Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____*інфокомунікацій*_____

Кафедра _____*інформаційно-мережної інженерії*_____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____*другий (магістерський)*_____

_____*Дослідження засобів безпеки в системах електронної комерції*_____
_____
(тема)

Виконав:
здобувач __2__ року навчання,
групи _*ІМІм-24-1*_____
_____*Данило Рудак*_____
(власне ім'я, прізвище)

Спеціальність_____*172 Електронні комунікації та радіотехніка*_____
(код і повна назва спеціальності)
Тип програми _____*освітньо-наукова*_____
(освітньо-професійна або освітньо-наукова)
Освітня програма_____*Інформаційно-мережна інженерія*_____
(повна назва освітньої програми)

Керівник _____*доц. к.т.н. Дарія Чеботарьова*_____
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ІМІ _____ _____*Микола Москалець*_____
(підпис) (власне ім'я, прізвище)

2025 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ *Данило Рудак*
(підпис) (власне ім'я, прізвище)

Керівник _____ *Дарія Чеботарьова*
(підпис) (власне ім'я, прізвище)

Харківський національний університет радіоелектроніки

Факультет *інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Електронні комунікації та радіотехніка*
(код і повна назва)

Тип програми *Освітньо-наукова*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри ІМІ_____
(підпис)

"*25*" *грудня* 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Рудаку Данилу Сергійовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження засобів безпеки в системах електронної комерції*

затверджена наказом університету від "*24*" *жовтня* 2025 р. № *959 Ст*

2. Термін подання здобувачем роботи до екзаменаційної комісії *20 грудня 2025 р.*

3. Вихідні дані до роботи *дослідити особливості систем електронної комерції, проаналізувати основні типи загроз в електронній комерції; дослідити засоби безпеки та механізми захисту в СЕК; розглянути та проаналізувати випадок реального зовнішнього втручання в СЕК, запропонувати на основі виконаного аналізу власні рекомендації щодо забезпечення безпеки СЕК.*

4. Перелік питань, що потрібно опрацювати в роботі

1. Основи електронної комерції

2. Основні загрози та вразливості в СЕК

3. Аналіз засобів безпеки в СЕК

4. Аналіз реального інцеденту та рекомендації щодо захисту СЕК

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____

Слайди у форматі Power Point (назва, мета та задачі роботи, типи електронної комерції,структура та компоненти СЕК, класифікація загроз в СЕК, внутрішні загрози, організаційні загрози, технічні загрози, засоби безпеки СЕК, аналіз реального інциденту, рекомендації щодо підвищення безпеки в СЕК , висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / термін виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*27.10.25*	*Виконано*
2	*Підбір літератури за темою роботи.*	*28.10 - 04.11.25*	*Виконано*
3	*Виконання розділу 1*	*05.11 - 14.11.25*	*Виконано*
4	*Виконання розділу 2*	*15.11 – 24.11.25*	*Виконано*
5	*Виконання розділу 3*	*25.11 – 04.12.25*	*Виконано*
6	*Виконання розділу 4*	*05.12 - 14.12.25*	*Виконано*
7	*Оформлення пояснювальної записки,*		
	презентаційного матеріалу та підготовка		
	до захисту у ЕК	*15.12 - 20.12.25*	*Виконано*

Дата видачі завдання *27 жовтня 2025 р.*

Здобувач _____
(підпис)

Керівник роботи _____ *доц. Дарія Чеботарьова*
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 100 с., 32 рис., 2 табл., 48 джерел, 2 додатки

Об'єкт дослідження – засоби безпеки в системах електронної комерції.

Мета роботи – дослідження загроз та засобів безпеки в системах електронної комерції.

Результати – в роботі розглянуто особливості систем електронної комерції; проаналізовано основні типи загроз в електронній комерції, зокрема соціальні, технічні та організаційні; досліджено засоби безпеки та механізми захисту в СЕК від різних видів загроз; розглянуто загрози від штучного інтелекта; виконано порівняння основних протоколів безпеки та порівняння програмних та апартних засобів безпеки в СЕК; проаналізовно випадок реального зовнішнього втручання в СЕК та на основі виконаного аналізу запропонувано власні рекомендації щодо забезпечення безпеки СЕК.

ЕЛЕКТРОННА КОМЕРЦІЯ, СЕК, БЕЗПЕКА, ЗАГРОЗА, АТАКА, ІНФОРМАЦІЯ, ЗАХИСТ, ШТУЧНИЙ ІНТЕЛЕКТ, ПРИНЦИП НУЛЬОВОЇ ДОВІРИ, ЗАСІБ БЕЗПЕКИ.

THE ABSTRACT

Explanatory note: 100 p., 32 fig., 2 tabl., 48 sources, 2 app.

Object of research - security measures in e-commerce systems.

The purpose of the work is to research into threats and security measures in e-commerce systems.

Results - the work examines the features of e-commerce systems; analyzes the main types of threats in e-commerce, including social, technical, and organizational ones; investigates security tools and protection mechanisms in SEC against various types of threats; examines threats from artificial intelligence; compares basic security protocols and compares software and hardware security tools in SEC; analyzes a case of real external interference in SEC and, based on the analysis, offers its own recommendations for ensuring SEC security.

ELECTRONIC COMMERCE, SECURITY, THREAT, ATTACK, INFORMATION, PROTECTION, ARTIFICIAL INTELLIGENCE, ZERO TRUST PRINCIPLE, SECURITY MEANS.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

ЕК – електронна комерція;

ПЗ – програмне забезпечення;

СЕК – система електронної комерції;

ШІ – штучний інтелект;

B2B (business-to-business) – бізнес-модель бізнес до бізнеса;

B2C (business-to-customer) – бізнес-модель бізнес до споживача;

CA (Certification Authority) – центр сертифікації;

CDM (Continuous Diagnostics and Mitigation) – безперервна діагностика та пом'якшення наслідків;

CRM (Customer Relationship Management) – технологія управління взаємовідносинами з клієнтами;

DPI (Deep Packet Inspection) – глибока перевірка пакетів;

E2E (exchange-to-exchange) – бізнес-модель біржа до біржі;

G2C (government-to-citizens) – бізнес-модель уряд до громадянина;

HSM (Hardware Security Module) – апаратні модулі безпеки

IPS (Intrusion Prevention System) – система запобігання вторгненням;

IPsec (Internet Protocol Security) – протокол безпеки інтернету;

LLM (Large Language Model) – велика мовна модель;

MITM (Man-in-the-Middle) – атака людина посередині;

NGFW (Next-Generation Firewall) – брандмауер нового покоління;

OWASP (Open Worldwide Application Security Project) – відкритий всесвітній проект безпеки додатків;

PKI (Public Key Infrastructure) – інфраструктура відкритих ключів;

SIEM (Security information and event management) – система управління подіями безпеки;

SQLi (Structured Query Language injection) – атака на бази даних;

SSH (Secure Shell) – протокол безпечного віддаленого керування комп'ютерами;

TLS (Transport Layer Security) – протокол безпеки транспортного рівня;

WAF (Web Application Firewall) – засоби захисту вебдодатків

XSS (Cross Site Scripting) – атака міжсайтового скриптингу;

C2C (customer-to-customer) – бізнес-модель споживач до споживача.

ВСТУП

Сучасний розвиток електронної комерції зумовлює необхідність забезпечення високого рівня інформаційної безпеки під час здійснення онлайн-операцій. Безпека електронної комерції є частиною проблем веббезпеки, що виникають у всіх інформаційних системах бізнесу в інтернеті. Секретність, цілісність та доступність в безпеці електронної комерції зосереджені на захисті активів споживача та системи електронної комерції від несанкціонованого доступу, використання, зміни або знищення [1].

Зростання кількості кібератак, фішингових схем, витоків персональних даних та шахрайських дій створює серйозні загрози як для бізнесу, так і для споживачів. Зі зростанням обсягів електронної комерції збільшується і кількість кібератак, шахрайства, фінансових втрат та витоків даних [2]. Дослідження засобів безпеки в системах електронної комерції (СЕК) є надзвичайно актуальним напрямом у сфері інформаційних технологій. Саме тому кваліфікаційна робота присвячена цим питанням є актуальною.

Метою кваліфікаційної роботи є аналіз сучасних засобів і технологій захисту даних у системах електронної комерції, а також розробка рекомендацій щодо підвищення рівня безпеки транзакцій і збереження конфіденційності користувачів.

Для досягнення мети поставлено такі завдання:

– дослідити особливості систем електронної комерції,

– проаналізувати основні типи загроз в електронній комерції;

– дослідити засоби безпеки та механізми захисту в СЕК;

– розглянути та проаналізувати випадок реального зовнішнього втручання в СЕК,

– запропонувати на основі виконаного аналізу власні рекомендації щодо забезпечення безпеки СЕК.

1 ОСНОВИ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Електронна комерція (ЕК) – це ділова активність з купівлі-продажу товарів та послуг, що передбачає взаємодію сторін на основі інформаційних мереж (без безпосереднього фізичного контакту). Останнім часом ЕК охоплює й інформаційну взаємодію партнерів в мережах з приводу купівлі-продажу [3].

1.1 Типи електронної комерції

Сьогодні існують наступні типи електронної комерції (рис. 1.1):

– C2C (customer-to-customer);
– B2B (business-to-business);
– B2C (business-to-customer);
– E2E (exchange-to-exchange).
– G2C (government-to-citizens).

Рисунок 1.1 – Типи електронної комерції

C2C (Consumer-to-Consumer) – це бізнес-модель (споживач-споживач), за якою споживачі зв'язуються з іншими споживачами, зазвичай на вебсайті, з метою продажу та купівлі товарів чи послуг один у одного. Приклади бізнесів C2C: OLX, eBay, Discogs, Depop, Airbnb, Etsy тощо.

B2B (Business-to-Business) – це бізнес-модель (бізнес-бізнес), за якою компанії продають продукти та послуги іншим підприємствам, а не безпосередньо споживачам. Це стосується комерційних операцій, що відбуваються між двома підприємствами, на відміну від бізнесу та окремого споживача. У моделі B2B одна компанія продає товари та послуги або інформацію іншій компанії, якій вони потрібні для її діяльності, виробництва або перепродажу.

B2C (Business-to-Consumer) – це бізнес-модель «бізнес-споживач» (B2C) – це поширена форма комерції, де підприємства продають товари чи послуги безпосередньо окремим особам. Ця структура лежить в основі повсякденних транзакцій – від купівлі продуктів до онлайн-шопінгу.

E2E (Exchange-to-Exchange) – це бізнес-модель (біржа-біржа). E2E позначає обмін інформацією або угодами між вебсайтами, що виступають в якості бірж або брокерів для обміну товарами і послугами між компаніями.

G2C (Government-to-Citizens) – це бізнес-модель «уряд-громадянин». До G2C відносяться: надання та отримання державних послуг та необхідної державної інформації, сплата податків, комунальних послуг, ліцензій тощо [4].

1.2 Структура системи електронної комерції

Система електронної комерції – це інформаційна система, в якій організаційною та технологічною основою є вебсайт.

Структура СЕК показана на рис. 1.2, а її ключові компоненти – на рис.1.3.

В рамках ЕК постійно відбувається взаємодія між 4 основними суб'єктами ЕК – фінансових установ, бізнес-організацій, клієнтів та держави.

Бізнес-організації	це будь-яке підприємство, яке здійснює повністю або частково свою фінансову діяльність за допомогою інформаційних мереж, тобто займається електронною комерією
Фінансові установи	це організації, які надають послуги, пов'язані з пересування фінансових потоків, у першу чергу - це банки та пов'язані з ними системи електронних платежів
Клієнти	це споживачі товарів або послуг, які вони можуть придбати
Держава	визначає правила ведення електронного бізнесу, та здійснює загальне регулювання цього процесу

Рисунок 1.2 – Структура СЕК

Рисунок 1.3 – Ключові компоненти сучасної системи ЕК

Фінансові установи – це організації, що надають фінансові послуги (наприклад банки). Бізнес-організації – це різні підприємства, що здійснюють комерційну діяльність за допомогою інформаційних мереж. Клієнти – це споживачі товарів або послуг. Держава визначає та регулює всі правила організації та експлуатації електронного бізнесу [3, 5].

До ключових компонент сучасної системи ЕК відносяться:

– фронтенд – це вебінтерфейс або мобільний додаток, через який користувач взаємодіє із системою (перегляд товарів, кошик, оформлення замовлення);

– бекенд – це серверна логіка, яка обробляє запити клієнтів, забезпечує бізнес логіку, авторизацію, роботу з базою даних;

– база даних (БД) – це зберігає інформацію про товари, замовлення, клієнтів, платежі;

– платіжні шлюзи – це інтерфейси для обробки платіжних операцій (інтеграції з банківськими сервісами та процесорами);

– API та інтеграції необхідні для зв’язку з ERP, CRM, системами логістики, аналітики;

– інфраструктурні елементи – це балансувальники навантаження, CDN, системи кешування, сховища об’єктів.

2 ОСНОВИ ЗАГРОЗИ ТА ВРАЗЛИВОСТІ СЕК

Загрози в системах електронної комерції поділяють на технічні, організаційні та соціальні, що показано на рис. 2.1.

Рисунок 2.1 – Класифікація загроз в СЕК

2.1 Соціальні загрози в СЕК

2.1.1 Фішинг

Фішинг – це тип кібератак, під час яких використовуються шахрайські електронні листи, текстові повідомлення, телефонні дзвінки або вебсайти, щоб обманом змусити людей поділитися конфіденційними даними, завантажити

шкідливе програмне забезпечення або іншим чином наразити себе на кіберзлочинність.

Фішингові атаки – це форма соціальної інженерії. На відміну від інших кібератак, які безпосередньо спрямовані на мережі та ресурси, атаки соціальної інженерії використовують людські помилки, фальшиві історії та тактику тиску, щоб маніпулювати жертвами, змушуючи їх ненавмисно завдавати шкоди собі або своїм організаціям.

У типовій фішинговій афері хакер видає себе за когось, кому жертва довіряє, наприклад, колегу, начальника, авторитетну особу або представника відомого бренду. Хакер надсилає жертві повідомлення з проханням оплатити рахунок, відкрити вкладення, натиснути посилання або виконати якусь іншу дію [6].

Сьогодні фішингові атаки здійснюються через різні канали: електронну пошту, телефонні дзвінки, месенджери, SMS-повідомлення, фішингові посилання, QR-коди тощо.

Запобігання фішингу та зменшення його впливу є складною задачею. Жоден засіб безпеки не дає 100%-ої гарантії від фішингу, але в комплексному використанні різних технічних рішень ризики суттєво зменшуються [7]. Схему сукупності технічних рішень для протистояння фішингу наведено на рис. 2.2.

Оскільки фішингові шахрайства спрямовані на людей, співробітники часто є першою та останньою лінією захисту організації від цих атак. Організації можуть навчити користувачів розпізнавати ознаки спроб фішингу та реагувати на підозрілі електронні листи та текстові повідомлення. Це може включати надання співробітникам простих способів повідомляти про спроби фішингу ІТ-відділу або команді безпеки.

Організації також можуть встановлювати політики та практики, які ускладнюють успіх фішерів.

Для захисту від фішингу необхідно впроваджувати культуру безпеки. Культура безпеки передбачає використання спеціальних освітніх програм, обмеження доступу, періодичні штучні фітингові атаки для оцінки готовності

персоналу, постійний моніторинг і швидка реакція на інциденти, а також культура здорового сумніву [6].

Рисунок 2.2 – Схема сукупності технічних рішень для протистояння фішингу

Організації можуть доповнити навчання співробітників та політики компанії інструментами безпеки, які допомагають виявляти фішингові повідомлення та перешкоджати хакерам, які використовують фішинг для злому мереж:

– фільтри спаму та програмне забезпечення для захисту електронної пошти,

– антивірусне програмне забезпечення,

– багатофакторна автентифікація,

– інструменти безпеки кінцевих точок,

– вебфільтри,

– рішення для корпоративної кібербезпеки тощо.

2.1.2 Соціальна інженерія

Соціальна інженерія або інженерія соціальних взаємодій у 2025 році визнана однією з найсерйозніших загроз безпеці, оскільки вона спрямована на найслабшу ланку будь-якої системи – людський фактор. Замість злому складного програмного коду, зловмисники маніпулюють психологією людей, щоб отримати доступ до конфіденційних даних або ресурсів.

