ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Удосконалення системи захисту мережевих каналів банківської установи від несанкціонованого доступу до конфіденційної інформації»

на здобуття освітнього ступеня магістра
зі спеціальності __125 __Кібербезпека та захист інформації»_____
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Євген НАГАЄВ

Виконала: здобувачка вищої освіти групи СЗДМ 61
Євген НАГАЄВ

Керівник: ТУРОВСЬКИЙ Олександр
д.т.н., професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Нагаєву Євгену Ігоровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Захист об'єкту банківської діяльності від несанкціонованого доступу до конфіденційної інформації мережевими каналами передачі даних»
керівник кваліфікаційної роботи Олександр ТУРОВСЬКИЙ д.т.н., професор
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: об'єкт банківської діяльності, нормативно-правова документація по розробці та контролю за системою інформаційної безпеки, доступ до систем за допомогою яких забезпечується інформаційна безпека.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1 Особливості функціонування інформаційно-комунікаційної мережі об'єкту банківської діяльності при передачі конфіденційних даних;
4.2 Побудова системи кібербезпеки мережевих каналів передачі інформації об'єкту банківської діяльності;
4.3 Рекомендації по підвищенню рівня захисту ІКМ ОБД в умовах мережевих атак

5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Євген НАГАЄВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олександр ТУРОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 77 сторінок, має 15 рисунків, 1 таблицю, 5 формул, 1 додаток. Список використаних джерел містить 53 найменування і займає 6 сторінок.

Метою кваліфікаційної роботи є підвищення ефективності захисту мережевих каналів банківської установи від несанкціонованого доступу до конфіденційної інформації.

В кваліфікаційній роботі подано особливості роботи інформаційних мереж банківських установ, розкрито елементи побудови системи кібербезпеки мережевих каналів передачі конфіденційних даних, запропоновано рекомендації щодо підвищення рівня захисту комунікаційної мережі в умовах мережевих атак.

Апробація:

Є.В. Бакум, Є.М. Шиньковий, Є.І. Нагаєв. Типи та механізми кібератак на мережеві канали передачі даних об’єктів інформаційної діяльності. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.34-35. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА МЕРЕЖА, ОБ’ЄКТ БАНКІВСЬКОЇ ДЯЛЬНОСТІ, КОНФІДЕНЦІЙНІ ДАНІ, МЕРЕЖЕВІ КАНАЛИ, МЕРЕЖЕВІ АТАКИ

ABSTRACT

The textual part of the qualification work consists of an introduction, three chapters, general conclusions, a list of references, the total volume of the work is 77 pages, has 15 figures, 1 table, 5 formulas, 1 appendix. The list of references includes 53 items and occupies 6 pages.

The purpose of the qualification work is to improve the protection of banking structures from unauthorized access to confidential information transmitted over network transmission channels.

The qualification work presents the peculiarities of the work of information networks of banking institutions, reveals the elements of building a cybersecurity system for network channels for the transmission of confidential data, and offers recommendations for improving the level of protection of the communication network in the face of network attacks.

Keywords: INFORMATION AND COMMUNICATION NETWORK, OBJECT OF BANKING ACTIVITY, CONFIDENTIAL DATA, NETWORK CHANNELS, NETWORK ATTACKS

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

API - Application programming interface (прикладний програмний інтерфейс)

DDoS – Distributed denial-of-service (розподілена відмова у обслуговуванні)

HTTP – Hypertext Transfer Protocol (протокол передачі гіпертексту)

ISO – International Organization for Standardization (Міжнародна організація зі стандартизації)

ML – Machine learning (машинне навчання)

SIEM – Security information and event management (система управління подіями та інформаційною безпекою)

VPN – Virtual private network (віртуальна приватна мережа)

БІС – Банківська інформаційна система

ІКМ – Інформаційно-комунікаційна мережа

КЦД – Конфіденційність, цілісність, доступність

НБУ – Національний банк України

ОБД – Об'єкт банківської діяльності

ПЗ – Програмне забезпечення

СЕМП – Система електронних міжбанківських переказів

СЕП – Система електронних платежів

СТП – Система термінових переказів

ШІ – Штучний інтелект

ШПЗ – Шкідливе програмне забезпечення

ВСТУП

Сьогодні фінансовий сектор вважається однією з найважливіших складових економіки, він забезпечує функціонування банківських систем, управління активами та широкий спектр послуг. Однак розвиток цифрових технологій та збільшення пропускної здатності мережі призвели до нових питань щодо захисту персональної інформації, що є конфіденційною. Особливе значення має питання захисту банківських активів від несанкціонованого доступу через канали передачі даних у мережі.

Значну небезпеку для банків становлять кібератаки, спрямовані на крадіжку фінансової інформації у клієнтів, порушення конфіденційності клієнтів та заподіяння шкоди репутації установи. Статистика свідчить про те, що фінансовий сектор є одним з найбільш вразливих до кібератак, ці атаки можуть призвести до значної фінансової шкоди та втрати довіри клієнтів. У зв'язку з цим створення та впровадження сучасних систем захисту інформації, спрямованих на запобігання викриттю даних, має першорядне значення.

Метою роботи є покращення захисту банківських структур від несанкціонованого доступу до конфіденційної інформації, яка передається мережевими каналами передачі.

У процесі підготовки кваліфікаційної роботи були поставлені наступні **задачі**:

- Вивчити особливості роботи інформаційних мереж банківських установ;
- Розкрити елементи побудови системи кібербезпеки мережевих каналів передачі конфіденційних даних;
- Дослідити та запропонувати рекомендації щодо підвищення рівня захисту комунікаційної мережі в умовах мережевих атак.

Об’єкт дослідження. Інформаційні мережі банківських установ.

Предмет дослідження. Системи кібербезпеки мережевих каналів передачі конфіденційних даних.

РОЗДІЛ 1.
ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ ОБ'ЄКТУ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ ПРИ ПЕРЕДАЧІ КОНФІДЕНЦІЙНИХ ДАНИХ

1.1. Протоколи та формати банківських мереж

1.1.1. Прямі з'єднання між хостами за допомогою H2H

З'єднанн я H2H є основним методом отримання даних рахунків через банківські виписки, що вимагає впровадження інструкцій банку та IT-відділу, здатного підтримувати дані. Ці зв'язки можна встановити за допомогою SFTP-серверів або інших методів, таких як SOAP, FTPS та AS2, які сприяють безпечному, зашифрованому зв'язку між банками та корпораціями. H2H має такі переваги, як прямі та безпечні з'єднання, знижений ризик та точна інформація щодо банківської справи, особливо коли використовується як сервіс для управління фінансами, оплати рахунків та планування грошових потоків. Однак, з'єднання H2H також мають недоліки, включаючи тривалий час налаштування, потенційно високі витрати на впровадження та дорогий процес обробки платежів. Впровадження одного банківського сервера займе приблизно 2-3 місяці, додатковий час потрібен для повного налаштування, якщо задіяно кілька банківських рахунків. Одноразові комісії та щомісячні платежі, що базуються на процесі впровадження, можуть становити всього 100 євро, а процес оплати є дорогим, тому важливо домовитися з банком про нижчу ціну. Публічний прайс-лист на ці послуги недоступний.

1.1.2. Європейський стандарт EBICS

EBICS – це веб-протокол для банківської справи, запроваджений у 2006 році, який широко використовується в Європі. Він сприяє безпечному та ефективному виявленню шахрайства з платежами, а також гарантує точну та актуальну інформацію в програмному забезпеченні ERP або системах управління грошима. Додаткові версії EBICS T та EBICS TS підвищують

безпеку передачі даних, вимагаючи додаткового підпису для схвалення транзакцій. Цей протокол усунув потребу в оформленні документів, підвищив безпеку та майже готовий стати універсальним стандартом банківського спілкування по всій Європі. Основними перевагами EBICS є його доступність, просте впровадження, підтримка кількох банків та децентралізований, безпечний зв'язок. Однак недоліком є наявність кількох локальних варіантів, які мають різні технічні властивості та шифрування. EBICS 3.0 намагається вирішити цю проблему, об'єднавши всі локальні банки в один міжнародний стандарт передачі даних.

1.1.3. Величезна мережа SWIFT

SWIFT, всесвітня мережа банківських послуг, забезпечує прямий доступ до понад 10 000 банків у понад 200 країнах. Вона забезпечує єдиний, безпечний та надійний спосіб зміни банківського партнера без створення нової асоціації. Однак, приєднання до SWIFT є повільним через тривалий процес подання заявки та перевірки, а обсяг оброблюваних даних збільшує витрати. SWIFT зазвичай використовується для зберігання готівки, агрегації банківських виписок та передачі платежів до місцевих та міжнародних установ через систему SWIFTNet.

