких як відбиток пальця, око, голос тощо.

Рис. 3. SUPREMA ID RealScan-S60

Джерело: [5]

Повідомлення (електронна пошта, телефон) з разовим паролем. В даному випадку користувачу надсилається разовий код на зареєстровану адресу електронної пошти або номер телефону.

Токен з разовим паролем. Користувач має пристрій, котрий постійно генерує нові паролі.

Програмні генератори разових паролей. Дуже розповсюджений спосіб двофакторної авторизації. Користувач встановлює додаток-генератор на телефон або комп'ютер (Google Authenticator [7], KeePassXC [8] та ін.) та додає секрет (введення користувачем, сканування QR-коду), після чого додаток буде постійно генерувати разові паролі.

Рис. 4. Токен з разовим паролем

Джерело: [6]

Загрози безпеки можна розділити на мережеві та локальні атаки, що відбуваються завдяки шкідливим програмам, таким як трояни та руткіти. Зазвичай оцінка безпеки авторизації зосереджена на мережевих атаках припускаючи, що користувацький термінал (персональний комп'ютер, ноутбук, мобільний пристрій) є захищеною платформою. Однак, зловмисник може отримати повний доступ до пристрою користувача через процеси зв'язку, що залишились від шкідливих програм.

Типові методи атак:

- Злам онлайн баз даних.
- Людина посередині (MITM, англ. Man-in-the-Middle), фішинг – третя сторона втручається і 3. представляє одразу і клієнт і сервер, прослуховуючи та змінюючи трафік.
- Соціальна інженерія – обман користувача з метою отримання особистих даних.
- Підбір пароля (англ. Brute Force).
- Крадіжка, підглядання.

Переваги та недоліки:

1. Разовий пароль через пошту або телефон:

1.1. Переваги:

1.1.1 При кожному вході відбувається генерація нового коду. Навіть якщо зловмисник перехопить логін та пароль, злам не буде можливим без додаткового коду.

1.1.2 Прив'язка до номеру телефону та/або пошти. Без доступу до них вхід не є можливим.

1.2. Недоліки:

1.2.1. Неможливість виконати вхід за відсутності мобільної мережі (в разі отримання кодів за допомогою SMS)

1.2.2. Якщо авторизація відбувається на тому ж пристрої, що генерує разовий код, авторизація перестає бути двофакторною.

2. Додатки-аутентифікатори:

2.1. Переваги:

2.1.1. Не потребує наявності мобільної мережі або мережі інтернет.

2.1.2. Підтримка декількох акаунтів.

2.2. Недоліки:

2.2.1 Існує вірогідність зламу первинного ключа. Тоді зловмисник отримує можливість генерувати всі наступні паролі.

2.2.2. Втрачається двофакторність при використанні на тому ж пристрої, з якого виконується авторизація.

3. Мобільні додатки:

3.1. Переваги:

3.1.1 Нема потреби додаткового введення паролю при виконанні авторизації.

3.1.2. Не потребують наявності мобільної мережі.

3.1.3. Підтримка декількох акаунтів.

3.2. Недоліки:

3.2.1. При перехопленні приватного ключа можлива підробка ідентифікатора.

3.2.2. Втрачається двофакторність при виконанні авторизації на тому ж пристрої, де встановлено додаток.

4. Токени:

4.1. Переваги:

4.1.1. Нема потреби у використанні мобільного телефону.

4.1.2. Самостійний пристрій.

4.2. Недоліки:

4.2.1. Пристрій купується окремо.

4.2.2. Менше сервісів підтримують даний метод двофакторної авторизації.

4.2.3. Загублений пристрій може призвести до зламу зловмисником.

PassWindow. PassWindow – спосіб надання двофакторної авторизації в онлайн середовищі. Він включає в себе дві частини матриці, котрі є фізичним ключем з надрукованим шаблоном на пластиковій картці, та шаблоном цифрового штрих-коду, що представляється у вигляді зображення на прозорому електронному дисплеї, такому як екран комп'ютера або мобільного пристрою. При накладенні одна на одну, вони створюють унікальний разовий пароль та набір чисел. Отриманий пароль використовується для виконання авторизації. Числа містять таку інформацію, як номер рахунку та сума транзакції, що дозволяє користувачу візуально підтвердити справжність запиту на авторизацію.

Ці особливості роблять PassWindow одним з небагатьох механізмів авторизації, що дають надійний захист від мережевих атак типу «людина посередині».

Технологія базується на можливості матриць передавати інформацію таким чином, при якому вона розшифровується лише при накладенні фізичного шаблону символів, після чого відображається шаблон штрих-коду на електронних мережевих пристроях користувача. Поєднання ключа та шаблону штрих-коду відображає закодовану інформацію лише одному користувачу, а повний перегляд шаблону доступний лише під прямим кутом. Будь-яке перехоплення штрих-коду через електронні пристрої зробить інформацію недостатньою для отримання секретного ключу шаблону користувача зловмисником, протягом усього строку дії карти.

Шаблони штрих-коду можуть бути як статичними зображеннями послідовності символів, так і більш розширеною анімованою версією. Ці анімовані штрих-коди містять послідовність статичних шаблонів, кожен з яких містить закодовані символи або нічого не означає і існує лише для додавання ентропії у весь шаблон. Послідовності шаблонів штрих-коду генеруються динамічно сервером авторизації таким чином, що кожен є унікальним лише при використанні разом з ключем, якому він відповідає.

Будь-який буквено-числовий код можна надійно передати за допомогою методу PassWindow, проте поточна реалізація направлена на передачу коротких рядків випадкових цифр для їх подальшого використання в якості разового коду, разом з цифрами, що ідентифікують унікальність транзакції.

Рис. 5. Процес авторизації PassWindow

Джерело: адаптовано з джерела [9].

Де необхідна двофакторна авторизація.

1. Віддалений доступ до корпоративної мережі. Велика кількість компаній використовує технології VPN, через які співробітники можуть підключатися віддалено. Додатковий спосіб авторизації допомагає покращити безпеку корпоративної мережі.

2. Сайти електронної торгівлі. Інтернет-бізнес потребує від користувача ділитися інформацією про платежі, персональними даними. Зберегти свої персональні дані користувачу допомагає двофакторна авторизація, що надає безпеку від зламу особистого кабінету шляхом підтвердження за допомогою SMS при зміні паролю, здійсненні покупки або будь-яких змінах в особистому кабінеті.

3. Завантаження додатків. Якщо користувач завантажує додаток з соціальних мереж, додаток для зв'язку, варто впевнитись, що це реальний користувач, що намагається увійти в систему, а не «бот».

Висновки. Проведений аналіз методів двофакторної авторизації показав, що практично усі системи використовують в своїй основі криптографічні алгоритми (таблиці) та піддаються як традиційним атакам на криптографігні процедури, так і атакам соціальної інженерії, не надають повної безпеки їх використання. Особливе місце серед них займає система двофакторної авторизації PassWindow. Вона заснована на використанні штрих-кодів для формування аутентифікатора, що є більш ефективним за інші та протистоїть онлайн-атакам.

Список використаних джерел

1. Налаштування двофакторної аутентифікації [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/en/wi-configure-two-factor-authentication-gransden.html.

2. Multi-factor authentication [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Multi-factor_authentication.

3. Що таке двохфакторна автентифікація? [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-two-factor-authentication-2fa.

4. Thales SafeNet Trusted Access demo [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.google.com/url?sa=i&url=https%3A%2F%2Fm.youtube.com%2Fwatch%3Fv%3D_moofzOJjfY&psig=AOvVaw1Pl5-aCAPD1mC8ZXXHR8xE&ust=1712087256256000&source=images&cd=vfe&opi=89978449&ved=0CBMQ3YkBahcKEwigmKma5KGFAxUAAAAAHQAAAAAQAw.

5. SUPREMA ID RealScan-S60 [Електронний ресурс] – Режим доступу до ресурсу: http://es-trade.kiev.ua/uk/realscan-s60.6XvLMh/.

6. Multi-factor Authentication (MFA) for Staff and Faculty [Електронний ресурс] – Режим доступу до ресурсу: https://it.sonoma.edu/kb/security/mfa-using-duo.

7. Get verification codes with Google Authenticator [Електронний ресурс] – Режим доступу до ресурсу: https://support.google.com/accounts/answer/1066447?hl=en&co=GENIE.Platform% 3DAndroid.

8. KeePassXC FAQ [Електронний ресурс] – Режим доступу до ресурсу: https://keepassxc.org/ docs/#faq-yubikey-otp.

9. An evaluation of hypothetical attacks against the PassWindow authentication method [Електронний ресурс] – Режим доступу до ресурсу: https://www.passwindow.com/ evaluation_of_hypothetical_attacks_against_passwindow.pdf

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ У СИСТЕМАХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

ОНОШЕНКО С.С., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

Технології зберігання та захисту інформаційних ресурсів в системах електронних платежів є надзвичайно актуальними. Завдяки постійному розвитку облачних платформ, методів шифрування та блокчейну, вдалося досягти високого рівня безпеки та надійності. Розширення мобільних платежів ставить завдання на оптимізацію зберігання та захисту даних.Нині безпека даних є надзвичайно важливою темою через зростання кіберзагроз та комп'ютерних злочинів. Розробники та експерти постійно вдосконалюють технології зберігання та методи захисту для забезпечення максимального рівня безпеки електронних платежів.

The technologies for storing and protecting information resources in electronic payment systems are highly relevant. Thanks to the continuous development of cloud platforms, encryption methods, and blockchain, a high level of security and reliability has been achieved.

The expansion of mobile payments poses a challenge for optimizing data storage and protection. Data security is now a critical issue due to the increasing cyber threats and computer crimes. Developers and experts constantly improve storage technologies and protection methods to ensure the highest level of security for electronic payments.

Актуальність. Технології зберігання інформаційних ресурсів у сфері електронних платежів є вкрай актуальними та затребуваними. У наш час все більше людей вважають за

краще використовувати електронні платіжні системи для проведення фінансових операцій замість традиційних способів розрахунків, таких як готівка або банківські перекази.

Це пов'язано як із зручністю та швидкістю, так і з можливістю здійснювати платежі у будь-який час та в будь-якому місці, адже для цього достатньо мати доступ до інтернету. Однак, така широка доступність електронних платіжних систем викликає загрози в галузі безпеки, адже дані користувачів зберігаються в системах, схильних до ризиків кібератак і хакерських атак.

Метою статті полягає в аналізі технологій захисту інформаційних ресурсів у системах електронних платежів. В ході дослідження метою є ідентифікація основних видів кіберзагроз, що становлять потенційну загрозу для електронного документообігу. Передбачається аналіз характеристик цих загроз та оцінка рівня їхньої небезпеки для ефективного функціонування інформаційно-комунікаційних систем, які використовуються у сфері електронного документообігу.

Предметом дослідження є основні технології захисту інформаційних ресурсів в системах електронних платежів,

Об'єктом дослідження є – електронні платежі.

Аналіз останніх досліджень і публікацій. Активно звертають увагу на проблеми кібербезпеки, зокрема в контексті війни, що вибухають в електронних системах платежів. Хоча ця тема стає все більш актуальною, дослідження, що конкретно стосуються видів кіберзагроз під час війни для електронного документообігу, залишаються обмеженими.

Виклад основного матеріалу. У зв'язку з цим розробники та експерти з безпеки інформації постійно працюють над удосконаленням технологій зберігання даних у сфері електронних платежів. Вони прагнуть запобігти можливим загрозам і забезпечити максимально високий рівень безпеки та надійності для користувачів.

Завдяки постійному розвитку та інноваціям, хмарні технології, методи шифрування та блокчейн стають все більш складними та надійними. Вони дозволяють зберігати дані безпечно та надійно, забезпечуючи конфіденційність та цілісність інформації. Більше того, сучасні технології можуть попередити можливі загрози ще до їх реалізації, що дає можливість швидко та ефективно реагувати на них.

Таким чином, актуальність технологій зберігання інформаційних ресурсів у сфері електронних платежів полягає у тому, щоб забезпечити користувачам безпеку та надійність під час здійснення онлайн-платежів. Інноваційні розробки та постійне вдосконалення технологій допомагають створити більш захищене середовище для зберігання та передачі даних, сприяючи розвитку та зростанню електронних платежів.

Крім того, актуальність технологій зберігання інформаційних ресурсів у сфері електронних платежів пов'язана з величезним обсягом даних, які генеруються та обробляються у цій галузі. З кожним роком кількість користувачів електронних платіжних систем, а також обсяг фінансових операцій, які здійснюються через них, зростає (рис. 1).

Тому необхідні ефективні технології зберігання та обробки даних, які можуть забезпечити їх збереження та доступність.

Розвиток технологій у сфері електронних платежів також стимулюється зростанням мобільних платежів. З розвитком смартфонів та мобільних додатків стало можливим здійснювати платежі за допомогою мобільних пристроїв. Це вимагає оптимізованих та безпечних методів зберігання даних, щоб користувачі могли здійснювати платежі в реальному часі та безпечно. Використання хмарного зберігання є найбільш практичним рішенням для мобільних платежів, оскільки не потребує великого обсягу пам'яті пристрою.

Нарешті, питання безпеки даних у сфері електронних платежів стає дедалі актуальнішим зі збільшенням числа кібератак та хакерських атак на платіжні системи.

Крадіжка фінансових даних та порушення конфіденційності є серйозними загрозами, які можуть завдати великої шкоди як користувачам, так і самим платіжним системам. Тому розробники та експерти з безпеки постійно працюють над удосконаленням технологій зберігання даних та методів захисту від кіберзагроз, щоб забезпечити максимально високий рівень безпеки електронних платежів.

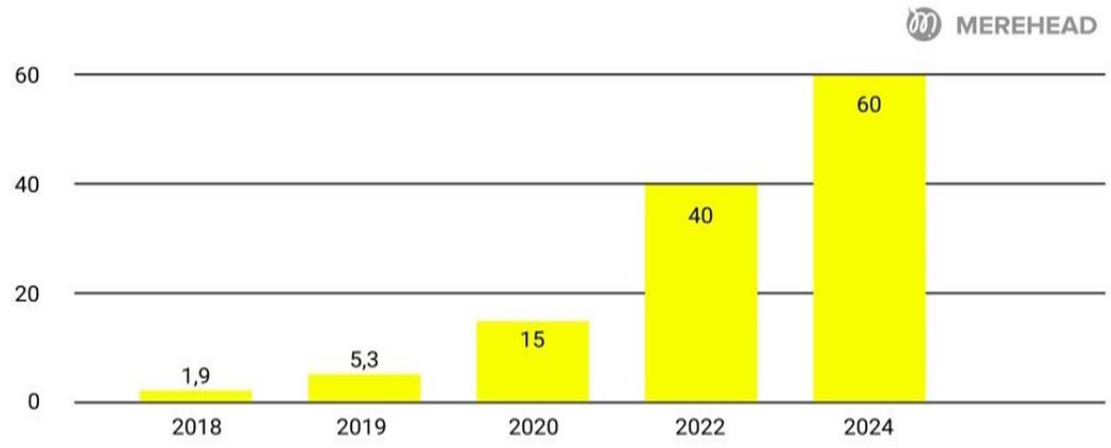


Рис. 1. Схема зросту обсягу фінансових операцій за період 2018-2024 роки

Джерело: Взято з інтернет ресурсу [1]

Загалом актуальність технологій зберігання інформаційних ресурсів у сфері електронних платежів пов'язана зі зростанням кількості користувачів та обсягу фінансових операцій, необхідністю забезпечення безпеки даних та конфіденційності інформації, а також з розвитком мобільних платежів. Постійний розвиток та вдосконалення цих технологій відіграють важливу роль у забезпеченні надійності та задоволенні потреб користувачів у сфері електронних платежів. Сукупність методів і засобів захисту інформації включає програмні й апаратні засоби, захисні перетворення та організаційні заходи (рис. 2).

Апаратний, або схемний, захист полягає в тому, що в приладах ЕОМ та інших технічних засобах обробки інформації передбачається наявність спеціальних схем, що забезпечують захист і контроль інформації, наприклад, схеми контролю на чесність, які контролюють правильність передачі інформації між різними приладами ЕОМ, а також екрануючими приладами, що локалізують електромагнітні випромінювання.

Програмні методи захисту – це сукупність алгоритмів і програм, які забезпечують розмежування доступу та виключення несанкціонованого використання інформації.

Сутність методів захисних перетворень полягає в тому, що інформація, яка зберігається в системі та передається каналами зв'язку, подається в деякому коді, що виключає можливість її безпосереднього використання.

Організаційні заходи із захисту інформації містять сукупність дій з підбору та перевірки персоналу, який бере участь у підготовці й експлуатації програм та інформації, чітке регламентування процесу розробки та функціонування інформаційної системи.

Лише комплексне використання різних заходів (рис. 3) може забезпечити надійний захист інформації, тому що кожний метод або захід має слабкі та сильні сторони.

Апаратні засоби	Програмні засоби	Захисні перетворення	Організаційні заходи
Захист центрального процесора	Ідентифікація користувача	Метод перестановки	Будівництво та керування ОЦ
Захист основної пам'яті	Ідентифікація термінала	Метод заміни	Протипожежний захист ОЦ
Захисит зовнішньої пам'яті	Захист файлів	Адитивні методи	Збереження документів
Захист терміналів	Допопміжні програми захисту	Добір та подготовка кадрів	Організація роботи в системах ОЦ
Загальні методи захисту		Організація системи спостереження в ОЦ	Заходи захисту під час внесення змін

Рис. 2. Методи та засоби захисту інформації

Джерело: Побудовано автором на основі джерела [1]

Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Відкритий ключ – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

Підписувач – особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа.

Документом, який засвідчує чинність і належність відкритого ключа підписувачу, є сертифікат відкритого ключа (далі – сертифікат ключа), виданий центром сертифікації ключів.

Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача.

Сертифікат ключа, що засвідчує відкритий ключ підписувача, згідно зі ст. 6 Закону містить такі обов'язкові дані: найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);

- зазначення, що сертифікат виданий в Україні;
- унікальний реєстраційний номер сертифіката ключа;
- основні дані (реквізити) підписувача – власника особистого ключа;
- дату і час початку та закінчення строку чинності сертифіката;

• відкритий ключ;

• найменування криптографічного алгоритму, що використовується власником особистого ключа;

• інформацію про обмеження використання підпису.

Рис. 3. Класифікація способів захисту конфіденційної інформації

Джерело: Побудовано автором на основі джерела [1]

PayPal – це одна з найпопулярніших і найпопулярніших електронних платіжних систем у світі. Вона надає зручний та безпечний спосіб здійснення онлайнплатежів, покупок та переказів коштів.

Технології, що використовуються PayPal для зберігання інформаційних ресурсів, включають:

• Хмарне зберігання даних: PayPal використовує хмарні платформи для зберігання інформації про своїх користувачів. Це забезпечує високу доступність та відмовостійкість даних, а також зручність використання та швидкість обробки транзакцій.

• Методи шифрування: PayPal застосовує різні методи шифрування даних, щоб забезпечити їхню конфіденційність та безпеку. Один із найпоширеніших методів шифрування, що використовуються PayPal, – це протокол SSL/TLS (Secure Sockets Layer/Transport Layer Security), який захищає передачу даних між користувачем та сервером від несанкціонованого доступу.

• Моніторинг та виявлення шахрайства: PayPal здійснює постійний моніторинг та аналіз транзакцій, щоб виявляти та запобігати можливим випадкам шахрайства.

• Технології машинного навчання та аналітики даних застосовуються для ідентифікації підозрілих операцій та блокування потенційно шкідливих дій.

• Захист від кібератак: PayPal постійно покращує свої системи захисту, щоб запобігти можливим кібератакам і хакерським атакам. Це включає застосування фаєрволу, системи виявлення вторгнень та інших методів захисту.

• Розвиток хмарного зберігання: Хмарні платформи продовжують розвиватися та надавати більш надійні та безпечні рішення для зберігання інформації у сфері електронних платежів. Великі компанії, включаючи PayPal, інтенсивно використовують хмарні рішення для забезпечення доступності та відмовостійкості даних користувачів.

• Зростання використання блокчейну: Технологія блокчейну продовжує привертати увагу у сфері електронних платежів. Її застосування дозволяє забезпечити надійність та безпеку транзакцій через децентралізовану та неможливу для зміни базу даних. Безліч стартапів та компаній працюють над розробкою та застосуванням блокчейну у платіжних системах.

• Розвиток технологій шифрування: Методи шифрування даних стають все більш складними та надійними. Криптографічні алгоритми, такі як RSA та AES, як і раніше, широко використовуються для захисту конфіденційності інформації та забезпечення безпеки платіжних систем.

Вище згадані досягнення є основними трендами та розробками у сфері технологій зберігання інформаційних ресурсів у сфері електронних платежів дотепер.

Висновки: Технології зберігання та захисту інформаційних ресурсів в системах електронних платежів є надзвичайно актуальними через зростання популярності електронних платежів і мобільних платежів, а також збільшення кіберзагроз. Завдяки постійному розвитку хмарних платформ, методів шифрування, блокчейну, біометричної аутентифікації та аналітики даних вдалося досягти високого рівня безпеки та надійності зберігання даних. Однак розробники й експерти продовжують вдосконалювати ці технології, щоб забезпечити максимальну конфіденційність та цілісність інформації в системах електронних платежів.