Станом на 2025 рік соціальна інженерія є основним вектором початкового доступу до мереж (близько 36% усіх інцидентів). Приблизно 98% кібератак тією чи іншою мірою використовують ці методи. [8]

Зловмисники активно використовують генеративний ШІ для створення дипфейків (аудіо та відео) та максимально персоналізованих фішингових листів. Більшість людей досі не можуть розпізнати фішингову атаку, написану штучним інтелектом [9].

У 2025 році атаки соціальної інженерії складають понад 40% усіх інцидентів у сфері криптовалют. Середня вартість компрометації ділової пошти може сягати мільйонів доларів [10].

Основні методи атак у 2025 році:

– смішинг та вішинг (шахрайство через SMS та телефонні дзвінки, що часто імітують банківські служби або техпідтримку) [8];

– претекстинг (використання вигаданої історії або приводу, щоб завоювати довіру жертви та обманом або маніпулювати нею, щоб вона поділилась конфіденційною інформацією, завантажила шкідливе програмне забезпечення, надсилала гроші злочинцям або іншим чином завдала шкоди собі чи організації, в якій вона працює [11]);

– ClickFix та фальшиві CAPTCHA (атаки, що змушують користувачів копіювати шкідливий код у командний рядок під виглядом виправлення помилки браузера) [12].

2.1.3 Внутрішні загрози

Внутрішні загрози в системах електронної комерції становлять одну з найнебезпечніших категорій ризиків інформаційної безпеки, оскільки їх джерелом є користувачі, які вже мають легітимний доступ до системи. До таких суб’єктів належать співробітники компанії, адміністратори, менеджери, а також підрядники чи партнери, що взаємодіють із СЕК на постійній основі; зловмисні внутрішні дії або випадкові помилки можуть спричиняти серйозні порушення безпеки та втрати даних. Ці загрози особливо складні для виявлення, оскільки дії «інсайдерів» часто виглядають як звичайна користувацька активність у системі**.** За даними досліджень, внутрішні загрози залишаються однією з головних проблем безпеки в організаціях – у 2025 році їх частота і вплив залишаються високими: 83% організацій повідомили про принаймні одну інцидентну внутрішню загрозу протягом року, що підкреслює важливість врахування цієї категорії ризиків у стратегіях оборони [13]. Основні типи внутрішніх загроз у СЕК наведено на рис. 2.3.

Рисунок 2.3 – Основні типи внутрішніх загроз у СЕК

Зловмисні внутрішні загрози – це тип загроз пов’язаний із навмисними діями співробітників або довірених осіб, які мають авторизований доступ до системи та використовують його для заподіяння шкоди організації чи крадіжки інформації. Зловмисник-інсайдер може викрадати дані, саботувати сервіси або передавати конфіденційну інформацію третім особам з метою особистої вигоди чи шкоди бізнесу. Дія таких осіб може включати проникнення до критичних систем або маніпуляції бізнес-процесами [14].

Ненавмисні внутрішні загрози виникають через людські помилки або недбалість: працівники можуть використовувати слабкі паролі, помилково завантажувати шкідливі файли, переходити за фішинговими посиланнями або неправильно налаштовувати доступи в СЕК. Часто ці дії не мають злого наміру, але все одно призводять до витоків даних або порушення безпеки [15].

Скомпрометовані облікові записи – це критичний тип внутрішньої загрози, коли облікові дані співробітника або адміністратора стають доступними зловмисникам (наприклад, через соціальну інженерію). Тоді атака формально виглядає як внутрішня, оскільки здійснюється через легітимний акаунт із правами доступу. У СЕК такі облікові записи можуть мати доступ до систем управління замовленнями, платіжних шлюзів, CRM-систем і баз персональних даних, що робить цей вид загроз надзвичайно небезпечним [16].

Внутрішні загрози можуть призводити до значних негативних наслідків (рис. 2.4):

Рисунок 2.4 – Наслідки внутрішніх загроз для СЕК

У сучасних системах електронної комерції внутрішні загрози є не менш небезпечними аніж зовнішні атаки зловмисників. Людський фактор є одним з ключових елементів ризику у СЕК , тому поєднання організаційних заходів та постійного контролю та моніторингу як втручань зовнішніх, так і контролю всередині є одним з найголовніших елементів безпеки кожної СЕК.

2.2 Організаційні загрози в СЕК

Організаційні загрози виникають не лише через технічні вразливості, а і через недоліки в управлінні, нормативах та процесах. До таких загроз належать слабкі паролі, відсутність політик безпеки, проблеми з контролем доступу та відсутність належних процедур резервного копіювання.

Для попередження організаційних загроз необхідно вживати певні заходи безпеки (рис. 2.5).

Рисунок 2.5 – Дії для зниження ризиків

2.2.1 Відсутність політик безпеки

Політики безпеки – це офіційні документи, що визначають порядок захисту інформації, ролі відповідальних осіб, правила доступу, реагування на інциденти та інші вимоги до безпеки даних. Їх відсутність означає, що співробітники діють як хто хоче, що значно підвищує ризик несанкціонованих дій, помилок і витоку даних. Політики безпеки включають правила з управління паролями, доступом, резервним копіюванням та інші техніки захисту.

2.2.2 Недостатній контроль доступу

Контроль доступу визначає, хто саме має доступ до яких даних і ресурсів. Недостатній контроль призводить до того, що співробітники можуть переглядати або змінювати інформацію, до якої вони не повинні мати доступ, що створює великий ризик несанкціонованого доступу та потенційних внутрішніх загроз. Якісний контроль доступу є одним з основних елементів політики інформаційної безпеки.

2.2.3 Відсутність резервного копіювання

Регулярне резервне копіювання забезпечує можливість відновлення даних і безперервної роботи системи після збоїв або атак (наприклад, вірусів-шифрувальників). Без резервних копій дані можуть бути безповоротно втрачені, що може зупинити роботу бізнесу та завдати серйозних фінансових збитків.

Створення, використання, підтримка, тестування, відповідні перевірки процедури резервного копіювання, а також відновлення систем та захисту резервних копій рекомендується наказом [17].

2.2.4 Слабкі паролі

Слабкі або типові паролі – це одна з найпоширеніших причин успішних зламів. Якщо користувачі використовують прості або повторювані паролі у багатьох системах, зловмисники можуть легко здобути доступ до облікових записів і систем. Через це важливо впроваджувати політики складних паролів, зберігання їх у безпечних менеджерах парольної інформації та періодичну зміну паролів [17].

2.3 Технічні загрози в СЕК

2.3.1 Експлуатація вразливостей вебдодатків

Результатом використання вразливостей вебдодатків можуть бути SQL-ін’єкції, міжсайтовий скриптинг XSS та інші атаки.

Атака міжсайтового скриптингу (XSS) – це атака, за якої зловмисник може змусити цільовий сайт виконувати шкідливий код так, ніби він є частиною вебсайту. XSS ін’єкції – одна з найбільш широкорозповсюджених проблем, що трапляється в багатьох застосунках. XSS полягає в тому, що зловмисник додає на сторінку JavaScript-код та отримує доступ до керування вебсторінкою застосунку. Цей код буде виконуватися щоразу, коли користувачі заходитимуть на сторінку застосунку, де цей код додав зловмисник [18].

Збережені XSS-атаки становлять серйозну небезпеку, оскільки вони непомітно використовують довіру користувачів, виконуючи шкідливі скрипти безпосередньо в браузері користувача – часто без будь-яких видимих ознак компрометації. На відміну від інших атак, які вимагають переходу за підозрілими посиланнями, жертвам достатньо відвідати легітимну, скомпрометовану сторінку, щоб стати жертвою.

Зловмисники часто використовують збережені XSS-атаки для крадіжки конфіденційних даних користувачів, таких як файли cookie сеансу, паролі або

особисті дані, що потенційно призводить до повного захоплення облікового запису. В екстремальних сценаріях, особливо з користувачами з високими привілеями, такими як адміністратори, зловмисники можуть отримати доступ високого рівня та скомпрометувати цілі системи [19].

Зловмисники також можуть використовувати ці скрипти для перенаправлення жертв на шахрайські вебсайти. Там вони можуть спонукати користувачів встановлювати шкідливе програмне забезпечення або навіть виконувати несанкціоновані дії від імені жертви, що значно посилює наслідки.

Веббраузер завантажує код з багатьох різних вебсайтів і запускає його на комп'ютері користувача. Деякі з цих вебсайтів будуть дуже надійними, і користувач може використовувати їх для конфіденційних операцій, таких як фінансові операції або медичні поради. З іншими сайтами користувач може не мати таких довірчих відносин. Основою моделі безпеки браузера є те, що ці сайти повинні бути відокремлені один від одного, тому код з одного сайту не повинен мати доступу до об'єктів або облікових даних на іншому сайті. Це називається політикою того ж походження [20].

В успішній XSS-атаці зловмисник може підірвати політику, обманом змусивши цільовий сайт виконати шкідливий код у власному контексті, ніби він має одне й те саме походження (рис. 2.6).

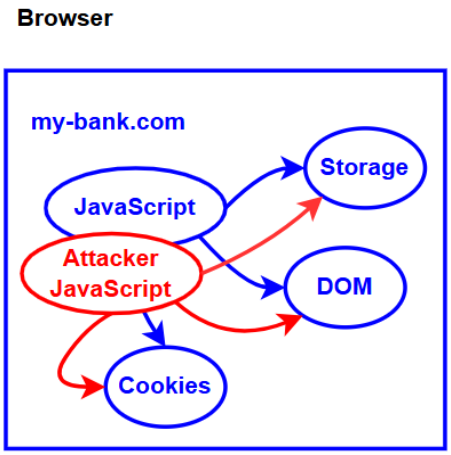

Рисунок 2.6 – Схематичний приклад успішної XSS атаки

Код потім може виконувати будь-які дії власного коду сайту. Наприклад: отримувати доступ до всього вмісту завантажених сторінок сайту та будь-якого вмісту в локальному сховищі, а також змінювати його, або здійснювати HTTP-запити з використанням облікових даних користувача, що дозволить йому видавати себе за нього або отримувати доступ до конфіденційних даних (рис. 2.6).

Розглянемо детально приклад атаки впровадження коду в браузер.

Наприклад, вебсайт банку користувача – my-bank.example.com. Користувач увійшов на нього, і код на вебсайті може отримати доступ до даних його рахунку та виконувати транзакції. Вебсайт хоче відобразити вітальне повідомлення, персоналізоване для поточного користувача. Він відображає вітальне повідомлення в елементі заголовка (рис. 2.7).

HTML

```
<h1 id="welcome"></h1>
```

Рисунок 2.7 – Вітальне повідомлення в елементі заголовка

Сторінка очікує знайти ім'я поточного користувача в параметрі URL-адреси. Вона витягує значення параметра та використовує його для створення персоналізованого вітального повідомлення (рис. 2.8).

Припустимо, що ця сторінка обслуговується з https://my-bank.example.com/welcome. Щоб скористатися цією вразливістю, зловмисник надсилає користувачеві таке посилання (рис. 2.9).

Коли користувач натискає на посилання браузер завантажує сторінку. Сторінка витягує параметр URL-адреси з назвою user, значення якого дорівнює <img src=x onerror=alert("hello!")>. Потім сторінка присвоює це значення властивості welcomeелемента innerHTML, що створює новий <img>елемент зі

srcзначенням атрибута x. Оскільки src значення генерує помилку, виконується onerror властивість обробника подій, і зловмисник отримує можливість запустити його код на сторінці.

JS

```
const params = new URLSearchParams(window.location.search);
const user = params.get("user");
const welcome = document.querySelector("#welcome");

welcome.innerHTML = `Welcome back, ${user}!`;
```

Рисунок 2.8 – Персоналізоване вітальне повідомлення

HTML

```
<a
  href="https://my-bank.example.com/welcome?user=<img src=x
onerror=alert('hello!')>">
  Get a free kitten!</a
>
```

Рисунок 2.9 – Посилання зловмисника

У цьому випадку код просто відображає сповіщення, але на реальному банківському вебсайті код зловмисника зможе робити все, що й власний фронтенд-код банку.

Розглянемо детально приклад атаки впровадження коду на сервер.

У цьому прикладі розглянемо вебсайт із функцією пошуку. HTML-код сторінки пошуку може виглядати так, як показано на рис. 2.10.

HTML

```html
<h1>Search</h1>

<form action="/results">
  <label for="mySearch">Search for an item:</label>
  <input id="mySearch" type="search" name="search" />
  <input type="submit" />
</form>
```

Рисунок 2.10 – HTML-код сторінки пошуку

Коли користувач вводить пошуковий термін і натискає кнопку «Надіслати», браузер надсилає GET-запит до «/results», включаючи пошуковий термін як параметр URL-адреси: https://example.org/results?search=bananas.

Сервер хоче відобразити список результатів пошуку із заголовком, який вказує на те, що шукав користувач. Він витягує пошуковий термін з параметра URL-адреси. На рис.2.11 показано як це може виглядати в Express.

JS Copy

```js
app.get("/results", (req, res) => {
  const searchQuery = req.query.search;
  const results = getResults(searchQuery); // Implementation not shown
  res.send(`
   <h1>You searched for ${searchQuery}</h1>
   <p>Here are the results: ${results}</p>`);
});
```

Рисунок 2.11 – Результати пошуку

Щоб скористатися цією вразливістю, зловмисник надсилає користувачеві таке посилання, як на рис. 2.12.

HTML

```
<a href="http://example.org/results?search=<img src=x
onerror=alert('hello')">
  Get a free kitten!</a
>
```

Рисунок 2.12 – Посилання зловмисника

Коли користувач натискає на посилання, браузер надсилає GET-запит на сервер. Параметр URL-адреси запиту містить шкідливий код. Сервер витягує значення параметра URL-адреси та вбудовує його на сторінку. Сервер повертає сторінку браузеру, який її запускає.

Як і всі XSS-атаки, ці два приклади можливі, оскільки вебсайт використовує вхідні дані, які міг би бути створені зловмисником, та включає вхідні дані на сторінку без їх очищення. В обох цих прикладах використовується один і той самий вектор для шкідливого введення: параметр URL-адреси. Однак є й інші вектори, які можуть використовувати зловмисники.

Наприклад, розглянемо блог із коментарями. У такому випадку вебсайт: дозволяє будь-кому надсилати коментарі за допомогою <form>елемента, зберігає коментарі в базі даних та включає коментарі на сторінках, які вебсайт надає іншим користувачам.

Якщо коментарі не очищені, то вони є потенційними векторами XSS. Такий вид атаки іноді називають збереженим або постійним XSS і є особливо серйозним, оскільки заражений контент буде надаватися всім користувачам, які

отримують доступ до сторінки, щоразу, коли вони отримують до неї доступ [20].

Головна відмінність між двома прикладами полягає в тому, що шкідливий код впроваджується в різні частини кодової бази вебсайту, і це відображає архітектуру кожного вебсайту.

Вебсайт, який використовує рендеринг на стороні клієнта, такий як односторінковий додаток, змінює сторінки у браузері, використовуючи веб-API document.createElement() для цього, безпосередньо або опосередковано через фреймворк, такий як React. Саме в ході цього процесу відбувається XSS-ін'єкція. Саме це відбувається в першому прикладі: шкідливий код вводиться в браузер скриптом, що працює на сторінці, який призначає значення параметра URL-адреси властивості Element.innerHTML, яка інтерпретує його значення як HTML-код.

Вебсайт, який використовує рендеринг на стороні сервера, створює сторінки на сервері, використовуючи фреймворк, такий як Django або Express, найчастіше шляхом вставки значень у шаблони сторінок. XSS-ін'єкція, якщо вона відбувається, відбуватиметься на сервері під час процесу створення шаблону. Саме це відбувається у другому прикладі: код вводиться на сервер, коли код Express вставляє значення параметра URL-адреси в документ, який він повертає. Код XSS-атаки потім виконується, коли браузер оцінює сторінку.

В обох випадках загальний підхід до захисту однаковий, і ми детально розглянемо це в наступному розділі. Однак конкретні інструменти та API, які ви використовуватимете, будуть різними [20].

В наш час XSS дуже актуальні, особливо у сферах електронної комерції, транспорту та фінансів. XSS є популярними оскільки багато сайтів та вебдодатків досі все ще не мають надійного захисту від впровадження скриптів.