Здатність вносити готівку в єдиній валюті є значною перевагою системи SWIFT. Ця система дозволяє агрегувати банківські виписки та повну агрегацію коштів, що є основним використанням SWIFT. Хоча транзакції зазвичай здійснюються локально за допомогою регіональних методів зв'язку, звітність інформації відбувається на колективному рівні. Як результат, SWIFT широко використовується для полегшення централізованої банківської звітності.

Основними перевагами використання SWIFT є його задокументована історія, швидка та надійна передача фінансової інформації та глобальний охоплення, що ідеально підходить для міжнародного бізнесу. Основними недоліками є потенційні затримки платежів через посередників, зокрема в

міжнародних транзакціях, високі комісії та високі обмінні курси, що може призвести до проблем з грошовими потоками.

1.1.4. Відкритий банкінг за допомогою PSD2

З'єднання PSD2 походять з Другої директиви про платіжні послуги, яка сприяє концепції відкритого банкінгу, вимагаючи від банків надавати доступ своїм клієнтам через API. Це полегшує контроль над фінансовими даними клієнтів та управління фінансами через третіх сторін, обидві ці функції посилюються двофакторною автентифікацією. Однак API наразі не мають такої ж інформаційної ємності та можливостей звітності, як інші протоколи та мережі, а їх технічна реалізація зазвичай складна через вимоги до сумісності з різними банками. Основними перевагами використання PSD2 є підвищені вимоги до безпеки, поява специфічних фінансових послуг та доступ до банківської інформації в режимі реального часу. Основними недоліками є нижча надійність порівняно з традиційними банківськими протоколами, нижча якість даних та складність впровадження API PSD2. Крім того, PSD2 обмежена банками, які є членами Європейської економічної зони (ЄЕЗ), що ускладнює встановлення зв'язків зі світовими банками.

1.1.5. Формат на вибір: ISO 20022

Коли йдеться про доступність банківських послуг, певні протоколи та мережі мають різні переваги та недоліки. Однак стандарт ISO 20022, який був впроваджений у 2004 році, забезпечує безпечний варіант для корпорацій, що мають багатонаціональний характер [1]. Цей формат XML перевершує традиційний формат MTO за популярністю та використанням, він також визнаний майбутнім банківської справи завдяки високому ступеню стандартизації, що дозволяє підвищити автоматизацію, ефективність та знизити ризики. Незважаючи на переваги стандарту ISO 20022, не всі банки мають час для впровадження варіантів підключення до банківських послуг та роботи з усіма форматами даних, пов'язаними з надсиланням та отриманням банківської

інформації. Як наслідок, вкрай важливо поговорити з представником вашого банку про те, що можливо та необхідно для спілкування з вашим конкретним банком.

1.2. Надійність системи передачі даних на об'єкті банківської діяльності

У статті обговорюється питання 99,999% надійності, яка була знищена 0,001% невеликих пожеж, що призвели до збою платформ Facebook та Yahoo 25 лютого. О 10:00 ранку 25 лютого 2013 року сталася пожежа, в результаті якої було перервано джерело живлення для ремонту обладнання. Аварійне живлення дизельного палива не активувалося через проблеми безпеки та знос обладнання. Конструкція, що сталася в ній, була ключовою для 80% зовнішньої енергоємності Тайваню. Незважаючи на те, що центр комутації мережі мав сертифікат TruSecure, невелика пожежа призвела до виходу з ладу систем живлення, Інтернету, безпеки, пожежної безпеки та кондиціонування повітря будівлі. Це збій тривало 17 годин і мало серйозний вплив на діяльність кількох компаній, включаючи комерційні банки, які здійснюють транзакції в мережі. Ця трагедія чи аварія показує адміністраторам, що безпека має першорядне значення при передачі даних.

Банки, особливо великі, усвідомлюють потенціал таких аварій, як невеликі пожежі, які можуть призвести до збоїв системи. Як наслідок, вищезгаданий приклад демонструє, що навіть якщо вузол (наприклад, центр обробки даних Інтернету (IDC) або відділення банку) є дуже надійним, збій цього вузла може вплинути на нормальне функціонування всієї системи. Важливість якості системи зростає як для компаній, так і для інтернет-провайдерів (ISP). Системні супервайзери намагаються забезпечити як безпеку даних, так і стабільність мережі. Сучасні банки пропонують різноманітні послуги, що зосереджені на електронних платформах для транзакцій, які є безпечними, швидкими, зручними та простими, і не мають обмежень у часі чи відстані. Ці електронні платформи для транзакцій мають менеджерів

управління, особисті фінанси, споживачів та підприємства, а також різні інші електронні фінансові продукти. Ці послуги надаються мережевими банками або мобільними банками. Поточні послуги, що надаються цими фінансовими продуктами, які є диверсифікованими електронними транзакціями, базуються на ступені передачі даних електронними засобами. Коли головний офіс банку передає дані про транзакції до своїх віддалених відділень електронними засобами, їхня система повинна підтримувати постійну пропускну здатність, щоб задовольнити попит кожного відділення за одиницю часу (наприклад, біти за секунду). Пропускна здатність передачі даних – це ймовірність успішної передачі даних від джерела до приймача. Ймовірність того, що система зможе успішно передати певний запит, називається системною надійністю (SR), що є метрикою, що використовується для оцінки передачі даних в угоді про рівень обслуговування (SLA). Системні менеджери часто базують свою політику попиту на попередньому використанні потужності та прогнозованому зростанні попиту, щоб оцінити очікувану потужність. Як наслідок, для оцінки SR спочатку необхідно зрозуміти стан системи.

Практичні системи, такі як Інтернет, транспорт та енергетика, можна розглядати як мережу, що складається з вузлів та ребер. У цьому контексті кожне ребро та вузол мережі можуть мати певну пропускну здатність, і цей тип мережі зазвичай використовується для передачі даних. Багато мереж передачі даних мають компоненти (ребра та вузли), які мають кілька станів. Кожне ребро або вузол може мати різні можливості щодо пропускної здатності, які можуть бути частковими або повними. Цей тип мережі називається стохастичною потоковою мережею (SFN)[4]. Можливо точно описати цей тип мережі та оцінити якість передачі даних. У системному середовищі стан передачі межі може мати кілька станів, а ймовірність кожного стану межі передачі змінюється через збої пристроїв або умови навколишнього середовища. Наприклад, в Інтернеті межа складається з фізичних сегментів, які мають різні рівні пропускної здатності від збою до найвищого рівня роботи. Як

результат, комп'ютерна мережа з такими характеристиками також має стохастичну швидкість потоку, що типово для SFN.

1.3. Тенденції IT-технологій у банківській сфері

Щоб залишатися актуальними, банки повинні використовувати інноваційні технології для покращення взаємодії з клієнтами, зниження витрат та збільшення доходів. Оскільки технології мають значний вплив на майбутнє банківської справи, IT-експерти, менеджери, віце-президенти та директори з інформаційних технологій стикаються з унікальними труднощами у визначенні відповідних рішень для впровадження.

1.3.1. Технічні складності при виборі найкращих технологій для ОБД

Банківська галузь унікальна тим, що їй доводиться мати справу з унікальними технологічними проблемами, які впливають на її діяльність. Орієнтація у величезній кількості технологічних варіантів може бути складною. Вони стикаються з такими труднощами [6]:

Складність

Ландшафт банківських технологій є складним і часто змінюється, що ускладнює вибір відповідних рішень, які відповідають цілям організації.

Ефективність та вартість

Рівновагу між вартістю та ефективністю має першорядне значення. Хоча нові технології можуть здаватися корисними, вартість впровадження та обслуговування необхідно ретельно враховувати.

інтеграція

Банкам важко інтегрувати нові технології з існуючими системами. Безперешкодна інтеграція є важливою для уникнення проблем і забезпечення безперебійної роботи.

Безпека

Поєднання технологічних рішень з конфіденційністю та безпекою даних може бути складним. Кібернетичні загрози мають значний вплив на банківську

галузь. Банки повинні вживати суворих заходів для захисту конфіденційності своїх клієнтів та транзакцій, пов'язаних з фінансами. У дослідженні, проведеному Gartner, 66% IT-директорів визнали кібербезпеку та конфіденційність своїм найбільшим пріоритетом на майбутнє.