Список використаних джерел

1. Stud.Lancer: Методи і засоби захисту інформації в інформаційних системах // Режим доступу: https://pidru4niki.com/17680410/informatika/metodi_zasobi_zahistu_informatsiyi_informatsiy nih_sistemah

2. Sloboda.Studio: Top 9 Marketplace Payment Solutions that Work Like a Charm // Режим доступу: https://sloboda-studio.com/blog/how-to-choose-a-marketplace-payment-solution/

3. TitanFile: 3 Methods to Ensure Confidentiality of Information // Режим доступу: https://www.titanfile.com/blog/3-methods-to-ensure-confidentiality-of-information/

4. Scitepress: Informal Methods and Means of Information Protection in Enterprise Information Security // Режим доступу: https://www.scitepress.org/Papers/2021/106168/106168.pdf

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

ТЕОРЕТИЧНІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ WEB-РЕСУРСІВ

ПАЦЕРА Б.В., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У наведеній статті досліджується тема теоретичних аспектів захисту персональних даних в web-середовищі. Аналізуються сутність терміну «персональні дані» та проблемні аспекти забезпечення безпеки персональних/конфіденційних даних у мережі Інтернет. Детально розглядається нормативно-правова база, що стосується захисту приватності та персональних даних в онлайн-середовищі, включаючи євроінтеграцію. Окрема увага приділяється аналізу викликів та перешкод, що виникають у забезпеченні ефективного захисту персональних даних під час використання технології блокчейн. Результати дослідження спрямовані на покращення стратегій та методів захисту особистої інформації користувачів в онлайн-середовищі, з метою забезпечення їхньої приватності та безпеки в Інтернеті.

This article examines the topic of theoretical aspects of personal data protection in the web environment. The essence of the term «personal data» and problematic aspects of ensuring the security of personal/confidential data on the Internet are analyzed. The legal framework relating to the protection of privacy and personal data in the online environment, including European integration, is considered in detail. Particular attention is paid to the analysis of challenges and obstacles arising in ensuring effective protection of personal data when using blockchain technology. The results of the study are aimed at improving strategies and methods for protecting users' personal information in the online environment in order to ensure their privacy and security on the Internet.

Актуальність теми полягає в тому, що в сучасному цифровому середовищі, де персональні дані користувачів є важливим ресурсом, стає все більш проблематичним забезпечення їхньої безпеки через різноманітні технологічні виклики та загрози. Швидкі зміни технологій, економічні і соціальні трансформації, а також динамічний характер кіберзлочинності створюють унікальні виклики для захисту персональних даних користувачів веб-ресурсів. Ефективне управління цими викликами потребує впровадження стратегічних підходів, включаючи системні методики планування, які дозволять державним та приватним установам розробляти стратегії захисту, моніторити їх впровадження та відповідати на зміни у відкритому та непередбачуваному цифровому середовищі. Розуміння та застосування теоретичних засад захисту персональних даних стає критичною складовою для забезпечення безпеки та конфіденційності веб-платформ для користувачів.

Метою статті є теоретичне обґрунтування та розробка пропозицій щодо моделі захисту персональних даних користувачів web-ресурсу.

Об'єктом дослідження є суспільні відносини та процеси, пов'язані з захистом персональних даних користувачів web-ресурсів.

Предметом дослідження є різноманітні механізми та інструменти впровадження моделі захисту персональних даних користувачів web-ресурсів.

Теоретичні засади та аспекти захисту персональних даних користувачів web-ресурсів проаналізовано в працях вітчизняних науковців таких як Балацька В. С., Опірський І. Р. [1] – забезпечення приватності даних за допомогою блокчейну; Бонк М. [2] – огляд найновіших тенденцій та корисні поради щодо захисту в інтернеті; Дем'янець В. [3] – GDPR – захист персональних даних ЄС; Онищенко С. В., Глушко А. Д. [6] – аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз; Похиленко І. С. [7] – правове регулювання

захисту персональних даних; Світличний В. А. [10] – захист персональних даних в умовах воєнного стану в Україні.

Станом на зараз в українському законодавстві існує спеціальне визначення терміну «персональні дані». Згідно з Законом України «Про захист персональних даних» персональні дані це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [8]. Проте Україна має й інші законодавчих актів, які визначають захист персональних даних та регулюють їх обробку. Основними є:

1. Закон України «Про інформацію» – цей закон регулює використання і захист інформації взагалі, включаючи персональні дані, зокрема принципи збору, обробки та зберігання персональних даних; права та обов'язки суб'єктів персональних даних; механізми захисту персональних даних від несанкціонованого доступу та незаконної обробки [9].

2. Цивільний кодекс України – встановлює правові норми, що регулюють права та обов'язки щодо захисту персональних даних в контексті їх визнання як інтелектуальної власності [11].

3. Кримінальний кодекс України – передбачає кримінальну відповідальність за порушення правил обробки та захисту персональних даних, наприклад, стаття 182 «Порушення недоторканності приватного життя» визначає штраф за вчинення незаконних дій щодо конфіденційної інформації [4].

В контексті євроінтеграції України, захист персональних даних стає однією з ключових складових гармонізації законодавства з нормами та стандартами Європейського Союзу (ЄС). Згідно з принципами ЄС, захист приватності та персональних даних має бути визнаний як основне право громадян, що вимагає належного захисту та регулювання на рівні законодавства [5].

Однією з ініціатив у цьому напрямі є впровадження загального регламенту ЄС про захист даних (GDPR – General Data Protectiom Regulation), який встановлює однакові стандарти захисту персональних даних для всіх країн-членів ЄС та їх партнерів. Однією з ключових ініціатив у напрямі гармонізації захисту персональних даних є впровадження Загального регламенту ЄС про захист даних (GDPR – General Data Protection Regulation), який є одним із найважливіших правових актів у сфері захисту приватності та персональних даних. Загальний регламент містить обов'язкові правила для збору, обробки та зберігання персональних даних, а також встановлює права осіб, які дані стосуються. Даний юридичний документ визначає широкий спектр питань, включаючи згоду на обробку інформації, право на доступ і коригування, обов'язки щодо захисту персональних даних, а також вимоги стосовно звітності та відповідальності суб'єктів обробки [3]. Основна мета GDPR полягає в посиленні захисту особистих даних громадян ЄС та забезпеченні їхнього контролю над власними даними. Даний регламент також сприяє створенню умов для більшої прозорості та відкритості у процесі обробки особистих даних, сприяючи підвищенню довіри між користувачами та організаціями, що збирають та обробляють їхні дані. Для України це означає необхідність адаптації внутрішнього законодавства та практик обробки даних до вимог GDPR.

Можливості в цьому процесі включають сприяння розвитку цифрової економіки та збільшення довіри до електронних сервісів через підвищений рівень захисту особистих даних. Це також може стати стимулом для розвитку інноваційних технологій у сфері кібербезпеки та захисту даних. Проте існують загрози та виклики, пов'язані з процесом євроінтеграції у контексті захисту персональних даних. Однією з них є потреба в значних інвестиціях у розробку та впровадження сучасних технологій захисту даних, що може стати фінансовим та технічним викликом для українських компаній та установ. Особливості цього процесу включають необхідність гармонізації внутрішнього законодавства України з правилами та стандартами ЄС, а також підвищення рівня обізнаності та кваліфікації фахівців у сфері захисту даних.

У цілому, євроінтеграція України в сфері захисту персональних даних відкриває нові можливості для розвитку та модернізації національного законодавства та практик, але

водночас потребує серйозних зусиль та ресурсів для впровадження необхідних змін та відповідності вимогам європейських стандартів.

Персональні дані стали важливим активом в цифровому віці, де вони використовуються для ідентифікації, аналізу та взаємодії з користувачами веб-ресурсів. Проте, разом із зростанням використання інтернету збільшується й загроза незаконного доступу до цих даних. Розуміння загроз, яким підлягають персональні дані в веб-середовищі, є важливим завданням для користувачів, розробників та управлінців інформаційних технологій.

Таблиця 1

Загрози персональних даних у веб-середовищі: огляд

Аспект	Опис
Витік персональних даних	Незаконне отримання та розголошення особистої інформації про користувачів веб-ресурсів, часто через порушення безпеки.
Фішинг	Використання підроблених веб-сторінок або електронних повідомлень для отримання конфіденційної інформації від користувачів.
Віруси та шкідливе програмне забезпечення	Вбудування шкідливих програм в веб-сайти або завантажуваних файлів з метою отримання доступу до особистих даних.
Крадіжка сесій	Незаконне отримання доступу до активної сесії користувача з метою перехоплення інформації, такої як паролі та інші особисті дані.
SQL-ін’єкції	Використання вразливостей в програмному забезпеченні для впровадження SQL-команд у веб-запити та отримання доступу до баз даних.
Соціальна інженерія	Стратегія, за допомогою якої зловмисники використовують обман та маніпуляцію для здобуття особистих даних, паролів та інших конфіденційних відомостей у користувачів.
Деніал-сервіс атаки (DDoS)	Напади на веб-сайти з метою перевантаження серверів та недоступності сервісу для користувачів.
Недостатня безпека мережі Wi-Fi	Використання незахищених або слабо захищених мереж Wi-Fi для перехоплення трафіку та отримання доступу до персональних даних.

Джерело: складено автором на основі [2]

Також однієї з проблемою захисту персональних даних є недостатня свідомість користувачів стосовно ризиків, пов’язаних з обробкою персональних даних в мережі, що може призвести до небезпечних ситуацій, таких як підкуп або маніпуляція з метою витоку конфіденційної інформації. Багато користувачів можуть бути несвідомі рівня загрози, яку представляють недобросовісні веб-ресурси або атаки зловмисників. Крім того, недостатня освіченість у сфері кібербезпеки може призвести до неналежного використання паролів, підвищуючи ризик несанкціонованого доступу до особистих облікових записів.

Недостатня захищеність веб-сайтів також є серйозною проблемою. У багатьох випадках веб-ресурси можуть бути недостатньо захищені від кібератак через слабкість у захисті баз даних або недостатній рівень шифрування даних. Це створює ризик витоку особистої інформації користувачів, такої як імена, адреси, номери телефонів та інші конфіденційні дані.

Зростання кіберагресії з боку росії, спрямованої на Україну, свідчить про загрозу, яку несуть кібератаки для безпеки веб-ресурсів та персональних даних користувачів. У період з початку 2022 року було зафіксовано значний приріст кількості кіберінцидентів, який становить серйозний виклик для інформаційної безпеки, зокрема було зупинено 121 кібератаку, а виявлено поняд 25 тис. інцидентів. Найбільш серйозними загрозами виявилися програми-вимагачі, інсайдерські атаки, фішинг, цільові кібератаки та DDoS-атаки, які призвели до серйозних фінансових втрат. Втрати від кібератак постійно зростають, і за оцінками експертів, у 2025 році можуть сягнути значної суми – понад 10,5 трлн. дол. США. Такі загрози вимагають відповідних заходів з захисту персональних даних користувачів web-ресурсів [6].

Цей контекст демонструє необхідність удосконалення теоретичних засад захисту персональних даних у веб-середовищі. Принципи захисту даних мають бути адаптовані до викликів сучасного кіберпростору та включати в себе ефективні стратегії захисту від різноманітних видів кіберзагроз.

Технологія блокчейн може відігравати важливу роль у боротьбі зі загрозами та проблемами, пов'язаними з безпекою та захистом персональних даних у веб-середовищі. Блокчейн – це розподілена база даних, що складається з блоків інформації, які зберігаються у вузлах мережі і зв'язані між собою за допомогою криптографічних методів. Кожен блок містить певну кількість даних, а також хеш-функцію, що вказує на попередній блок, утворюючи ланцюжок блоків. Ця технологія дозволяє створювати надійні та незмінні записи про транзакції чи події без потреби в централізованому управлінні, тим самим забезпечуючи високий рівень безпеки та достовірності даних. Отже, блокчейн є системою, яка гарантує децентралізований та надійний обмін даними, завдяки чому вона стає основою для розподілених обчислень і багатоагентних систем [1].

Таблиця 2

Загрози та переваги використання технології блокчейн для захисту персональних даних

Назва загрози / вразливості	Опис	Перевага блокчейну
Витік персональних даних	Несанкціонований доступ до особистої інформації користувачів, що може призвести до її використання в шахрайських цілях або для ідентифікації осіб.	Використання криптографії для забезпечення конфіденційності та недоступності даних.
Фальсифікація даних	Можливість зміни або підробки персональних даних користувачів, що може призвести до порушення їхньої достовірності.	Наявність децентралізованої системи, де дані зберігаються у блоках, які підтверджуються мережею вузлів.
Атаки на приватні ключі	Спроби злому або крадіжки приватних ключів, що дозволяють доступ до персональних даних.	Застосування криптографічних методів для захисту приватних ключів та автентифікації користувачів.
Відсутність централізованого контролю	Небезпека втрати даних через відсутність централізованого органу, який контролює та відновлює доступ до інформації.	Децентралізована природа блокчейну, що унеможливлює втрату даних через один центральний пункт вразливості.
Недостатня масштабованість	Проблеми зі збільшенням кількості та обсягу обробки персональних даних у великому масштабі.	Можливість використання розподіленої системи блокчейну для забезпечення швидкої та масштабованої обробки даних.
Відсутність дозволу на обробку даних	Можливість неконтрольованого використання особистої інформації без згоди власника.	Можливість використання смарт-контрактів у блокчейні для автоматизації управління доступом та обробки даних за умовами згоди.
Ризик втрати даних	Небезпека втрати персональних даних через випадкові або намірені дії, такі як збої систем або кібератаки.	Надійність зберігання даних у розподіленій системі, де інформація розміщується на кількох вузлах мережі.
Недоступність для видалення	Складність або неможливість видалення особистої інформації з блокчейн-мережі після її збереження.	Можливість розробки протоколів анонімізації або забезпечення права на забування у блокчейні для захисту приватності користувачів.

Джерело: складено автором на основі [10]

Таблиця наводить ретельний огляд загроз та переваг використання технології блокчейн для захисту персональних даних. Як видно з аналізу, хоча існують певні загрози, такі як можливість атак, втрата доступу до даних та використання неправомірними особами,

переваги використання блокчейну значно переважають. Технологія блокчейн дозволяє забезпечити високий рівень безпеки та конфіденційності персональних даних завдяки децентралізації, надійності та прозорості системи. Ці переваги роблять блокчейн привабливим інструментом для захисту персональних даних у веб-середовищі.

Блокчейн, як децентралізована система, не позбавлений своїх недоліків, які можуть впливати на його широкомасштабне застосування. На нашу думку, варто виділити наступні [5]:

- Хоча дані на блокчейні можуть бути зашифровані, недосконаліть алгоритмів шифрування може створювати ризик злому та несанкціонованого доступу до особистої інформації.
- В багатьох публічних блокчейн-мережах інформація, збережена на ланцюжку блоків, доступна для загального перегляду. Це може створювати проблеми з конфіденційністю особистих даних.
- З ростом обсягу даних на блокчейні, може виникати проблема масштабування, що впливає на швидкість обробки та витрати енергії, що може негативно позначитися на загальній ефективності системи захисту даних.
- Втрата ключа доступу до особистих даних на блокчейні може призвести до втрати доступу до даних без можливості відновлення. Це особливо важливо в контексті захисту персональних даних, де втрата доступу може призвести до серйозних наслідків для користувача.

Ці недоліки показують, що використання блокчейну для захисту персональних даних потребує уважного вивчення та урахування ризиків для забезпечення ефективного захисту приватності та безпеки даних користувачів.

Висновки. Швидке розширення технологій та зростаюча кількість кіберзагроз надають актуальність розробці та впровадженню ефективної системи захисту персональних даних. Забезпечення захищеності цих даних є ключовим аспектом для збереження довіри користувачів до інтернет-ресурсів та забезпечення їхньої приватності.

У контексті вирішення цих проблем, технологія блокчейн виокремлюється як інноваційний інструмент, що відкриває нові можливості для захисту персональних даних. Блокчейн дозволяє створювати надійні та безпечні цифрові бази даних, які не піддаються змінам без погодження всіх учасників мережі. Це дозволяє мінімізувати ризик несанкціонованого доступу до даних та забезпечує їхню конфіденційність та цілісність. Крім того, блокчейн може допомогти підвищити довіру користувачів до веб-ресурсів, оскільки він створює прозорі та перевірені механізми обробки даних.

Проте, варто враховувати недоліки технології блокчейн та потенційні загрози. Наприклад, обмежена масштабованість та високі витрати на енергію при майнінгу можуть ускладнити широке впровадження цієї технології. Крім того, необхідно ретельно вивчати можливість використання блокчейну для зберігання особистих даних, оскільки відомо, що вони можуть залишатися незмінними назавжди, що може створити проблеми в майбутньому.

Отже, враховуючи як переваги, так і недоліки, можна зробити висновок, що технологія блокчейн має значний потенціал у захисті персональних даних та збереженні довіри користувачів до інтернет-ресурсів. Однак для максимальної ефективності використання цієї технології необхідно ретельно вивчити її можливості та обмеження, а також вирішувати проблеми її масштабованості та енергоефективності.

У підсумку, можна зазначити, що з огляду на швидке розширення технологій та зростаючу кількість кіберзагроз, ефективна система захисту персональних даних стає необхідністю для збереження довіри користувачів до інтернет-ресурсів та забезпечення їхньої приватності. У контексті вирішення цих проблем, однією з інноваційних технологій, яка пропонує нові можливості для захисту персональних даних, є технологія блокчейн, яка дозволяє забезпечити надійний захист персональних даних, зменшити ризик їхнього несанкціонованого доступу та підвищити довіру користувачів до веб-ресурсів. Проте варто врахувати недоліки цієї технології та зважати на потенційні загрози.

Список використаних джерел

1. Балацька В. С., Опірський І. Р. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. Кібербезпека: освіта, наука, техніка. 2023. Т. 4, № 20. С. 6–16. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/463/368 (дата звернення: 16.04.2024).
2. Бонк М. Захист в інтернеті – огляд найновіших тенденцій та корисні поради. Mediacom. URL: https://mediacom.com.ua/zaxist-v-interneti-oglyad-najnovishix-tendentsij-ta-korisni-poradi/ (дата звернення: 16.04.2024).
3. Дем'янець В. GDPR – це європейський регламент щодо захисту персональних даних. суть та штрафи за GDPR. Legal IT group. URL: https://legalitgroup.com/gdpr-novi-eu-tendentsii/ (дата звернення: 16.04.2024).
4. Кримінальний кодекс України : Кодекс України від 05.04.2001 р. № 2341-III : станом на 28 берез. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 16.04.2024).
5. Механізми досягнення надійності в блокчейні для захисту персональних даних. Захист інформації і безпека інформаційних систем : Матеріали іх міжнар. науково-техн. конф., 25 трав. 2023 р. Львів, 2023. С. 17. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/12355/1/Тези%20Політех%202023.pdf (дата звернення: 15.04.2024).
6. Онищенко С. В., Глушко А. Д. Аналітичний вимір кібербезпеки україни в умовах зростання викликів та загроз. Економіка і регіон. 2022. Т. 1, № 84. С. 13–17. URL: https://journals.nupp.edu.ua/eir/article/view/2540/2000 (дата звернення: 15.04.2024).
7. Похиленко І. С. Правове регулювання захисту персональних даних. Юридичний вісник. 2023. Т. 4, № 69. С. 94–98. URL: https://repositary.knuba.edu.ua/items/5eb87853-7589-40f6-8bcd-15daea8c2ee0 (дата звернення: 15.04.2024).
8. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 16.04.2024).
9. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 16.04.2024).
10. Світличний В. А. Захист персональних даних в умовах воєнного стану в Україні. Право і безпека – Law and Safety. 2023. Т. 3, № 90. С. 226–234. URL: https://doi.org/10.32631/pb.2023.3.19 (дата звернення: 16.04.2024).
11. Цивільний кодекс України : Кодекс України від 16.01.2003 р. № 435-IV : станом на 8 берез. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 16.04.2024).

Робота виконана під науковим керівництвом старшого викладача
ШЕСТАКА Я.І.

РОЛЬ ІНТЕРНЕТУ В СУЧАСНІЙ ПРОМИСЛОВОСТІ ТА ОСНОВНІ ЗАГРОЗИ, ЯКІ ВІН СТВОРЮЄ

ПРАЛАТ М.М., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто роль інтернету в сучасній промисловості та основні загрози, які він створює, розглядає важливість Інтернету у виробничих процесах та ідентифікує ризики, пов'язані з його використанням. Наведено переваги, які принесла цифрова трансформація в промисловості, такі як полегшений доступ до інформації та оптимізація виробничих процесів. Також в статті також розглянуто загрози кібербезпеки, приватності даних та поширення недостовірної інформації, які виникають в контексті використання Інтернету у промисловості. Також наведено рекомендації щодо захисту підприємств від цих загроз та наголошують на важливості впровадження ефективних стратегій кібер-безпеки та управління ризиками в цифровому середовищі.

The article examines the role of the Internet in modern industry and the main threats it poses, considers the importance of the Internet in production processes and identifies the risks associated with its use. The benefits brought by digital transformation in industry, such as easier access to information and optimization of production processes, were discussed. The article also examines threats to cyber security, data privacy and the spread of false information that arise in the context of the use of the Internet in industry. Recommendations are given to protect enterprises from these threats and emphasize the importance of implementing effective cyber security and risk management strategies in the digital environment.

Актуальність. Інтернет, одне з найбільш вражаючих досягнень людства, став невід'ємною частиною сучасного світу, проникаючи у всі сфери нашого життя.

Його революційний вплив не оминув і промисловість, кардинально змінюючи спосіб ведення бізнесу та виробництва. Інтернет став каталізатором цифрової трансформації, надаючи промисловим підприємствам безпрецедентні можливості для підвищення ефективності, оптимізації процесів, співпраці та інновацій.