SQL-ін'єкція (SQLi) – це вразливість веб-безпеки, яка дозволяє зловмиснику втручатися в запити, які програма робить до своєї бази даних. Це може дозволити зловмиснику переглядати дані, які він зазвичай не може отримати. Це може включати дані, що належать іншим користувачам, або будь-

які інші дані, до яких програма має доступ. У багатьох випадках зловмисник може змінити або видалити ці дані, що призведе до постійних змін у вмісті або поведінці програми.

У деяких ситуаціях зловмисник може ескалувати атаку SQL-ін'єкції, щоб скомпрометувати базовий сервер або іншу серверну інфраструктуру. Це також може дозволити йому виконувати атаки типу «відмова в обслуговуванні» [21].

Успішна атака SQL-ін'єкцією може призвести до несанкціонованого доступу до конфіденційних даних, таких як паролі, дані кредитної картки, персональна інформація користувача тощо.

Існує багато вразливостей, атак та методів SQL-ін'єкцій, які виникають у різних ситуаціях. Деякі поширені приклади SQL-ін'єкцій включають:

– отримання прихованих даних, де можна змінити SQL-запит для повернення додаткових результатів;

– підрив логіки застосунку, коли можна змінити запит, щоб втрутитися в логіку за стосунку;

– атаки UNION, за допомогою яких можна отримувати дані з різних таблиць бази даних;

– сліпа SQL-ін'єкція, коли результати керованого запиту, не повертаються у відповідях застосунку [21].

Розглянемо приклад SQL ін’єцкції, що ілюструє код для отримання імені користувача та пароля.

Надані користувачем дані створюють SQL-запит для виконання в базі даних. База даних містить таблицю з надписом «користувач» зі стовпцями для імені та пароля (рис.2.13).

Розглянемо користувача, який автентифікується в програмі, використовуючи ім'я користувача «admin» та пароль «xDK9&GoP1». Це дійсні облікові дані. Під час входу в програму виконайте інструкції SQL, які виконуються на сервері бази даних: SELECT name FROM user WHERE name=‘admin’ AND passwd=‘xDK9&GoP1’. Цей запит виконується до бази даних та автентифікує користувача на основі дійсних облікових даних.

```
1  Public Boolean authenticate (String name, String pass)
2
3  {
4
5  Statement stmt = this.conn.createStatement();
6
7  String sql = "SELECT name FROM user WHERE name=' " + name + " ' AND     passwd =' " + pass +
8
9  ResultSet results = stmt.executeQuery(sql);
10
11 return results.first();
12
13 }
```

Рисунок 2.13 – Код для отримання імені користувача та пароля

Тепер розглянемо зловмисника, який намагається автентифікуватися в програмі, використовуючи значення пароля “password’ OR ‘a’=’a” як корисне навантаження ін'єкції. Під час входу в програму на сервері бази даних виконується наступний SQL-запит: SELECT name FROM user WHERE name=‘admin’ AND passwd=‘password’ OR ‘a’=‘a’.

Після виконання цього запиту зловмисник успішно автентифікується в програмі, оскільки ‘a’=‘a’ завжди повертає значення true, що призводить до обходу автентифікації.

У разі успішної атаки зловмисник може отримати:

– несанкціонований доступ до програми (зловмисник може успішно обійти механізм автентифікації програми, щоб отримати до неї незаконний доступ);

– розкриття інформації (атака може призвести до повного витоку даних із сервера бази даних);

– втрата доступності даних (зловмисник може видалити записи із сервера бази даних);

– порушення цілісності даних (оскільки SQL-запитувачі також використовуються для зміни або додавання запису, зловмисник може використовувати SQL-ін'єкцію для зміни або додавання даних, що зберігаються в базі даних. Це призведе до порушення цілісності даних) [22].

SQL-ін'єкції відносяться до найнебезпечніших вразливостей програмного забезпечення. SQL-ін'єкції продовжують бути дуже актуальними. Причин актуальності є декілька:

– людський фактор (програмісти продовжують припускатися помилок, використовуючи склеювання рядків замість параметризованих запитів, особливо під час швидкої розробки або в складних запитах);

– застарілі системи (велика кількість сайтів та корпоративних систем працюють на базі небезпечного коду, який складно або дорого оновлювати);

– популярність CMS (SQL-ін'єкції залишаються ключовою загрозою для популярних систем керування контентом, де вразливість в одному плагіні може поставити під удар мільйони сайтів);

– складність виявлення (запити SQLi виглядають як справжні звернення до бази даних, що ускладнює їхнє виявлення стандартними системами захисту без глибокого аналізу трафіку).

2.3.2 Неправильно налаштовані сервери

Неправильно налаштовані сервери є джерелом системних вразливостей. Сервери є основою для обробки запитів в електронній комерції, включно з обробкою транзакцій, збереженням конфіденційних даних та взаємодією з платіжними шлюзами.

Вразливості та неправильні конфігурації серверів становлять значні ризики для конфіденційної інформації, часто призводячи до несанкціонованого доступу, витоків даних та збоїв у роботі. Такі вразливості, як невстановлене програмне забезпечення, конфігурації за замовчуванням, слабкі паролі, є деякими поширеними експлойтами, які використовують зловмисники [23].

До основних причин неправильної конфігурації відносять:

– використання стандартних облікових даних або слабких паролів;

– відсутність перевірки оновлень та патчів;

– недостатня політика прав доступу;

– відкриті сервіси з небезпечними налаштуваннями;

– відключені або неправильно налаштовані механізми безпеки.

Неправильна конфігурація безпеки є однією з головних вразливостей Open Worldwide Application Security Project (OWASP) і частою точкою входу для атак [24].

Для реалізації цієї загрози зловмисники часто використовують автоматизовані сканери для виявлення серверів з неправильними налаштуваннями або без базових оновлень. Потім вони експлуатують слабкі місця. Це дозволяє отримати несанкціонований доступ, впровадити бекдори або вкрасти дані.

Вплив вразливостей серверів та неправильних конфігурацій на конфіденційну інформацію може бути серйозним та багатогранним, впливаючи як на організацію, так і на її зацікавлені сторони. Ключові наслідки включають:

– витік персональних і платіжних даних;

– повна втрата контролю над платформою;

– зниження довіри користувачів;

– проблеми цілісності даних;

– втрата конкурентної переваги;

– юридична відповідальність за порушення захисту даних.

Дані наслідки підтверджуються у багатьох сучасних дослідженнях щодо серверних вразливостей і їх впливу на безпеку корпоративної та комерційної інформації [24].

2.3.3 Відкриті мережні порти

Мережні порти – це логічні кінцеві точки для з’єднань протоколів, необхідні для зв’язку між клієнтом і сервером (HTTP, HTTPS, FTP, SSH тощо). Вони реалізують обмін даними між різними компонентами СЕК.

Відкриті порти, які не фільтруються належним чином через firewall або контроль доступу, значно розширюють вразливості мережі. Відкриті порти

часто використовуються для сканування системи та пошуку вразливих служб. Зловмисник може сканувати мережу, ідентифікувати відкритий порт і методом повного перебору проникнути на сервер [25].

Реалізація атак через відкриті порти надає зловмисникам такі можливості:

– сканувати доступні порти;

– визначати працюючі служби;

– експлуатувати відомі уразливості цих служб;

– запускати атаки відмови в обслуговуванні (DDoS);

– отримувати доступ до систем без додаткової автентифікації.

Результати широкомасштабних мережних сканувань показують, що служби на нестандартних або незахищених портах суттєво частіше містять уразливості.

Відкриті мережні порти можуть бути причиною негативних наслідків, зокрема:

– недоступність сервісу для користувачів;

– порушення транзакційних процесів;

– використання ресурсів сервера проти самої системи (DDoS);

– потенційна компрометація внутрішніх систем.

2.3.4 Незашифровані канали передачі даних

Шифрування є ключовим елементом захисту даних під час передачі між клієнтом і сервером, оскільки воно забезпечує конфіденційність та цілісність інформації (наприклад даних платіжної картки або сесійних токенів користувача). Стандартний механізм шифрування – Transport Layer Security (TLS), який реалізує захищені HTTPS-з’єднання.

Передача даних через незашифровані канали (HTTP замість HTTPS) робить можливим перехоплення, читання або зміни інформації в мережі. Це істотно знижує рівень захисту даних у транзиті.

Однією з відомих технік є атака Man-in-the-Middle (MITM), коли зловмисник перехоплює та може змінювати дані під час передачі. Крім того, сесійні токени та cookies можуть бути викрадені через незашифровані канали, що дозволяє зловмиснику здійснювати перехоплення сесії.

Незашифровані канали передачі даних можуть призвести до таких наслідків:

– викрадення облікових даних клієнтів;

– компрометацію платіжної інформації;

– втрату довіри користувачів;

– юридичні санкції за порушення стандартів захисту даних (наприклад, PCI DSS).

Поєднання неправильно налаштованих серверів, відкритих портів і незашифрованих каналів значно підвищує загальні ризики для СЕК. Ці вразливості:

– створюють множинні точки входу для атак;

– послаблюють механізми захисту даних;

– збільшують потенційні втрати від кібератак;

– впливають на доступність, конфіденційність та цілісність системи.

Такий комплексний підхід до оцінки ризиків та характеристик загроз підтверджують сучасні дослідження та практики оцінки безпеки інформаційних систем.

2.4 ШІ як основна загроза СЕК

Окремої уваги заслуговує найсучасніший тип загрози для СЕК – штучний інтелект (ШІ). Сьогодні ШІ є революційною технологією, що змінює образ ЕК. ШІ дозволяє покращити користувацький досвід, автоматизувати взаємодію з клієнтами, аналізувати дані та прогнозувати продажі, оптимізувати внутрішні процеси, відкрити нові можливості для розвитку СЕК, підвищувати

ефективність та безпеку, забезпечити потужні інструменти для зростання та конкурентоспроможності СЕК [26].

Водночас, з безперервним розвитком ШІ розвивається і шахрайська діяльність, яка базується на ньому. В основному, вона націлена на малі і великі СЕК з цілями заволодіння інформацією про користувачів для подальших зловмисних дій, починаючи від зламу та спроб шантажу завершуючи продажом або зливом даних у відкриті джерела.

На момент 2025 року кіберзлочинність коштує світовій економіці понад 10,5 трильйонів доларів щорічно [27]. Однією з важливих причин цього є швидке і часто неконтрольоване впровадження ШІ, який тривожно збільшує прогалини в безпеці. Згідно з нещодавніми дослідженнями 90% компаній наразі не мають достатньої зрілості для ефективної протидії сучасним загрозам, що базуються на передовому ШІ [27].

Щоб побудувати ефективний захист, спочатку потрібно зрозуміти наступальну стратегію. Зловмисники систематично інтегрують ШІ у свої операції, щоб підвищити масштаб, швидкість та витонченість своїх атак, що мають великий діапазон методів від обману масового ринку до цілеспрямованих, адаптивних загроз [27].

2.4.1 Соціальні загрози СЕК на основі ШІ

Раніше тренінги з безпеки навчали користувачів розпізнавати ознаки фішингових електронних листів: погана граматика, незграбні фрази та шаблонні вітання. Сьогодні це втрачає актуальність. ШІ докорінно змінив ландшафт фішингу, зробивши його головною загрозою електронної пошти 2025 року.

Фундаментальний перехід полягає від легко помітного спаму до фішингових матеріалів, що генеруються ШІ, які є граматично бездоганними, контекстуально залежними та глибоко персоналізованими. Сучасні моделі великих мов (LLM) можуть сканувати публічний цифровий слід цілі, публікації

в соціальних мережах, професійні профілі, новини компанії, щоб створювати унікальні, переконливі наративи, що використовують людську довіру.

Кількість фішингових атак, пов’язаних з генеративним ШІ, зросла на 1265% , а в деяких звітах йдеться про ще більше зростання – 4151% [27]. В одному звіті на початку 2025 року зазначалося збільшення кількості повідомлень про фішинг на 466% лише за один квартал [27]. Зростання кількості та ефективності атак зловмисників на основі ШІ показано на рис.2.14.

Рисунок 2.14 – Зростання атак на основі ШІ

Цих електронних листів, створених ШІ, не тільки багато, але вони також небезпечно ефективні. Дослідження показують, що фішингові електронні листи, створені ШІ, можуть переконати 60% одержувачів взаємодіяти, що відповідає показнику успішності кампаній, розроблених експертами з соціальної інженерії людини [27]. Крім того, ця ефективність досягається за значно менших витрат та зусиль. Зловмисник може використовувати ШІ для створення цільового, переконливого фішингового електронного листа всього за декілька хвилин, у експерта таке завдання займає близько 16 годин . Це означає

зниження витрат для зловмисників на 95%, що дозволяє їм запускати індивідуальні кампанії в масштабах, які раніше були немислимими [27].

2.4.2 Технічні загрози СЕК на основі ШІ

Зловмисники також використовують ШІ для революціонізування розробки шкідливих програм, створюючи загрози, які є більш стійкими, ніж будь-коли раніше. Найзначнішим розвитком у цій галузі є зростання кількості поліморфних шкідливих програм, що генеруються ШІ, також дуже розповсюдженим є використання ШІ для написання шкідливого програмного забезпечення (ПЗ) та скриптів типу XSS і SQL-ін’єкцій [27].

Ще в 2023 році експерти з кібербезпеки Check Point Research повідомили, що після запуску ChatGPT учасники форумів кіберзлочинності використовували чат-бот для написання шкідливого ПЗ та фішингових листів. Зазначається, що деякі користувачі навіть не мали досвіду програмування [28].

Існують інцеденти, коли ChatGPT пише скрипти мовою Python, які можуть бути використані як програми-вимагачі. За допомогою такого ПЗ зловмисники можуть шифрувати дані на комп'ютері користувача.

Зараз ШІ набув набагато більших потужностей, з його допомогою можна отримати базу, код або основу для майже будь-якого ПЗ та проводити соціально-психологічні, програмні або комбіновані атаки на будь які види СЕК.

3 АНАЛІЗ ЗАСОБІВ БЕЗПЕКИ В СЕК

Кожен бізнес повинен докласти додаткових зусиль, щоб зробити свої сайти, сховища інформації та дані максимально безпечними. Це особливо важливо для брендів електронної комерції, які мають справу з величезною кількістю інформації про клієнтів та даних про транзакції.

Створення максимально безпечного досвіду покупок – це не одноразова акція після запуску електронного магазину. Безпека повинна регулярно проходити технічне обслуговування та перевірку, а також додаткові перевірки щодо оновлення платформи, оновлень плагінів та будь-яких змін у коді. Навіть якщо проблема, яка на перший погляд незначна, її недолгляд може мати дуже серйозні наслідки.

Витоки даних стосуються не лише великих брендів. За даними Trustwave 90% порушень спрямовані на дрібних торговців [29]. Великі бренди, які постраждають, можуть зіткнутися зі збитками до 4 мільйонів доларів за кожне порушення. Власники малого бізнесу страждають не так сильно; в середньому їхні витрати за витік даних становлять 37 000 доларів [29]. Ці збори починають накопичуватися, оскільки вони надходять з різних боків:

– плата за дотримання вимог PCI,

– відповідальність за звинувачення у шахрайстві,

– покращення POS-терміналів та обробки платежів,

– вартість заміни картки та обслуговування рахунку від емітентів карток,

– ресурси, задіяні в інформуванні клієнтів,

– обов'язковий перегляд коду та судово-медична оцінка для зменшення подальших ризиків.

Також існують негрошові витрати від порушення, включаючи втрату довіри, клієнтів, які розривають свої відносини (рис. 3.1), та вплив на репутацію бренду [29].

Рисунок 3.1 – Обсяги постраждалих користувачів СЕК

Як вже було зазначено, СЕК є одними з пріорітетних цілей для зловмисників, тому для успішного та ефективного існування необхідно на постійній основі захищати дані клієнтів та максимально зменшувати потенційні втрати. Єдиний спосіб це зробити – проактивно вирішувати ключові проблеми безпеки за допомогою існуючих механізмів захисту.

3.1 Аналіз засобів безпеки та механізмів захисту від соціальних та організаційних загроз

Організаційні засоби безпеки є першою лінією протидії соціальній інженерії, оскільки безпосередньо впливають на поведінку користувачів та персоналу. До них належать політики інформаційної безпеки, регламенти доступу, навчальні програми та формування культури безпеки.