Банки підпадають під дію дуже суворого регуляторного середовища, яке вимагає впровадження суворих протоколів та норм безпеки, таких як GDPR та KYC. Банки зобов'язані дотримуватися численних правил та вимог щодо звітності. Запобігання дотриманню вимог законодавства, що постійно змінюються, є специфічним для рішень, спеціально розроблених для задоволення цих конкретних вимог.

Багато банків досі використовують застаріле програмне забезпечення, що створює проблеми під час спроб впровадження сучасних технологій. Модернізація або заміна цих компонентів – це складне завдання, яке ретельно планується.

Банки виробляють великі обсяги інформації. Ефективне управління цією інформацією та її використання для бізнес-аналізу є складним завданням. Розширені інструменти аналітики та управління даними мають вирішальне значення для отримання корисної інформації.

1.3.2. IT-технології, які необхідно мати ОБД

Банківська галузь переживає значні зміни, спричинені технологічним прогресом. Цифровізація, автоматизація та аналіз даних стали важливими напрямками, на яких банки повинні зосередитися, щоб покращити взаємодію з клієнтами, скоротити операції та отримати конкурентну перевагу. Ось загальний опис поточного стану технологій у банківській галузі [6]:

Онлайн-банкінг

Еволюція цифрового банкінгу призвела до зміни способу спілкування клієнтів зі своїми банками. Мобільні банківські додатки, веб-сайти онлайн-банкінгу та функції самообслуговування стали звичайним явищем,

забезпечуючи клієнтам легкість та доступ до своїх рахунків у режимі реального часу.

Автоматизація найвищого ступеня.

Гіперавтоматизація поєднує роботизоване виконання процесів зі штучним інтелектом та машинним навчанням для автоматизації всього складного бізнес-процесу. Банки можуть використовувати гіперавтоматизацію для автоматизації буденних та формальних завдань, таких як введення даних, обробка документів та реєстрація клієнтів. Автоматизуючи ці процеси, банки можуть зменшити кількість помилок, підвищити ефективність роботи та звільнити співробітників, щоб вони могли зосередитися на важливіших видах діяльності.

Створення з низьким кодом

Платформи з низьким кодом для розробки дозволяють банкам створювати додатки, які потребують мінімального кодування. Ця платформа сприяє прискоренню розробки та зменшує потребу в традиційних методах. Ці платформи забезпечують візуальні інтерфейси, попередньо розроблені шаблони та можливості перетягування елементів, які мають як технічний, так і нетехнічний характер. Ці платформи можуть використовуватися як технічними, так і нетехнічними учасниками розробки додатків. Банки можуть використовувати методи розробки з низьким кодом для створення власних додатків, які швидко створюються, спрощують внутрішні процеси та забезпечують передовий клієнтський досвід.

• Інтелектуальний інтелект (ШІ) та навчальний інтелект (МН)

Банки все частіше використовують ШІ та машинне навчання для підвищення ефективності операцій, розпізнавання шахрайства та ефективнішої взаємодії з клієнтами. Чат-боти на базі ШІ та віртуальні помічники використовуються для надання індивідуальної допомоги та керівництва. Поєднання ШІ з великими наборами даних дозволяє нам отримувати важливу інформацію для оцінки ризиків та сегментації клієнтів.

• Автоматизація роботизованих процесів

RPA набув популярності в банківській галузі, він автоматизує рутинні адміністративні завдання та підвищує операційну ефективність. Використовуючи програмних роботів для автоматизації таких процесів, як реєстрація клієнтів, введення даних та перевірка відповідності, банки можуть зменшити кількість помилок, одночасно підвищуючи продуктивність.

• Автоматизоване проектування

Банки використовують хмарні обчислення для зменшення витрат, пов'язаних з інфраструктурою, підвищення ефективності та спрощення швидкої доставки додатків. Хмарні рішення сприяють покращеному захисту даних, гнучкості та інтеграції з іншими системами, що дозволяє банкам швидко впроваджувати нові послуги та впроваджувати інновації.

Технологія блокчейн

Блокчейн став значною силою в банківській галузі, яка змінила спосіб здійснення платежів через кордони, фінанси та перевірку особи. Його децентралізований та безпечний характер може сприяти оптимізації процесів, зниженню витрат та підвищенню прозорості транзакцій.

Аналіз даних та великі дані

Банки використовують технології аналізу даних та великих даних для отримання корисної інформації з величезної кількості даних, пов'язаних з клієнтами. Використовуючи аналітику даних, банки можуть краще розуміти поведінку клієнтів, персоналізувати свої пропозиції та приймати рішення на основі даних, що знижують ризики та покращують операції.

Кібербезпека та запобігання шахрайству

Зі зростанням поширеності цифровізації в банківських послугах, кібербезпека та запобігання шахрайству стали важливими питаннями. Банки присвячують себе розробці передових технологій кібербезпеки, включаючи виявлення загроз, шифрування та біометричну автентифікацію. Ці технології використовуються для захисту даних клієнтів та запобігання виникненню нових небезпек.

Інтернет речей (IoT)

Технології IoT сприяють об'єднанню фізичних об'єктів та пристроїв, ці технології дозволяють колективне та спільне зберігання даних. IoT може бути використаний у банківській галузі для різних цілей, включаючи дистанційний моніторинг активів, миттєве виявлення шахрайства та персоналізований досвід для клієнтів. Наприклад, банки можуть використовувати пристрої IoT для спостереження за банкоматами, контролю рівня запасів та надання індивідуальних пропозицій, що базуються на місцезнаходженні клієнта та його уподобаннях.

Розробка та автоматизація

Методи DevOps поєднують розробку програмного забезпечення з інформаційними технологіями для забезпечення постійної інтеграції, постійної доставки та швидкого впровадження додатків. Дотримуючись методу DevOps, банки можуть скоротити час, необхідний для виведення нових послуг на ринок, посилити співпрацю між командами розробки та операцій, а також покращити загальну якість та узгодженість своїх додатків. Інструменти автоматизації сприяють швидшому прогресу процесів розробки та розповсюдження, що дозволяє банкам досягти вищого рівня операційної ефективності.

1.4. Призначення банківських інформаційних систем

Банківська інформаційна система (БІС) – це система всередині банку, яка спрощує введення, обробку, зберігання та передачу даних для досягнення основних цілей управління банківською установою.

Інформаційна система банку повинна сприяти інтеграції всіх відділів в єдину інформаційну платформу та аналітичні інструменти. Це полегшує доступ до інформації для користувачів, від клієнтів до фінансового менеджменту, в межах їхніх прав доступу до інформації, вони можуть швидко, легко та без перешкод отримувати всю інформацію щодо всіх фінансів, позабюджетних рахунків та історичних даних.

Програмне забезпечення має сприяти розвитку банку, збору та аналізу інформації щодо клієнтів та транзакцій, підтримці безпеки системи, проведенню фінансових операцій, оновленню процентних ставок та обмінних курсів. Крім того, система повинна сприяти прийняттю рішень щодо управління, модернізації правил проведення операцій, включаючи використання кредитів, облігацій, ринку капіталу та міжнародних платежів.

Банківська система повинна враховувати доходи та витрати, створювати баланс, який відповідає вимогам Національного банку, та займатися міжнародним аудитом. Для успішного функціонування та розвитку банку система повинна сприяти всім аспектам діяльності, пов'язаної з валютою, а також реалізовувати додаткові функції, такі як документування акредитивів, дистанційне виконання транзакцій, управління запасами та інвестиціями. Як результат, банківська інформаційна система повинна вирішувати широкий спектр питань, вона є критично важливою для діяльності банку. Вона повинна задовольняти потреби клієнтів, бути гнучкою, мати кілька валютних опцій, бути ефективною та інтегрованою.

Згідно з визначенням банківської інформаційної системи (БІС), можна виділити різні класи завдань.

Це:

• оплата клієнтам, отримання інформації про них та виконання договорів в організації• обробка даних, включаючи виконання фінансових операцій, нарахування відсотків, оплату послуг, розрахунок залишків на рахунках тощо;

довгострокове зберігання всієї фінансової інформації;

Процес передачі платіжних даних до електронних платіжних систем або інших платіжних сервісів, а також надсилання фінансової та статистичної інформації до відділень НБУ називається передачею платіжних даних.

Основні можливості BIS, засновані на сучасних мережевих технологіях, включають використання електронної пошти, баз даних на базі клієнт/сервер, віддалений доступ до мережевих ресурсів, підтримку роботи мережі банкоматів та додаткові функції.