У сучасній промисловості Інтернет відіграє вирішальну роль, забезпечуючи зв'язок між різними системами, обладнанням та людьми. Промисловий інтернет речей (IIoT) дозволяє збирати та аналізувати величезні обсяги даних в режимі реального часу, надаючи можливість для точного моніторингу, прогнозування та прийняття рішень. Це сприяє оптимізації виробничих процесів, підвищенню продуктивності та ефективності використання ресурсів.

Крім того, Інтернет забезпечує безперешкодний обмін інформацією та співпрацю між підприємствами, постачальниками та клієнтами, полегшуючи інтеграцію ланцюгів поставок та дозволяючи швидше реагувати на зміни ринкових вимог.

Електронна комерція та онлайн-продажі також стали невід'ємною частиною промислової діяльності, відкриваючи нові можливості для збуту продукції та залучення клієнтів.

Однак, поряд з величезними перевагами, використання Інтернету в промисловості створює низку серйозних загроз та ризиків. Кібератаки, крадіжка даних, витік конфіденційної інформації, зловмисне кодування та саботаж можуть завдати значної шкоди підприємствам та підірвати їх конкурентоспроможність.

Проблеми безпеки мереж, відмова в обслуговуванні та шкідливе програмне забезпечення також є серйозними викликами, які необхідно вирішувати.

Таким чином, поєднання величезних можливостей та потенційних загроз робить всебічне вивчення ролі Інтернету в промисловості та розробку ефективних стратегій захисту надзвичайно важливим завданням для забезпечення сталого розвитку та конкурентоспроможності промислових підприємств

Метою статті є дослідження вивчення ролі Інтернету в сучасній промисловості та ідентифікації основних загроз, пов'язаних із його використанням.

Об'єктом дослідження є вплив Інтернету на промислову діяльність, а предметом є особливості використання Інтернету в промислових процесах та загрози, що виникають у зв'язку з цим.

Предмет дослідження є вплив інтернету на промисловий сектор сучасного світу та аналіз його впливу на різні аспекти промислового виробництва.

Аналіз попередніх досліджень. Внесок у розуміння ролі Інтернету в сучасній промисловості, аналізуючи його вплив на різні аспекти, такі як операції, ланцюги поставок, конкурентні стратегії, великі дані та цифрова трансформація внесли такі вчені Майкл Е. Портер – професор з корпоративної стратегії в Гарвардській бізнес-школі, автор книги «Конкурентна перевага: Створення та утримання найвищого рівня продуктивності» де обговорюється вплив Інтернету на конкурентні стратегії підприємств; Ерік Бриньолфссон та Ендрю Макафі (Andrew McAfee) – дослідники з Массачусетського технологічного інституту (MIT), автори книги «Друга ера машин», яка аналізує вплив цифрових технологій, включаючи Інтернет, на бізнес та суспільство; Майкл Чуі який досліджував трансформаційний вплив Інтернету та цифрових технологій на різні галузі промисловості та інші.

Виклад основного матеріалу. Інтернет в сучасній промисловості відіграє надзвичайно важливу роль, перетворюючи спосіб, яким бізнеси функціонують та спілкуються. Він впливає на всі аспекти виробництва, від управління ланцюгами постачання до маркетингу та зв'язків з клієнтами.

Інтернет значно впливає на промислову сферу, полегшуючи доступ до інформації, автоматизуючи виробничі процеси та забезпечуючи зв'язок між компаніями та їх клієнтами. Проте він також приносить певні загрози, такі як кібератаки, порушення конфіденційності даних та поширення дезінформації.

Спочатку розглянемо позитивний вплив інтернету на промисловість. Однією з ключових переваг є полегшення доступу до інформації та ресурсів. Бізнеси можуть швидше та ефективніше знаходити постачальників, аналізувати ринки та реагувати на зміни у галузі.

Крім того, інтернет сприяє автоматизації та оптимізації процесів виробництва, що дозволяє підвищити продуктивність та знизити витрати.

Інтернет дозволяє підприємствам в реальному часі відстежувати стан свого обладнання та виробничих процесів, а також вдало керувати ними віддалено.

Це дозволяє оперативно реагувати на проблеми та уникати непередбачених збоїв, що забезпечує підвищення ефективності та зниження витрат на обслуговування [1, с.34].

Інтернет забезпечує швидкий та зручний обмін даними між промисловими підприємствами, постачальниками та клієнтами. Це сприяє оптимізації ланцюга постачання, підвищенню швидкості виробництва та реагування на зміни на ринку. Крім того, інтернет забезпечує можливість віддаленої співпраці та вирішення проблем, що робить бізнес-процеси більш гнучкими та ефективними.

Він дозволяє автоматизувати та інтегрувати різні бізнес-процеси, що сприяє підвищенню продуктивності та зниженню ризиків помилок. Завдяки інтеграції систем керування та виробничих процесів, підприємства можуть швидше реагувати на зміни в умовах ринку та вимоги споживачів.

Рис. 1. Інтернету в сучасній промисловості

Джерело: [1, с.66]

Інтернет відкриває безмежні можливості для промислових підприємств у сфері електронної комерції та онлайн-продажів. Відкриття власних онлайн-магазинів або участь у електронних торгових платформах дозволяє розширити аудиторію та збільшити обсяги продажів.

Інтернет дозволяє передавати дані в реальному часі з датчиків та обладнання, що дозволяє здійснювати швидку реакцію на зміни у виробничих процесах та мінімізувати час, необхідний для прийняття рішень, дозволяє співробітникам працювати віддалено, що робить робочий процес більш гнучким та зручним.

Крім того, віддалене управління дозволяє керувати виробництвом та бізнес-процесами з будь-якої точки світу.

Отже, інтернет відіграє важливу роль у сучасній промисловості, забезпечуючи підприємствам доступ до нових технологій, засобів комунікації та ринків, що допомагає їм досягати успіху та стабільності у глобальному економічному середовищі.

Однак разом з численними перевагами, Інтернет також створює загрози, які потребують уваги та відповідних заходів з безпеки.

Існують і загрози, пов’язані з використанням Інтернету у промисловості.

По-перше, це загрози кібербезпеки. Зловмисники можуть атакувати системи керування виробництвом, викрадати конфіденційну інформацію або блокувати роботу підприємства шляхом використання шкідливих програм. Це може призвести до серйозних фінансових втрат та порушень у виробничому процесі.

Зловмисники можуть намагатися проникнути до систем керування промисловим обладнанням через Інтернет з метою перешкодження виробничому процесу або навіть заволодіння контролем над системами.

Інтернет дозволяє автоматизувати та інтегрувати різні бізнес-процеси, що сприяє підвищенню ефективності та швидкості виробництва [2, с.35].

Можливість кібератак та зловживання доступом може призвести до порушень у роботі автоматизованих систем та втрати даних. Інтернет надає можливість підприємствам реалізувати свою продукцію та послуги через онлайн-платформи, що розширює аудиторію та забезпечує більш швидку та зручну торгівлю. Ризики безпеки оплати онлайн та можливість шахрайства можуть стати загрозою для якості послуг та довіри споживачів.

Інтернет дозволяє передавати дані в реальному часі з датчиків та обладнання, що дозволяє здійснювати швидку реакцію на зміни у виробничих процесах.

Недостатня кібербезпека може призвести до перехоплення або зміни переданих даних, що може спричинити неправильні рішення та втрати.

Дистанційна робота та віддалене управління є ключовими аспектами в сучасній промисловості, які значною мірою підтримуються та сприяються за допомогою Інтернету. Розглянемо їхню роль і основні загрози, які вони створюють:

Роль Інтернету в дистанційній роботі та віддаленому управлінні:

1. Забезпечення зв'язку: інтернет забезпечує можливість спілкування та обміну інформацією між віддаленими працівниками та керівництвом. Це дозволяє зберігати зв'язок та координувати робочі процеси незалежно від фізичного місця розташування.

2. Забезпечення доступу до ресурсів: інтернет дозволяє віддаленим працівникам отримувати доступ до необхідних даних, програм та інших ресурсів, які необхідні для виконання їхніх обов'язків.

3. Підтримка віртуальних зустрічей та конференцій: інтернет дозволяє проводити віртуальні зустрічі, конференції та тренінги, що сприяє підтримці комунікації та співпраці між віддаленими командами.

4. Моніторинг та управління віддаленими процесами: інтернет дозволяє керівництву в реальному часі відстежувати стан виробничих процесів та надавати необхідні вказівки віддаленим працівникам для оптимізації робочих процесів.

Таблиця 1

Роль інтернету в промисловості : основні загрози

Роль інтернету в промисловості	Основні загрози
1. Дистанційний моніторинг та управління обладнанням	1. Витік конфіденційної інформації
2. Обмін даними та співпраця між підприємствами	2. Зловмисне кодування та саботаж
3. Автоматизація та інтеграція бізнес-процесів	3. Порушення цілісності даних
4. Електронна комерція та онлайн-продажі	4. Відмова в обслуговуванні (DDoS-атаки)
5. Телеметрія та передача даних в реальному часі	5. Шкідливе програмне забезпечення та віруси
6. Дистанційна робота та віддалене управління	6. Людський фактор та соціальна інженерія
7. Доступ до інформації та навчальних ресурсів	7. Проблеми з безпекою мереж та підключень

Джерело: [1, с.43]

Інформаційні системи промислових підприємств можуть бути ціллю для кібер-злочинців, які шукають доступ до конфіденційних даних про виробничі процеси, технології або клієнтську базу.

Зловмисники можуть використовувати шкідливі програми, такі як віруси, черви або троянські коні, для атак на комп'ютерні системи промислових підприємств, що може призвести до блокування роботи або втрати даних.

Зловмисники можуть використовувати соціальний інженерінг та фішингові атаки для викрадення облікових даних або надання співробітників промислових підприємств для отримання несанкціонованого доступу до систем.

Аналіз цих загроз може допомогти в розробці ефективних стратегій кібербезпеки та заходів захисту для промислових підприємств.

Другою загрозою є проблеми з приватністю даних. Інтернет дозволяє збирати великі обсяги інформації про споживачів, але недостатня захищеність цих даних може призвести до їхнього витоку або неправомірного використання.

Це ставить під загрозу довіру споживачів до підприємства та може призвести до судових позовів або втрати клієнтів.

Крім того, інтернет може сприяти поширенню недостовірної інформації або фейкових новин, що може вплинути на репутацію підприємства або його продукції.

Отже, інтернет в сучасній промисловості є невід'ємною частиною, яка принесла багато переваг. Проте, для забезпечення успішності та безпеки промисловості необхідно враховувати також і загрози, пов'язані з його використанням [1, с.69].

Висновок. Отже, можна зазначити, що роль інтернету в сучасній промисловості надзвичайно важлива і корисна. Він полегшує роботу підприємств, сприяючи швидкому обміну інформацією, автоматизації виробничих процесів та покращенню комунікації між учасниками ринку. Проте разом з перевагами Інтернет також приносить загрози, такі як кібератаки та ризики порушення конфіденційності даних.

Попередні дослідження підкреслюють необхідність удосконалення кібербезпеки в промисловості та розробки ефективних стратегій управління ризиками. Вони також вказують на важливість подальшого дослідження цієї теми для забезпечення безпеки та стійкості промислових підприємств у цифрову епоху.

Необхідно активно працювати над удосконаленням кібербезпеки в промисловості та розробляти ефективні стратегії управління ризиками.

Отже, розуміння ролі інтернету та усвідомлення його потенційних загроз є ключовими для успішної адаптації промислових підприємств до швидкозмінного цифрового середовища.

Список використаних джерел

1. Баранов О.А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія// О.А. Баранов; НДІІП НАПрН України – К.: Видавничий дім «АртЕк». – 2018. – 344 с.

2. Баранов О. А. Правові аспекти національних стратегій розвитку штучного інтелекту.//О.А. Баранов. Юридична Україна. – 2019. – № 7. – 538 с.

3. Вінник О.М. Правове забезпечення цифрової економіки та електронного бізнесу: монографія // О.М. Вінник. – К.: НДІ приватного права і підприємництва ім. академіка Ф.Г. Бурчака НАПрН України, 2018. – 212 с.

4. Дмитренко В.С. Правове регулювання електронного підприємництва в Україні: монографія // В.С. Дмитренко. – К.: Юрінком Інтер, 2019. – 424 с.

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д.О.

КАДРОВА БЕЗПЕКА ПІДПРИЄМСТВА ЯК ОБ'ЄКТ УПРАВЛІННЯ

ПРОКОПЕНКО М.В., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто основні засади для будування і подальшого функціонування кадрової безпеки підприємства. Також, розглянуто принципи формування кадрової безпеки підприємства, функції й задачі кадрової безпеки в системі управління персоналом, визначення ризиків і загроз, пов'язані с діяльністю персоналу, формування системи заходів управління кадровою безпекою та запобігання ризикам обумовленим персоналом.

The article discusses the basic principles for the construction and further functioning of the personnel security of the enterprise. The principles of the formation of personnel security of the enterprise, the functions and tasks of personnel security in the personnel management system, the identification of risks and threats related to the activities of the personnel, the formation of a system of measures for the management of talent security and the prevention of risks caused by personnel are also considered.

Актуальність. «Кадрова безпека підприємства як об'єкт управління» в сучасних умовах неможливо переоцінити через кілька ключових тенденцій та викликів, з якими стикаються підприємства в галузі управління персоналом:

1. Зміна ролі людських ресурсів: у сучасному бізнес-середовищі людські ресурси стають стратегічним ресурсом, який визначає конкурентні переваги підприємства. Забезпечення кадрової безпеки стає ключовим фактором для залучення та утримання кваліфікованих працівників.

2. Зростання загрози кібербезпеки: у цифрову епоху підприємства стикаються зі зростаючими загрозами кібербезпеки, включаючи крадіжку конфіденційної інформації та атаки на інформаційні системи. Забезпечення безпеки персоналу у цьому контексті стає надзвичайно важливим.

3. Ризики здоров'я та безпеки на робочому місці: охорона здоров'я та безпека праці є важливою складовою кадрової безпеки, оскільки нещасні випадки або професійні захворювання можуть суттєво вплинути на ефективність працівників та репутацію підприємства.

4. Глобалізація ринку праці: з розвитком глобальних технологій та збільшенням міжнародного співробітництва підприємства стикаються з новими викликами у управлінні багатокультурним персоналом та вирішенні конфліктів на міжнаціональному рівні.

5. Пандемія COVID-19: пандемія значно змінила способи роботи та взаємодії між працівниками. Забезпечення безпеки та здоров'я працівників стало пріоритетом для багатьох підприємств, що вимагає впровадження нових стратегій та підходів до управління персоналом. Врахування цих та інших факторів у контексті кадрової безпеки підприємства стає важливим завданням для керівництва та менеджменту, оскільки від цього залежить успішність та стійкість підприємства в сучасних умовах.

Метою статті є виявлення причин послаблення кадрової безпеки, визначення класифікації ризиків та загроз кадровій безпеці

Об'єктом дослідження є розробка методів попередження загроз кадровій безпеці підприємства

Предмет дослідження – кадрова безпека, як об'єкт управління.

Аналіз попередніх досліджень. Дослідженню загроз, ризиків, функцій та методів управління присвячені праці вітчизняних науковців: Г. В. Назарова, О.Я. Гримак, І.Я. Бурда, Г. Коптєва, та ін.

Виклад основного матеріалу. Кадрова безпека підприємства може бути визначена як елемент загальної економічної безпеки або як основна підсистема корпоративної безпеки,

залежно від оцінки її місця в організації. Сукупність принципів, методів і форм організаційних механізмів для вирішення цілей і завдань, захисту, зміцнення та розвитку людських ресурсів і створення відповідальних та продуктивних команд.

Метою є створення відповідальної, продуктивної та згуртованої команди, здатної своєчасно реагувати на постійномінливі вимоги ринку, враховуючи стратегію розвитку організації.

Система кадрової безпеки – це не просто набір заходів, а система взаємодії, носіями якої є люди. Це пов'язано з тим, що кадрова безпека є адаптивною системою, яка постійно і динамічно розвивається, пристосовуючись до нових загроз, розвиваючись під їх впливом і, де це можливо, запобігаючи їм. Розробка системи кадрової безпеки на підприємстві повинна починатися з усвідомлення проблеми недостатності і недієвості заходів з забезпечення кадрової безпеки. Суб'єктом ухвалення рішення про впровадження цієї системи є вище керівництво підприємства на основі чіткого визначення проблем підприємства в контексті кадрової безпеки. Перш за все, необхідно провести аналіз потенційних ризиків і загроз, що обумовлені персоналом, наприклад, за допомогою системи аналізу і управління кадровими ризиками «ГРИФ», що входить до пакету Digital Security Office фірми «Діджитал Сек'юріті».

Основним етапом формування системи кадрової безпеки є організація та реалізація розроблених заходів, методів і засобів забезпечення кадрової безпеки підприємства. Необхідно контролювати працездатність системи кадрової безпеки компанії. У результаті модифікуються всі параметри та характеристики, а також, використані засоби та методи.

Для запровадження системи особистої безпеки на підприємстві необхідно прийняти рішення щодо предмета реалізації запропонованих заходів. Якщо немає потреби у створенні окремого відділу, його функції слід визначити серед персоналу відділу кадрів. У будь-якому випадку конфігурація функцій повинна включати аналіз психологічного контролю, лояльність, запобігання стресу та виявлення залежності.

Предметом кадрової безпеки можна вважати негативні ризики та загрози, пов'язані з кадровою діяльністю. Тому всі фактори ризику, небезпеки та загрози можна згрупувати за різними класифікаційними ознаками. Варто розрізняти передбачувані та непередбачувані загрози відповідно до їх передбачуваності.

Найбільш значними внутрішніми загрозами є: невідповідність кваліфікації працівників вимогам, що пред'являються до них; недостатня кваліфікація працівників; слабка організація системи управління персоналом; слабка організація системи навчання; неефективна система мотивації; помилки в плануванні персоналу; звільнення кваліфікованих працівників; відсутність або «слабка» організаційна культура; неякісні перевірки кандидатів при прийомі на роботу.

Функції для реалізації кадрової безпеки та завдання обов'язкові для виконання наведені у табл. 1.

Загрози й негативні ризики, які пов'язані с персоналом та його діяльністю, можна вважати об'єктом кадрової безпеки. Так всі фактори ризику, небезпек й загроз можуть бути згруповані по різним класифікаційним ознакам. Залежно від можливості їхнього прогнозування варто виділити передбачувані і непередбачувані загрози. До перших відносяться ті, які виникають у певних умовах, відомі з досвіду господарської діяльності, вчасно виявлені й узагальнені економічною наукою.

Під час долсідження було виявленно дві класифікації ризиків. Деякі фахівці, а саме Кібанов А. Я., Чумарін І.Г. та Лисенко М. С. дають на розгляд класифікацію за ознакою на становище співробітника в компанії щодо його ролі і можливостей: під час прийняття працівника на вакансію, під час праці персоналу, під час звільнення. Інші дослідники пропонують класифікацію загроз за сферою виникнення – внутрішні та зовнішні. Негативні впливи зовнішнього характеру – це дії, процеси, що не стосуються свідомості співробітника компанії або підприємства і завдають збитки. До негативних впливів внутрішнього характеру відносять навмисні дії, або дії які склалися внаслідок необережної роботи чи недбальства з боку працівників.

Таблиця 1

Функції кадрової безпеки в системі управління персоналом

№	Функція	Роботи, які повинні виконуватись за функцією
1	Загальне керівництво	1) централізація управління системою кадрової безпеки 2) інформування персоналу на періодичній основі
2	Юридичний супровід	1) представництво в органах судової влади з питань трудових спорів; 2) розробка контрактів з персоналом підприємства; 3) юридичне забезпечення безпечного найму та звільнення персоналу; 4) участь конфліктній комісії в трудових спорах
3	Технічне забезпечення	1) розробка комп'ютерних програм для системи кадрової безпеки; 2) безпека комп'ютерних даних системи кадрової безпеки; 3) консультації по технічних рішеннях
4	Організація безпечного прийому та звільнення персоналу	1) психодіагностичне тестування персоналу при прийомі на роботу, звільненні та у процесі праці; 2) розробка соціограм, психограм, психологічних портретів нанятих працівників; 3) проведення соціометричних досліджень; 4) розробка планів ротації персоналу; 5) сприяння в наступному працевлаштуванні при звільненні персоналу; 6) ведення бази даних особистих справ персоналу
5	Розвиток персоналу	1) розробка й реалізація програми психологічних тренінгів особистісного розвитку, згуртування, командних тренінгів; 2) навчання персоналу загальним і спеціальним методам розпізнавання шахрайських дій з боку клієнтів підприємства й інших контрагентів; 3) навчання менеджерів всіх рівнів способам виявлення й запобігання неправомірних дій підлеглих; 4) навчання персоналу методам захисту інформації й інтелектуальної власності; 5) навчання (інформування) співробітників правилам особистої безпеки; 6) навчання працівників порядку колективних й індивідуальних дій в екстрених ситуаціях
6	Умови праці та ергономіка	1) розробка робочих приміщень з урахуванням індивідуальних особливостей персоналу; 2) рекомендації по колірному оформленню приміщень; 3) постійний моніторинг психологічного стану персоналу від перебування на робочому місці за розробленими показниками; 4) забезпечення та моніторинг безпечних умов праці 5) рекомендації по підбору офісної техніки та обладнання
7	Забезпечення лояльності	1) проведення оперативного контролю робочих телефонних переговорів й електронної пошти співробітників; 2) підготовка щоденного й щотижневого звіту по внутрішній безпеці персоналу для керівництва підприємства; 3) організація інспекцій по моралі; 6) профілактика поведінки, що відхиляється від норми (чутки, інтриги, привілеї, пільги, плітки); 4) виявлення нелояльного персоналу й розслідування дій стосовно крадіжок, комерційного шпигунства, протидії статутній діяльності
8	Індивідуальна та колективна психотерапія	1) психологічна освіта персоналу підприємства; 2) індивідуальне психологічне консультування персоналу підприємства; 3) сімейна психотерапія членів родин співробітників підприємства; 4) надання екстреної психологічної допомоги в складних емоційних станах; 5) участь фахівців у конфліктній комісії
9	Попередження стресів та залежностей	1) розробка програм психічного й фізичного здоров'я персоналу підприємства; 2) профілактика наркотичної залежності у персоналу підприємства; 3) підготовка звітів щодо рівня здоров'я персоналу для керівництва підприємства; 4) профілактика захворювань, у т.ч. інфекційних захворювань; 5) розробка й впровадження програми по адекватному режиму робочих навантажень

Джерело: згенеровано на основі [3]

Відповідно до існуючих видів загроз, можна назвати такі основні методи забезпечення кадрової безпеки підприємства:

Адміністративні методи для забезпечення кадрової безпеки підприємства треба трактувати, як сукупність заходів з перевірки кандидатів на етапі прийому на роботу, проводження періодичного аудиту діяльності персоналу та дотримання вимог у випадку звільнення працівників.