Організаційні засоби безпеки відіграють ключову роль у протидії загрозам соціальної інженерії, оскільки основним об’єктом таких атак є людина, а не технічна інфраструктура. Навіть за наявності сучасних технічних засобів захисту, недостатній рівень обізнаності персоналу або відсутність чітко визначених процедур може призвести до компрометації системи електронної

комерції [30]. Організаційні заходи спрямовані на формування правильної поведінки користувачів, регламентацію дій у критичних ситуаціях та мінімізацію ризиків, пов’язаних із людським фактором [30].

Одним із основних організаційних механізмів є розробка та впровадження політик інформаційної безпеки. Такі політики визначають правила використання інформаційних ресурсів, порядок доступу до систем електронної комерції та вимоги до захисту конфіденційних даних.

Наявність чітко задокументованих політик (рис. 3.2) дозволяє зменшити ймовірність помилкових дій користувачів та спрощує процес реагування на інциденти [30]. До таких політик відносяться:

– навчання та підвищення обізнаності персоналу (рис. 3.3),

– процедури контролю та перевірки дій користувачів (рис. 3.4),

– формування культури інформаційної безпеки (рис. 3.5) тощо.

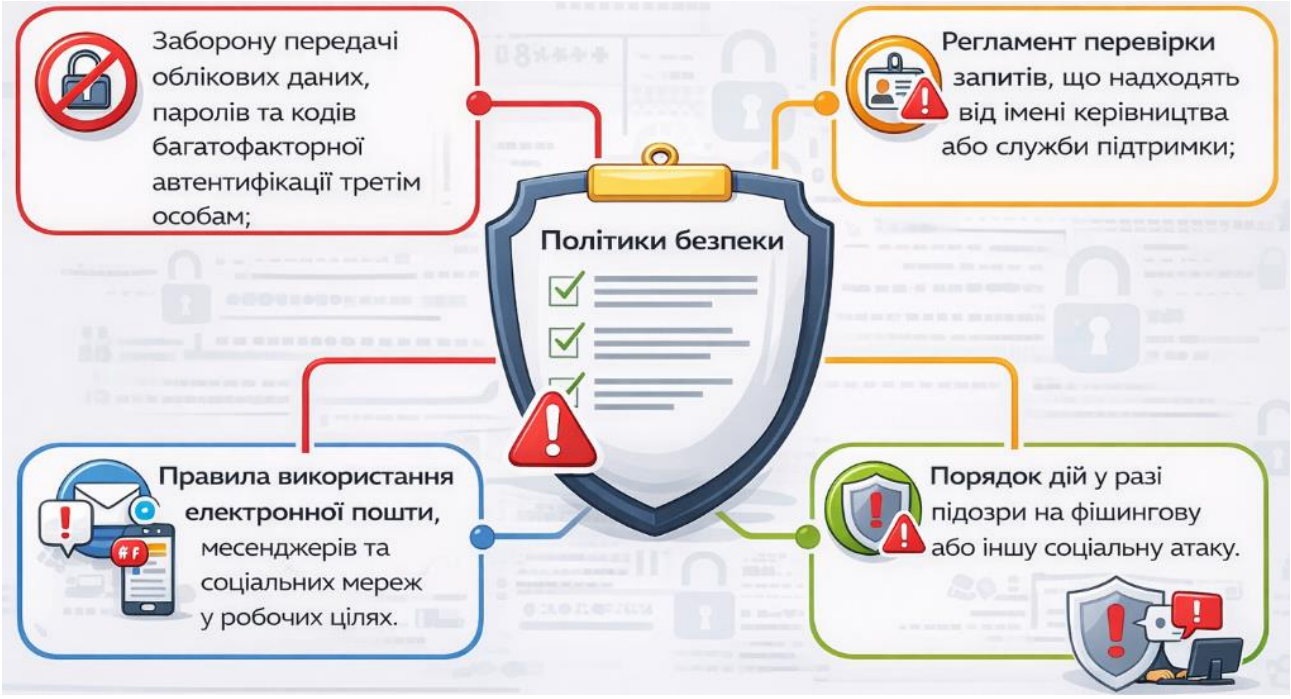

Рисунок 3.2 – Складові політики безпеки в контексті соціальних загроз

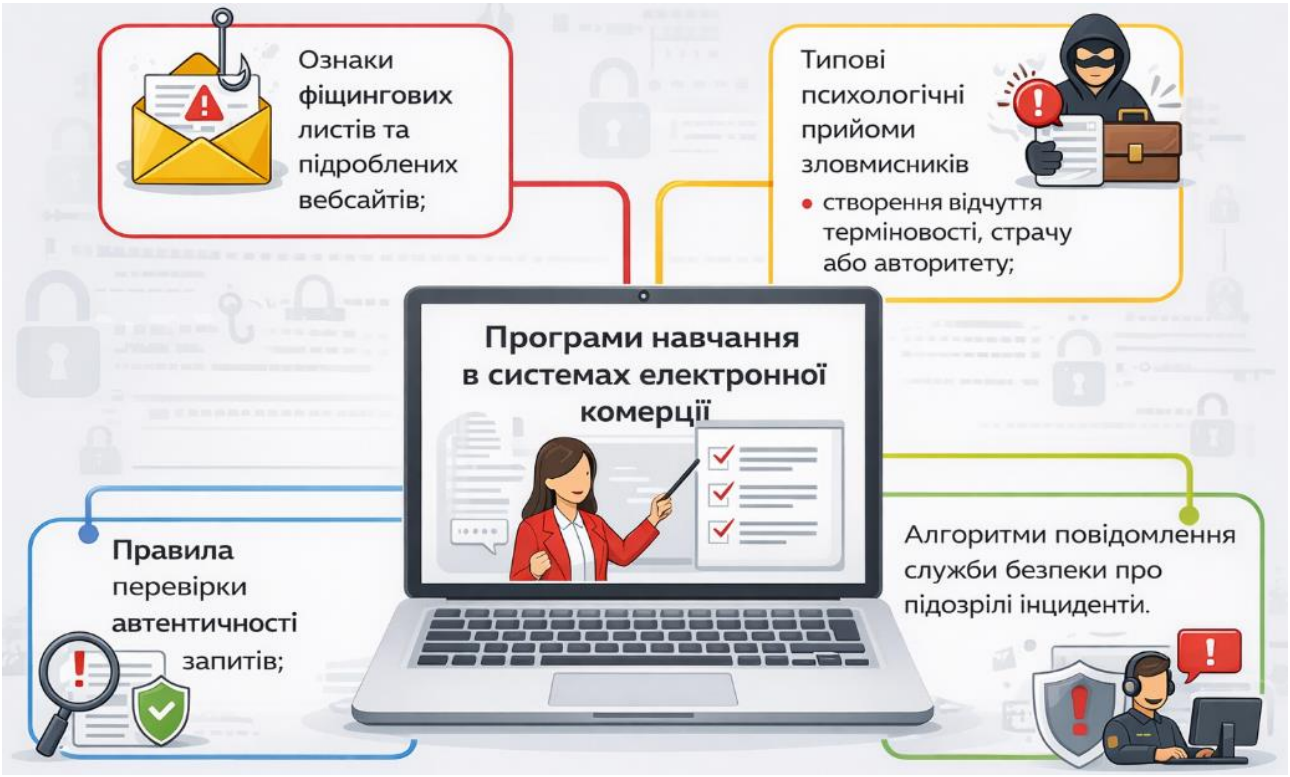

Рисунок 3.3 – Складові програми навчання в СЕК

Рисунок 3.4 – Складові процедури контролю та перевірки дій користувачів

Рисунок 3.5 - Складові культури інформаційної безпеки

Навчання персоналу є одним із найефективніших засобів боротьби із соціальною інженерією. Регулярні тренінги дозволяють формувати у користувачів навички розпізнавання потенційно небезпечних ситуацій та правильного реагування на них. Додатково можуть застосовуватися імітаційні фішингові кампанії, результати яких використовуються для оцінки рівня підготовки персоналу та коригування навчальних програм.

Важливим елементом організаційного захисту є впровадження процедур контролю, які зменшують ризик успішної реалізації соціальних атак. Зазначені заходи дозволяють знизити ймовірність того, що один скомпрометований користувач призведе до масштабних наслідків для всієї системи.

Формування культури інформаційної безпеки є довгостроковим, але критично важливим організаційним механізмом. Вона передбачає створення середовища, в якому кожен користувач усвідомлює свою відповідальність за захист інформації.

Перевагою організаційних засобів безпеки є їх здатність знижувати ймовірність успішної атаки шляхом підвищення обізнаності користувачів. Водночас їх ефективність значною мірою залежить від людського фактору. Навіть добре підготовлений персонал може допустити помилку через втому, стрес або складність атаки.

Дані процедури є необходніми у кожній СЕК та мають виконуватися кожними її частинами для захисту даних користувачів, але жодні процедури з кібергігієни ніколи не зможуть надати 100%-ої гарантії безпеки СЕК через насамперед людський фактор, який є найслабкішою ланкою. Тому для протидії спробам втручань на базі соціальної інженерії ці заходи є необхідним комбінувати в комплексний підхід.

3.1.1 Принцип нульової довіри

Принцип нульової довіри (Zero Trust) є сучасною концепцією кібербезпеки, що базується на припущенні про відсутність довіри до будь-якого користувача, пристрою або компонента системи незалежно від його розташування у внутрішній чи зовнішній мережі. На відміну від традиційних периметрових моделей безпеки, Zero Trust виходить з того, що загрози можуть існувати як поза межами системи, так і всередині неї, а тому кожен запит на доступ має бути перевірений, автентифікований та авторизований [31].

Архітектура Zero Trust представлена на рис.3.6.

У системах електронної комерції принцип нульової довіри набуває особливого значення через постійну взаємодію з великою кількістю користувачів, платіжних сервісів, сторонніх API та хмарних платформ. Такі системи обробляють фінансові операції та персональні дані, що робить їх привабливою ціллю для кіберзлочинців. Zero Trust дозволяє зменшити ризики, пов’язані з компрометацією облікових даних, оскільки навіть після успішної автентифікації користувач не отримує повного доступу до ресурсів системи.

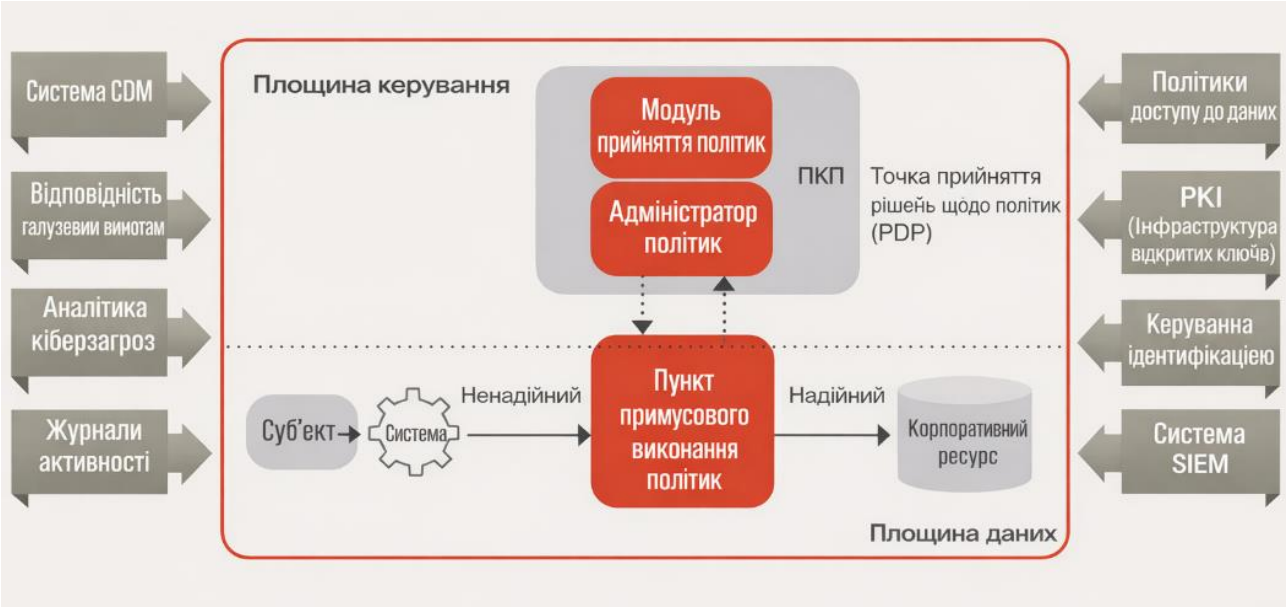

Рисунок 3.6 – Архітектура Zero Trust

Одним із ключових компонентів Zero Trust є принцип мінімальних привілеїв (least privilege), відповідно до якого користувачам та сервісам надається лише той рівень доступу, який є необхідним для виконання конкретних завдань. У контексті ЕК це дозволяє обмежити наслідки можливих атак, наприклад, у разі викрадення облікового запису співробітника або адміністратора. Таким чином, навіть у випадку соціальної інженерії зловмисник не зможе отримати повний контроль над системою [32].

Ще одним важливим елементом архітектури Zero Trust є безперервна перевірка контексту доступу. Це означає, що рішення про надання доступу приймається не лише на основі логіна та пароля, але й з урахуванням таких факторів, як тип пристрою, місцезнаходження, час доступу та поведінка користувача. Для систем електронної комерції такий підхід дозволяє виявляти аномальні дії, які можуть свідчити про шахрайство або компрометацію облікових даних.

Архітектура Zero Trust також передбачає мікросегментацію інформаційних ресурсів, яка полягає у поділі системи на окремі ізольовані сегменти. В системах електронної комерції це дозволяє відокремити платіжні

модулі, бази даних клієнтів та адміністративні інтерфейси, що значно знижує ризик поширення атаки у разі порушення безпеки одного з компонентів.

CDM (Continuous Diagnostics and Mitigation) – це компонент, що забезпечує безперервний збір та аналіз інформації про стан кібербезпеки системи. У рамках архітектури Zero Trust (рис.3.6) CDM надає контекстні дані для прийняття рішень щодо доступу, що дозволяє динамічно оцінювати ризики та адаптувати політики безпеки в режимі реального часу. CDM виконує такі функції:

– безперервно збирає дані про пристрої, користувачів і програмне забезпечення;

– аналізує ризики та вразливості;

– передає цю інформацію в механізми ухвалення рішень безпеки (у Zero Trust – у PDP / Policy Engine).

У моделі Zero Trust жоден запит не вважається надійним за замовчуванням. CDM саме й дає актуальний контекст, на основі якого система вирішує дозволити доступ, обмежити його або повністю заблокувати.

CDM передає інформацію про стан пристрою (наприклад, на наявність антивірусу, відповідність СЕК до політик безпеки, повідомлення про аномальну активність користувача) [33].

Інфраструктура відкритих ключів (PKI) – це система апаратного та програмного забезпечення, політик і процедур, яка управляє цифровими сертифікатами та шифруванням з відкритим ключем. Кожен користувач або система має: відкритий ключ (відкритий для загального доступу) та приватний ключ (закритий). Ці ключі математично пов'язані між собою.

PKI є надзвичайно ефективною у забезпеченні безпеки транзакцій електронної комерції, оскільки відповідає чотирьом основним вимогам безпеки:

– конфіденційність → надійне шифрування (TLS/SSL),

– автентифікація → перевірені цифрові ідентичності,

– цілісність → виявлення підробки за допомогою цифрових підписів,

– невідмовність → криптографічне підтвердження транзакцій.

На практиці PKI є основою HTTPS, без якої безпечні онлайн-покупки не могли б функціонувати.

PKI є технічно надійною, перевірена на глобальному рівні та має промисловий стандарт безпеки. PKI значною мірою покладається на довіру до центрів сертифікації (CA). Сильними сторонами є централізована довіра, яка спрощує перевірку та той факт що браузери заздалегідь довіряють основним CA, забезпечуючи безперебійну роботу користувачів. Але якщо CA скомпрометований, зловмисники можуть видавати підроблені сертифікати. Користувачі рідко розуміють або перевіряють сертифікати самостійно.

Переваги та недоліки PKI наведено на рис. 3.7..

Рисунок 3.7 – Переваги та недоліки PKI

PKI має надзвичайно високу масштабованість, щодня видається та перевіряється мільйони сертифікатів. Оптимізовано TLS-рукостискання (ECDHE, відновлення сеансу). Однак управління життєвим циклом сертифікатів (видача, поновлення, скасування) є складним. Механізми скасування (CRL, OCSP) часто працюють повільно або ігноруються браузерами. Як підсумок, PKI є досить складною системою в експлуатації та потребує спеціальних навичок у налаштуванні.