1.5. Технологічні режими опрацювання банківської інформації

Найпоширенішими методами обробки економічної інформації, як правило, є пакетні та інтерактивні. Сама технологія, як наслідок, може включати обробку даних у режимі реального часу. Далі ми обговоримо переваги роботи з банківською інформацією таким чином.

Метод пакетної обробки стосується обробки та передачі партії платіжних доручень. Лише остаточне завершення кількох складних операцій документується на рахунках клієнтів після визначеного періоду. При такому підході окремі доручення накопичуються, об'єднуються в партії та обробляються з певною частотою.

Цей метод зазвичай використовується для роздрібних транзакцій, які потребують великої кількості транзакцій на невеликі суми. Системи, що обробляють платежі, пов'язані з роздрібними транзакціями, відрізняються своєю здатністю обробляти великі обсяги транзакцій за розумний проміжок часу з невеликими витратами, зберігаючи при цьому базовий рівень надійності. Крім того, вимоги до систем зв'язку та обробки даних все ще відносно низькі, що дозволяє обробляти операції партіями та мати встановлений час для цього.

В інтерактивній обробці кожен платіж передбачає надсилання спеціального повідомлення на рахунок клієнта, яке супроводжує транзакцію, та одночасний переказ коштів, цей процес гарантує потік відповідної інформації про транзакції.

Для реалізації інтерактивного методу необхідно розробити систему комунікацій та обміну даними. У режимі реального часу платіжні доручення оцінюються та виконуються на основі їхнього порядку надходження. Цей метод вимагає використання сучасних, високоефективних та надійних систем зв'язку, а також потужної обчислювальної інфраструктури.

1.6. Характеристика механізмів міжбанківських переказів

Загальні вимоги до функціонування міжбанківських платіжних систем та систем переказу грошей в Україні викладені в Інструкції про перекази грошей в Україні, яка була затверджена постановою Правління НБУ від 17 березня 2004 року № 110 [8].

Міжбанківський переказ – це обмін грошима між різними банками в безготівковій формі, оскільки необхідність погашення боргів клієнтів або виконання інших банківських зобов'язань вимагає переказу грошей. Єдиним компонентом електронних платіжних документів, який може бути отриманий з банківських інформаційних систем, є процес оплати.

Процес функціонування міжбанківської платіжної системи, визначений платіжною організацією, а також методи документування та обробки платежів повинні забезпечувати безпеку та конфіденційність даних, своєчасне виконання щоденних завдань, високий ступінь безпеки та надійності, а також їх відновлення у разі збоїв або надзвичайних ситуацій.

Система електронних міжбанківських переказів Національного банку України (СЕМП) – це система, що включає цифрову платіжну систему (ЦПС) та систему швидких переказів (СШП), остання координується системою технічного управління рахунками.

Технологія, що використовується для роботи EITS, визначається Національним банком, а учасники зобов'язані дотримуватися встановленого протоколу щодо роботи. Міжбанківські транзакції через EITS здійснюються за допомогою криптографічних методів захисту інформації, які є частиною апаратних та програмних компонентів EITS та надаються Національним банком.

EITS пропагує метод переказу кількох валют, цей метод забезпечує передачу та зберігання даних щодо платежів у різних валютах з однаковою обчислювальною потужністю та технологією обробки.

Крім того, EITS має систему отримання інформації (IRS), яка дозволяє дізнаватися про хід платежів, та систему резервного копіювання та відновлення, яка забезпечує відновлення функціональності EITS у разі збоїв або надзвичайних ситуацій.

З точки зору безпеки та функціональності, NBUSEM є однією з найефективніших платіжних систем у світі, не поступаючись провідним аналогам. Завдяки своїй ефективності та надійності, SEMP дозволяє банкам здійснювати миттєві платежі між установами, що гарантує, що їхні кредитні кошти будуть негайно перераховані на рахунки інших банків-учасників.

1.7. Типи конфіденційних даних в банківській мережі

Банківська мережа вразлива до ризиків інформаційної безпеки через обсяг конфіденційної персональної інформації. Дані, що циркулюють у банківських інформаційних системах, можна класифікувати за ступенем їхньої конфіденційності та метою, для якої вони використовуються.

1) Персональні дані клієнтів.

Персональні дані є основою будь-якої банківської інформаційної системи. Ця категорія є частиною 9-го видання DSM, яке вийшло у 2019 році.

Прізвище та ім'я,

Дата та місце народження;

Зберігаються персональні дані про паспорт або інші документи, що ідентифікують власника.

Контактна інформація (телефон, адреса, електронна пошта).

Рівень секретності: високий, оскільки несанкціонований доступ до даних може призвести до крадіжки особистих даних або фінансових шахрайств [10].

2) Грошова інформація

Цей клас включає інформацію про банківські рахунки та транзакції:

• Номери рахунків, пов'язані з банківськими картками,

Інформація про кредитні та дебетові картки (номер картки, код CVV, дата закінчення терміну дії);

Історія транзакцій;

Загальна сума грошей на вашому рахунку.

Рівень конфіденційності: надзвичайно високий, оскільки розголошення цієї інформації може призвести до значних фінансових збитків [10].

Дані про операції клієнтів

Це дані про фінанси клієнтів:

Інформація щодо позик (термін, сума, графік платежів);

• Ділова діяльність, що передбачає інвестиції,

Інші фінансові послуги, такі як позики, облігації, банкноти та валюта.

Рівень конфіденційності: високий, оскільки розголошення цієї інформації може негативно вплинути на репутацію клієнта або призвести до фінансових ризиків [10].

4) Інформація про співробітників щодо банку.

Інша конфіденційна інформація про співробітників міститься в банківських інформаційних системах, ця інформація не є загальнодоступною, як зазначено в пункті 9.

Персональні дані співробітників подібні до даних клієнтів і також зберігаються в системах компанії.

Інформація щодо посад, зарплат та графіків;

Інформація щодо доступу до інформаційних систем та рівня привілеїв.

Рівень конфіденційності: середній, але чутливість цієї інформації може призвести до внутрішніх небезпек або порушень трудових прав [10].

Комерційні та операційні деталі

Цей клас внутрішніх даних важливий для роботи банку:

• Бізнес-планування та економічний аналіз;

Інформація як про партнерів, так і про опонентів;

Інформація щодо внутрішніх систем безпеки.

Технічні дані, такі як паролі сервера та архітектура IT-інфраструктури, не є приватними.

Рівень конфіденційності: змінний – залежить від конкретного типу інформації. Технічні специфікації або стратегічні плани щодо безпеки мають високий ступінь секретності [10].

6) Інформація щодо регулювання

Цей клас даних стосується нормативних вимог:

Звіти для відповідальних осіб;

Інформація щодо підозрілих фінансових операцій (AML – боротьба з відмиванням грошей);

Інформація для податкових службовців.

Рівень конфіденційності: високий, оскільки розголошення цієї інформації може призвести до юридичних наслідків або санкцій на розсуд банку [10].

Технічна інформація

Це інформація щодо роботи IT-систем банку:[11]:

Системні журнали.

Дані, пов’язані з мережевим підключенням;

Сервер та база даних є важливими компонентами програмного забезпечення.

Рівень конфіденційності: середній, але розголошення цієї інформації може надати зловмисникам можливість отримати доступ до важливих систем.

1.8. Висновки до першого розділу

У цьому розділі описано фундаментальні принципи того, як інформаційна система та система зв'язку фінансової установи здійснюють передачу конфіденційних даних. Атрибути цих мереж були ретельно досліджені з метою визначення ключових цілей управління інформацією та безпеки, які потім використовувалися для підтримки стабільності фінансових установ.

Було виявлено, що основними характеристиками мережевих банківських систем є висока швидкість передачі даних, використання різних протоколів зв'язку та необхідність швидкого доступу до інформації для клієнтів та внутрішніх співробітників. Особлива увага була приділена розпізнаванню потенційних небезпек під час обробки або передачі важливої інформації.

Таким чином, інформаційна система та система зв'язку банківської організації є складними та багаторівневими, що вимагає цілісного підходу до її захисту. Результати цього розділу забезпечать основу для додаткового аналізу ризиків та створення стратегій збереження конфіденційних даних під час виконання обов'язків.