Організаційні методи потрібні для забезпечення необхідних умов функціонування організації, а також, створення меж, в яких вона функціонує і розвивається.

Суть *економічних* методів полягає у створенні сприятливого матеріально-мотиваційного поля для співпрацівників підприємства та не спонукатимуть їх до переходу в організацію конкурентів.

Під сферою застосування *дисциплінарних* методів слід розуміти передбачення юридичних та дисциплінарних зобов'язань і відповідальності щодо роботи з окремою категорією інформації.

Соціально-психологічні методи становлять собою сукупність специфічних засобів впливу на міжособисті стосунки і зв'язки, які виникають у трудового колективу. Дивлячись зі сторони кадрової безпеки підприємства такі методи необхідні для створення сприятливого соціально-психологічного клімату та формування стабільних відносин у колективі.

Головними цілями забезпечення кадрової безпеки підприємства є: запобігання ризикам, небезпекам і загрозам; захист інтересів і майна підприємства від протиправних дій; запобігання втрати матеріальних та нематеріальних ресурсів; забезпечення нормального функціонування всіх підрозділів підприємства тощо (рис. 1).

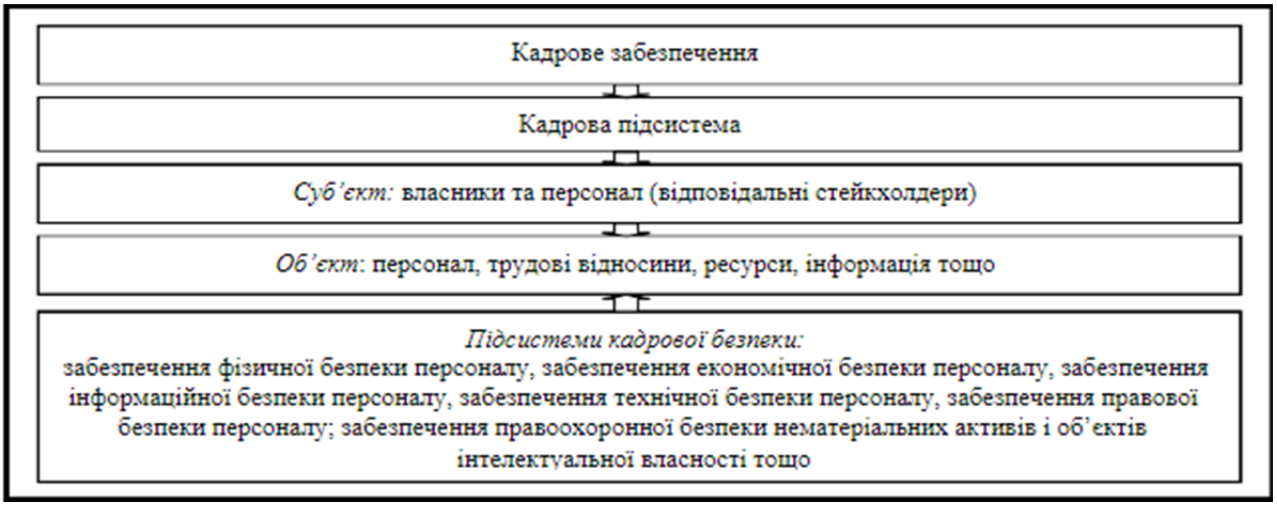


Рис. 1. Структурна характеристика кадрового забезпечення підприємства

Джерело: [2]

Складовими механізму кадрового забезпечення безпеки підприємства є: об'єкт, що піддається небезпеці; суб'єкт, що забезпечує безпеку; фактори, які загрожують безпеці об'єкта; інструменти, методи і засоби забезпечення безпеки. При цьому, під кадровим забезпеченням розуміється система принципів, форм і методів формування необхідного кількісного та якісного складу персоналу, спрямована на вдосконалення кадрового потенціалу та ефективне його використанняПри цьому головним завданням служби персоналу є обов'язок забезпечити їх наявність, правильність, регламентацію і організацію документообігу, і відсутність негативних юридичних наслідків. До внутрішніх регламентаційних документів відносять: трудовий договір (контракт), правила внутрішнього трудового розпорядку, договір про повну індивідуальну (колективну) матеріальну відповідальність, посадову інструкцію, документацію з охорони праці, положення про комерційну таємницю

та інші. Виходячи з цього, в сучасних умовах убезпечення кадрової діяльності як діяльності з продукування, обміну, використання людських ресурсів, вона виступає пріоритетною складовою безпеки розвитку персоналу та економічної безпеки.

Висновки. Під час дослідження було виявлено причини послаблення кадрової безпеки на підприємстві, визначенні класифікації ризиків та загроз кадровій безпеці, вказані функції кадрової безпеки підприємства та роботи, які повинні за нею проводитись. Також досліджені методи для мінімізації появи та протидії внутрішнім та зовнішнім ризикам, детально розглянута співпраця, взаємодія та прийняття на роботу співпрацівників. За результатами проведеного дослідження визначено, що більшість авторів до основних складових кадрової безпеки відносять фізичну і психологічну безпеку, а також безпеку здоров'я, фінансову, інтелектуальну і кар'єрну. Інші складові кадрової безпеки є менш популярними серед науковців і вивчаються переважно в контексті більш вузьких досліджень, що жодним чином не заперечує їх важливості.

Список використаних джерел

1 Козаченко А. В. Економічна безпека підприємства. Сутність і механізм забезпечення: монографія/ А. В. Козаченко, В. П. Пономарьов, А. Н Лещенко. – К.: Видавництво «Лібра». (https://old-zdia.znu.edu.ua/gazeta/evzdia_7_028.pdf)

2. Швець І. Б. Економічна безпека в управлінні персоналом. // Наукові праці ДонНТУ. (https://ea.donntu.edu.ua/bitstream/123456789/12922/1/Shvez%20I.B..pdf)

3. Назарова Г. В. Передумови створення системи кадровоїЇ безпеки підприємства (http://rarrpsu.wunu.edu.ua/index.php/rarrpsu/article/view/58)

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л.О.

ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ОСНОВІ БАГАТОРІВНЕВОГО АНАЛІЗУ

**РОМАНЬКО В.В., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»**

У статті проаналізовано особливості захисту конфіденційної інформації на основі багаторівневого аналізу. Обґрунтовано використання інструментарію Pleak для аналізу процесів захисту інформації та покращення моделей бізнес-процесів щодо конфіденційності.

In the article analyzes the peculiarities of protecting confidential imformation based on a multi-level analysis. The use of the Pleak toolkit for information security processes and improving business process models in terms of privacy is substantiate.

Актуальність обраної теми полягає у проблемах з конфіденційністю та витоку інформації. Сучасний етап розвитку суспільства характеризується значним підвищенням цінності інформації, інформаційних ресурсів та технологій. Це призводить до активізації інформаційних відносин у різних сферах життя людини під час виконання різних видів діяльності, пов'язаних з отриманням, зберіганням, користуванням та поширенням відомостей. Конфіденційна інформація, незалежно від сфери відносин, в якій вона використовується, має вагоме значення і цінність для особи, що має доступ до неї. Використання

інформації визначається її значущістю у сфері публічного управління для забезпечення державного управління в різних сферах суспільного життя. У приватній сфері інформація є важливою для реалізації та захисту прав держави, фізичних та юридичних осіб. Неправомірний доступ сторонніх осіб до такої інформації може значно пошкодити інтереси як держави, так і приватних осіб, а також загрожувати загальним суспільним інтересам [1].

Метою статті є обґрунтування та аналіз особливостей захисту конфіденційної інформації на основі багаторівневого аналізу.

Об'єктом дослідження є методи та процеси захисту конфіденційної інформації на основі багаторівневого аналізу.

Предметом дослідження є теоретико-методологічні аспекти багаторівневого аналізу на основі PE-BPMN інструментарію PLEAK.

Аналіз останніх досліджень. Василікі Діамантопулу, Ніколаос Аргіропулос, Христос Каллоніатіс і Стефанос Грицаліс у своїй роботі «Підтримка розробки бізнес-процесів з урахуванням конфіденційності за допомогою шаблонів процесів конфіденційності» роблять спробу висвітлити кілька шаблонів процесу конфіденційності [2]. Вважається, що ці шаблони подолають розрив між прототипами конфіденційності та реалізацією, виявляючи необхідні варіанти використання та цілі. Замість створення прототипів систем безпеки у формі бізнес-процесу з нуля можна вибрати з ієрархії типових проблем конфіденційності та додати готовий шаблон. Передбачається, що цей підхід пришвидшить початкове створення прототипів і уникне основних помилок завдяки врахуванню більшості потенційних проблем у запропонованому шаблоні процесу BPMN. Дослідники також представляють набір із восьми сфер конфіденційності, які вони визнали можливими: автентифікація, авторизація, анонімність, псевдонімність, незв'язність, невиявленість, неспостережливість і захист даних. Основною перевагою запропонованих шаблонів є їхня типова поведінка, яка використовується в бізнес-процесах, що відповідають за безпеку, автори стверджують, що були з'ясовані основні цілі безпеки, побудувано власну класифікацію технології підвищення конфіденційності (PET) і запропоновано рішення для кожної цілі безпеки на основі комплексного огляду літератури. Отже, в статті зосереджуємося на роботі PE-BPMN, яка вже є частиною PLEAK. Підхід, запропонований авторами дослідження, можна використати для розширення аналізу, запропонованого PE-BPMN.

Виклад основного матеріалу. Впровадження багаторівневого підходу сприяє створенню стійкої системи, яка забезпечує конфіденційність, цілісність та доступність інформації, що є основними аспектами інформаційної безпеки.

Багаторівневий аналіз здійснюється за допомогою інструментарію, заснованого на штучному інтелекті Pleak. Це інструмент для збору та аналізу моделей бізнес-процесів з розширеною конфіденційністю, щоб охарактеризувати та кількісно оцінити, якою мірою результати процесу призводять до витоку інформації про його входи. Pleak включає розширюваний набір плагінів аналізу, які дозволяють користувачам перевіряти потенційні витоки на кількох рівнях деталізації.

Інструмент Pleak призначений для підтримки аналізу приватних потоків даних у бізнес-процесах (БП) і програмах підприємства. Він може використовуватися аналітиками, розробниками та супровідниками бізнес-процесів для того, щоб зрозуміти вплив на конфіденційність бізнес-процесів, які використовуються або плануються їхніми організаціями або клієнтами.

Управління бізнес-процесами (BPM) має за мету надання інструментів для визначення, регулювання та покращення роботи організацій. Центральним є поняття бізнес-процесів, які зазвичай фіксуються у формі моделей. З цією метою практики BPM зазвичай використовують графічну нотацію для запису бізнес-процесів, серед яких модель бізнес-процесу. Схвалений BPMN версія 2.0 є стандартом [3], який визначає графічну нотацію та її семантику, яка служить інструментом для представлення сторін організації чи системи, їхніх дій, даних, комунікацій та послідовності виконання процесу. BPMN містить великий набір графічних елементів, але приділимо увагу лише основними елементами нотації, які узагальнено на рисунку 1.

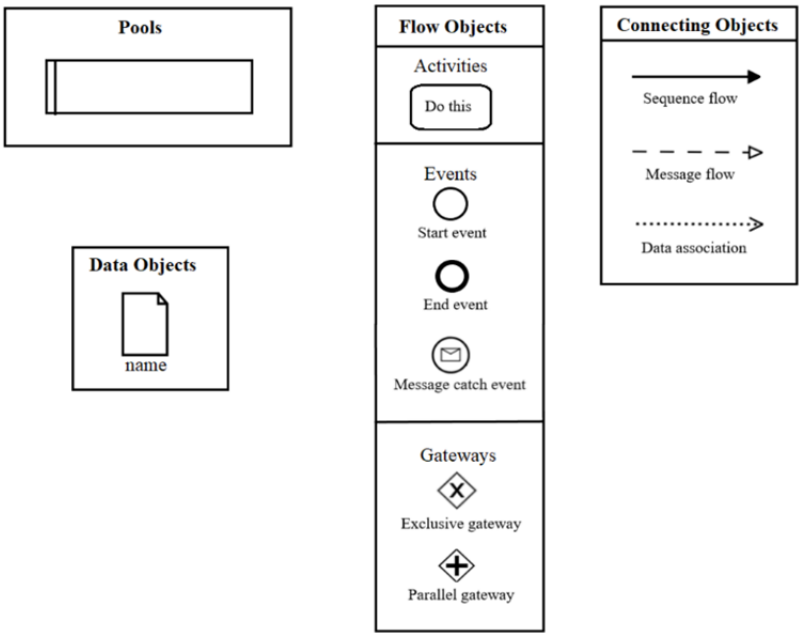


Рис. 1. Підмножина елементів BPMN

Джерело: [3]

«Пули» представляють учасників (стейкхолдерів) процесу. Якщо модель процесу має лише одну сторону, то пул зазвичай не використовується. «Об'єкти потоку» складаються з подій, дій і шлюзів, вони визначають більшість логіки процесу та рішень щодо виконання. Використовуються три типи елементів події BPMN: початкова подія, подія перехоплення повідомлення та кінцева подія.

«Початкова подія» означає початок бізнес-процесу. «Подія перехоплення повідомлення» вказує на момент, коли процес має чекати повідомлення (тригера) для продовження. «End event» означає завершення процесу. У разі використання пулів, кожен пул має власну кінцеву подію.

«Дії» – це елементи з роботою, яка має бути виконана для процесу. «Завдання» являють собою дрібну одиницю роботи, яку не можна розділити на менші дії. «Шлюзи» об'єднують і розділяють потоки в моделі процесу. «Ексклюзивні шлюзи» відповідають потоку «якщо-тоді-інше», тому процес розбивається на ексклюзивні гілки. Умова, пов'язана зі шлюзом, визначає, яку гілку слід вибрати. Навпаки, «паралельні шлюзи» виконують усі гілки одночасно без умов. Після поділу потоку на кілька гілок ексклюзивний або паралельний шлюз має бути синхронізований шлюзом того самого типу, що об'єднує гілки.

«З'єднувальні об'єкти» будують послідовність з елементів потоку. «Потоки послідовності» з'єднують завдання, події та шлюзи. «Потоки повідомлень» потрібні для обміну інформацією від однієї сторони (пулу) до іншої.

«Асоціації даних» виражають потік інформації та їх напрямок між видами діяльності. «Об'єкти даних» представляють дані, які використовуються, виробляються та зберігаються діяльністю моделі процесу.

Крім того, розглядається модель процесу BPMN як модель спільної роботи BPMN, якщо вона складається з кількох пулів і, отже, кількох сторін.

Враховуючи, що BPMN залишається нотацією загального призначення, стандартна графічна нотація фіксує лише потік керування, потік даних і точки зору учасників. Таким чином, стандартна нотація недотягує, коли йдеться про представлення аспектів, пов'язаних із сферою конфіденційності та безпеки. Щоб впоратися з цим обмеженням, існує розширення до стандартного BPMN під назвою «Модель і нотація бізнес-процесу з покращеною конфіденційністю» [4], щоб додати концепції та елементи нотації, які дозволяють аналітикам

коментувати Моделі BPMN з інформацією, пов'язаною з конфіденційністю. На додаток до визначення, реалізовано деякі інструменти навколо PE-BPMN, які включають графічний редактор, який дозволяє аналітикам додавати інформацію про використання PET для обробки моделей для вирішення проблем безпеки.

PET є загальноприйнятою концепцією для позначення будь-якого інструменту безпеки, але в конкретному моделюванні BPMN використовуються конкретні стереотипи, щоб розрізнити PET. Ці стереотипи впливають на те, які дані будуть захищені та як під час виконання процесу. Можна прикріпити PET, вибравши об'єкт даних або завдання в редакторі PE-BPMN і перейшовши в меню «Стереотипи».

Усі стереотипи відображаються на діаграмі бізнес-процесу, а входи/виходи стереотипного завдання виділені різними кольорами, що робить його візуально зручним для спостереження. На рисунку 2 показано частину деякого концептуального бізнес-процесу. Завдання, які виконують багатостороннє обчислення виділені синім кольором, їхні відповідні входи виділені зеленим, а виходи червоним. Методи безпечного багатостороннього обчислення (MPC) – це підходи, які дозволяють учасникам захищати свою інформацію та обробляти її розподіленим способом, зберігаючи при цьому конфіденційність усіх вхідних даних. Також використано стереотипи DifferentialPrivacy і SKEncrypt (шифрування секретним ключем).

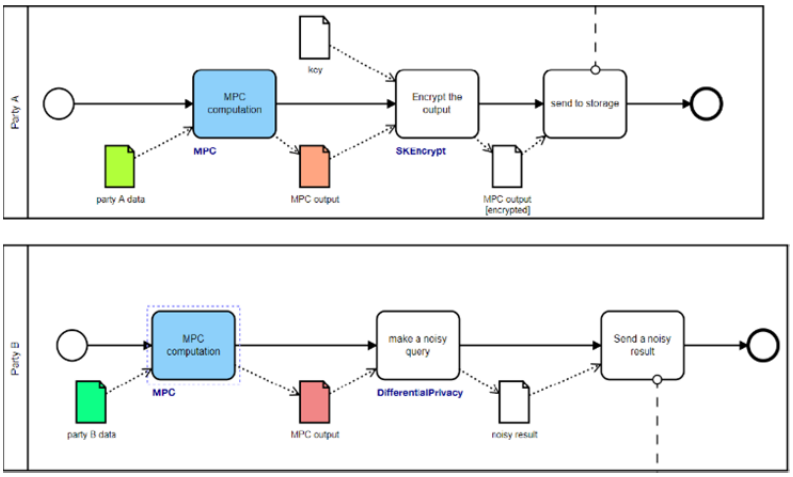
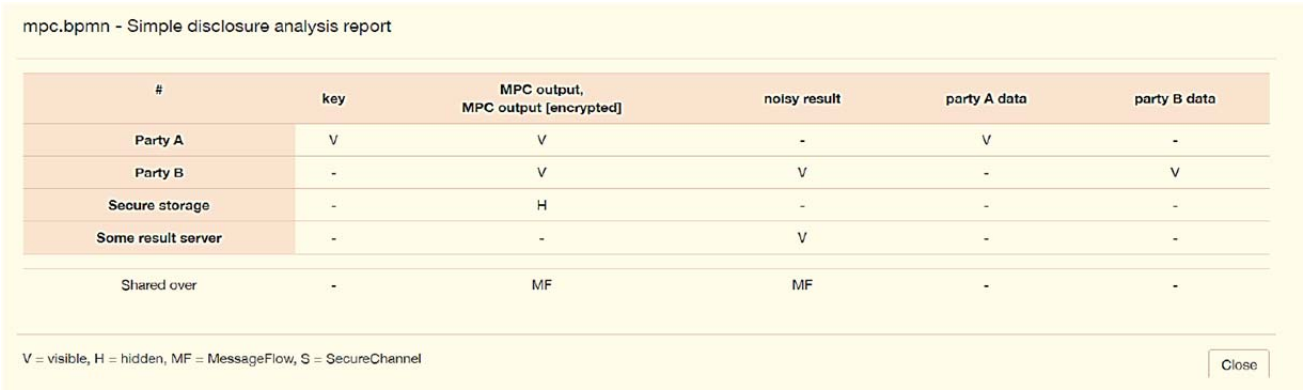


Рис. 2. Концептуальний приклад застосування PET

Джерело: [4]

Поточна версія редактора PE-BPMN складається з двох аналізаторів: аналізатора Simple Disclosure і аналізатора залежностей даних. На рисунку 3 показано результат аналізатора Simple Disclosure – матрицю видимості. Simple Disclosure Analysis – це високорівнева модель процесу, розташована в редакторі PE-BPMN PLEAK. Він приймає вхідні дані моделі процесу BPMN, а також розглядає PET, прикріплені до моделі. Для цілей PE-BPMN об'єкт вважається розкритим, якщо він отриманий або перехоплений іншою стороною, незалежно від наміру чи політики. Редактор PE-BPMN використовується для розуміння обміну даними між пулами, пов'язаних з ними об'єктів даних і взаємозалежностей між входами та результатами діяльності. Основною метою цього аналізу є виявлення того, що розкривається, коли процес виконується за призначенням.