З точки зору користувача PKI є невидимою моделлю захисту. Користувачі все одно можуть бути обмануті фішинговими сайтами з дійсними сертифікатами та за допомогою атак на основі соціальної інженерії.

PKI має обмеження захисту. PKI не захищає від:

– скомпрометованих кінцевих точок (шкідливе ПЗ на пристроях користувачів),

– слабких паролів або неналежних практик автентифікації,

– внутрішніх загроз,

– фішингових атак із використанням законних сертифікатів.

Саме тому PKI необхідно поєднувати з багатофакторною автентифікацію, безпечними платіжними шлюзами, системами виявлення шахрайства. Тож PKI необхідна, але не є самодостатньою системою сама по собі.

PKI є фундаментальним і незамінним методом безпеки в СЕК. Хоча вона має структурні слабкі сторони, особливо в питаннях централізації довіри та обізнаності користувачів, на даний момент немає жодної життєздатної альтернативи, яка б забезпечувала такий самий баланс безпеки, масштабованості та практичності.

Принцип нульової довіри розглядається як відповідь на неефективність традиційної периметрової моделі безпеки, яка передбачає довіру до користувачів після входу у внутрішню мережу. Для СЕК така модель є вразливою, оскільки компрометація одного облікового запису або сервісу може призвести до повного порушення безпеки. Zero Trust усуває цю проблему шляхом повної відмови від неявної довіри та постійної перевірки доступу.

З позиції захисту від соціальної інженерії Zero Trust значно знижує ефективність атак, спрямованих на викрадення облікових даних. Англомовні дослідження зазначають, що навіть успішне отримання логіна та пароля не гарантує зловмиснику доступу до ресурсів, оскільки рішення про авторизацію залежить від багатьох додаткових факторів. У контексті електронної комерції це є критично важливим, адже більшість атак спрямовані саме на користувачів і персонал, а не на технічні вразливості.

Окрему увагу слід приділити тому, що Zero Trust не усуває повністю людський фактор, але майже повністю зменшує його вплив. Соціальна інженерія в будь-якому випадку залишається можливою, проте її наслідки суттєво обмежуються майже до мінімального рівня завдяки безперервному контролю доступу, журналюванню дій та поведінковій аналітиці. Це робить Zero Trust ефективним доповненням до архітектури захисту СЕК від соціального впливу, майже унеможливлює компроментацію та викрадення даних СЕК через навіть внутрішні загрози та є найбільш ефективним підходом до захисту СЕК в умовах зростання кількості соціальних атак. Його впровадження дозволяє мінімізувати наслідки людських помилок, обмежити можливості зловмисників та забезпечити високий рівень захисту фінансових і персональних даних.

3.1.2 Цифрові підписи

Цифрові/електронні підписи (digital/electronic signatures) є критично важливим механізмом забезпечення автентичності, цілісності та невідмовності цифрових документів і транзакцій. Ці підписи базуються на криптографії з відкритим ключем і пов’язані з інфраструктурою PKI, що дозволяє підтвердити, що документ підписано конкретною особою або системою та не змінювався після підписання. Це особливо важливо для електронної комерції, де транзакції, договори та підтвердження повинні бути юридично чинними і захищеними від підробки чи змін.

Крім цього, цифрові підписи гарантують, що жодні зміни у підписаному документі не залишаться непоміченими. Це досягається завдяки криптографічній перевірці підпису, що пов’язує документ з особою підписанта і забезпечує незаперечність їх дій. У контексті електронної комерції та обміну юридично значущими даними це означає зниження ризику шахрайства та підвищення довіри між сторонами, які взаємодіють онлайн [34].

Цифровий підпис використовує криптографічну пару ключів: закритий ключ, який зберігається в секреті у підписанта та відкритий ключ, який є доступним до перевірки підпису. Тобто цей механізм є основою для побудови цифрового підпису (документ підписується за допомогою закритого ключа, а перевіряється – за допомогою відповідного відкритого ключа).

Хешування документа. Підписуваний документ проходить через криптографічну хеш-функцію (наприклад, SHA-256), яка обчислює хеш-значення (digest) – короткий унікальний набір бітів, що представляє документ.

Шифрування хеш-значення закритим ключем. Отриманий хеш шифрується за допомогою закритого ключа підписанта. Це і є цифровий підпис – зашифрований хеш документа. Це гарантує, що підпис може створити тільки власник закритого ключа.

Для перевірки цифрового підпису отримувач виконує два основні кроки. Обчислення хеш-значення документа. Отриманий документ знову пропускають через ту саму хеш-функцію для генерації локального хеш-значення.

Цифровий підпис (шифрований хеш) розшифровується за допомогою відкритого ключа підписанта. Це дає хеш-значення підписанта. Якщо цей розшифрований хеш співпадає з локально обчисленим хеш-значенням документа – підпис вважається дійсним. Приклад процедури підписання показано на рис. 3.8.

PKI забезпечує механізми довіри для цифрових підписів.

Центр сертифікації (CA) видає цифрові сертифікати, які пов’язують відкритий ключ з ідентичністю (людина/організація). Сертифікат гарантує, що підпис дійсно належить певному суб’єкту.

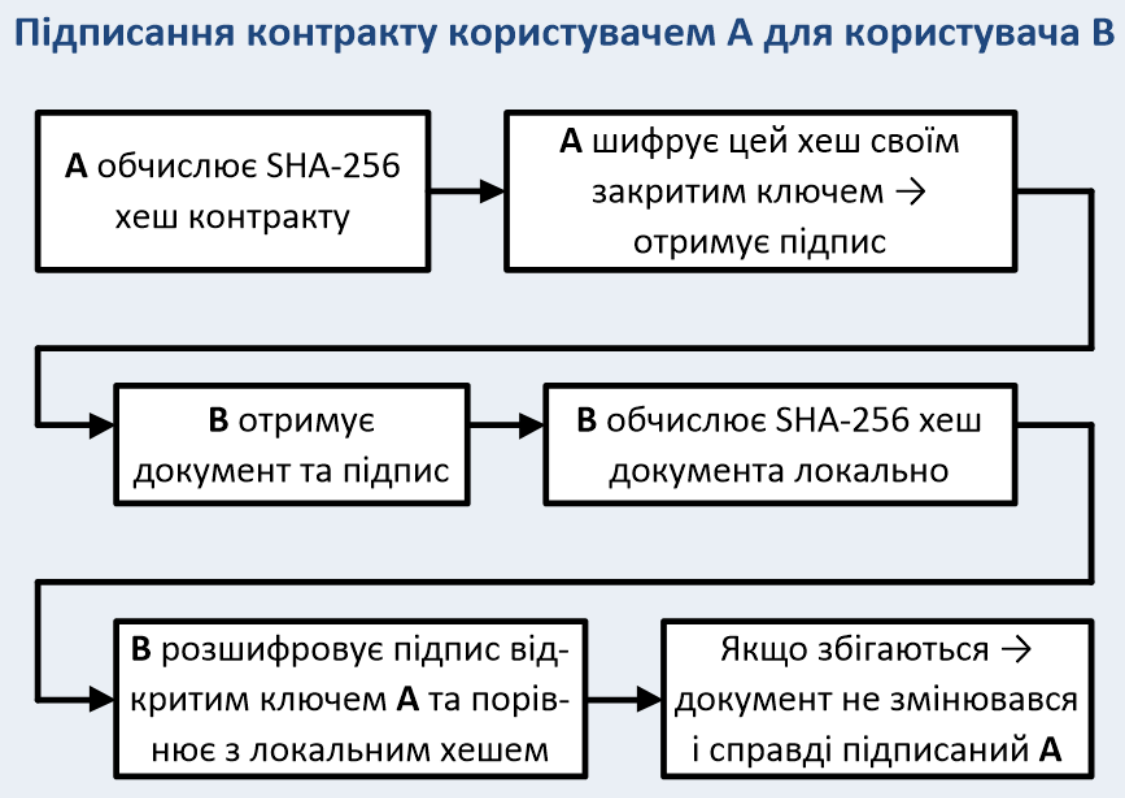

Рисунок 3.8 – Приклад процедури цифрового підпису

Таким чином, PKI робить роботу цифрових підписів масштабованою і придатною для великих систем (електронна комерція, документообіг тощо).

Цифровий підпис забезпечує:

– автентичність (підтверджує автора документа),

– цілісність (будь-яка зміна документа після підпису робить підпис недійсним),

– невідмовність (підписант не може заперечити факт підписання).

Це фундаментально важливо для бізнес-процесів, де потрібна юридична дія та довіра між сторонами.

Цифровий підпис – це криптографічний механізм, який забезпечує юридично значущу автентичність, цілісність та невідмовність документів шляхом шифрування хеш-значення документа закритим ключем та перевірки розшифрованого хеша відкритим ключем.

Ефективність електронного підпису значною мірою визначається використанням криптографічно стійких алгоритмів, таких як RSA, DSA або ECDSA, у поєднанні з надійними хеш-функціями (наприклад, SHA-256). Дослідження та рекомендації NIST підтверджують, що за умови правильного вибору алгоритмів і довжин ключів цифрові підписи залишаються стійкими до криптоаналізу та атак перебору [35].

З точки зору забезпечення цілісності даних, цифровий підпис є надзвичайно ефективним, оскільки навіть мінімальна зміна підписаного документа призводить до невідповідності хеш-значень і автоматично робить підпис недійсним. Це дозволяє швидко виявляти будь-які спроби модифікації інформації, що особливо важливо для електронної комерції, фінансових операцій та електронного документообігу.

Важливою складовою ефективності цифрових підписів є використання PKI, яка забезпечує надійний зв’язок між відкритим ключем і ідентифікацією підписанта. Завдяки сертифікаційним центрам CA користувачі можуть перевіряти справжність підписів без попереднього обміну ключами, що робить цей механізм масштабованим і придатним для використання у великих розподілених системах.

Ефективність цифрового підпису напряму залежить від захищеності закритого ключа. У випадку його компрометації зловмисник може створювати дійсні підписи від імені власника. Саме тому сучасні рекомендації передбачають використання апаратних засобів захисту ключів (HSM, smart cards), а також багатофакторної автентифікації для доступу до операцій підписання.

З практичної точки зору цифрові підписи довели свою ефективність як механізми зменшення рівня шахрайства та підвищення довіри між сторонами в цифрових середовищах. Використання цифрових підписів значно знижує кількість спірних ситуацій, пов’язаних із запереченням факту підписання документів, що є критично важливим для юридично значущих електронних транзакцій.

У контексті сучасних моделей безпеки, зокрема Zero Trust, цифровий підпис виступає як ефективний механізм підтвердження довіри на рівні транзакцій та дій користувача. Він дозволяє перевіряти не лише особу суб'єкта, а й автентичність кожної окремої операції, що повністю відповідає принципу «never trust, always verify» [31].

Таким чином, цифровий підпис є високоефективним механізмом інформаційної безпеки, який забезпечує автентичність, цілісність та невідмовність даних. За умови використання сучасних криптографічних алгоритмів, надійної інфраструктури PKI та захисту закритих ключів, цифрові підписи демонструють високий рівень стійкості до технічних і організаційних загроз та є доцільними для застосування у критично важливих інформаційних системах.

3.2 Аналіз засобів безпеки та механізмів захисту від технічних загроз

3.2.1 Брандмауери

Брандмауери є фундаментальним компонентом мережевої безпеки та виконують функцію контролю трафіку між внутрішніми сегментами СЕК і зовнішніми мережами. Їх основне завдання полягає у застосуванні правил фільтрації на основі IP-адрес, портів, протоколів і контексту з'єднання. У системах електронної комерції брандмауери розміщуються на периметрі мережі та між критично важливими сегментами, такими як вебсервери, сервери додатків і бази даних.

Брандмауери нового покоління (NGFW) значно розширюють функціональність традиційних рішень, забезпечуючи глибоку перевірку пакетів DPI (Deep Packet Inspection), контроль застосунків та інтеграцію з системами запобігання вторгненням. У контексті СЕК NGFW дозволяють ідентифікувати та блокувати атаки на прикладному рівні, зокрема SQL-ін'єкції та XSS-атаки, які часто використовуються для компрометації онлайн-магазинів.

Брандмауер наступного – це пристрій безпеки, який обробляє мережевий трафік і застосовує правила для блокування потенційно небезпечного трафіку. NGFW розвиваються та розширюють можливості традиційних брандмауерів [36]. Вони роблять те саме, що й брандмауери, але потужніше та з додатковими функціями (рис. 3.9).

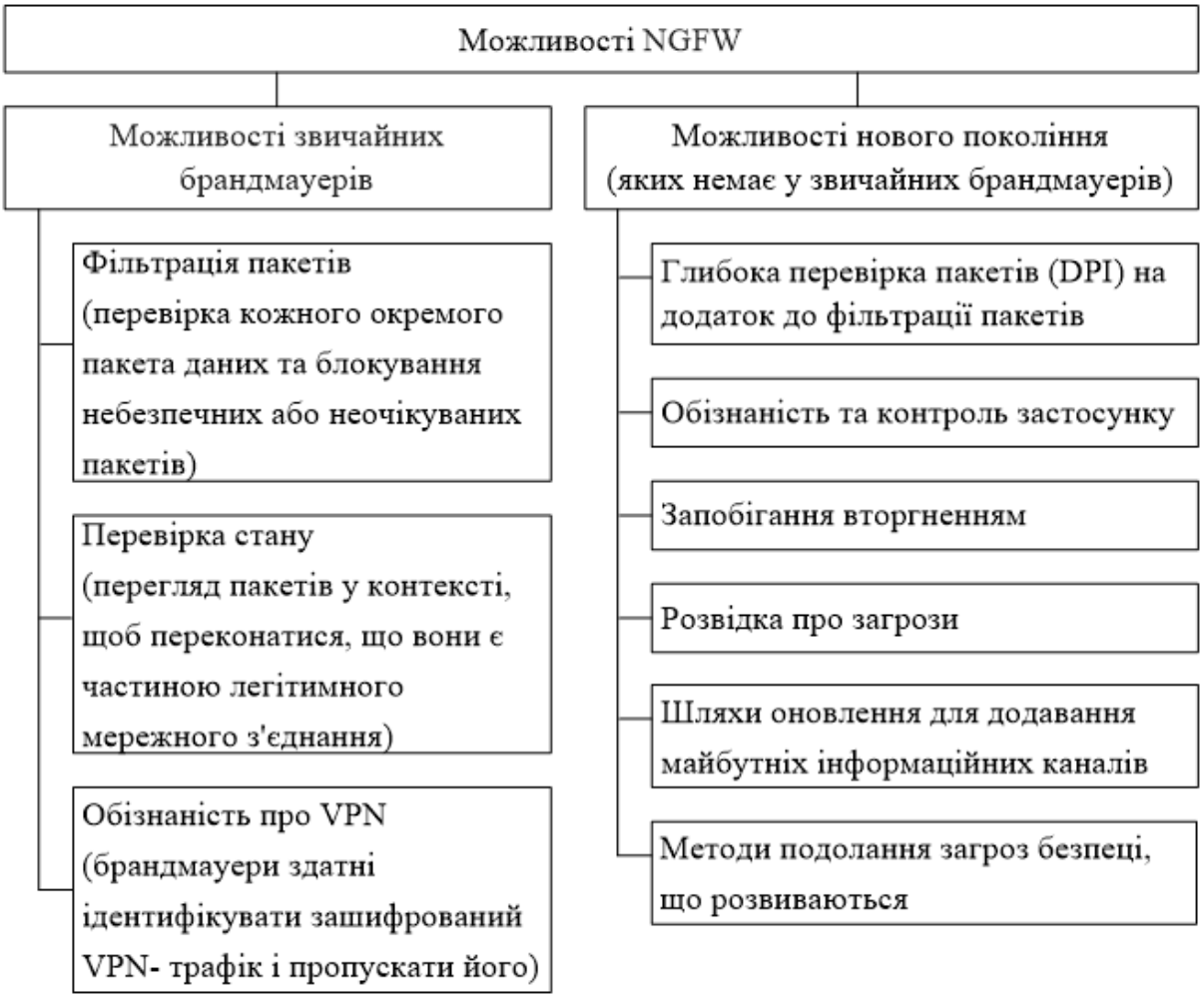

Рисунок 3.9 – Можливості брандмауерів наступного покоління

Більшість цих функцій можливі завдяки тому, що, на відміну від звичайних брандмауерів, NGFW можуть обробляти трафік на кількох рівнях моделі OSI, а не лише на рівнях 3 (мережевий рівень) та 4 (транспортний рівень). NGFW можуть переглядати HTTP- трафік 7-го рівня та визначати, які програми використовуються, наприклад. Це важлива можливість, оскільки 7-й

рівень (рівень додатків) все частіше використовується для атак, щоб обійти політики безпеки, що застосовуються на рівнях 3 та 4 традиційними брандмауерами [36].