Розділ 2.
СИСТЕМА КІБЕРБЕЗПЕКИ МЕРЕЖЕВИХ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ ОБ'ЄКТУ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

2.1. Аналіз архітектури кібербезпеки

Раніше ізольовані системи тепер з'єднані та обмінюються інформацією. Меллер [13] стверджує, що цей зв'язок також має негативні наслідки, оскільки щоразу, коли пристрій підключається до Інтернету, він стає загальнодоступним. Після ідентифікації цих пристроїв вони стають вразливими до кібератак. Кібербезпека стала звичайною частиною повсякденного життя, оскільки частота та серйозність кібератак зросли. Експертам з кібербезпеки важко виміряти успіх тактик кібербезпеки в організаціях. Ще однією перешкодою є пошук ефективної архітектури кібербезпеки, яка є ефективною та може бути адаптована до різних ситуацій. У цій частині проекту буде обговорено створення комплексної архітектури кібербезпеки, яку можуть використовувати фахівці з кібербезпеки для оцінки ефективності своєї кібербезпеки. Також буде надано загальний опис архітектур кібербезпеки, а потім методологію дослідження. Потім буде пояснено запропоновану архітектуру кібербезпеки, а потім буде поставлено питання.

2.1.1. Огляд архітектур кібербезпеки

Архітектура кібербезпеки складається з кількох окремих доменів, присвячених кібербезпеці. Різні домени, що складають кібербезпеку, часто називають категоріями. Інші можуть називатися областями контролю або доменами можливостей [13]. Коли ми обговорюємо домени кібербезпеки, ми конкретно маємо на увазі конкретну галузь кібербезпеки, яка розглядається. Коротко кажучи, домен – це певний сектор або жанр фокусу, це особливо актуально в кібербезпеці. Коли різні домени кібербезпеки об'єднуються, формується архітектура кібербезпеки. Організації та структури кібербезпеки

мають різні визначення доменів. Ідея архітектури кібербезпеки є складною, і кожна концепція має свою мету та силу. Кілька ідей щодо архітектури кібербезпеки є популярними, але найпоширенішими є NIST Framework, архітектура з відкритим кодом та Міжнародний консорціум сертифікації безпеки інформаційних систем, також відомий як (ISC)2.

Деякі з цих архітектур кібербезпеки є додатковими та можуть мати спільні функції. Безпека програми, фізична безпека програми, ризик програми та розвідка загрози – все це спільні області кібербезпеки. У таблиці 2.1 нижче наведено деякі поширені схеми кібербезпеки.

Таблиця 2.1. Домени кібербезпеки

Домени можливостей NIST	**Сертифікація CISSP**	**Сертифікація GSEC**	**Архітектура з відкритим кодом**	**Розшифрована зона**
Контроль доступу	Безпека та управління ризиками	Активна оборона	Шаблони безпеки IT-послуг	Безпека мережі
Оцінка безпеки	Безпека активів	Криптографія	IT шаблони рівня додатків	Хмарна безпека
Обізнаність і навчання	Інженерія безпеки	Захищена мережева архітектура	Шаблони IT-інфраструктури	Безпека програми
Управління ризиками	Комунікаційна та мережева безпека	Обробка інцидентів і реагування	Центральна служба безпеки	Безпека критичної інфраструктури
Ситуаційна обізнаність	Керування ідентифікацією та доступом	Безпека Linux	Управління	Безпека кінцевого користувача
Управління активами	Оцінка безпеки та тестування	Політика безпеки		Аварійне відновлення
Захист медіа	Операції безпеки	Безпека веб-підключень		Інформаційна безпека
Технічне обслуговування	Безпека розробки ПЗ			Безпека зберігання
Персональна безпека				Мобільна безпека
Аудит та звітність				
Захист системи та зв'язку				
Ідентифікація та автентифікація				

Складність полягає у створенні ефективної та специфічної для унікальної ситуації організації системи кібербезпеки. Друга складність, пов'язана з фахівцями та менеджерами з кібербезпеки, полягає у створенні найефективнішої архітектури кібербезпеки з численних варіантів.

2.1.2. Приклад архітектури кібербезпеки

Рішення з кібербезпеки повинні враховувати кожен крок з конкретним рішенням, зберігаючи при цьому підхід, орієнтований на безпеку. Повного розуміння ландшафту кібербезпеки більше недостатньо. Це складна мережа з кількох рівнів заходів безпеки, які об'єднані, щоб утворити єдиний домен кібербезпеки. Домени кібербезпеки – це термін, що описує різні сфери, в яких практикується кібербезпека. Кожен аспект кіберпростору становить унікальну загрозу безпеці та потребує уваги. Щоб забезпечити кібербезпеку, організації повинні розуміти та запобігати потенційним небезпекам, пов'язаним з кожним піддоменом. Цілісний підхід до інформаційної безпеки в організаціях дозволяє фахівцям з кібербезпеки використовувати різні методи для різних частин кібердомену.

Спільні зусилля є важливими для підтримки здорового стану кібербезпеки, оскільки активи організації складаються з різних цифрових платформ. Сукупність інструментів кібербезпеки, що використовуються для захисту системи, називається доменом кібербезпеки.

Запропонована архітектура кібербезпеки використовує структуру NIST (ідентифікувати, захищати, виявляти, реагувати, відновлювати), відому як "GOALS", основу архітектури складають три стовпи CCD (конфіденційність, цілісність, доступність). 2.1 та рис. 2.2.

Рис. 2.1 - Запропонована комплексна архітектура кібербезпеки

Рис. 2.2 – Структура NIST

2.1.3. Обговорення запропонованої архітектури кібербезпеки

Тут буде пояснено запропоновану архітектуру кібербезпеки та розглянуто кожен компонент запропонованої архітектури. Пояснено п'ять функцій NIST, а потім тріаду CCD та дев'ять доменів кібербезпеки.

2.1.3.1. Цілі NIST

Національний інститут стандартів і технологій (NIST) є всесвітньо визнаною системою для найкращих практик інформаційної безпеки [16]. Система інформаційної безпеки NIST – це набір стандартів і практик, призначених для застосування в галузі. Система NIST складається з п'яти функцій, які діють у поєднанні та послідовно 13. У поєднанні ці функції

пропонують комплексний та стратегічний підхід до управління ризиками кібербезпеки. Система інформаційної безпеки NIST складається з п'яти різних можливостей/цілей:

• Відстеження: стосується методів відстеження кожного IT-ресурсу в організації.

• Збереження: стосується методів, що використовуються для збереження всіх ідентифікованих активів [18];

• Виявлення: стосується інструментів, які використовуються для спостереження за організацією та ідентифікації винних у атаці [13];

Реагування: стосується автоматизованих інструментів, які розпізнають інциденти та спрямовують запити відповідно до їх пріоритету.

• Відновлення: стосується відновлення нормальної роботи після кібератаки [19].

2.1.3.2. Тріада КЦД

Тріада CCS, що складається з трьох стовпів інформаційної безпеки, покликана забезпечити конфіденційність, відшкодування збитків та доступність. Слова «конфіденційність», «цілісність» та «доступність» зазвичай використовуються в галузі інформаційної безпеки та в академічній літературі для оцінки та проектування інформаційних систем. Ці слова також широко використовуються в юридичній сфері. Тріада CCS досі має значний вплив на практику інформаційної безпеки, оскільки вона вказує на фундаментальні компоненти безпеки в інформаційних системах. По суті, це означає, що надійна система інформаційної безпеки повинна зберігати конфіденційність, цілісність та доступність. Тріада CCS призвела не лише до теоретичного розуміння інформаційної безпеки, але й до практичних методів, що використовуються для впровадження безпеки в організаціях. [22]. Нижче наведено описи кожного компонента інформаційної безпеки:

• Секретність: Вона стосується захисту інформації від випадкового або ненавмисного розголошення.

Цілісність: Це запобігання незаконним змінам або знищенню інформації [22].

Доступність: Це доступність даних та інформації, коли вони потрібні цільовим сторонам.

2.1.3.3. Домени кібербезпеки

Останнім компонентом запропонованої архітектури кібербезпеки є дев'ять доменів кібербезпеки. Кожен домен повинен відповідати вимогам конфіденційності, цілісності та доступності, а також п'яти цілям NIST (ідентифікувати, захищати, виявляти, реагувати та відновлювати).

Безпека додатків та систем: це включає додавання функцій безпеки до додатків, які запобігають кібератакам та забезпечують їхню безпеку. Збереження безпеки існуючого програмного забезпечення та додатків і запобігання загрозам на етапі розробки додатків. Це сприяє організаціям у створенні кількох рівнів безпеки програмного забезпечення та будь-якої пов'язаної з ним інформації, крім того, це обмежує небажані зміни інформації в програмному забезпеченні.

Інформаційна безпека: ця галузь захищає всі типи даних від несанкціонованого доступу та запобігає будь-яким змінам, модифікаціям, розголошенням або видаленню. Вона захищає критично важливу бізнес-інформацію та гарантує безпеку даних [24].