Матриця видимості надає огляд об'єктів даних, якими володіє кожна сторона в певний момент під час виконання процесу. Це також надає кожній із сторін ступінь видимості даних. Сторони спостерігають за вмістом даних, надісланих їм або обчислених ними, але деякі об'єкти даних приховують фактичні дані, які вони кодують (наприклад, через шифрування або обмін стереотипами). Такий аналіз також можна проводити на основі загальних стереотипів, які просто визначають, захищений об'єкт даних чи ні.



mpc.bpmn - Simple disclosure analysis report

#	key	MPC output, MPC output [encrypted]	noisy result	party A data	party B data
Party A	V	V	-	V	-
Party B	-	V	V	-	V
Secure storage	-	H	-	-	-
Some result server	-	-	V	-	-
Shared over	-	MF	MF	-	-

V = visible, H = hidden, MF = MessageFlow, S = SecureChannel

Close

Рис. 3. Зразок простого звіту розкриття інформації

Джерело: скрін екрану

Стовпці стосуються всіх об’єктів даних BPMN у моделі процесу, тоді як рядки відповідають пулам BPMN. У комірці матриці можливі такі значення:

‘V’ – видимий, сторона має доступ до об’єкта даних.

‘H’ – прихований, сторона має доступ лише до захищеної (криптографічно зашифрованої або секретної спільної) версії об’єкта даних.

‘-’ – об’єкт даних не розкривається стороні.

У нижньому рядку таблиці вказано канал, який використовується для розкриття інформації між пулами. Тут «MF» означає Message Flow, а «S» означає застосований стереотип SecureChannel.

Моделі співпраці BPMN можуть володіти деякою конфіденційною інформацією про одну зі сторін, тому наголос робиться на зв’язку між пулами. У реальному бізнесі, представленому моделлю процесу, дані зазвичай зберігаються в базах даних SQL.

У робочому процесі SQL кожне завдання або об’єкт даних BPMN відповідає оператору SQL, що виконується для бази даних. Кожен оператор SQL або визначає нову таблицю SQL, або виконує запит до набору вхідних таблиць [4]. Виконання запиту завжди створює нові таблиці SQL або вихідні дані, які можна використовувати як вхідні дані для наступних завдань робочого процесу.

Таблиця (або набір таблиць), які беруться як вхідні дані першими операторами SQL у робочому процесі, називаються вхідними. І навпаки, таблиці, створені останніми інструкціями SQL у робочому процесі, називаються кінцевими результатами, тоді як таблиці, створені проміжними завданнями в робочому процесі, називаються проміжними результатами.

Диференціальна конфіденційність – це сучасний підхід до конфіденційності для експертів з безпеки. Ідея ґрунтується на гарантії того, що включення або виключення будь-якого окремого запису в досить великому наборі даних не впливає істотно на результати статистичного аналізу даного набору даних. Це важливе поняття для конфіденційних (наприклад, статистичних) баз даних, де дозволено розголошувати лише сукупні результати через конфіденційну інформацію, яка захищається законом, наприклад, медичні записи або поліцейські/кримінальні записи. Виникла концепція зміни впливу конкретного запису на всю статистичну операцію таким чином, що цей запис не було включено до набору даних. Проте, виконання цієї суворої вимоги на практиці може суттєво спотворити дані та обмежити використання даних, погіршуючи кінцеву корисність цих відмінно приватних результатів.

Диференційовану парадигму конфіденційності можна підтримувати, використовуючи концепцію чутливості. Залежно від конкретної статистичної бази даних основним кроком зазвичай є визначення функції, яка має використовуватися для обчислення статистики та

додавання шуму до виводу. Диференційне значення конфіденційності призводить до співвідношення чутливості функції для різних атрибутів і величини генерованого шуму [5]. Оскільки диференціальний аналіз конфіденційності та чутливості виконується в статистичних базах даних, передбачається розробка та запуск цих методів для запитів SQL, а також створення цих запитів у робочих процесах SQL.

Аналіз витоків – це техніка та відповідний інструмент у інструменті PLEAK, який приймає робочий процес SQL як вхідні дані та розкриває дані та умови, за яких такі дані будуть розкриті під час виконання процесу. У цьому контексті розглядаються робочі процеси SQL, де завдання та об'єкти даних BPMN містять оператори SQL. Аналіз Leaks-When можна використовувати, щоб отримати інформацію про умови, за яких дані розкриваються сторонам, що мають доступ до проміжних і/або остаточних результатів обчислення робочого циклу SQL. Інструмент генерує обчислення проміжного процесу в області реляційної алгебри, використовуючи мову програмування OCaml. Потім цей проміжний рівень використовується для аналізу та побудови підсумкового графіка залежностей. Ці графіки обробляються та відображаються як звіт про витоки.

На рисунку 5 зображено зведений сценарій «розподілу допомоги». У цьому сценарії країна просить про допомогу після стихійного лиха та очікує, що товари будуть розподілені кораблями, які належать різним країнам, що надають допомогу. Розкриття даних про кораблі країні, яка запитує допомогу, здійснюється поступово.

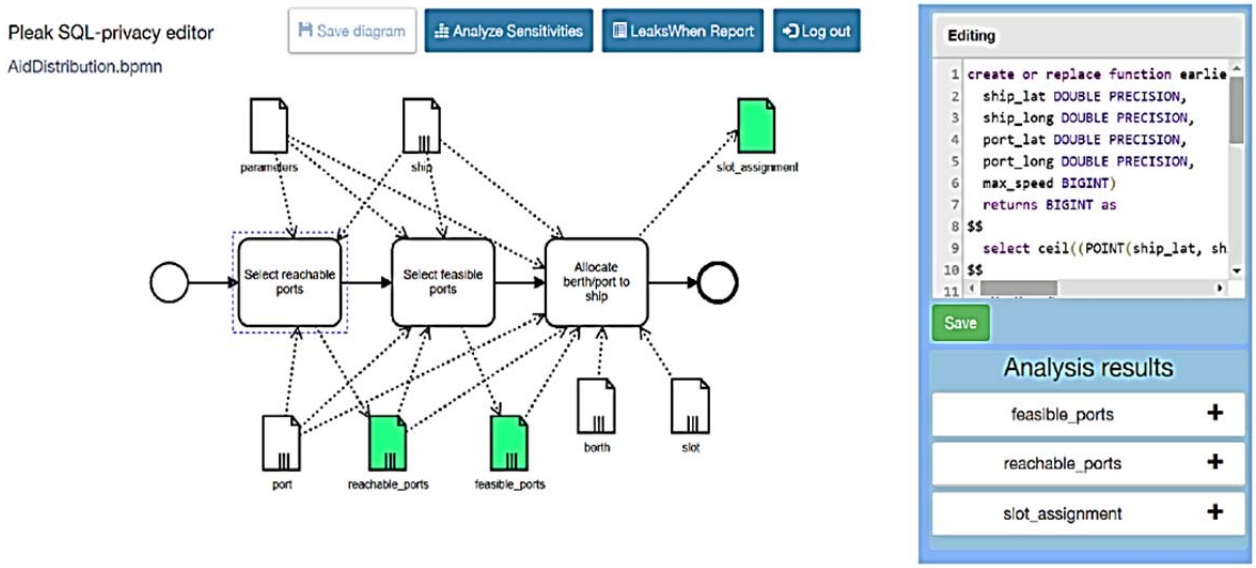


Рис. 5. Зведений сценарій «розподілу допомоги»

Джерело: скрін екрану

Щоб виконати аналіз Leaks-When, користувачеві слід вибрати один або кілька об'єктів вихідних даних (тих, що створюються завданнями або подіями) і натиснути кнопку «SQL LeaksWhen». Бічна панель виводу показує одну вкладку для кожного з вибраних об'єктів даних. У кожній із вкладок створюється окремий звіт для кожного атрибута SQL у вихідній таблиці SQL. Звіт створюється шляхом застосування методів аналізу потоку даних у робочому процесі SQL для побудови підсумкового графіка залежностей.

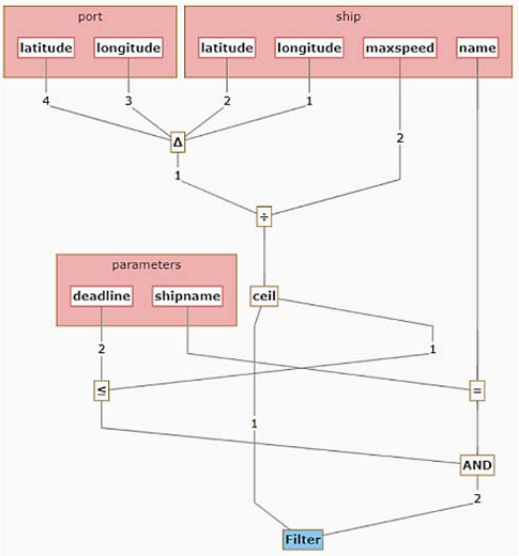


Рис. 6. Зразок звіту про витік

Джерело: скрін екрану

Висновки. Отже, існують різні підходи покращення моделей бізнес-процесів щодо конфіденційності. Існують також аналізатори та підходи до аналізу конфіденційних даних з точки зору робочих процесів SQL. Однак, варто не дотримуватись політики конфіденційності щодо конфіденційної інформації, здебільшого через те, що аналізатори відокремлені та вимагають іншого введення. Основну увагу слід зосередити на аналізі впровадження політики конфіденційності в моделі бізнес-процесів, інтеграції та розширенні існуючих інструментів аналізу.

Багаторівневий підхід дозволяє створити комплексну систему заходів, яка ускладнює злочинцям доступ до інформації і забезпечує високий рівень безпеки. Захист інформації на основі багаторівневого аналізу є ефективною стратегією безпеки в різних контекстах, включаючи захист даних, мереж та систем. Кожен рівень виконує своє завдання у створенні комплексної системи заходів. Застосування фізичного захисту, логічного контролю, мережевого захисту, програмних засобів, соціальної усвідомленості та стратегічного планування створює високий рівень безпеки, ускладнюючи можливість несанкціонованого доступу та забезпечуючи конфіденційність та цілісність інформації. Регулярний аудит та оновлення заходів безпеки важливі для адаптації до змін в ландшафті загроз та збереження ефективності заходів безпеки в часі.

Список використаних джерел

1. Закон України «Про доступ до публічної інформації». – URL: https://ips.ligazakon.net/document/T112939?an=251

2. Підтримка розробки бізнес-процесів з урахуванням конфіденційності за допомогою шаблонів процесів конфіденційності. 11-та Міжнародна конференція з дослідницьких проблем в інформаційній науці, RCIS 2017, Брайтон, Велика Британія, 10-12 травня 2017 р. – С. 187-198.

3. Модель і нотація бізнес-процесів (BPMN). – URL: https://www.omg.org/spec/BPMN/2.0/

4. PE-BPMN: модель і нотація бізнес-процесу з підвищеною конфіденційністю. Управління бізнес-процесами. 15-та Міжнародна конференція, BPM 2017, Барселона, Іспанія, 10-15 вересня 2017 р. – С. 40-56.

5. Аналіз чутливості SQL запитів. Матеріали 13-го семінару з мов програмування та аналізу безпеки, PLAS@CCS 2018, Торонто, Онтаріо, Канада, 15-19 жовтня 2018 р. – С. 2-12.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т.В.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МОНІТОРИНГУ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ DECEPTION

СІРЕНКО М.М., 1 курс 8м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

В сучасних умовах зростаючих кіберзагроз та величезного потоку даних, пов'язаних з безпекою, фахівцям центрів моніторингу та реагування на інциденти (SOC) стає все важче ефективно виявляти реальні атаки серед безлічі спрацьовувань систем захисту та розрізнених індикаторів. Ця стаття представляє технологію кіберобману (Deception) як перспективний підхід до підвищення ефективності кіберзахисту. Він ґрунтується на створенні фальшивих систем, мереж та об'єктів-приманок, які виглядають реалістично для зловмисників, відволікаючи їхню увагу від справжніх цінних ресурсів. Технології обману дозволяють залучити й аналізувати атакуючих, розкриваючи їхні наміри та методи на ранніх стадіях, що скорочує час виявлення і підвищує оперативність реагування. Водночас стаття визнає певні ризики та обмеження цього підходу й наголошує на важливості інтегрувати рішення як елемент комплексної багаторівневої стратегії кібербезпеки організації.

Amid escalating cyber threats and overwhelming security data volumes, analysts at Security Operations Centers (SOCs) face mounting challenges in effectively detecting real attacks amidst a plethora of system alerts and disparate indicators. This article presents Deception technology as a promising approach to enhance cybersecurity effectiveness. It relies on creating fake systems, networks, and decoy objects that appear realistic to attackers, diverting their attention from genuine valuable assets. Deception technologies enable luring and analyzing attackers, exposing their intent and methods at early stages, reducing detection times and improving incident response agility. Meanwhile, the article acknowledges certain risks and limitations of this approach and emphasizes the importance of integrating deceptive solutions as part of an organization's multi-layered, comprehensive cybersecurity strategy.

Актуальність. В епоху постійно зростаючих кіберзагроз та величезних обсягів даних, пов'язаних з кібербезпекою, перед фахівцями центрів кібермоніторингу (SOC) постає серйозна проблема – ефективно виявляти реальні атаки серед безлічі спрацьовувань систем захисту та розрізнених індикаторів. Тема статті, присвячена впровадженню технології кіберобману deception як методу підвищення результативності моніторингу, є вкрай актуальною. Стрімке зростання кіберзагроз – організації стикаються з дедалі більш витонченими та цілеспрямованими атаками, від яких традиційні засоби захисту не завжди здатні достатньо захистити. Величезні обсяги даних про безпекові події – для своєчасного виявлення загроз потрібно обробляти колосальні потоки даних від різноманітних систем захисту, що стає непосильним завданням для аналітиків. Недостатня ефективність існуючих методів – спрацювання систем виявлення вторгнень, сигнатурний аналіз, індикатори компрометації тощо не завжди дозволяють вчасно помітити озпаки цілеспрямованих атак на ранніх стадіях. Потреба в активних, проактивних підходах – на противагу традиційній реактивній моделі кібербезпеки, необхідні рішення, які дозволяють активно виявляти загрози та відслідковувати наміри атакуючих.

Саме технологія deception, яка полягає у створенні приманок та пасток для залучення і аналізу дій зловмисників, здатна вирішити зазначені проблеми. Автор докладно пояснює принцип дії декептивних систем, наводить переваги їх використання – від підвищення оперативності виявлення загроз до можливості аналізу тактики і методів атакуючих на ранніх етапах.Водночас стаття визнає обмеження та ризики такого підходу, зокрема потенційні помилкові спрацювання та можливість розпізнавання декепційних механізмів досвідченими зловмисниками. Тому робиться виважений акцент на необхідності інтегрувати

технології обману як допоміжний компонент у загальну комплексну стратегію кібербезпеки організації. Таким чином, в контексті безпрецедентного зростання кіберзагроз, збільшення обсягів та складності безпекових даних, розробка та впровадження новітніх підходів до кібермоніторингу та виявлення атак на кшталт декептивних технологій є надзвичайно актуальним завданням. Стаття представляє обґрунтоване теоретичне дослідження цієї проблематики, аналізує переваги та недоліки такого рішення, окреслює оптимальні шляхи його інтеграції в комплексну стратегію захисту.

Метою статті дослідження є висвітлення можливостей застосування технології Deception для підвищення ефективності моніторингу та реагування на кібератаки в корпоративних середовищах.

Предметом дослідження є використання технології Deception у процесах кібермоніторингу та реагування на інциденти інформаційної безпеки.

Об'єктом дослідження виступають процеси моніторингу та реагування на кіберзагрози в центрах безпеки SOC (Security Operations Center) підприємств та організацій.

Аналіз попередніх досліджень. Сьогодні в галузі реагування на кіберінциденти спостерігається тенденція до збільшення кількості правил кореляції та підписок на індикатори компрометації/атак IoC (Indicator of Compromise) і IoA (Indicator of Attack). Чи правильно це? Скоріше так ніж ні. Але я хочу показати ситуацію в іншій площині та розповісти про клас засобів захисту, який точно складе конкуренцію за корисністю черговому фіду з IoC або додатковим правилом кореляції. Залежно від технологічних можливостей та особливостей корпоративної мережі кожна компанія по-різному реалізовує функції моніторингу та реагування на кіберінциденти, використовує різні засоби (за класами рішень, виробниками).

Використання технології Deception: Технологія Deception є досить ефективним способом захисту від кібератак. За допомогою цієї технології, можна створити вигляд того, що важливі ресурси компанії доступні для злочинців. Це може включати створення фальшивих систем або мереж, які можуть здатися реальними для злочинців, що намагаються зламати систему. [1, с. 124] Розділи книг «The Art of Deception: Controlling the Human Element of Security» та «Deception-Based Threat Detection: Solutions for Cybersecurity» містять відомості про технології Deception та її застосування для виявлення загроз кібербезпеці.Моніторинг споживачів: Під час моніторингу засобами обману, важливо не тільки виявляти кібератаки, але й аналізувати споживачів та їх поведінку в мережі. Наприклад, аналізуючи поведінку користувачів у мережі, можна виявити підозрілі дії або незвичайну активність у мережі. [2, с. 39] Розділ «Deception in the Digital Age: Exploiting and Defending Human Targets Through Computer-Mediated Communication» містить відомості про моніторинг поведінки користувачів у мережі.

Застосування аналітики даних: Аналітика даних може бути корисною для виявлення підозрілих дій та аномальної активності в мережі. Наприклад, можна використовувати аналітику даних, щоб виявити незвичайну кількість трафіку або підозрілу активність на певній мережі. Для цього можна використовувати різноманітні програмні засоби, такі як системи виявлення вторгнень, програмні рішення для моніторингу мережі тощо. [3, с. 271] Розділ «Data Analytics for Cyber Security: A Roadmap for Research» містить відомості про застосування аналітики даних у кібербезпеці. Використання штучного інтелекту: Штучний інтелект може бути корисним для виявлення підозрілих дій у мережі. Наприклад, системи машинного навчання можуть використовуватися для автоматичного виявлення аномальної поведінки в мережі. [4, с. 76] Розділи книг «Machine Learning and Data Mining for Computer Security: Methods and Applications» та «Artificial Intelligence for Cybersecurity» містять відомості про застосування штучного інтелекту у кібербезпеці. Використання багаторівневої системи захисту: Для захисту від кібератак важливо мати багаторівневу систему захисту. Це може включати в себе не тільки застосування технологій захисту, але й навчання користувачів, щоб вони були більш уважними при роботі в мережі. [4] Розділи книг «Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices» та

«Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare» містять відомості про розробку багаторівневих систем захисту.Загальний висновок полягає в тому, що підвищення ефективності моніторингу засобами обману включає в себе застосування різноманітних технологій та програмних засобів. Для досягнення кращих результатів у кібербезпеці, важливо використовувати багаторівневу систему захисту та залучати користувачів до процесу моніторингу мережі.

Кобб наголошує, що технології Deception потрібно інтегрувати в загальну стратегію кібербезпеки організації як допоміжний компонент, а не покладатися на них як на єдиний засіб захисту [5, с. 183]. Він наводить приклади, як рішення можуть ефективно доповнювати традиційні засоби захисту, такі як системи виявлення/запобігання вторгнень, шляхом створення приманок, які відволікають та виявляють зловмисників. Конті та ін. попереджають, що успішні зловмисники можуть навчитися розпізнавати механізми та контрзаходи [6, с. 7]. Тому автори пропонують підхід «Byzantine deception» – ускладнення декептивних технік за рахунок введення елементів невизначеності та непередбачуваності, що утруднює можливість зловмисників відрізнити справжні та фейкові системи.

Як зазначають Гафір та ін., технології Deception дозволяють створювати приманки та пастки, які виглядають реалістично для зловмисників, захищаючи таким чином справжні цінні ресурси від атак. Їхнє дослідження представляє безпечний механізм обману з динамічним декептивним середовищем, що ефективно виявляє шкідливу активність і сповільнює просування атаки.Дослідження Ghafir et al. «Secure deception mechanism for defending against targeted attacks» [7, с. 13] представляє безпечний механізм обману для захисту від цілеспрямованих атак у кіберфізичних системах. Їхній підхід ґрунтується на створенні динамічного декептивного середовища з фейковими активними та пасивними приманками. Автори доводять, що це ефективно виявляє шкідливу активність і сповільнює просування атаки. Стаття Shin et al. «Tactical Deception Using Decoy Host Response for Dynamically Deceiving Remote Cyber Attackers» [8, с. 1-26] пропонує тактичний підхід до обману з використанням імітації відгуків декой-хостів. Їхній метод динамічно генерує реалістичні фейкові відгуки систем на запити зловмисників, вводячи їх в оману щодо успішного проникнення. Це дозволяє виявляти та аналізувати тактику, методи атаки на ранніх стадіях. Van Der Walt et al. у розділі «Deception in Cyber Attack Prevention» [9, с. 25-44] книги «Cyber Defense Mechanisms» досліджують роль технологій обману в запобіганні кібератакам. Автори наголошують на важливості інтегрувати засоби, такі як медові пастки, фейкові об’єкти та приманки, в комплексну стратегію кібербезпеки організацій. Вони аналізують переваги та виклики використання обманних технік проти різних типів загроз. Розглядають різні види декептивних рішень, включаючи медові пастки, системи-приманки та механізми імітації уразливостей. Водночас визнаються ризики помилкових спрацювань та адаптації хакерів. Автори наполягають на інтегруванні декептивних рішень як компонента комплексного багаторівневого захисту разом з іншими засобами безпеки. Детально розглядаються архітектура, особливості впровадження та застосування різних декепційних систем проти різних типів загроз. Також обговорюються питання безпеки, юридичні аспекти та етичні міркування. У висновках відзначається потенціал технологій обману для посилення кібербезпеки та наголошується на необхідності подальших досліджень.