NGFW покращують фільтрацію пакетів, виконуючи глибоку перевірку пакетів DPI (рис. 3.10). Як і фільтрація пакетів, DPI передбачає перевірку кожного окремого пакета, щоб побачити IP-адресу джерела та призначення, порт джерела та призначення тощо. Вся ця інформація міститься в заголовках 3-го та 4-го рівнів пакета [36].

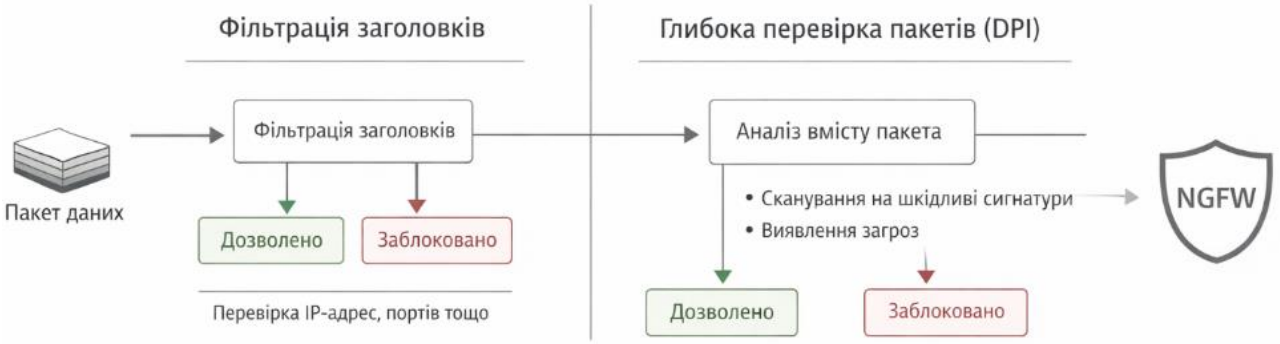

Рисунок 3.10 – Глибока перевірка пакетів в NGFW

DPI також перевіряє тіло кожного пакета, а не лише заголовок. Зокрема, DPI перевіряє тіла пакетів на наявність сигнатур шкідливого ПЗ та інших потенційних; порівнює вміст кожного пакета з вмістом відомих шкідливих атак.

NGFW блокують або дозволяють пакети залежно від того, до якої програми вони прямують. Вони роблять це, аналізуючи трафік на 7-му рівні, рівні програми. Традиційні брандмауери не мають такої можливості, оскільки вони аналізують трафік лише на 3-му та 4-му рівнях.

Обізнаність про програми дозволяє адміністраторам блокувати потенційно небезпечні програми. Якщо дані програми не можуть пройти крізь брандмауер, то вона не може створювати загрози в мережі.

Запобігання вторгненням (рис. 3.11) аналізує вхідний трафік, виявляє відомі та потенційні загрози, а також блокує ці загрози. Таку функцію часто називають системою запобігання вторгненням (IPS). NGFW включають IPS як частину своїх можливостей DPI.

Рисунок 3.11 – Запобігання вторгненням в NGFW

Системи IPS можуть використовувати кілька методів для виявлення загроз, зокрема:

– виявлення сигнатур (сканування інформації у вхідних пакетах та порівняння її з відомими загрозами),

– виявлення статистичних аномалій (сканування трафіку для виявлення незвичайних змін у поведінці порівняно з базовим рівнем),

– виявлення протоколу з урахуванням стану (подібне до виявлення статистичних аномалій, але зосереджене на використовуваних мережевих протоколах та порівнянні їх із типовим використанням протоколів).

Деякі NGFW – це апаратні пристрої, призначені для захисту внутрішньої приватної мережі. NGFW також можна розгортати як програмне забезпечення, але вони не обов'язково повинні бути програмними, щоб вважатися наступним поколінням. Зрештою, NGFW може бути розгорнутий як хмарний сервіс; це називається хмарним брандмауером або брандмауером як послуга (FWaaS), який нерідко використовують СЕК.

СЕК працюють у постійній взаємодії з зовнішніми користувачами та сторонніми сервісами, що створює підвищений рівень мережевих ризиків. За таких умов традиційні міжмережеві екрани, які здійснюють фільтрацію трафіку лише за формальними мережевими ознаками, не забезпечують належного рівня захисту. Саме тому у сучасних СЕК широко застосовуються брандмауери нового покоління, які орієнтовані на комплексний аналіз мережевої взаємодії та поведінки користувачів [36].

У типовій СЕК NGFW виконує роль центрального контрольного вузла між публічним доступом і внутрішньою інфраструктурою. На відміну від класичних рішень, він аналізує не лише технічні параметри з'єднання, а й логіку роботи застосунків, що дозволяє точніше оцінювати допустимість кожного запиту. Такий підхід суттєво ускладнює реалізацію атак, що маскуються під легітимний вебтрафік, який є основним каналом взаємодії клієнтів із СЕК [37].

Важливою перевагою NGFW є можливість відмови від статичних правил доступу, прив'язаних до IP-адрес. В СЕК це дозволяє реалізувати політики безпеки, які враховують роль користувача та контекст його дій. Наприклад, доступ до адміністративних функцій може надаватися лише після підтвердження ідентичності, незалежно від місця підключення. Це суттєво зменшує ризики, пов'язані з внутрішніми загрозами та компрометацією облікових даних.

Оскільки більшість взаємодій у СЕК здійснюється через захищені канали, здатність NGFW аналізувати зашифрований трафік є критично важливою. Брандмауер може тимчасово розкривати вміст захищених сесій для перевірки їх безпечності, що дозволяє виявляти приховані загрози. Водночас такий механізм створює додаткове навантаження на інфраструктуру та вимагає ретельного налаштування, аби уникнути зниження продуктивності системи.

Незважаючи на розширений функціонал, NGFW не здатний повністю усунути всі загрози безпеці СЕК. Його ефективність значною мірою залежить від коректності налаштувань та актуальності політик безпеки. Крім того,

NGFW має обмежені можливості у протидії атакам, що ґрунтуються на соціальній інженерії або використанні скомпрометованих облікових записів. Це свідчить про те, що брандмауер нового покоління має розглядатися не як універсальне рішення, а як складова багаторівневої системи захисту [31].

У сучасних англомовних дослідженнях NGFW розглядається як технічний елемент архітектури Zero Trust, що забезпечує контроль мережних взаємодій без припущення довіри [31]. У поєднанні з постійною перевіркою ідентичності та контексту доступу NGFW дозволяє знизити ймовірність успішної атаки навіть у разі порушення периметра. Такий підхід є найбільш доцільним для систем електронної комерції, які працюють у динамічному та потенційно ворожому середовищі.

Проведений аналіз свідчить, що брандмауер нового покоління є ефективним інструментом захисту систем електронної комерції на мережевому та прикладному рівнях. Водночас його застосування повинно поєднуватися з іншими механізмами безпеки та сучасними архітектурними підходами. Максимальна ефективність NGFW досягається лише у складі комплексної системи захисту, побудованої на принципах нульової довіри.

3.2.2 Протоколи безпеки СЕК

В СЕК протоколи безпеки (рис. 3.12) відіграють ключову роль у забезпеченні захисту інформаційних потоків між клієнтами, серверами та платіжними сервісами. Оскільки більшість транзакцій відбувається через відкриті мережі, зокрема Інтернет, виникає необхідність у застосуванні криптографічних протоколів, які гарантують конфіденційність, цілісність і автентичність переданих даних. Протоколи безпеки реалізують ці властивості шляхом використання симетричного та асиметричного шифрування, цифрових сертифікатів і механізмів перевірки цілісності повідомлень.

Протокол TLS (Transport Layer Security) є базовим протоколом захисту даних у сучасних СЕК і використовується для створення захищеного каналу

зв’язку між клієнтом і сервером. Технічно TLS працює поверх транспортного рівня моделі OSI та застосовує асиметричне шифрування для обміну ключами, після чого переходить до симетричного шифрування для ефективної передачі даних. Такий підхід дозволяє поєднати високий рівень безпеки з мінімальними накладними витратами [38].

Рисунок 3.12 – Протоколи безпеки в СЕК

У контексті електронної комерції TLS забезпечує захист платіжної інформації, облікових даних користувачів та персональних даних клієнтів. Його застосування у вигляді HTTPS є обов’язковим стандартом для онлайн-магазинів і платіжних шлюзів. Водночас ефективність TLS напряму залежить від коректності конфігурації та використання сучасних версій протоколу.

Незважаючи на високу криптографічну стійкість, TLS не усуває всі загрози автоматично. Помилки в управлінні сертифікатами, використання застарілих алгоритмів або компрометація центрів сертифікації можуть звести ефективність протоколу нанівець. Таким чином, TLS потребує постійного оновлення та інтеграції з іншими механізмами контролю безпеки.

Протокол IPsec (Internet Protocol Security) є набором протоколів, призначених для захисту трафіку на мережному рівні. На відміну від TLS, IPsec шифрує весь IP-трафік незалежно від прикладного протоколу, що дозволяє

забезпечити комплексний захист з’єднань між мережевими вузлами. Це особливо актуально для СЕК із розподіленою серверною інфраструктурою [39].

У практичному використанні IPsec часто застосовується для побудови захищених VPN-каналів між дата-центрами, хмарними сервісами та платіжними провайдерами. Такий підхід знижує ризик перехоплення або модифікації даних у процесі міжсистемної взаємодії.

Основним недоліком IPsec є складність налаштування та високе навантаження на мережеві ресурси. Неправильна конфігурація може призвести до зниження продуктивності або створення вразливостей. Тому IPsec доцільно використовувати у поєднанні з іншими протоколами, а не як універсальне рішення.

Протокол SSH (Secure Shell) є криптографічним протоколом, який забезпечує безпечний віддалений доступ до серверних систем. У СЕК SSH використовується для адміністрування веб-серверів, баз даних і платіжних систем, дозволяючи захистити керування інфраструктурою від перехоплення або підміни команд [40].

SSH реалізує механізми автентифікації на основі криптографічних ключів і забезпечує цілісність переданих даних. Це дозволяє мінімізувати ризики компрометації адміністративних облікових записів у разі атак на мережеву інфраструктуру.

Попри високий рівень захисту, SSH залишається вразливим до атак у разі слабкої політики управління ключами або використання паролів замість ключової автентифікації. У СЕК це може призвести до повної компрометації серверів, що підкреслює важливість жорсткого контролю доступу.

На основі інформаційних джерел [38 – 40] було виконано порівняльний аналіз протоколів TLS, IPsec, SSH. Результати аналізу наведено в табл. 3.1.

Порівняльний аналіз показує, що TLS, IPsec та SSH виконують різні функції в архітектурі безпеки СЕК і не можуть взаємно замінювати один одного.

Таблиця 3.1 – Порівняльний аналіз протоколів TLS, IPsec, SSH

Критерій	TLS	IPsec	SSH
Рівень моделі OSI	Транспортний / прикладний рівень	Мережевий рівень	Прикладний рівень
Основне призначення	Захист клієнт–серверних з'єднань (HTTPS)	Захист IP-трафіку між мережами	Безпечне віддалене адміністрування
Тип захищених даних	Веб-трафік, платіжні дані, персональна інформація	Увесь IP-трафік незалежно від сервісу	Адміністративні команди, службові дані
Метод шифрування	Асиметричне (обмін ключами) + симетричне (передача даних)	Симетричне та асиметричне	Асиметричне та симетричне
Автентифікація	Сертифікати X.509 (PKI)	Ключі та сертифікати	Криптографічні ключі або паролі
Типова сфера застосування в СЕК	Онлайн-магазини, платіжні шлюзи, API	VPN між серверами та дата-центрами	Керування серверами СЕК
Рівень прозорості для користувача	Повністю прозорий	Прозорий для прикладних сервісів	Вимагає явної взаємодії
Переваги	Стандарт де-факто, висока сумісність, масштабованість	Повний захист мережевого трафіку	Надійний контроль доступу
Недоліки	Залежність від конфігурації та CA	Складність налаштування, навантаження	Ризики при слабкому управлінні ключами
Стійкість до атак соціальної інженерії	Середня (не захищає від фішингу)	Висока (не залежить від користувача)	Низька без MFA та політик доступу
Відповідність Zero Trust	Часткова	Часткова	Висока при інтеграції з MFA

TLS є ключовим для захисту взаємодії з клієнтами, IPsec забезпечує безпечну міжмережеву комунікацію, а SSH – контроль адміністративного

доступу. Найвищу ефективність ці протоколи демонструють у поєднанні, особливо в рамках архітектури Zero Trust, де кожен рівень комунікації підлягає окремій перевірці.

Розглянуті протоколи безпеки забезпечують захист даних на різних рівнях мережної взаємодії, однак жоден із них не є самодостатнім. У сучасних СЕК вони все частіше інтегруються в архітектуру Zero Trust, де кожне з'єднання перевіряється незалежно від його походження. Такий підхід дозволяє мінімізувати ризики внутрішніх атак і зменшити наслідки компрометації окремих компонентів системи.

Протоколи безпеки є критично важливими елементами захисту систем електронної комерції, забезпечуючи безпечну передачу даних, автентифікацію сторін та цілісність інформації. Їх ефективність залежить не лише від криптографічної стійкості, а й від коректної інтеграції в загальну архітектуру безпеки та відповідності сучасним моделям, таким як Zero Trust.

3.2.3 Програмне та апаратне забезпечення СЕК

У системах електронної комерції програмне та апаратне забезпечення відіграють фундаментальну роль у забезпеченні комплексного захисту інформаційних ресурсів. На відміну від окремих протоколів або організаційних заходів, ці механізми формують технічну основу безпеки СЕК, забезпечуючи захист на рівні інфраструктури, обробки даних і контролю доступу. Їх ефективність полягає у можливості автоматизованого виявлення, запобігання та реагування на кіберзагрози в реальному часі.

Програмне забезпечення безпеки в СЕК охоплює широкий спектр рішень, зокрема системи виявлення та запобігання вторгненням (IDS/IPS), антивірусні платформи, засоби захисту вебдодатків (WAF) та системи управління подіями безпеки (SIEM). Дані рішення аналізують мережевий трафік, журнали подій та поведінку користувачів з метою виявлення аномалій і потенційних атак [41].

У контексті СЕК програмні засоби дозволяють оперативно реагувати на спроби SQL-ін’єкцій, міжсайтового скриптингу, фішингових атак та несанкціонованого доступу до облікових записів користувачів. Особливо важливою є інтеграція таких рішень із платіжними шлюзами та вебплатформами ЕК.

Апаратне забезпечення безпеки включає спеціалізовані пристрої, такі як апаратні брандмауери, апаратні модулі безпеки (HSM), мережеві шлюзи та системи балансування навантаження з функціями захисту. Ці рішення забезпечують ізоляцію критичних операцій і виконання криптографічних функцій на фізичному рівні, що значно ускладнює їх компрометацію.

В СЕК широко використовуються HSM для безпечного зберігання криптографічних ключів, обробки платіжних транзакцій і генерації цифрових підписів. Завдяки фізичному захисту такі пристрої відповідають вимогам стандартів PCI DSS і значно знижують ризик витоку ключової інформації [42].

Було виконано порівняльний аналіз програмного та апаратного забезпечення безпеки в СЕК. Результати аналізу наведено в табл. 3.2.

Порівняльний аналіз показує, що програмне та апаратне забезпечення виконують різні, але взаємодоповнювальні функції у системах електронної комерції. Програмні рішення забезпечують гнучкий і адаптивний захист, тоді як апаратні механізми формують надійну фізичну основу безпеки. Найвищий рівень захисту СЕК досягається за умови їх комплексного використання в рамках архітектури Zero Trust.

В якості приклада програмного забезпечення безпеки в СЕК розглянемо Cloudflare WAF, а апаратного забезпечення безпеки в СЕК – Thales Luna HSM.