Мережева безпека: включає захист комп'ютерних мереж та ресурсів, доступних через мережу, від несанкціонованого вторгнення та зміни. Мережева безпека включає поєднання тактик, інструментів та процесів, які оберігають мережу від вторгнення.

Безпека кінцевих точок: вона захищає пристрої кінцевих користувачів, такі як настільні комп'ютери, ноутбуки, мобільні телефони та планшети, від зловмисного вторгнення та кіберзагроз. Це включає моніторинг усіх пристроїв у мережі на наявність небезпек, порушень та підозрілої поведінки [24].

Безпека критичної інфраструктури: вона стосується захисту інфраструктури; якщо цього бракує, безпека країни буде під загрозою. Вона складається з кібер- та фізичних систем, які є важливими для кібербезпеки. Безпека кіберпростору організації може бути гарантована, коли фізичні активи компанії захищені [25].

Управління, ризики та відповідність: це створення та розробка політик компанії щодо внутрішньої та зовнішньої безпеки. План організації щодо вирішення потенційних та реальних кібернегроз. Це включає створення превентивних та відновлювальних систем для вирішення та управління потенційними кібернегрозами.

Мобільна безпека: захист мобільних пристроїв або планшетів від будь-яких шкідливих атак, втрати даних або втрати активів. Зі зростанням поширеності мобільних технологій вони стали важливим компонентом кібербезпеки.

Безпека кінцевих користувачів: навчання співробітників та широкої громадськості щодо небезпеки кіберзлочинності та передового досвіду галузі має вирішальне значення, поряд із захистом від загроз соціальної інженерії. Це або запобіжить насильству, або дозволить людям самостійно розпізнавати небезпеки [27].

Безпека хмари: Захищає інфраструктуру, середовища, програми та дані хмари від шкоди. Це сприяє автентифікації користувачів та захисту конфіденційності даних як для кінцевого користувача, так і для самого пристрою [27].

2.1.3.4. Переваги запропонованої архітектури кібербезпеки

Фахівці з кібербезпеки повинні представляти дані про кібербезпеку таким чином, щоб це задовольняло цікавість керівників, призводило до практичних результатів, було простим для розуміння та практичним. Переваги запропонованої архітектури кібербезпеки включають:

• комплексна структура кібербезпеки: запропонована архітектура кібербезпеки є гібридом кількох систем кібербезпеки, які об'єднані для підвищення їхньої ефективності та результативності.

• забезпечує повний огляд організації: запропонована архітектура кібербезпеки дозволяє одночасно реагувати на кілька рівнів кібератак;

• запропонована архітектура кібербезпеки сприяє кращому контролю над середовищем: вона дозволяє визначити ступінь, до якої ви готові прийняти ризик та контролювати його.

• контекстуалізує рішення з кібербезпеки: залежно від ситуації та цілей середовища, домени можуть бути включені або видалені з запропонованої архітектури кібербезпеки. Однак деякі компанії мають більш передові технології, ніж інші.

Фахівці з безпеки повинні ретельно вибирати найбільш релевантні показники для звітування перед бізнес-виборцями. Вкрай важливо повідомляти про результати рішень щодо кібербезпеки та їхній вплив на активи, операції та репутацію організації. Ви можете поєднувати як кількісні, так і якісні показники, включаючи ключові показники ефективності (KPI), ключові показники ризику (KRI), повернення інвестицій (ROI), вартість ризику (COR), задоволеність клієнтів та відгуки зацікавлених сторін.

2.2. Концепція для моделювання завадостійкої передачі цифрових даних

Перешкоди, що перешкоджають цілісності та конфіденційності передачі інформації, бувають як природними, так і штучними. Штучні бар'єри зазвичай виникають внаслідок втручання злочинців у процес передачі даних. Природні бар'єри виникають через ослаблення сигналу під час передачі, помилки кодування або інші природні причини. Проблеми з безпечною передачею цифрової інформації можуть бути спричинені різноманітними небезпеками, слабкими місцями та технічними несправностями.

Зловмисники використовують збої програмного забезпечення або мережі, щоб отримати несанкціонований доступ до інформації. Фішинг – це форма кібершахрайства, яка передбачає обман, щоб обманом змусити користувачів поділитися секретною інформацією, такою як паролі чи фінансова інформація. Шкідливе програмне забезпечення, таке як віруси, трояни та руткіти, може знищити або викрасти інформацію. Програми-вимагачі запобігають доступу до даних і вимагають плату за їх відновлення. Атаки «людина посередині», які характеризуються тим, що зловмисник контролює дані, що передаються між сторонами, або прослуховує незашифровані повідомлення.

В результаті технічні невизначеності та навмисні дії зловмисника сприяють створенню перешкод, що перешкоджають передачі інформації.

Технічні проблеми та прогалини можуть значно вплинути на безпеку передачі даних. Ключовими причинами цих проблем є використання незашифрованих посилань, погані або застарілі алгоритми шифрування, недостатня перевірка та авторизація, а також недоліки програмного чи апаратного забезпечення. Незашифровані посилання, такі як ті, що використовуються в HTTP замість HTTPS, дозволяють хакерам отримати доступ до даних. Пошкоджені або застарілі алгоритми, такі як MD5 або SHA-1, легко зламати, що дозволяє отримати доступ до секретної інформації. Помилка автентифікації або відсутність авторизації призводить до несанкціонованого доступу до системи. Крім того, помилки та експлойти в програмному чи апаратному забезпеченні можуть бути використані для злому системи та отримання інформації.

Іншими важливими факторами забезпечення безпеки даних є організаційні та людські. Відсутність достатньої підготовки та обізнаності користувачів щодо питань безпеки може призвести до серйозних помилок, таких як використання слабких паролів або відкриття страшних електронних листів. Ігнорування безпечних політик, таких як зберігання даних небезпечним способом або їх передача через небезпечний канал, також несе ризик. Дії

співробітників, які є навмисними або випадковими, а також ті, що є зловмисними, становлять окрему загрозу.

Крім того, природні та техногенні фактори впливають на безпеку передачі даних. Відключення електроенергії часто призводить до втрати інформації або руйнування обладнання. Стихійні лиха, такі як пожежі, повені чи землетруси, можуть негативно вплинути на фізичну інфраструктуру, яка використовується для зберігання або передачі інформації. Також вихід з ладу критично важливого обладнання, такого як сервери чи мережеві компоненти, може призвести до втрати даних або порушення процесу передачі. Природні перешкоди, такі як втрата сигналу, магнітні перешкоди, пошкодження бітів або фазовий зсув, можуть негативно вплинути на якість передачі даних.

Щоб запобігти цьому, використовуються різні методи, спрямовані на забезпечення безпеки передачі та зберігання даних. Серед основних дій:

Шифрування даних. Використання сучасних алгоритмів шифрування для захисту інформації як під час передачі, так і під час її зберігання;

Постійні оновлення програмного забезпечення. Встановлення нових патчів та оновлень, що усувають існуючі недоліки;

Двоетапна автентифікація. Вищий ступінь безпеки під час входу в систему за допомогою кількох методів перевірки особи;

Навчання та навчання користувачів. Постійно навчайте своїх співробітників передовим практикам у сфері кібербезпеки;

Використання VPN. Безпечні канали передачі даних, які створюють безпечний прохід для зв'язку через незахищену мережу.

Завадостійке кодування. Використання кодів з додатковою надмірністю, що дозволяє виправляти недоліки фізичних каналів зв'язку.

Використання цих заходів має значний вплив на зниження ймовірності кібератак та забезпечує передачу цифрових даних у різних ситуаціях з високим ступенем довіри.

2.2.1. Верхній рівень концепції

Оскільки конфіденційність, цілісність та доступність інформації можуть бути під загрозою на різних етапах передачі даних, необхідний комплексний підхід до захисту, який охоплює кожен рівень передачі даних. Загальна модель OSI може служити орієнтиром для визначення цих методів.

Одним із ефективних методів захисту конфіденційності є використання VPN (віртуальних приватних мереж). VPN пропонують приватний, безпечний доступ до мережі через зашифрований канал між пристроєм користувача та віддаленим сервером.

Основні принципи роботи VPN:

Шифрування трафіку. VPN використовують сучасні протоколи шифрування (наприклад, OpenVPN, IKEv2 та IPSec), які запобігають перехопленню даних.

Розподіл трафіку. Трафік користувача потім перенаправляється через VPN-сервер, який функціонує як посередник між користувачем та Інтернетом. Цей сервер приховує справжню IP-адресу.