Виклад основного матеріалу. Сучасний кібербезпековий ландшафт характеризується стрімким зростанням кіберзагроз та безпрецедентним збільшенням обсягів даних, пов’язаних з безпекою. Перед фахівцями центрів моніторингу та реагування на інциденти (SOC) постає серйозне випробування – ефективно виявляти реальні атаки серед величезної кількості спрацьовувань систем захисту та розрізнених індикаторів. У цьому контексті технологія кіберобману (deception) постає як перспективний підхід, здатний суттєво підвищити результативність моніторингу та оперативність протидії загрозам у корпоративних середовищах. Принцип дії декептивних рішень базується на створенні фальшивих, але реалістичних для кіберзлочинців систем, мереж та об’єктів-приманок. Ця «підроблена» інфраструктура виглядає привабливою для атакуючих, відволікаючи їхню увагу від

справжніх критично важливих активів організації. При цьому захисники можуть залучати зловмисників до взаємодії з фейковими декой-системами, ретельно відстежуючи та аналізуючи їхню шкідливу активність, тактику, методи та наміри на ранніх стадіях. Сюди відносяться «системи мережевого обману», «локальні deception системи» та «системи обману для захисту кінцевих точок». Їх спільна мета – створити враження наявності слабких місць в IT-інфраструктурі, які представляють цінність для кіберзлочинців і можуть бути атаковані. Коли зловмисники «клюнуть» на цю приманку і спробують зламати фейкову систему, захисники отримують унікальну можливість розкрити їхні справжні цілі та підготуватися до блокування реальної атаки.

Одна з головних переваг технологій обману полягає в здатності знизити час виявлення кібератак та відповідно пришвидшити реагування на них. Якщо кіберзлочинці витрачають свій час та ресурси на зламування фальшивих об'єктів-приманок, це дозволяє експертам з безпеки виявити їхні наміри на ранніх стадіях та вчасно вжити необхідних контрзаходів для захисту справжніх критичних активів організації. Показовим прикладом такого підходу є тактика «візантійського обману» (Byzantine deception) – ускладнення декептивних механізмів за рахунок введення елементів невизначеності та непередбачуваності. Це утруднює для досвідчених зловмисників можливість відрізнити справжні системи від підроблених. На додачу, технології deception демонструють переваги в аналітичному плані. Зокрема, вони дозволяють відслідковувати дії кіберзлочинців та збирати цінні дані про використовувані ними тактики, методи та інструменти. Експерти можуть вивчати спосіб мислення та поведінкові моделі атакуючих під час їхньої взаємодії з декепційними системами.

Проте, як і будь-яке рішення в сфері безпеки, технології обману мають певні обмеження та ризики. Серед них експерти виділяють можливі помилкові спрацювання – ситуації, коли легітимні користувачі можуть бути ненавмисно визначені як зловмисники та потрапити під вплив контрзаходів. Також існує загроза, що з часом досвідчені кіберзлочинці зможуть адаптуватися і навчитися розпізнавати механізми, нівелюючи їхню ефективність. Тому провідні експерти і дослідники наполягають на тому, що технології deception не слід розглядати як самодостатній універсальний захист від усіх можливих загроз. Натомість їх варто інтегрувати як допоміжний, але критично важливий компонент загальної комплексної стратегії кібербезпеки організації. Лише така гармонійна інтеграція з іншими засобами захисту, антивірусами, брандмауерами, системами виявлення та реагування на інциденти, процедурами оцінки ризиків, навчанням кібергігієні для персоналу тощо дозволить розкрити повний потенціал декептивних технологій.Водночас, це не применшує їхньої цінності в боротьбі з кіберзагрозами. Застосування обманних технік дає захисникам унікальну тактичну перевагу – можливість змінити правила гри, перехопити ініціативу і активно впливати на дії зловмисників. На відміну від традиційної реактивної моделі кібербезпеки, технологія deception переносить боротьбу на територію захисників, дозволяючи створювати пастки та контрольовані умови для виманювання, виявлення та аналізу атакуючих. Таким чином, вона потенційно здатна подолати «часову перевагу» кіберзлочинців на ранніх стадіях.

Загалом, з огляду на безпрецедентне зростання кіберзагроз, застарілість багатьох існуючих механізмів боротьби та величезні обсяги даних безпеки, впровадження технологій обману в центрах кібермоніторингу SOC виглядає дуже перспективним і актуальним кроком. Звісно, їх потрібно впроваджувати як частину збалансованої багаторівневої стратегії безпеки відповідно до потреб та вимог організації. Разом з іншими засобами технологія кіберобману сприятиме підвищенню оперативності виявлення атак, розкриттю намірів і методів зловмисників на ранніх стадіях, зрештою покращуючи загальний рівень кіберзахисту корпоративних середовищ.

Висновки. У світі, де кіберзагрози невпинно зростають, а обсяги даних про безпекові події стрімко збільшуються, фахівцям з кібербезпеки стає дедалі важче ефективно виявляти реальні атаки серед безлічі спрацьовувань систем захисту та розрізнених індикаторів. У цьому контексті технологія кіберобману (deception) постає як перспективний підхід, який

може суттєво підвищити результативність моніторингу та реагування на інциденти в корпоративних середовищах. Принцип дії декептивних рішень базується на створенні фальшивих, але реалістичних для зловмисників систем, мереж та об'єктів-приманок. Це відволікає увагу атакуючих від справжніх цінних ресурсів організації, залучаючи їх до взаємодії з декой-системами. При цьому захисники отримують можливість виявляти шкідливу активність, аналізувати тактику, методи і наміри кіберзлочинців на ранніх стадіях, що значно скорочує час реагування. Головними перевагами технологій обману є підвищення оперативності виявлення загроз, відволікання атакуючих від критичних активів, розкриття їхніх дій та намірів. Вдосконалені підходи на кшталт «Byzantine deception» роблять механізми більш стійкими до розпізнавання з боку досвідчених зловмисників. Разом з тим, застосування обманних технік має свої обмеження та ризики. Зокрема, існує ймовірність помилкових спрацювань з визначенням легітимних користувачів як атакуючих. Тому ключовою рекомендацією експертів є інтегрування декептивних засобів як допоміжного компонента в загальну комплексну стратегію кібербезпеки організації. Лише у поєднанні з іншими інструментами (антивірусами, файрволами, засобами виявлення та реагування на інциденти тощо) та заходами (навчанням персоналу, оцінкою ризиків і т.д.) технології обману зможуть розкрити свій повний потенціал. Загалом, технологія deception є перспективним та ефективним рішенням для підвищення спроможностей центрів моніторингу SOC у сфері виявлення та протидії цілеспрямованим кібератакам. Її впровадження дозволяє захисникам кардинально змінити підхід – від статичної реактивної моделі до активного розставляння пасток та приманок для викриття намірів та дій зловмисників. Хоча вона й не забезпечує 100% захисту, інтегрована декептивна складова значно підсилює комплексну стратегію кібербезпеки, забезпечуючи своєчасне виявлення і протидію кібератакам.

Список використаних джерел

1. «The Art of Deception: Controlling the Human Element of Security» by Kevin D. Mitnick and William L. Simon (розділ «The Art of Deception» та «Deception in the Real World) – с. 124
2. «Deception in the Digital Age: Exploiting and Defending Human Targets Through Computer-Mediated Communication» by Robin Dreeke (розділ «Deception and Counter-Deception in Cyberspace» та «Deceptive Strategies in Cyberspace») – с. 39
3. «The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations» by Ben Buchanan (розділ «Deception in Cyberspace») – с. 271
4. «Deception-Based Threat Detection: Solutions for Cybersecurity» by Chuvakin, Anton and Shackleford, John – с. 76
5. «The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations» by Ben Buchanan (розділ «Deception in Cyberspace») – с. 183
6. «Deception Technology for Cybersecurity Defense» by Michael Cobb (стаття у ISACA Journal, випуск 5, 2021 рік) – с. 7
7. «Byzantine Deception: Attacking Anti-Deception with Deception» by Giovanni Conti, John Aycock, Adam Doupé, Frank Turrise (стаття на Annual Computer Security Applications Conference, 2021 рік) – с. 13
8. «Secure deception mechanism for defending against targeted attacks» by Ibrahim Ghafir, Vaclav Prenosil, Nasser Alhebaishi, Anas N. Jaber, Raed Mohammed (розділ у ACM Transactions on Cyber-Physical Systems, том 4, випуск 4, 2020 рік) – с. 1-26
9. «Deception in Cyber Attack Prevention» by Erica Van Der Walt, Jarred Jansen Van Vuuren, Louis Leenen (розділ у книзі «Cyber Defense Mechanisms», видавництво Springer, Cham, 2019 рік) – с. 25-44

Робота виконана під науковим керівництвом старшого викладача
ШЕСТАКА Я.І.

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ ДЛЯ ЗАХИСТУ ДАНИХ ДИСТРИБ'ЮТОРСЬКИХ ПІДПРИЄМСТВ

СУХОЦЬКИЙ І.В., 1 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто актуальність використання біометричних технологій, використання біометричних технологій для доступу даних, захист персональних даних клієнтів у дистриб'юторських компаніях, збір та аналіз даних з метою поліпшення обслуговування та забезпечення безпечної доставки даних.

The article considered the relevance of using biometric technologies, the use of biometric technologies for data access, the protection of personal data of customers in distribution companies, the collection and analysis of data in order to improve service and ensure safe delivery of data.

Актуальність. В сучасному цифровому світі, коли дані набувають величезного значення як людський ресурс, забезпечення безпеки даних для захисту від несанкціонованого доступу стає все більш критично важливим завданням для підприємств усіх галузей, включаючи дистриб'юторські підприємства. Біометричні технології є одним із найефективніших інструментів у цьому відношенні.

Використання біометрії, такої як відбитки пальців, розпізнавання обличчя, сканування радужної оболонки ока тощо, може забезпечити високий рівень безпеки та захисту важливих даних, що містяться на дистриб'юторському підприємстві, від несанкціонованого доступу, та викрадання даних.

Завдяки унікальності біометричних даних для кожної особи та їх складній підробці, вони можуть стати найбільш ефективним засобом автентифікації та авторизації користувачів у системі.

Використання цих технологій також може підвищити продуктивність робочих процесів, оскільки вони забезпечують швидку та зручну ідентифікацію користувачів і надання їм доступу до необхідних ресурсів. Однак, при впровадженні біометричних систем важливо враховувати аспекти приватності та захисту даних користувачів. Необхідно приділяти увагу забезпеченню безпеки та конфіденційності зібраних біометричних даних, а також дотримуватися відповідних правових норм і регуляції, щоб уникнути можливих проблем зі збереженням і обробкою цих даних.

Отже, біометричні технології можуть бути дуже корисними для захисту даних дистриб'юторських підприємств, проте, їх впровадження вимагає уважного планування та врахування різних аспектів безпеки та приватності.

Метою статті є використання біометричних технологій у дистриб'юторських підприємствах, спрямованих на забезпечення високого рівня безпеки й захисту конфіденційної інформації, такої як особисті дані клієнтів, постачальників та фінансова інформація. Ці технології ефективно впроваджують систему ідентифікації й контролю доступу, що сприяє зменшенню ризику витоку або крадіжки даних.

Предметом дослідження є методи біометричних технологій, які ідентифікуються за допомогою їх унікальних фізичних особливостей, а саме відбитків пальців, розпізнавання міміки та м'язів обличчя, сканування райдужної оболонки ока чи сканування голосу. Ці біометричні технології застосовуються для забезпечення безпеки доступу до будівель, інформації в комп'ютерних системах та інших ресурсів дистриб'юторських підприємств.

Об'єктом дослідження біометричних технологій є захист дистриб'юторських підприємств, які мають справу з великим обсягом конфіденційної інформації та потребують

надійного збереження даних. Це можуть бути всі дані про клієнтів їх замовлення, фінансові операції тощо.

Аналіз попередніх досліджень. Дослідження біометричних технологій базується на роботах таких науковців як Стефан В. Джонсон, Андреас У. Ветерленд, Анджело Коломбо та Андреас Н. Андреасен.

Дистриб'юторське підприємство є посередником між виробниками товарів і кінцевими споживачами. Основна функція дистриб'юторського підприємства – це розподіл товарів або послуг від виробника до роздрібних магазинів, оптових покупців або інших клієнтів. Ці підприємства можуть працювати у різних галузях, включаючи продаж продуктів харчування, електроніки, автомобілів, медичного обладнання тощо.

Виклад основного матеріалу. Дистриб'юторські підприємства мають значний обсяг конфіденційної та критично важливої інформації, яку потрібно захищати від несанкціонованого доступу та недобросовісного використання. Серед основних категорій інформації, які потребують захисту на дистриб'юторських підприємствах, можна виділити наступні [1]:

- Інформація про клієнтів, включаючи їх контактні дані, історію замовлень, пріоритети та інші конфіденційні дані, повинна бути надійно захищена, щоб уникнути її неправомірного розголошення чи зловживання.
- Дані про продукцію, включаючи її характеристики, ціни, умови постачання тощо, є конфіденційною і має бути захищена від несанкціонованого доступу.
- Фінансова інформація, така як дані про фінансові транзакції, рахунки, платежі, бюджети, документація тощо, повинна бути захищена від несанкціонованого доступу.
- Інформація щодо партнерів, продажів філії та дистриб'юторів, аналізів ефективності роботи філії та працівників, включаючи постачальників та інших співробітників, їх умови співпраці та укладені контракти, також має бути об'єктом захисту.

Для захисту цих даних є актуальним використовувати біометричні технології. Згідно з принципом дії, біометричні методи ідентифікації можна розділити на статичні (засновані на ознаках, які притаманні людині з народження), динамічні (засновані на ознаках, які набуваються протягом життя) та комбіновані (поєднання двох попередніх) [2].

Фізіологічні (статичні) методи біометричної ідентифікації включають:

- Сканування райдужної оболонки ока.
- Сканування сітківки ока.
- Сканування рисунку вен долоні.
- Геометрія кисті руки, яка включає в себе відбитки пальців (дактилоскопія), розмір, довжину і ширину долонь.
- Розпізнавання рис обличчя, таких як контур, форма, розташування очей і носа, та структуру ДНК-сигнатури.

Поведінкові (динамічні) методи включають:

- Аналіз підпису, що охоплює форму букв, манеру письма та натиск.
- Аналіз тембру голосу.
- Аналіз клавіатурного почерку та інші подібні характеристики.

Комбіновані методи біометричної ідентифікації використовують два або більше види біометричних ознак, щоб забезпечити вищу точність та надійність у процесі ідентифікації, але є більш затратним у процесі експлуатації.

Сканування райдужної оболонки та відбитки пальців є найбільш поширеними методами біометричної ідентифікації особистості, які в сукупності становлять близько 2/3 від усього обсягу систем ідентифікації.

Для користувачів важливо, щоб метод біометричної ідентифікації був швидким, швидким та легким у використані, саме тому більшість людей обирають сканування райдужної оболонки ока або відбитків пальців.

Класифікацію методів біометричної ідентифікації зображено на Рис. 1.

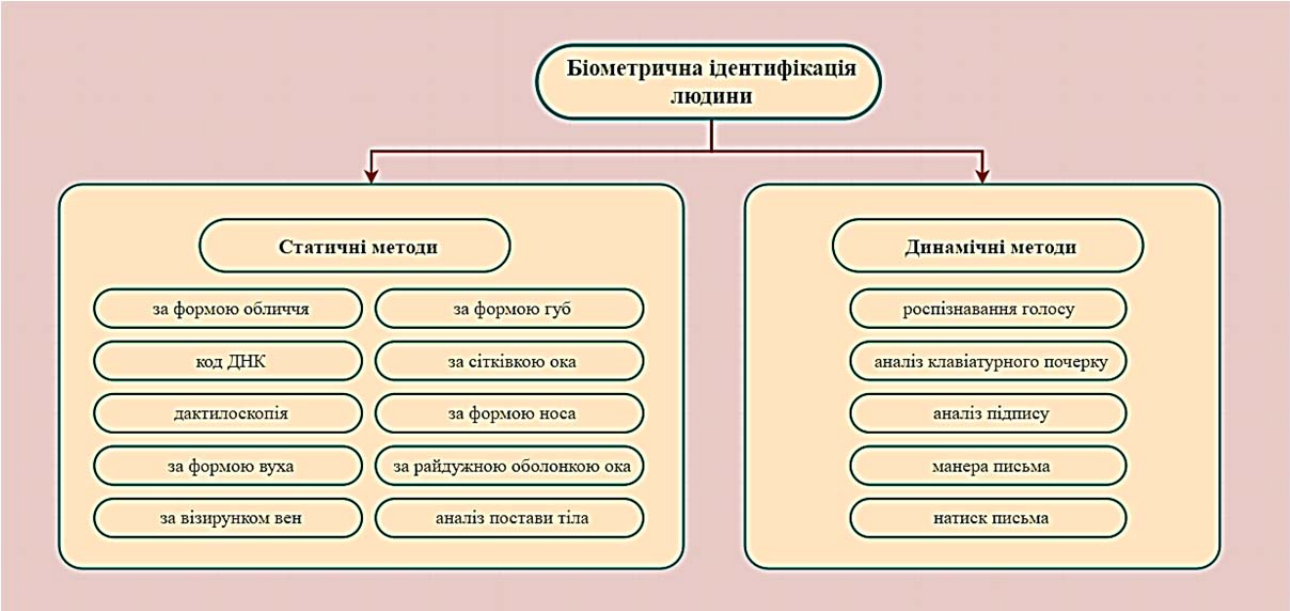


Рис. 1. Класифікація методів біометричної ідентифікації людини

Джерело: розроблено автором

Виходячи з наведених прикладів біометричних технологій зведемо інформацію до Таблиці 1, де вказано сферу застосування, ймовірність помилки ідентифікації та її надійність.

Таблиця 1

Надійність та сфера застосування методів ідентифікації

Метод	Носій біометричної інформації	Імовірність помилки	Надійність	Сфера застосування
Розпізнавання райдужної оболонки ока	Візерунок райдужки	1/1200000	Висока	Критичні до кількості помилок сервіси
Розпізнавання малюнка вен кисті руки	Візерунок вен	1/1100000	Висока	Критичні до кількості помилок сервіси
Дактилоскопія	Відбиток пальців	1/1000	Середня	Універсальні
Форма руки	Розмір, довжина й ширина долонь	1/700	Низька	Некритичні до кількості помилок сервіси
Розпізнавання обличчя	Контур, форма; розташування очей і носа	1/100	Низька	Некритичні до кількості помилок сервіси
Підпис	Форма букв, манера листа, натиск	1/100	Низька	Некритичні до кількості помилок сервіси
Розпізнавання голосу	Характеристики голосу	1/30	Низька	Некритичні до кількості помилок сервіси

Джерело: [2]

Як результат аналізу даних з таблиці можна виокремити переваги та недоліки застосування певних біометричних технологій.

Для дактилоскопії.

Переваги:

- Висока достовірність, оскільки статистичні показники цього методу перевищують показники інших способів ідентифікації, таких як обличчя, голос або підпис.

- Низька вартість пристроїв для сканування зображення відбитка пальця.
- Проста процедура сканування відбитка, що дозволяє легко виконувати цей процес.

Недоліки:

- Папілярний візерунок відбитка пальця може легко пошкодитися дрібними подряпинами або порізами, що може ускладнити його ідентифікацію.
- Метод не має достатньої захищеності від підроблення зображення відбитка, що може викликати проблеми з безпекою.

Для розпізнавання райдужної оболонки ока.

Переваги:

- Велика статистична надійність, що підтверджується високим рівнем.
- Завдяки обмеженому розповсюдженню систем імовірність створення засобів їх «обману» виявляється досить низькою.
- Райдужна оболонка має захист від пошкоджень рогівкою.
- Метод реєстрації даних є безконтактним, що є його важливою перевагою.

Недоліки:

- Система є складною у використанні і потребує значного часу для оброблення.
- Велика вартість системи
- Недостатнє поширення системи та відсутність широкого ринку призводять до обмеженої доступності та низького темпу розвитку методу.

Для розпізнавання голосу.

Переваги:

- Висока ступінь безпеки.
- Зручність використання.
- Високий спектр застосування.
- Низькі операційні витрати

Недоліки:

- Вплив фізичних факторів. Зміни в голосі через захворювання, стрес або втома можуть вплинути на точність розпізнавання.
- Неідеальна точність

Для розпізнавання малюнка вен кисті руки.

Переваги:

- Достовірність результатів висока.
- Відсутність необхідності у прямому контакті зі скануючим пристроєм.
- Високий рівень захищеності, оскільки неможливо отримати рисунок від людини у вуличних умовах, а при використанні муляжу кисті інфрачервона камера не зможе зчитати вени.

Недоліки:

- Чутливість до освітлення з сонячних променів і променів галогенних ламп, що може призводити до неправильного функціонування сканера.
- Вплив певних захворювань, таких як артрит, на точність прийняття рішень методом сканування.

Кожен з цих методів має свої переваги і недоліки, тому вибір найкращого залежить від конкретних потреб і умов. Але, більш зручним, практичним та біометричним методом для використання та експлуатації в дистриб'юторських підприємствах на погляд оточуючих людей, які з цими методами зіштовхуються є звичний метод сканування відбитку пальця, адже він має високу популярність в багатьох сферах де залучені біометричні технології. Наприклад, якщо важлива висока достовірність, простота процедури та низька вартість, то сканування відбитків пальців може бути найбільш відповідним варіантом.