WAF (Web Application Firewall) є спеціалізованим програмним засобом захисту вебдодатків, який аналізує HTTP/HTTPS-трафік між користувачами та серверами системи електронної комерції. Cloudflare WAF працює на прикладному рівні та застосовує набір правил, сигнатур і поведінкових моделей для виявлення та блокування типових вебатак, зокрема SQL-ін’єкцій, міжсайтового скриптингу та спроб обходу автентифікації [43].

Таблиця 3.2 – Порівняння програмного та апаратного забезпечення безпеки в СЕК

Критерій	Програмне забезпечення безпеки	Апаратне забезпечення безпеки
Призначення	Аналіз, моніторинг і реагування на загрози на логічному рівні	Фізичний захист, ізоляція та виконання критичних операцій
Рівень реалізації	Прикладний та мережевий рівні	Фізичний та мережевий рівні
Типи загроз	Шкідливе ПЗ, вебатаки, вторгнення, аномальна поведінка	Крадіжка ключів, перехоплення трафіку, компрометація інфраструктури
Гнучкість	Висока, легко оновлюється та масштабується	Обмежена, залежить від фізичних ресурсів
Швидкість впровадження	Висока (швидке розгортання)	Середня або низька
Вартість	Відносно нижча	Висока
Залежність від конфігурації	Висока	Середня
Стійкість до компрометації	Залежить від ОС та середовища	Висока завдяки фізичній ізоляції
Роль у СЕК	Оперативний захист вебсервісів і користувачів	Захист платіжних операцій і криптографічних ключів
Відповідність Zero Trust	Забезпечує постійний моніторинг	Формує апаратну основу довіри

У СЕК Cloudflare WAF виконує роль першого рубежу захисту, фільтруючи зловмисний трафік ще до його потрапляння на серверну інфраструктуру. Це дозволяє зменшити навантаження на внутрішні системи та

знизити ризик компрометації баз даних із платіжною та персональною інформацією.

Попри високу ефективність проти відомих атак, WAF має обмеження у протидії складним логічним атакам і атакам нульового дня. Крім того, некоректна конфігурація правил може призвести до блокування легітимного трафіку, що негативно впливає на доступність сервісів електронної комерції.

HSM (Hardware Security Module) є спеціалізованим апаратним пристроєм, призначеним для захищеного зберігання криптографічних ключів та виконання операцій шифрування і цифрового підпису. Thales Luna HSM широко застосовується в системах електронної комерції для обробки платіжних транзакцій та управління ключами відповідно до стандартів PCI DSS [44].

У СЕК використання HSM дозволяє ізолювати критичні криптографічні операції від основної операційної системи, що значно зменшує ризик компрометації ключів навіть у разі успішної атаки на сервер

Незважаючи на високий рівень захисту, HSM характеризуються високою вартістю та складністю інтеграції. Для невеликих систем електронної комерції їх впровадження може бути економічно недоцільним, що обмежує сферу застосування таких рішень.

3.3 Проактивний механізм захисту СЕК на основі ШІ

Найважливішою перевагою, яку ШІ пропонує захисникам, є можливість переходу від реактивної до проактивної моделі безпеки (рис. 3.13).

Найбільшою захисною силою ШІ є його здатність вивчати, як виглядає нормальний стан у складному цифровому середовищі, в даному випадку це СЕК. Аналізуючи величезні обсяги даних, ШІ створює динамічну поведінкову базову модель для кожного користувача, пристрою та програми. Замість пошуку відомих сигнатур шкідливого програмного забезпечення, системи на базі ШІ шукають аномалії (ледь помітні відхилення від усталених шаблонів). Ця здатність, яку часто називають аналітикою поведінки користувачів та

сутностей (UEBA), дозволяє системам безпеки виявляти нові, нульові та поліморфні атаки, які були б невидимими для традиційних інструментів. У середовищах з високим рівнем ризику системи на базі ШІ продемонстрували рівень виявлення загроз до 98% [27].

Рисунок 3.13 – Протоколи безпеки в СЕК

Окрім виявлення в реальному часі, ШІ дозволяє використовувати прогнозну аналітику в кібербезпеці. Платформи розвідки загроз на базі ШІ безперервно отримують та аналізують величезні обсяги даних з широкого кола джерел. Виявляючи тонкі кореляції та нові закономірності, ці платформи можуть прогнозувати майбутні загрози, наприклад, передбачати, яка вразливість буде широко використана. Ця прогностична здатність є ключовою відмінністю між простою оцінкою вразливостей та тестуванням на

проникнення, оскільки вона зміщує фокус з пошуку існуючих дірок на передбачення того, де з'являться наступні.

Однією з найактуальніших проблем кібербезпеки сьогодні є людське вигорання. Центри операцій безпеки (SOC) часто перевантажені невпинним потоком сповіщень.

ШІ пропонує потужне рішення цієї проблеми, діючи як «множник навичок» для команд безпеки. Платформи на базі ШІ для управління інформацією та подіями безпеки (SIEM) та оркестрації, автоматизації та реагування на безпеку (SOAR) трансформують операції SOC:

– автоматизоване сортування (ШІ автоматично співвідносить та контекстуалізує тисячі низькорівневих сповіщень, об’єднуючи їх в один інцидент високого пріоритету для розгляду людиною),

– автоматизоване реагування (для чітко визначених загроз платформи SOAR можуть виконувати автоматизовані схеми реагування без втручання людини, такі як ізоляція зараженої кінцевої точки або блокування шкідливої IP-адреси) [27].

Згідно зі звітом IBM про вартість порушення даних за 2025 р., організації, які широко використовують ШІ та автоматизацію в галузі безпеки, скорочують свої середні витрати на усунення порушень на 1,9 мільйона доларів і скорочують життєвий цикл порушень в середньому на 80 днів [27]. Ця автоматизація звільняє аналітиків-людей від повторюваних завдань, дозволяючи їм зосередитися на складнішій роботі, такій як пошук та розслідування загроз. Це підвищення ефективності є основною причиною важливості безперервного тестування на проникнення; воно дозволяє командам постійно перевіряти ефективність цих складних автоматизованих систем захисту.

Для зміцнення стійкості, окрім впровадження захисних інструментів ШІ, організації також повинні впровадити чітке управління для управління ризиками, пов’язаними з цією потужною технологією.

Одна з найважливіших проблем полягає в тому, що впровадження ШІ значно випереджає нагляд за безпекою. Бізнес-підрозділи часто впроваджують тіньовий ШІ – несанкціоновані інструменти та програми ШІ – без відома команди безпеки, створюючи величезні прогалини у видимості.

Структура управління ризиками, пов'язаними зі ШІ (RMF) NIST є важливим посібником для структурованого та відповідального управління ризиками, пов'язаними зі ШІ. Структура побудована навколо чотирьох основних функцій:

– управління (створення політик, культури та структур підзвітності, необхідних для управління ризиками, пов'язаними зі ШІ),

– карта (визначення контексту, в якому використовуються системи ШІ, та нанесення на карту потенційних ризиків),

– вимірювання (розробка та використання методів для аналізу, оцінки та моніторингу ризиків, пов'язаних зі ШІ, та їхнього впливу),

– управління (врегулювання ризиків, які були виявлені та виміряні, шляхом розподілу ресурсів для їх пом'якшення).

Прийняття NIST AI RMF є критично важливим кроком до побудови надійних систем ШІ та демонстрації належної перевірки [27].

До найважливіших ризиків відносяться:

– LLM01 (впровадження підказки: зловмисник створює шкідливий вхідний сигнал, який обманом змушує LLM ігнорувати його початкові інструкції та виконувати команди зловмисника),

– LLM02 (розкриття конфіденційної інформації: LLM ненавмисно витікає конфіденційні дані або зі свого навчального набору, або з підключених систем, до яких він має доступ).

Захист застосунків на базі LLM від цих загроз вимагає поєднання фільтрації вводу/виводу та суворого контролю доступу, що робить такі концепції, як передові практики безпеки OAuth, дуже актуальними [27].

Основні кроки для посилення безпеки при впровадженні ШІ в роботу СЕК показані на рис. 3.14.

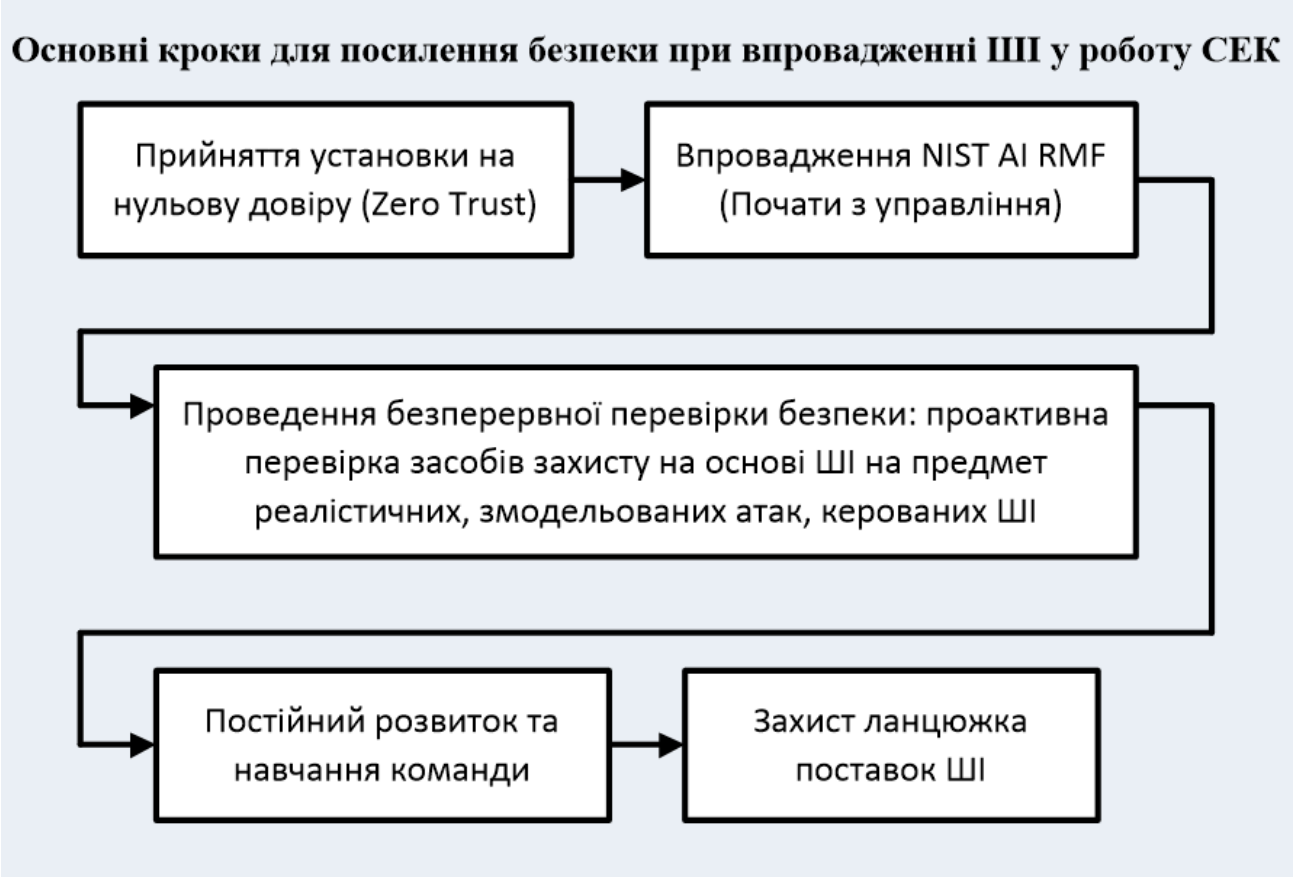

Рисунок 3.14 – Основні кроки для посилення безпеки в СЕК

Найпоширенішою точкою входу для злому платформи ШІ було вторгнення в ланцюжок поставок через скомпрометований сторонній додаток або плагін. Розуміння того, як захистити ці інтеграції, є критично важливим.

4 АНАЛІЗ РЕАЛЬНОГО ІНЦЕДЕНТУ ТА РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ СЕК

4.1 Аналіз інциденту у фірмі Arup

У січні 2024 року британська інженерна компанія Arup Group Limited**,** відома як глобальний консультант у сферах проєктування та інженерії, стала жертвою складної схеми фінансового шахрайства на основі штучно згенерованих медіа (deepfake)**.** Напад не був стандартною технічною кібератакою, але використав сучасні технології ШІ для маніпуляції довірою співробітника компанії.

За даними корпоративної звітності Arup та розслідування поліції Гонконгу, співробітник офісу Arup у Гонконгу отримав електронне повідомлення, яке нібито походило від головного фінансового директора компанії, із проханням про виконання конфіденційної трансакції. Повідомлення виглядало змістовним і відповідало стилю корпоративної комунікації, що знизило рівень підозр [45].

Після отримання такого листа співробітник був запрошений на відеоконференцію з нібито керівництвом компанії. На відео він бачив знайомі обличчя колег, включно з директором, які «розмовляли» із ним у реальному часі. Але згодом з’ясувалося, що й аудіо, й відео у цій конференції були штучно згенеровані за допомогою deepfake-технологій ШІ підозр [46].

Внаслідок цієї маніпуляції співробітник здійснив серію фінансових переказів на загальну суму приблизно 200 мільйонів гонконгських доларів (≈ $25 млн США) на рахунки, що контролювалися зловмисниками. Платежі були розбиті на 15 транзакцій до п’яти різних рахунків, що ускладнило оперативне виявлення шахрайства системами фінансового контролю [45].

Компанія підтвердила, що саме шахрайство не включало технічного зламу її IT-систем: мережне середовище Arup залишилося недоторканим, не було викрадено жодних даних, не виявлено шкідливого ПЗ і не сталося витоку конфіденційної інформації. Усі традиційні цифрові засоби захисту, включно з брандмауерами, автентифікацією та іншими мерами кібербезпеки, працювали штатно [47].

Технічний аналіз інциденту Arup демонструє такі основні особливості:

– відсутність класичного технічного зламу,

– використання легітимних каналів зв'язку,

– застосування deepfake-технологій як технічного інструменту обману,

– обхід фінансового контролю без технічного втручання.

З технічної точки зору інцидент у компанії Arup не відповідав типовому сценарію кіберінциденту, оскільки жодні інформаційні системи, сервери або мережеві компоненти не були зламані. Не зафіксовано проникнення до корпоративної мережі, компрометації облікових записів, експлуатації вразливостей програмного забезпечення або використання шкідливого коду. Це підтверджує, що традиційні засоби технічного захисту, такі як брандмауери, системи виявлення вторгнень і механізми автентифікації, виконували свої функції коректно.

Атака була реалізована через легітимні комунікаційні канали, зокрема електронну пошту та відеоконференції, які є стандартними інструментами корпоративної взаємодії. З технічного боку ці канали не демонстрували ознак компрометації: електронні листи не містили шкідливих вкладень, а відеозв'язок не використовував експлойти чи уразливості програмного забезпечення. Це унеможливило автоматичне виявлення атаки традиційними засобами кіберзахисту, орієнтованими на аналіз трафіку або шкідливого коду [45].

Ключовим технічним елементом атаки стало використання deepfake-технологій, заснованих на алгоритмах машинного навчання та генеративного ШІ. Зловмисники створили реалістичні відео- та аудіомоделі керівників компанії, які імітували зовнішність, голос і манеру мовлення реальних осіб.

Важливо зазначити, що ці технології не атакували інфраструктуру напряму, а лише підвищували правдоподібність соціальної інженерії, виступаючи допоміжним інструментом психологічного впливу.

Фінансові операції були здійснені через стандартні банківські механізми, без злому платіжних систем або втручання в їхню логіку роботи. Технічні системи контролю транзакцій не розпізнали шахрайство, оскільки перекази виконувалися авторизованим співробітником з використанням чинних процедур доступу. Це демонструє обмеженість технічних засобів безпеки у випадках, коли дії виконуються легітимним користувачем у межах наданих повноважень [46].

З технічної точки зору інцидент Arup показує, що високий рівень кіберзахисту не гарантує повної безпеки, якщо атака не націлена на інфраструктуру. Сучасні системи безпеки ефективні проти шкідливого ПЗ, мережевих атак та експлойтів, однак вони практично безсилі перед сценаріями, де технічні механізми використовуються коректно, а зловмисний намір реалізується через маніпуляцію довірою користувача.