Адресація IP-адреси. VPN змінюють IP-адресу користувача на адресу VPN-сервера, що забезпечує анонімність та дозволяє обійти географічні обмеження доступу до контенту.

Автентифікація. VPN використовують різні засоби автентифікації, включаючи пароль та двофакторну автентифікацію, або цифрові сертифікати, для автентифікації користувача.

Продуктивність VPN оцінюється за кількома показниками, зокрема швидкістю їхніх з’єднань. Швидкість вимірюється різницею між пропускною здатністю мережі без активованої VPN та з нею.

$$\Delta V = (\frac{V - V_{VPN}}{V})\text{X}100\,, \tag{1}$$

де ΔV – зниження швидкості (%);

V – швидкість без VPN;

V_{VPN} – швидкість з VPN.

Затримка вимірюється як час (у мілісекундах), який потрібен для передачі даних від користувача до сервера і у зворотному напрямку [30]:

$$D = \left(\frac{t_f - t_b}{2}\right), \quad (2)$$

де D – затримка;

t_f – це час передачі даних до сервера;

t_b – це час повернення даних.

Надійність підключення вимірюється як кількість успішних підключень до VPN-сервера без розривів [30]

$$R = \left(\frac{C_S}{C_O}\right), \quad (3)$$

де R – надійність (%);

C_S – кількість успішних підключень;

C_O – кількість спроб підключень.

Час підключення вимірюється як середній час, необхідний для встановлення VPN-з'єднання [30].

$$T_{ca} = \left(\frac{t_c}{C_O}\right), \quad (4)$$

де T_{ca} – середній час підключення;

t_c – загальний час підключення.

Ефективність шифрування залежить від ступеня захисту даних, наприклад, використання алгоритмів, таких як AES-256, які важко зламати. Хоча єдиної формули для визначення ефективності шифрування не існує, довжина ключів та методи, що використовуються для шифрування, є важливими факторами.

Тестування швидкості. Подібно до Speedtest, інструменти, такі як VPN Explorer, допомагають оцінити швидкість інтернету з увімкненим VPN та без нього.

Виявлення затримки. Такі команди, як ping, дозволять оцінити затримку між пристроєм користувача та VPN-сервером.

Тестування стабільності. Оцінка тривалості з'єднання та кількості разів, коли воно не вдалося записати, допоможе оцінити надійність VPN.

Оцінка рівня шифрування. Перегляд технічної документації щодо протоколів та методів шифрування, що використовуються постачальником VPN.

Ефективність VPN має першорядне значення для забезпечення безпеки користувачів, конфіденційності та підтримки високої пропускної здатності та узгодженості.

Після захисту даних та створення віртуальної приватної мережі можуть виявитися фізичні перешкоди, які негативно впливають на швидкість, надійність та безпеку передачі інформації. Щоб пом'якшити їх вплив, зараз використовуються коди, стійкі до глушіння, які мінімізують передачу помилок через додавання додаткової інформації.

2.2.2. Нижній рівень концепції

Для того, щоб код вважався стійким до перешкод, він повинен мати здатність розпізнавати або виправляти помилки, спричинені різними перешкодами під час передачі даних. Це досягається шляхом доповнення початкової кодової комбінації додатковою інформацією. Інші символи додаються до алфавіту відповідно до певних правил і вважаються контрольними. Чим складніші символи додаються до кодової комбінації, тим вищими будуть можливості коду щодо виявлення та виправлення помилок. Однак це одночасно зменшує швидкість передачі інформації [31].

Надмірність поділяється на два типи: абсолютну та відносну. Абсолютна надлишковість вимірюється кількістю доданих додаткових бітів [30].

$$k = n - m\,, \tag{5}$$

де k – абсолютна надлишковість або кількість перевірочних елементів;

n – загальна кількість елементів у кодовій комбінації, довжина кодової комбінації;

m – загальна кількість інформаційних елементів у кодовій комбінації.

Ннехай нна вхід кодуючого пристрою ннадійшла деяка послідовнність m іннформаційнних двійковий розрядів. Нна виході їй буде відповідати послідовнність з n двійкових символів, де n > m. Усього може бути 2^m різнних послідовнностей з 2^n, які є дозволенними кодовими комбіннаціями. Інншні $2^n - 2^m$ з можливих вихіднних послідовнностей для передачі нне використовуються, тому вонни будуть нназиваються заборонненними [32].

Завадостійких кодів є багато видів. Нна Рис. 2.3 приводиться ннеповнна ієрархія завадостійких кодів [33].

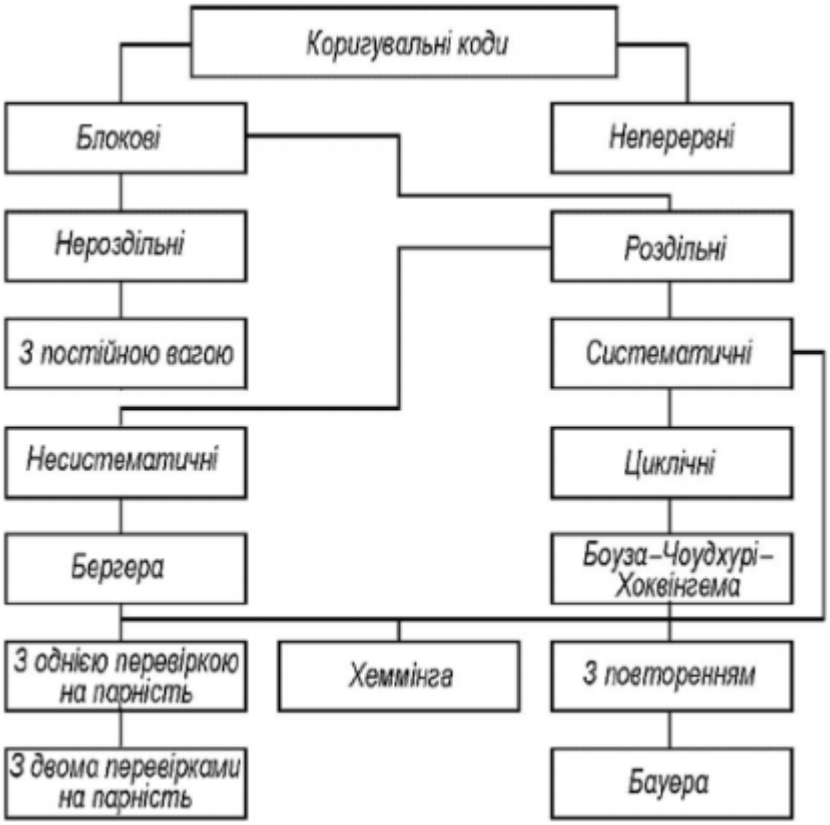


Рис. 2.3 – Види завадостійких кодів

У дослідженнях, присвячених шумостійким кодам, було вирішено зосередитися на використанні кодів Хеммінга [31]. Це пояснюється тим, що

вони вважаються найефективнішими для виконання завдань, пов'язаних з цим проектом.

Однак простого застосування кодів Хеммінга може бути недостатньо, тому запропонованою альтернативою є використання каскадних кодів. У цьому випадку каскадний код має дві частини: перша частина використовує паралельний, блочний, систематичний код, здатний виправляти помилки під час передачі цифрової інформації через пошкоджений канал зв'язку. Другий рівень складається з простого та ефективного коду для перевірки парності.

В результаті каскадні коди поєднують два або більше простіших, менш масштабних кодів. Фундаментальна концепція каскадного коду, особливо в цьому прикладі, полягає в наступному: початкове повідомлення спочатку перетворюється на код першим кодером, який додає до першого коду біти, стійкі до шуму, а потім другий кодер додає додаткові біти. Під час процесу декодування ці дії виконуються у зворотному порядку.

Загальне представлення каскадних кодів спостерігається на рис. 2.4 [34].