Але в реаліях сьогодення, найголовнішою метою в дистриб'юторських компаніях в першу чергу повинно бути забезпечення захисту даних від витоку та крадіжки. Тому не можна покладатися на метод, заснований лише на одному фактору ідентифікації, адже дані – це головний продукт, який більш вразливий для шахрайських дій, та першим піддається злому.

Тому для забезпечення безпеки даних слід використовувати комбінований метод, адже, по-перше, збільшується точність ідентифікації особи, яка має позбавитись всіх непотрібних стереотипів та попередніх уявлень щодо самоідентифікації особи, а, по-друге, декілька біометричних характеристик важче підробити, ніж одну.

Для використання двохфакторного біометричного захисту за мету візьмемо сканування біометричного відбитка пальця та розпізнавання голосу, який буде зберігатися технологією блокчейн.

Технологія блокчейн – це система, яка дозволяє зберігати та передавати інформацію у вигляді послідовності блоків. Коли нова інформація внесена в блокчейн, мережа перевіряє її, криптографічно захищає і додає до блоку. Цей блок потім включається в ланцюг блоків в хронологічному порядку, який неможливо змінити [3].

Поєднання блокчейну з ідентифікацією за допомогою біометричних технологій може бути реалізовано шляхом створення цифрових ідентифікаторів, а саме сканування відбитку пальця та розпізнавання голосу, які базуються на біометричних даних користувачів. Ці дані можуть бути збережені в блокчейні, де вони захищені від модифікацій та змін. Під час ідентифікації користувача його біометричні дані порівнюються зі збереженими в блокчейні, що дозволяє впевнитися в його особистості безпеки та недоступності цих даних. Такий підхід дуже підходить до дистриб'юторських підприємств.

Як результат поєднання сканування відбитку пальців та розпізнавання голосу які будуть зберігатися технологією блокчейн має наступні переваги та недоліки.

Переваги:

- Висока безпека. Біометричні дані, такі як відбитки пальців і розпізнавання голосу, є унікальними для кожної особи, що робить їх важкими для підробки або використання несанкціонованими особами. Їх зберігання в блокчейні забезпечує додатковий рівень захисту.
- Недоступність даних для сторонніх. Блокчейн забезпечує надійну захист від несанкціонованого доступу до біометричних даних, тим самим забезпечуючи приватність і конфіденційність користувача.
- Висока точність ідентифікації. Поєднання двох біометричних методів (відбиток пальця і розпізнавання голосу) може забезпечити більш високу точність ідентифікації користувача, порівняно з використанням лише одного методу.

Недоліки:

- Технічні обмеження. Незважаючи на значний прогрес у розробці біометричних технологій, вони все ще можуть допускати помилки або неправильно реагувати на деякі фактори, такі як зміни в голосі або фізичному стані пальця.
- Ціноутворення. Впровадження системи, яка поєднує біометричні технології і блокчейн, може вимагати значних витрат на розробку та інтеграцію.

Проаналізувавши перелічені переваги і недоліки можна зробити наступний висновок. Введення системи двофакторного біометричного захисту з використанням сканування відбитка пальця та розпізнавання голосу, що базується на технології блокчейн, може бути важливим кроком у забезпеченні безпеки та ефективності операцій на дистриб'юторських підприємствах. Інтеграція цієї новаторської технології в процеси, зазначені в Таблиці 2, може значно підвищити швидкість, безпеку та точність виконання операцій на дистриб'юторських підприємствах. Вона дозволить автоматизувати процеси, зменшити ризики витрат та забезпечити високий рівень захисту конфіденційної інформації.

Таблиця 2

Впровадження системи захисту запропонованим комбінованим методом

Технічна складова	Опис
Доступ до складських приміщень	Система керування доступом до складських приміщень використовує сканування відбитка пальця та розпізнавання голосу для ідентифікації працівників перед входом
Автентифікація працівників	Технологія може бути використана для аутентифікації працівників під час входу в систему обліку робочого часу або доступу до комп'ютерних систем компанії
Забезпечення безпеки даних	Технологія використовується для аутентифікації працівників перед доступом до конфіденційної інформації про клієнтів та операцій на дистриб'юторських підприємствах, що забезпечує їх безпеку
Автоматизація операцій	Система захисту може спростити та прискорити процеси, такі як реєстрація замовлень, прийом товарів на склад або відправка продукції, забезпечуючи безпеку та автоматизацію операцій
Контроль доступу до важливих приміщень об'єктів	Технологія може бути використана для контролю доступу до важливих приміщень, наприклад, до кімнат, де зберігається цінний інвентар або обладнання

Джерело: Розроблено автором

Висновки. Сучасний світ більше переходить на технічну складову і зберігає всі дані в електронній формі, через це зростає необхідність технічного захисту із залученням біометричних технологій. Впровадження комбінованого методу цієї технології, що включає сканування відбитку пальця та голосу, разом із збереженням даних за допомогою технології блокчейн для надійного та незмінного зберігання даних, у дистриб'юторських підприємствах забезпечує високий рівень захисту від крадіжок або витоку даних, оскільки вона використовує два унікальні біометричні параметри, які важко підробити. Важливим завданням також є реалізація та підключення цієї системи в дистриб'юторському підприємстві до засобів інформації, яка зберігається в компаніях або для ідентифікації користувача.

Список використаних джерел

1. Жуков С.А. Дистрибуція та координація каналів розподілу з елементами маркетинг-міксу. – Наукові праці ДонНТУ. Серія: економічна. – № 2, 2019 р. – С. 48-56. – URL: http://surl.li/sewre

2. Коваль Л.Г., Злепко С.М., Новіцький Г.М., Крекотень Є.Г. Методи і технології біометричної ідентифікації за результатами літературних джерел. – Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. – Том 30(69), Ч. 1, № 2, 2019. – С. 104-112. – URL: https://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf

3. Кучеренко О. Що таке блокчейн? Основи та як він працює. – URL: http://surl.li/sutkq

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т.В.

PERSONAL DATA PROTECTION TECHNOLOGIES IN ELECTRONIC PAYMENT SYSTEMS

ТЕРЕМОК М.В., 1 курс 6мз група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто використання персональних даних у фінансових установах та електронних платіжних системах з акцентом на правових аспектах, загрозах безпеці даних і заходах протидії цим загрозам. Підкреслено важливість надійних гарантій для збереження конфіденційності та запобігання несанкціонованому доступу. Аналізуючи правові рамки, вразливості та передові технології захисту, дослідження підкреслює необхідність комплексних стратегій захисту даних у сфері фінансів і цифрових платежів. Забезпечення безпеки даних має вирішальне значення для підвищення довіри споживачів та уможливлення безпечних цифрових транзакцій.

This study delves into the pervasive use of personal data in financial institutions and electronic payment systems, focusing on legal aspects, threats to data security, and protective measures. It emphasizes the importance of robust safeguards to preserve privacy and prevent unauthorized access. By analyzing legal frameworks, vulnerabilities, and advanced protective technologies, the research underscores the need for comprehensive data protection strategies in finance and digital payments. Ensuring data security is crucial for enhancing consumer trust and enabling secure digital transactions.

Relevance. The proliferation of e-commerce and widespread access to mass communication tools have amplified the risks associated with the collection and accumulation of personal information. The development and deployment of advanced tools for integrating and rapidly processing personal data may pose a threat to the rights, freedoms, and interests of individuals.

Instances of attackers attempting to gain unauthorized access to confidential information by targeting the information systems of various organizations are rapidly escalating. This issue affects not only individuals, private institutions, and enterprises but also the public sector, as well as the finance, banking, and electronic payments industries. In the event of personal data loss, leakage, or compromise, commercial organizations risk incurring severe financial and reputational consequences, while data owners may face moral, financial, or physical harm.

Consequently, given the constant evolution and emergence of new threats, the protection of personal information has become an extremely critical area within the realm of information security, necessitating robust measures to safeguard sensitive data.

The aim of this article is to investigate the unique aspects and considerations involved in employing personal data protection technologies within electronic payment systems.

The object of research centers around the processes and mechanisms for countering threats to personal information and mitigating the risks associated with such threats.

The subject of study encompasses the various approaches, techniques, and measures employed to ensure the security and safeguarding of personal information, particularly in the context of electronic payment systems and the handling of sensitive data.

Analysis of previous studies. The existing literature on data protection within electronic payment systems encompasses various facets of security and technology implementations. Farawn, Rjeib, Ali, and Al-Sadaw highlight the evolution of electronic payment systems, emphasizing their efficiency compared to traditional methods. They discuss the widespread adoption of RFID technology, which has been extensively researched and applied to maximize its benefits in secure electronic transactions, particularly in academic settings. Their study proposes a multifaceted RFID-based payment system designed to manage student payments securely through multiple applications and security measures such as SHA-256 encryption and multi-level security privileges, aiming to

enhance both security and functionality within an academic context [2, p. 542]. However, their discussion lacks a thorough analysis of potential risks and threats to personal data, which is crucial for devising effective protection strategies.

In another significant contribution, Hassan, Shukur, Hasan, and Al-Khaleefa explore the security dimensions of e-wallets and online payments through a systematic review of 131 studies conducted between 2010 and 2020. Their analysis identifies critical security properties necessary for safeguarding electronic payments, including availability, authorization, integrity, non-repudiation, authentication, and confidentiality. This research underscores the growing concern for security in light of increased electronic payment adoption and pinpoints the higher security demands compared to general web security issues. Their findings suggest enhancements in security practices to address vulnerabilities and meet comprehensive service requirements, pointing out future areas for advancing e-wallet and online payment system security and interoperability [3, p. 1344]. However, the focus remains narrowly on online payment mechanisms, somewhat neglecting other crucial payment platforms like point-of-sale systems and mobile payments.

Lastly, Sahi, Khalid, Abbas, Zedan, Khatib, and Al Amosh offer a broad review of 591 studies addressing the privacy and security risks in digital payments. Utilizing a bibliographic approach, their evaluation spans the intellectual evolution of the field and proposes new research directions. The analysis reveals a primary focus on perceived privacy and security issues and suggests that future research should delve deeper into the interrelationships between different risk attributes and consider cultural factors affecting user behavior in digital payments. This comprehensive review aims to inform future research by highlighting geographical and theoretical gaps and proposing a detailed risk framework for digital payment systems [6, p. 32]. Although insightful, their review does not extensively cover the technical mechanisms of data protection, which are pivotal in mitigating privacy and security risks in digital transactions.

Presentation of the main material. In today's landscape, especially within financial institutions, organizations prioritize the storage and management of data related to various individuals, such as employees, partners, and customers. Safeguarding this information, particularly within banking systems that house extensive personal data, is crucial for both governmental bodies and the entities responsible for managing this data. Recognizing the significance of citizens' personal data and aiming to uphold their fundamental rights, countries worldwide are enacting legislation to ensure its security.

For instance, Ukraine, in alignment with global standards, has established the Law No. 2297-VI «On Protection of Personal Data» [11], which defines personal data and outlines the principles and procedures for its processing, storage, and transfer. Additionally, Ukraine looks to international models, such as the European Union's General Data Protection Regulation (GDPR), introduced in 2018 [5]. The GDPR mandates transparent practices regarding data collection and processing, granting users rights such as access, correction, deletion, and portability of their data, as well as the right to object to processing. Non-compliance with GDPR regulations can result in significant fines.

Concerns over information security threats are heightened by breaches that jeopardize the confidentiality, integrity, and availability of data. According to IBM's 2023 report, the average cost of a data breach in the United States was $4.45 million, with sectors like healthcare, finance, and technology being prime targets [4]. Effective information security requires identifying potential threats, avenues of leakage, and unauthorized access methods. Figure 1 illustrates general classification of data threats.

External threats can be broadly classified into various categories, including organized groups of hackers (such as activists, cybercriminals, and terrorists), professional hackers (including black, white, and gray hat hackers), and amateur hackers.

On the other hand, insider threats pertain to cyber threats originating from within an organization, often due to actions by authorized users with access to the organization's network and data. Examples of insider threats include insider attacks, accidental breaches, poor password management, abuse of privileges, and negligent behavior.

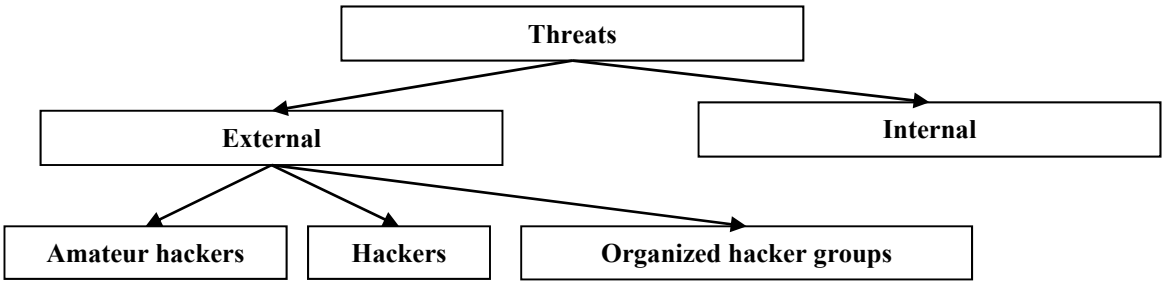


Figure 1. Classification of threats caused by humans

Source: elaborated based on [7; 9]

Detection and response involve a collaborative process between individuals and technology to address breaches effectively. A comprehensive security policy encompassing threat detection and response integrates people, procedures, and technology to identify intrusion signs promptly and take appropriate action.

The typical process of a security system includes auditing, technical measures, organizational strategies, and recovery. During the auditing phase, specialists assess the security of the system by scanning all information resources, identifying vulnerabilities, and providing recommendations for mitigation. Regular audits are essential to keep the security system current against emerging threats.

When establishing a security system, organizations must first define requirements and adhere to relevant regulations, such as ND TZI 3.7-003-2005 [10]. Following the formulation of requirements, a technical task is developed, and the system is constructed. Testing identifies deficiencies, problems, and vulnerabilities, facilitating necessary improvements. Successful compliance with requirements leads to the issuance of a certificate of compliance.

Organizational measures for information security commonly involve crafting a suitable security policy. Companies may develop their policies from scratch or based on established international standards, tailored to their specific needs and business characteristics. Many adopt plans outlined by NIST, including stages like preparation, detection and analysis, containment, elimination, recovery, and evaluation.

ISO/IEC 27001 serves as a regulatory framework defining requirements for an information security management system in organizations [12]. Its implementation emphasizes an integrated approach to risk management, wherein all information security risks are identified, assessed, and managed within acceptable levels. Compliance with regulatory and legal requirements often necessitates employee awareness and appropriate training.

Table 1 outlines the main disparities between NIST standards and ISO/IEC 27001.

Table 1

The main differences between NIST and ISO/IEC 27001

Features	NIST	ISO 27001
Objectives	Designed as a guide (guidelines)	Designed as a compliance standard
Compliance	No certification	Pre-certification audit required
Maturity	Used in early stages of company development	Used in organizations with advanced security and high risks
Price	Free to download and implement	Requires the purchase of a standard and hiring an auditor

Source: elaborated based on [8]

Ensuring the security of personal data within a system is crucial among a wide array of measures needed to effectively counter cyber threats. Contemporary security strategies continuously evolve to tackle new challenges, relying on various established technical methods for safeguarding data, including: implementation of firewalls; employment of multi-factor authentication; utilization of antivirus software; deployment of intrusion detection and prevention systems (IDS and IPS); integration of user behavioral analysis systems.

In recent times, anti-fraud systems have gained widespread adoption, especially in the realm of online purchases and payments. These systems encompass a suite of measures aimed at evaluating banking or online transactions for potential fraudulent activities. Each transaction undergoes scrutiny against predefined criteria; if it fails to meet these criteria, further investigation ensues.

Assessment criteria for transaction legitimacy encompass a multitude of factors. Beginning with authorization, the system scrutinizes whether the user input their password manually or through copy-paste methods. Additionally, it compares various parameters such as IP address, cookies, average website dwell time, typical purchase amounts, and standard user behavior patterns. Based on these factors, a decision regarding transaction authorization is made.

Following the assessment, the system assigns conditional «labels» to transactions: «red» indicates a high risk of fraud, prompting additional authentication of the cardholder; «yellow» suggests a moderate risk of fraud, possibly necessitating further verification and confirmation; «green» implies minimal risk of fraud, allowing the transaction to proceed in most cases.

The effectiveness of these systems is bolstered by the integration of artificial intelligence, facilitating more efficient checks. Additionally, the exchange of datasets pertaining to fraudsters and their behavioral patterns between financial institutions and banks enhances the ability to identify and prevent fraudulent payments.

The protocol operates on the principle of three domains: the acquirer's domain (comprising the merchant and the bank receiving funds), the issuer's domain (the bank issuing the card), and the compatibility domain (provided by the payment system to support the protocol). This arrangement is illustrated in Figure 3.

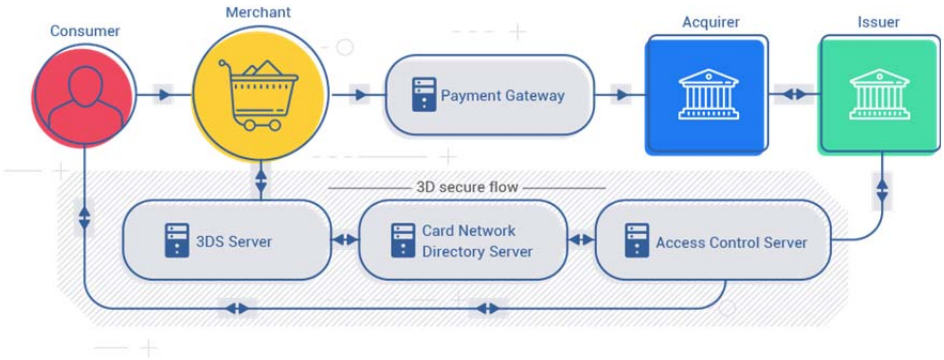


Figure 2. Scheme of 3-D Secure protocol functioning

Source: [1]

Ukraine presently enforces regulations dictating how public authorities and specific financial institutions, such as the National Bank, banks, and other entities within financial service markets overseen by the National Bank, respond to different cyber events. These regulations also apply to payment system operators, participants, and payment service technology operators, including those classified as critical infrastructure by the National Bank.

Notably, the Cabinet of Ministers of Ukraine issued Resolution No. 299 on April 4, 2023, titled «Some Matters Concerning Response by Cybersecurity Entities to Various Types of Events in Cyberspace». This resolution outlines five levels of criticality for cyber incidents: level 0 (non-critical or white), level 1 (low or green), level 2 (medium or yellow), level 3 (high or orange), level 4 (critical or red), and level 5 (emergency or black).

Government agencies, financial institutions, and banks have the authority to engage state teams to address cyber incidents: 1) CERT-UA (Governmental Computer Emergency Response Team of Ukraine), operating under the State Service for Special Communications and Information Protection of Ukraine; 2) CSIRT-NBU (Cyber Incident Response Team of the National Bank of Ukraine), responsible for cyber defense in Ukraine's banking system and part of the National Bank of Ukraine's Cyber Defense Center, overseeing cybersecurity in the country's financial sector; 3) other structures, groups, and teams, along with their affiliations, as well as specialized platforms.

Conclusions. This article examines the significance of safeguarding personal data within electronic payment systems. Banks and financial institutions handle and manage sensitive details of their clients (such as full name, passport information, ID numbers, residential address, date and place of birth, social status), along with data acquired during service provision, credit history records, biometric information (such as photos and voice samples), technical data from websites or apps, and sensitive categories of personal data. They commit to implementing all necessary measures to protect this information from unauthorized access, tampering, or other illicit activities. The article delineates the primary risks to personal data and explores various measures and strategies adopted by companies to uphold its confidentiality and integrity.

References

1. 3DSecure2 (2024). Early day authentication did not have mobile payments in mind. URL: https://3dsecure2.com/ (останнє звернення 20.04.2024 р.).

2. Farawn, A.A., Rjeib, H.D., Ali, N.S., Al-Sadaw, B. (2020). Secured e-payment system based on automated authentication data and iterated salted hash algorithm. TELKOMNIKA Telecommunication, Computing, Electronics and Control, Vol. 18, No. 1, pp. 538-544. DOI: http://doi.org/10.12928/telkomnika.v18i1.15623

3. Hassan, M.A., Shukur, Z, Hasan, M.K., Al-Khaleefa, A.S. (2020). A Review on Electronic Payments Security. *Symmetry*, 12 (8), p. 1344. DOI: https://doi.org/10.3390/sym12081344

4. IBM (2023). Cost of a Data Breach Report 2023. URL: https://www.ibm.com/ reports/data-breach (останнє звернення 20.04.2024 р.).

5. Intersoft Consulting (2024). General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. URL: https://gdpr-info.eu/ (останнє звернення 20.04.2024 р.).

6. Sahi, A.M., Khalid, H., Abbas, A.F., Zedan, K., Khatib, S.F.A., Al Amosh, H. (2022). The Research Trend of Security and Privacy in Digital Payment. *Informatics,* Vol. 9, p. 32. DOI: https://doi.org/10.3390/informatics9020032

7. SecureTriad (2024). Internal Vs External Threats – Here's All You Need to Know. URL: https://securetriad.io/internal-vs-external-threats/ (остання звернення 20.04.2024 р.). 4

8. Vanta (2024). NIST CSF vs. ISO 27001: What's the difference? URL: https://www. vanta.com/collection/iso-27001/nist-csf-vs-iso-27001 (останнє звернення 20.04.2024 р.).

9. Zerofox (2024). External Threats vs. Internal Threats in Cybersecurity. URL: https://www.zerofox.com/blog/external-threats-vs-internal-threats-in-cybersecurity/ (останнє звернення 20.04.2024 р.).