Проаналізований інцидент свідчить, що технічні загрози самі по собі дедалі рідше є основною причиною масштабних втрат у сучасних організаціях. У випадку Arup усі ключові технічні компоненти інформаційної безпеки функціонували належним чином, однак атака була успішною через експлуатацію людського фактору – довіри, авторитету керівництва та психологічного тиску.

Таким чином, можна стверджувати, що загрози, спрямовані на людину як елемент системи безпеки, є більш небезпечними, ніж класичні технічні атаки. Технології ШІ лише посилюють цей ризик, оскільки дозволяють створювати переконливі сценарії обману без втручання в ІТ-інфраструктуру. Це зумовлює необхідність переходу від виключно технічного підходу до кібербезпеки до комплексної моделі, яка поєднує технологічні, організаційні та поведінкові заходи захисту.

Arup Global Group – компанія з передовими системами захисту систем ЕК, зазнала багатомільйонних збитків через необачність однієї людини. Цей випадок став важливим прикладом того, що сучасні загрози виходять за межі класичних технічних векторів атак і вимагають комплексних рішень, які включають захист людини як слабкого, так і критичного елементу системи безпеки.

4.2 Рекомендація впровадження принципу нульової довіри в СЕК

В результаті детального аналізу джерел [1 – 47] рекомендується впроваджувати принцип Zero Trust в системах електронної комерції (рис. 4.1).

Рисунок 4.1– Впровадження принципу Zero Trust в СЕК

Інцидент 2024 року у міжнародній інженерній компанії Arup наочно продемонстрував обмеженість традиційних підходів до інформаційної безпеки, що базуються на довірі до внутрішніх користувачів і легітимних бізнес-процесів. Незважаючи на відсутність технічного зламу інфраструктури, зловмисникам вдалося реалізувати масштабне шахрайство шляхом маніпуляції

довірою співробітників, використовуючи легальні канали комунікації та переконливі deepfake-технології. Цей випадок є показовим для систем електронної комерції, де більшість критичних операцій також виконуються авторизованими користувачами.

Принцип Zero Trust, який базується на концепції «never trust, always verify», безпосередньо відповідає викликам, продемонстрованим інцидентом Arup. У контексті СЕК Zero Trust передбачає, що жоден користувач, пристрій або запит не вважається надійним за замовчуванням, навіть якщо він походить з внутрішньої мережі або ініційований співробітником з відповідними повноваженнями. Це дозволяє мінімізувати ризики, пов’язані з соціальною інженерією, коли атака здійснюється не через технічні вразливості, а через обман людини.

У системах електронної комерції впровадження Zero Trust означає постійну перевірку контексту кожної дії: автентичності користувача, стану пристрою, місця доступу та характеру операції. Навіть якщо запит виглядає легітимним, наприклад фінансовий переказ або зміна платіжних реквізитів, він підлягає додатковій верифікації. Такий підхід значно ускладнює реалізацію сценаріїв, подібних до інциденту Arup, оскільки рішення не ґрунтується виключно на авторитеті джерела або посаді користувача.

Інцидент Arup також підкреслює необхідність застосування принципу мінімальних привілеїв, який є одним з ключових елементів Zero Trust. У СЕК це означає, що доступ до платіжних систем, фінансових API та адміністративних функцій має бути суворо обмежений і надаватися лише в межах конкретної бізнес-задачі та на визначений час. Таким чином, навіть у разі успішної соціальної атаки потенційні збитки можуть бути локалізовані й не матимуть системного характеру.

Крім того, Zero Trust передбачає безперервний моніторинг дій користувачів і автоматичне виявлення аномалій, що є критично важливим для СЕК, де фінансові транзакції мають високий ризик зловживань. На відміну від традиційних моделей безпеки, які зосереджуються на периметрі мережі, Zero

Trust дозволяє виявляти підозрілу активність навіть тоді, коли вона виконується з використанням коректних облікових даних. Це безпосередньо відповідає характеру загроз, продемонстрованих у випадку Arup.

Таким чином, інцидент Arup підтверджує, що основною загрозою для сучасних СЕК є не стільки технічна уразливість, скільки зловживання довірою до користувача. У цьому контексті впровадження принципу Zero Trust є навіть не рекомендацією, а об’єктивною необхідністю. Лише модель безпеки, яка системно виключає довіру за замовчуванням і забезпечує постійну верифікацію кожної дії, здатна ефективно протидіяти сучасним атакам, орієнтованим на людину.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було проаналізовано основні загрози безпеці СЕК, а також сучасні технічні та організаційні механізми їх нейтралізації. Проведений аналіз показав, що на сьогодні існує широкий спектр атак, спрямованих як на технічну інфраструктуру СЕК (мережеві атаки, шкідливе ПЗ, компрометація протоколів безпеки), так і на користувачів цих систем шляхом застосування методів соціальної інженерії. Водночас сучасні засоби захисту, зокрема брандмауери нового покоління, криптографічні протоколи, програмні та апаратні механізми безпеки, дозволяють ефективно знижувати ризики технічних загроз.

Разом із тим результати дослідження підтверджують, що навіть за умови високого рівня технічного захисту найбільш уразливим елементом систем електронної комерції залишається людський фактор. Атаки, побудовані на маніпуляції довірою, авторитетом або психологічним тиском, зокрема фішинг, бізнес-email-компрометація та використання технологій deepfake, здатні обходити традиційні механізми захисту без необхідності експлуатації технічних вразливостей. Приклад інциденту 2024 року в компанії Arup наочно демонструє, що критичні наслідки можуть виникати виключно внаслідок помилкових дій легітимних користувачів.

У цьому контексті встановлено, що ефективна протидія загрозам, орієнтованим на людину, неможлива лише за рахунок навчання персоналу або підвищення обізнаності користувачів. Найбільш результативним підходом є впровадження принципу нульової довіри (Zero Trust), який передбачає відмову від довіри за замовчуванням і базується на постійній верифікації кожної дії, запиту та транзакції. Архітектура Zero Trust дозволяє обмежити можливість виконання критичних операцій навіть для авторизованих користувачів без додаткових перевірок і контекстної оцінки ризиків.

Таким чином, у сучасних системах електронної комерції принцип Zero Trust слід розглядати не як окремий інструмент захисту, а як фундаментальну модель побудови безпеки. Саме блокування або обмеження виконання ключових дій без багатоетапної перевірки дозволяє мінімізувати вплив людського фактора та забезпечити стійкість СЕК до сучасних комплексних загроз.

Часткові результати роботи було представлено на 13-тій міжнародній науково-практичній конференції «Проблеми інформатизації» ПІ-2025 та опубліковано тези доповіді [48] за тематикою кваліфікаційної роботи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Dakov S., Malinova A. A Survey Of E-Commerce Security Threats and Solutions. *International Conference On Innovations In Science and Education (Natural Sciences and ict) March 17, 2021, Prague, Czech Republic.* DOI: https://doi.org/10.12955/pns.v2.135.

2. Карабанов Д., Чеботарьова Д. Дослідження засобів безпеки в системах електронної комерції. *Збірник доповідей 28-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». Т.4., Харків, Україна*. Харків: ХНУРЕ, 2024. С. 116 – 117.

3. Царьов Р.Ю. Електронна комерція: навчальний посібник з підготовки бакалаврів / Царьов Р.Ю. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 112 с.

4. Що таке електронна комерція? E-commerce для початківців. *Interkassa*. 20.02.2020. URL: https://interkassa.com/blog/shho-take-elektronna-komerciya-e-commerce-dlya-pochatkivciv.

5. Sen, Sagor, and Charlie Natarajan. Security Analysis for E-Commerce Business. // International journal of progressive research in science and engineering, Vol.3, No.10, October 2022.

6. Kosinski M. What is phishing?. IBM. URL: https://www.ibm.com/think/topics/phishing (дата звернення: 18.12.2025).

7. Драгунцов Р. Фішинг 2.0: як вас зламають і що з цим робити. Порада експерта. *IT specialist.* 27.06.2025. URL: https://my-itspecialist.com/phishing-2-0-zagroza-i-zakhyst.

8. Chheda H. 100+ Latest Social Engineering Statistics: Costs, Trends, AI [2025]. *Sprinto*. 22.08.2025. URL: https://sprinto.com/blog/social-engineering-statistics/.

9. Jennings-Trace E. Most people still can’t identify a phishing attack written by AI - and that’s a huge problem, survey warns. *TechRadar*. 30.09.2025. URL:

https://www.techradar.com/pro/security/most-people-still-cant-identify-a-phishing-attack-written-by-ai-and-thats-a-huge-problem-survey-warns.

10. Khalil M. Phishing Statistics 2025: AI-Driven Attacks, Costs & Trends. *DeepStrike*. 29.04.2025. URL: https://deepstrike.io/blog/Phishing-Statistics-2025.

11. Holdsworth J., Kosinski M. What is pretexting?. *IBM*. URL: https://www.ibm.com/think/topics/pretexting (дата звернення: 18.12.2025).

12. 100+ cybersecurity statistics published in July and August 2025. *Medium. CyberSecStats*. 02.09.2025. URL: https://medium.com/%40laura_80636/ 100-cybersecurity-statistics-published-in-july-and-august-2025-d00173430c65.

13. Holdsworth J., Kosinski M. What is pretexting? *IBM*. URL: https://www.ibm.com/think/topics/pretexting (дата звернення: 18.12.2025).

14. Що таке внутрішня загроза? Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-insider-threat (дата звернення: 18.12.2025).

15. Insider threats: types, warning signs and examples. *Felix Software*. 22.05.2024. URL: https://www.felix.net/blog/insider-threat-cyber-crime.

16. What is an Insider Threat? A Guide for Businesses. *Symbol Security*. 23.09.2025. URL: https://symbolsecurity.com/blog/what-is-an-insider-threat-a-guide-for-businesses.

17. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами: Адміністрація державної служби спеціального зв'язку та захисту інформації України від 29.05.2023, № 463. URL: https://zakon.rada.gov.ua/rada/show/v0463519-23#Text.

18. Найвідоміші вразливості веб застосунків. XSS та SQL ін'єкції, вразливості автентифікації. *DOU. SET University*. 22.10.2025. URL: https://dou.ua/forums/topic/40613/.

19. Understanding Stored XSS: Risks and Prevention. *Legit Security*. 05.05.2025. URL: https://www.legitsecurity.com/aspm-knowledge-base/stored-xss.

20. Cross-site scripting (XSS). *Mozilla Foundation*. URL: https://developer.mozilla.org/en-US/docs/Web/Security/Attacks/XSS (дата звернення: 18.12.2025).

21. SQL injection. *PortSwigger*. URL: https://portswigger.net/web-security/sql-injection (дата звернення: 18.12.2025).

22. SQL Injection. *Black Duck Software*. URL: https://www.blackduck.com/glossary/what-is-sql-injection.html (дата звернення: 18.12.2025).

23. Mohan M. Server vulnerabilities and misconfiguration for sensitive information. *Beagle Security*. 27.05.2024. URL: https://beaglesecurity.com/blog/vulnerability/server-vulnerabilities-misconfiguration-sensitive-information.html.

24. O'Donnell J. Understanding and Detecting Security Misconfigurations. *Cymulate*. 04.11.2025. URL: https://cymulate.com/blog/security-misconfiguration/.

25. Saif Ali. The Hidden Risks of Network Security Misconfigurations: A Practical Guide to Prevention. *Medium*. 19.02.2025. URL: https://medium.com/%40saifaliunity/the-hidden-risks-of-network-security-misconfigurations-a-practical-guide-to-prevention-5a607fca7b3e.

26. Вплив штучного інтелекту на електронну комерцію. *VRESURSI*. 12.12.2024. URL: https://vresursi.com/uk/poradi-uk/vplyv-shtuchnoho-intelektu-na-elektronnu-komertsiyu/.

27. Khalil M. AI Cybersecurity Threats 2025: How to Survive the AI Arms Race. *DeepStrike*. 06.08.2025. URL: https://deepstrike.io/blog/ai-cybersecurity-threats-2025.

28. Ворожко В. Навіть без досвіду кодування. Хакери використовують штучний інтелект ChatGPT для створення вірусів. *Money & Career*. 09.01.2023. URL: https://mc.today/dazhe-bez-opyta-kodirovaniya-hakery-ispolzuyut-iskusstvennyj-intellekt-chatgpt-dlya-sozdaniya-virusov/.

29. Dod R. E-Commerce Website Security: 10 Best Ways to Protect Your Online Store. Chetu Inc. URL: https://www.chetu.com/blogs/retail/10-ways-to-improve-ecommerce-security.php#:~:text=Security%20tips%20to%20protect%20yo

ur%20e%2Dcommerce%20business&text=Encrypt%20your%20entire%20store.,Help%20customers%20be%20more%20secure (дата звернення: 18.12.2025).

30. Жмурко О. Соціальна інженерія як загроза кібербезпеці:методи запобігання та захисту. *Педагогіка безпеки.* 2024. Т. 9. № 1. С. 37 – 42. URL: https://doi.org/10.31649/2524-1079-2024-9-1-037-042.

31. Rose S. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology, 2020. 59 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

32. Zero Trust Guidance Center. *Microsoft.* URL: https://learn.microsoft.com/en-us/security/zero-trust/ (дата звернення: 21.12.2025).

33. Continuous Diagnostics and Mitigation (CDM) Program. An official website of the U.S. Department of Homeland Security. URL: https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program (дата звернення: 21.12.2025).

34. Jain Y. Top Benefits of Electronic Signatures in 2025. *Certinal Inc*. 18.01.2025. URL: https://www.certinal.com/blog/benefits-of-electronic-signatures.

35. Withdrawn NIST Technical Series Publication. Digital Signature Standard (DSS). *Federal Information Processing Standards Publication*. 03.02.2023. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

36. What is a next-generation firewall (NGFW)?. *Cloudflare.* URL: https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/?utm_source=chatgpt.com (дата звернення: 19.12.2025).

37. How Next-Generation Firewalls Strengthen Enterprise Security Posture. *Fortinet.* URL: https://www.fortinet.com/resources/cyberglossary/next-generation-firewall (дата звернення: 21.12.2025).

38. The Transport Layer Security (TLS) Protocol Version 1.3. *Mozilla.* URL: https://datatracker.ietf.org/doc/html/rfc8446 (дата звернення: 18.12.2025).

39. Kent S. Security Architecture for the Internet Protocol. *BBN Technologies*. URL: https://datatracker.ietf.org/doc/html/rfc4301 (дата звернення: 18.12.2025).

40. SSH Protocol – Secure Remote Login and File Transfer. *SSH Academy*. URL: https://www.ssh.com/academy/ssh/protocol (дата звернення: 18.12.2025).

41. What is security information and event management (SIEM)? *IBM*. URL: https://www.ibm.com/think/topics/siem (дата звернення: 18.12.2025).

42. Information Supplement: PCI DSS for Large Organizations. *PCI DSS for Large Organizations.* URL: https://listings.pcisecuritystandards.org/documents/PCI_DSS_for_Large_Organizations_v1.pdf (дата звернення: 18.12.2025).

43. What is a WAF? | Web Application Firewall explained. *Cloudflare*. URL: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/ (дата звернення: 18.12.2025).

44. Hardware Security Modules (HSMs). *Thales*. URL: https://cpl.thalesgroup.com/encryption/hardware-security-modules (дата звернення: 18.12.2025).

45. Young K. Cyber Case Study: $25 Million Deepfake Scam. *Customer Login.* 11.08.2025. URL: https://coverlink.com/case-study/case-study-25-million-deepfake-scam/.

46. The Arup Deepfake Fraud. *PRMIA.* URL: https://prmia.org/common/Uploaded%20files/eCyber/PRMIA%20Case%20study%20-%20ARUP.pdf (дата звернення: 18.12.2025).

47. The Rise of Deepfake Scams: A $25 Million Lesson from Arup . *RealTyme SA.* 01.08.2024. URL: https://www.realtyme.com/blog/the-rise-of-deepfake-scams-a-25-million-lesson-from-arup.

48. Чеботарьова Д.В., Рудак Д.С. Аналіз проблем безпеки в електронній комерції // Тези доповідей тринадцятої міжнародної науково-технічної конференції «Проблеми інформатизації», 27 – 28 листопада 2025 р., Баку – Харків – Бельсько-Бяла. 2025. – Том 2. – С. 84.