10. Головне управління технічного захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (2005). Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі : НД ТЗІ 3.7-003-2005 від 08.11.2005 р. № 125. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf (останнє звернення 20.04.2024 р.).

11. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (останнє звернення 20.04.2024 р.).

12. Національний стандарт України «Методи захисту системи управління інформаційної безпеки». Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) від 18.12.2015 р. № 193. URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf (останнє звернення 20.04.2024 р.).

Робота виконана під науковим керівництвом д-ра екон. наук, професора
ТОКАРЯ В.В.

ЕФЕКТИВНІСТЬ DLP-ТЕХНОЛОГІЙ У КОНТЕКСТІ СУЧАСНИХ ВИКЛИКІВ ЗАХИСТУ ІНФОРМАЦІЇ

ЧЕРЕДНЮК Д.С., 1 курс 6мз група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

В статті досліджується ефективність технологій запобігання витоку даних (DLP) у контексті сучасних викликів у сфері захисту інформації. Аналізується роль DLP-технологій у вирішенні основних загроз для безпеки даних, таких як кібератаки, внутрішні загрози та ризики, пов'язані з розподіленими робочими місцями. Через призму практичних прикладів і висновків відображається важливість і потенціал DLP-технологій у сфері кібербезпеки та рекомендуються шляхи подальшого розвитку цих технологій для ефективного захисту інформації в майбутньому.

This scientific article explores the effectiveness of Data Loss Prevention (DLP) technologies in the context of modern challenges in information security. It analyzes the role of DLP technologies in addressing key threats to data security, such as cyber attacks, insider threats, and risks associated with distributed workspaces. Through practical examples and conclusions, this article reflects on the importance and potential of DLP technologies in the field of cybersecurity and recommends pathways for further development of these technologies for effective information protection in the future.

Актуальність. Останнім часом постійно зростає загроза для нашої особистої інформації в Інтернеті. Це стає серйозною проблемою, оскільки все більше даних зберігається та обробляється в цифровому форматі, отже, захист цих даних стає все важливішим. Технології, що допомагають забезпечити нашу інформацію від несанкціонованого доступу або витоку, стають надзвичайно актуальними.

Більше того, зусилля щодо запобігання втраті даних ускладнюються та стають більш вразливими через зростання використання мобільних пристроїв та хмарних сервісів на робочому місці. Забезпечити повний захист від втрати даних стає складніше, оскільки співробітники отримують доступ та обмінюються конфіденційною інформацією на різних платформах і пристроях. Ці проблеми посилилися зростанням організації віддаленої роботи після світових подій. Це відбувається тому, що тепер компаніям необхідно захищати дані, до яких здійснюється доступ з потенційно незахищених мереж та особистих пристроїв.

DLP-технології дуже важливі для компаній будь-якого розміру, фінансових установ, медичних організацій, урядових установ та освітніх закладів. DLP-технології дуже популярні в організаціях будь-якої сфери через зростання свідомості про кібербезпеку. Вони застосовуються для захисту конфіденційної інформації від витоку даних та забезпечення відповідності регуляторним вимогам.

Щоб запобігти випадкам втрати даних, було створено різні системи запобігання викрадення інформації. Різні продукти DLP можна придбати у кількох виробників, таких як Symantec, InfoWatch, Trend Micro та інші. Незважаючи на це, проблема запобігання витоку даних існує завжди, тому у цій роботі обговорюється поточний стан технологій DLP, сучасні виклики та майбутні напрямки розвитку технологій запобігання втраті даних.

Метою даної роботи є дослідження ефективності технологій запобігання втраті даних (DLP) у контексті сучасних викликів забезпечення безпеки інформації. Шляхом аналізу їх поточного стану, виявлення їхніх переваг та обмежень в сучасному цифровому середовищі.

Об'єктом дослідження є процес застосування технологій запобігання втраті даних (DLP) у контексті сучасних викликів забезпечення безпеки інформації.

Предметом дослідження є самі технології запобігання втраті даних (DLP) та їхня ефективність у вирішенні сучасних викликів безпеки інформації

Аналіз попередніх досліджень. Було проведено багато досліджень в галузі технологій запобігання втраті даних (DLP), включаючи Ніколь ван де Мейден, Річарда Стілінгса, Ребекку Херрон, Джона Лопеза та Джона Макдермотта, а також, найбільш відомі організації, які також проводили дослідження в цій області, а саме: Cisco, Symantec, Gartner, Forrester Research, IBM, McAfee.

Виклад основного матеріалу. Запобігання втраті даних (Data Loss Prevention) – це набір технологій та методик, які допомагають організаціям запобігти втраті, крадіжці або витоку конфіденційної інформації за межі організації. Рішення DLP призначені для виявлення, моніторингу та захисту конфіденційних даних від несанкціонованого доступу, розголошення або зміни. Вони зазвичай працюють шляхом сканування та аналізу даних в стані спокою, в роботі та в русі через різні канали, такі як електронна пошта, хмарне сховище, мережеві файлові сховища та кінцеві точки, для виявлення та запобігання витокам даних [1, 2].

DLP-технології можуть допомогти організаціям вирішити багато сучасних викликів у сфері захисту інформації. Основні функції DLP-систем показано на рисунку 1.

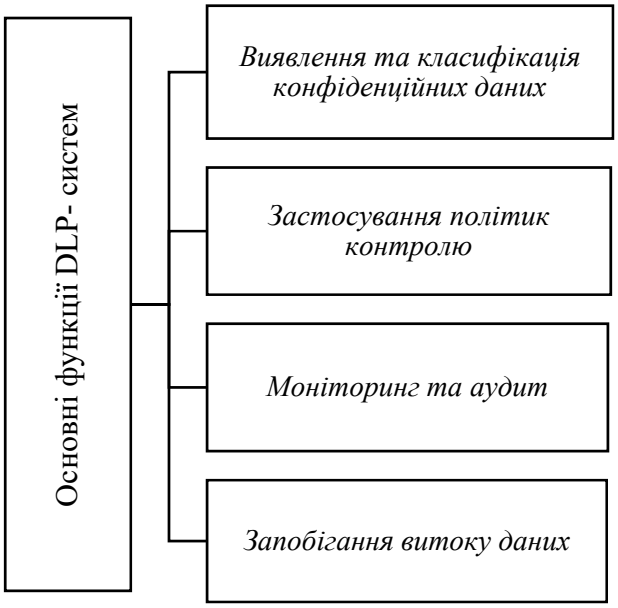


Рис. 1. Основні функції DLP-систем

Джерело: Розроблено автором

Озброєні набором потужних функцій, DLP-системи діють як охоронці конфіденційних даних. Вони сканують різноманітні формати, від документів до зображень, щоб знайти та класифікувати чутливу інформацію. Потім, ці системи застосовують політики контролю,

які обмежують, хто може отримувати доступ до даних, як їх можна використовувати та куди передавати. Більше того, DLP-системи постійно моніторять активність, генеруючи звіти для відстеження використання даних. І нарешті, вони можуть блокувати передачу даних, що порушують політику, ефективно запобігаючи витокам, захищаючи конфіденційну інформацію організації.

Організації зазвичай використовують DLP для наступних цілей.

1. *Захисту персональної інформації (PII) та дотримання відповідних правил*. DLP допомагає захищати конфіденційні дані, такі як імена, адреси, номера соціального страхування та номери кредитних карт, від втрати або витоку. Це також допомагає організаціям відповідати різним нормам конфіденційності даних, таким як GDPR, CCPA та HIPAA.

2. *Захисту інтелектуальної власності, критичної для організації*. Захист конфіденційної інформації, такої як торговельні секрети, формули та авторські права, від несанкціонованого доступу або витоку, що може запобігти конкурентній перевазі та фінансовим втратам.

3. *Досягнення видимості даних у великих організаціях.* DLP може допомогти організаціям визначити, де зберігаються конфіденційні дані, хто має до них доступ, і як вони використовуються.

4. *Захисту мобільних працівників та забезпечення безпеки в середовищах BYOD (Bring Your Own Device).* Захист конфіденційних даних на мобільних пристроях, таких як смартфонах і ноутбуках.

5. *Захисту даних на віддалених хмарних системах*. Захист конфіденційних даних, що зберігаються в хмарних сховищах, що може допомогти запобігти несанкціонованому доступу та витоку даних.

Приклад різних джерел, з яких можна запобігти втраті даних за допомогою DLP-технологій продемонстровано на рисунку 2.

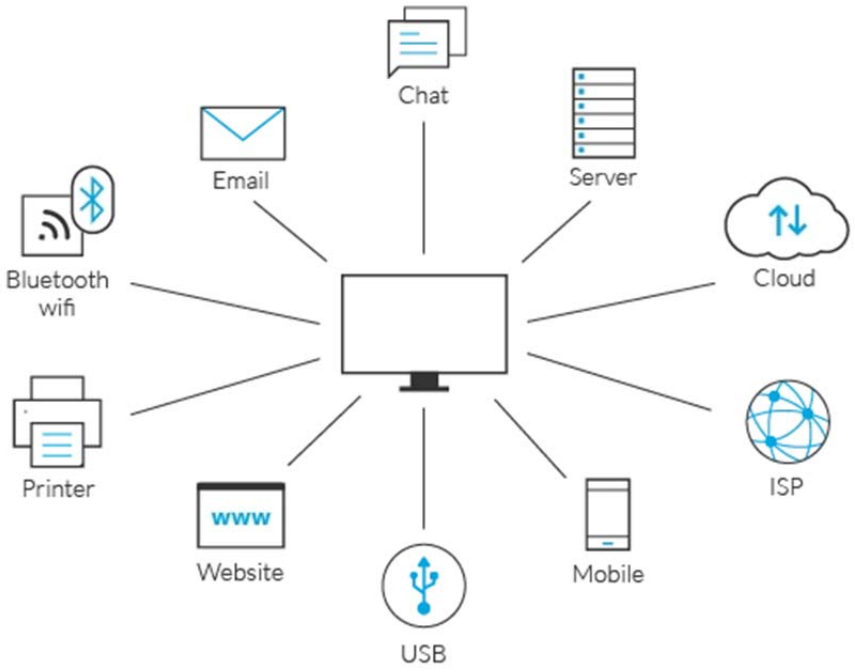


Рис. 2. Джерела запобігання втраті даних за допомогою DLP-технологій

Джерело:[3]

До провідних постачальників DLP-технологій належать наступні.

- *McAfee.* McAfee Data Loss Prevention (DLP) Suite пропонує широкий спектр функцій для захисту даних, включаючи фільтрування даних, шифрування даних, контроль доступу та моніторинг даних.

- *Symantec.* Symantec Data Loss Prevention (DLP) Suite пропонує схожий набір функцій, як і McAfee DLP Suite.
- *Cisco.* Cisco Cloud DLP пропонує хмарне DLP-рішення, яке може допомогти вам захистити ваші дані в хмарі (Рис. 3).
- ***IBM.*** IBM Data Loss Prevention (DLP) Suite пропонує потужне DLP-рішення, яке може відповідати потребам великих організацій.
- ***Intel Security.*** Intel Security McAfee Data Loss Prevention (DLP) Suite пропонує DLP-рішення, яке є частиною більшого набору продуктів безпеки Intel Security.

При визначенні постачальників DLP-технологій важливо дослідити та порівняти різні доступні рішення, щоб вибрати те, яке найкраще відповідає потребам та бюджету компанії.

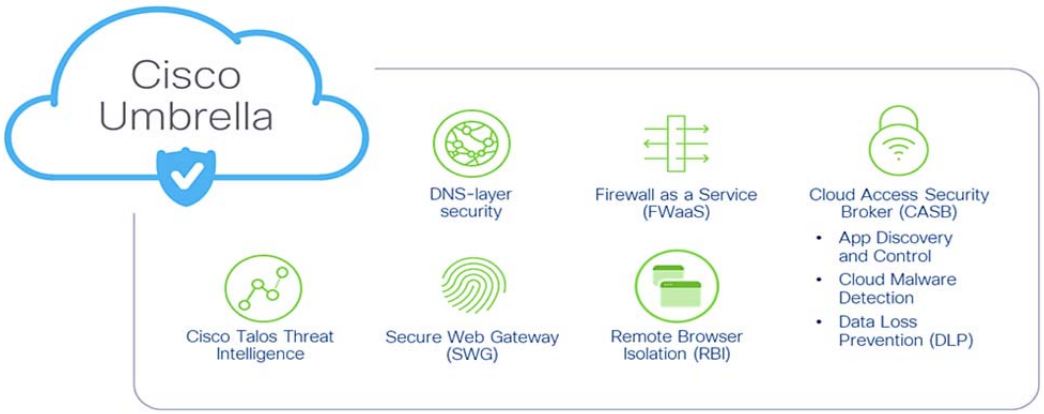


Рис. 3. Хмарне DLP-рішення Cisco Cloud

Джерело: [4]

У сучасному світі, де дані стають все більш цінними, захист конфіденційної інформації стає все більш важливим завданням. Організації стикаються з безліччю викликів у цій сфері, адже дані генеруються, обробляються та зберігаються у все більших обсягах та у все більш різноманітних форматах. Системи запобігання втраті даних (DLP) відіграють важливу роль у захисті конфіденційної інформації, але вони не позбавлені своїх недоліків.

Організації стикаються з безліччю викликів у сфері захисту інформації, які роблять DLP-технології ще більш актуальними. Серед основних викликів можна виділити наступні.

- *Зростання кібератак* – зловмисники постійно вдосконалюють свої методи, використовуючи все більш складні атаки для проникнення в інформаційні системи та крадіжки даних.
- *Внутрішні загрози* – не всі загрози для даних походять ззовні. Співробітники, які випадково або навмисно розголошують конфіденційну інформацію, можуть становити значний ризик.
- *Розподілені робочі місця* – зростання популярності віддаленої роботи та використання мобільних пристроїв ускладнює контроль над даними та їх захист.

Іншими, актуальними викликами, які необхідно вирішити сучасним системам DLP є наступні:

- Проблема шифрування та контролю доступу.
- Виклик соціальних мереж.
- Нові данні і налаштування.

Системи запобігання втраті даних (DLP) пройшли значний шлях з часів свого зародження, коли вони стикалися з численними обмеженнями в аналізі текстових даних. Завдяки вдосконаленню технологій та появі нових методів аналізу даних, DLP-системи стали значно потужнішими та ефективнішими. Сучасні DLP-системи використовують машинне навчання, яке дозволяє їм «навчатися» на великих обсягах даних та самостійно виявляти

закономірності. Це робить їх значно гнучкішими та адаптивними, адже вони можуть розпізнавати конфіденційну інформацію навіть у нетипових форматах або з незвичайним формулюванням.

Наприклад, відбитки пальців хешу, які використовувалися в ранніх DLP-системах, могли пропустити конфіденційну інформацію, якщо її можна було перефразувати або змінити формат. Також сучасні DLP-системи використовують методи природно-мовної обробки (NLP) для аналізу тексту на більш глибокому рівні. NLP дозволяє їм розуміти семантику та контекст мови, а також виявляти конфіденційну інформацію незалежно від її формулювання. Ранні DLP-системи працювали як автономні інструменти, не маючи зв'язку з іншими системами безпеки, проте, наразі вони інтегруються з іншими системами кібербезпеки, такими як брандмауери, системи запобігання вторгненням (IDS) та системи виявлення вторгнень (IPS). Це дозволяє їм отримувати ширший контекст про те, що відбувається в мережі, та більш ефективно реагувати на загрози. З поширенням хмарних технологій та мобільних пристроїв DLP-системи еволюціонували, щоб захищати конфіденційні дані незалежно від їх розташування [1].

Завдяки вдосконаленню методів аналізу даних та інтеграції з іншими системами безпеки, DLP-системи стали незамінними інструментами для захисту конфіденційної інформації.

Сучасні підприємства, як правило, накопичують значні обсяги даних у своїй IT-інфраструктурі. Однак, величезний обсяг збережених даних може спровокувати серйозний ризик втрати даних організацій, що ставить під загрозу конфіденційність та цілісність критичної інформації. Таким чином, впровадження надійної стратегії запобігання втраті даних є обов'язковим для мінімізації таких ризиків.

В таблиці 1 наведено приклади конкретних практик, які можна застосувати для підвищення безпеки IT-інфраструктури.

Таблиця 1

Характеристика практик для запобігання втрати даних

Визначення та класифікація даних за важливістю	**Шифрування для захисту файлів**	**Контроль доступу**	**Моніторинг доступу до даних**	**Навчання співробітників**
Визначення різних типів даних, якими користується організація, та їх категоризації за рівнем конфіденційності, цінності та потенційного впливу на організацію	Передбачає перетворення даних на код, який можна розшифрувати лише за допомогою ключа дешифрування	Облікові записи із захистом паролем та багатофакторна автентифікація, сканування відбитків пальців або токена	Ведення журналу спроб доступу та аналіз журналів системи; перегляд журналів активності	Виявлення фішингових електронних листів; уникання натискання на підозрілі посилання або вкладення; надійні паролі та багатофакторна автентифікація
Зниження ризику втрати чи крадіжки даних, підтримання конфіденційності приватної інформації та відповідності нормативним вимогам	Забезпечує додатковий рівень захисту для конфіденційної інформації, такої як фінансові записи, дані клієнтів та інша конфіденційна інформація компанії	Допомагає запобігти доступу до конфіденційних даних сторонніми особами, знизити ризик внутрішніх загроз та обмежити збитки, завдані витоком даних	Можливість швидко виявляти та реагувати на потенційні витоки даних, мінімізувати збитки, завдані витоком, і запобігати подальшому несанкціонованому доступу	Зниження ризику втрати або крадіжки даних через людську помилку

Джерело: Розроблено автором [2]

Забезпечивши належну інтеграцію цих п’ятьох компонентів, організації можуть отримати ефективний захист своїх цінних інформаційних активів та зменшити ризик правових та репутаційних наслідків. Окремо можна згадати про захист мобільних пристроїв: впровадження політики безпеки мобільних пристроїв, яка регулює використання мобільних пристроїв для доступу до даних компанії. Шифрувати потрібно дані, які зберігаються на мобільних пристроях в разі існування несанкціонованого доступу, а також варто використовувати мобільні VPN для безпечного підключення до корпоративної мережі.

Висновок. Для підприємств запобігання втраті даних є складною багатогранною проблемою, що потребує поєднання технологічних рішень, навчання користувачів і чіткої політики з процедурами. Ніхто не хоче, щоб виникали обставини, коли важливі дані втрачаються. Хакери та злодії даних стають все більш кваліфікованими, і щодня розробляються нові методи отримання доступу до мереж. Втрати даних можуть коштувати компаніям багато грошей у вигляді штрафів, поганої репутації та втрати клієнтів. У зв’язку з цим є критично важливим активно моніторити нові ризики.

Організації повинні посилити свої зусилля щодо запобігання втраті даних та захисту конфіденційної інформації в сучасному цифровому середовищі, долаючи перешкоди, створені динамічними кіберзагрозами, внутрішніми загрозами, тіньовою IT-інфраструктурою, шифруванням та нормативним регулюванням.

У світі, що дедалі більше залежить від даних, організації можуть знизити ризики, захистити свій бренд і зберегти довіру клієнтів та інших зацікавлених сторін, застосовуючи проактивний та комплексний підхід до запобігання втраті даних.

Крім того, компаніям необхідно стежити за новими технологічними розробками та відповідно змінювати свої плани захисту даних. Це означає бути в курсі нових вразливостей безпеки та кіберзагроз, а також інвестувати в постійне навчання та підвищення кваліфікації співробітників для розвитку культури обізнаності щодо кібербезпеки. Окрім цього, підприємствам слід регулярно переглядати та оновлювати свою політику та процедури запобігання втраті даних, щоб вони відповідали передовим галузевим практикам та регуляторним вимогам.

Отже, хоча запобігання втраті даних є серйозним викликом для сучасних підприємств, воно є критично важливим для захисту конфіденційної інформації та підтримки довіри в дедалі більш цифровізованому світі. Застосовуючи технологічні рішення, навчання співробітників та надійну політику, бізнес може ефективно пом’якшити ризики, пов’язані з втратою даних, та захистити свої цінні активи. Оскільки організаціям доводиться долати складність захисту даних, проактивний та комплексний підхід до запобігання втраті даних буде критичним для захисту безперервності бізнесу та репутації перед лицем мінливих кіберзагроз. DLP-системи постійно розвиваються, й в майбутньому вони стануть ще більш потужними та ефективними, адже будуть використовувати нові технології, такі як штучний інтелект та аналітика великих даних.

Список використаних джерел

1. CISCO. (2008). Data Leakage Worldwide: Common Risks and Mistakes Employees Make. Cisco white paper Public Information. – URL: http://surl.li/svvgk

2. Sortware. What Are The Best Practices for Data Loss Prevention (DLP) – URL: https://storware.eu/search/blog/dlp

3. What is DLP. – URL: https://www.imperva.com/learn/data-security/data-loss-prevention-dlp

4. Baumgartner T. Cisco Enhances Cloud DLP With Unified Management and More. – URL: https://umbrella.cisco.com/blog/cisco-enhances-cloud-dlp-with-unified-management-more

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т.В.

Наукове електронне видання

ПРОГРАМУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ

**Збірник наукових статей студентів,
які здобувають освітній ступінь «магістр»
за спеціальностями 121 «Інженерія програмного забезпечення», 125 «Кібербезпека та захист інформації»**

Частина 2

Видавець і виготовлювач
Державний торговельно-економічний університет
вул. Кіото, 19, м. Київ-156, Україна, 02156
Тел. (044) 513 74 18
Електронна пошта knute@knute.edu.ua
230Е-2024