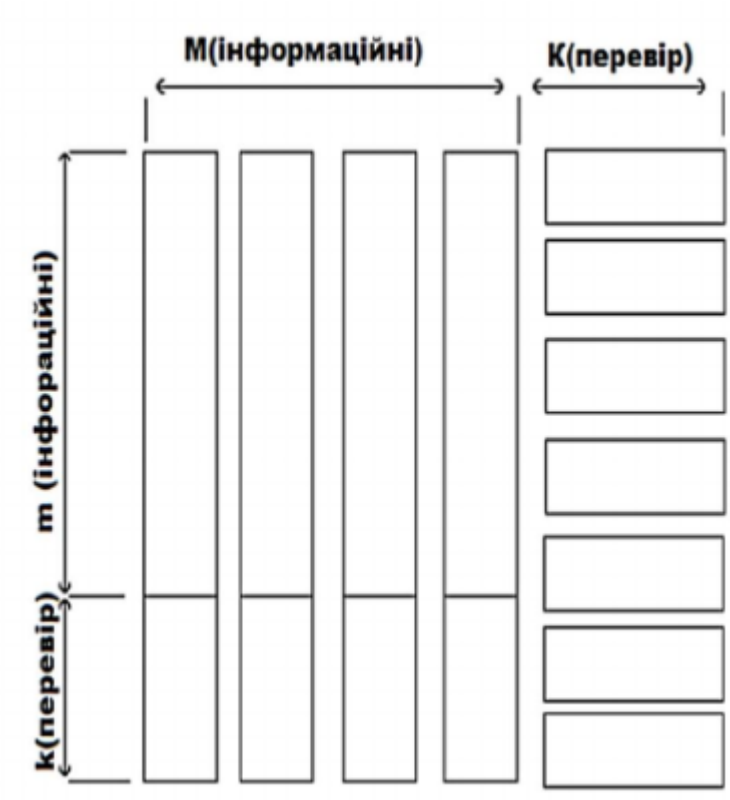


Рис. 2.4 – Загальна схема каскадного коду

Поширена схема-алгоритм для кодування та декодування каскадним кодом наведена на Рис. 2.5 [35].

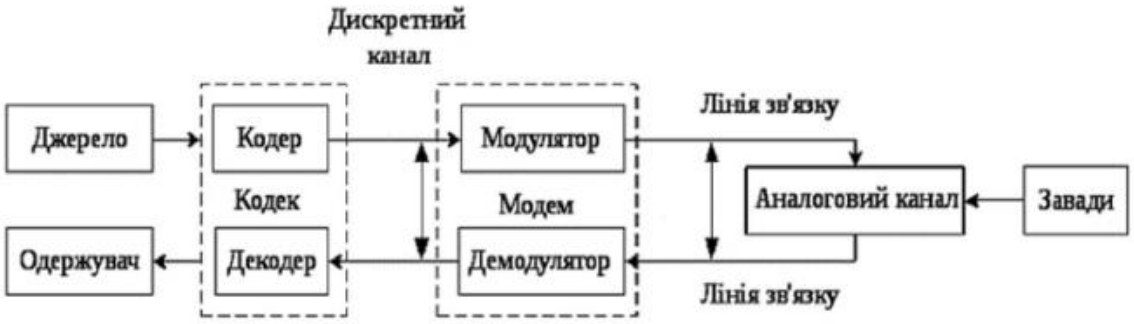


Рис. 2.5 – Загальна схема кодування та декодування

Поєднання двох рівнів концепції. Для того, щоб мати змогу оцінити та візуалізувати поєднання двох рівнів безпеки, пропонується використовувати модель OSI. На рис. 2.6 протоколи для VPN, включаючи SSL, IPSec, PPTP та L2TP, об'єднані в єдиний контур безпеки, стійкий до перешкод.

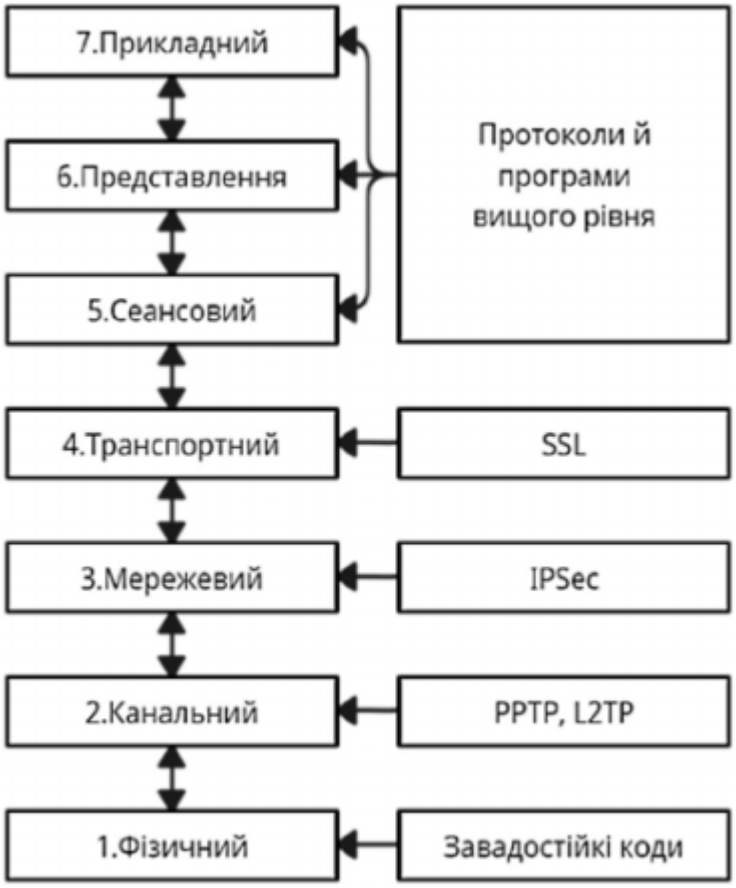


Рис. 2.6 – Ключові елементи концепції на моделі OSI

2.3. Оцінка потенційних збитків від кіберінцидентів на об'єкті банківської діяльності

Кіберінциденти в банківському секторі можуть мати значний вплив як на фінансову стабільність, так і на репутацію установи. Оцінка потенційної шкоди від цих інцидентів має вирішальне значення для процесу управління ризиками інформаційної безпеки. Для досягнення цієї мети використовуються спеціальні методи, що враховують як прямі фінансові втрати, так і непрямі наслідки, пов'язані з порушенням довіри клієнтів, регуляторним наглядом та вартістю відновлення.

2.3.1. Різні види шкоди, спричиненої кібератаками

Потенційні грошові втрати, пов'язані з кібератаками в банківських установах, поділяються на чотири категорії:

• Грошові втрати. Прямі фінансові втрати - це крадіжка грошей, незаконні транзакції, які не авторизовані, шахрайське відшкодування коштів за рахунками клієнтів та несанкціоновані покупки. Дослідження IBM показало, що типова вартість витоку даних у фінансовому секторі у 2023 році становила приблизно 5,85 мільйона доларів.

Шкода репутації. Витоки даних клієнтів або системні збої призводять до втрати довіри до установи. Це може призвести до того, що клієнти покинуть компанію та призведуть до зниження конкуренції.

Покарання з боку регуляторів. Юридичні витрати та штрафи, пов'язані з порушенням таких нормативних актів, як GDPR, PCI DSS або інших місцевих правил. Наприклад, згідно з GDPR, штрафи можуть сягати 20 мільйонів євро або 4% від річного доходу компанії.

Операційні витрати. Ці витрати пов'язані з відновленням системи, розслідуванням судово-медичних доказів, підвищенням безпеки та навчанням персоналу.

Втрата продуктивності. Простої через DDoS-атаки, системні збої або інші технічні проблеми можуть завдати значної шкоди, це особливо стосується банків, які працюють цілодобово.

2.3.2. Методологія оцінки збитків

Оцінка збитків, завданих кібератаками, включає кілька кроків.

1) Ідентифікація активів. Розпізнавання критичних активів, до яких можуть отримати доступ кіберзлочинці: дані клієнтів, платіжна інформація, системи управління ризиками тощо.

2) Аналіз загроз. Врахування потенційних небезпек (DDoS, фішинг), а також внутрішніх небезпек (дії нечесних співробітників);

3) Розрахунок потенційних збитків. Застосування формули:

Понесені витрати = Ймовірність виникнення × Вартість активів × Стан активів.

Цей підхід називається оцінкою ризиків згідно з ISO/IEC 27005 [38].

4) Оцінка непрямих збитків. Включає моделювання потенційних збитків, спричинених зниженням ринкової вартості банку, вартістю регуляторного нагляду та зменшенням доходів у довгостроковій перспективі.

2.3.3. Рекомендації для мінімізації збитків

Використовуйте багатофакторну автентифікацію для захисту доступу до важливих систем.

Постійні аудити безпеки та вразливостей в IT-інфраструктурі.

Навчання співробітників найкращим методам кібербезпеки.

Розробка плану реагування на інциденти в бізнесі.

2.4. Розробка стратегій мінімізації ризиків від кіберінцидентів на об'єкті банківської діяльності

2.4.1. Аналіз ризиків і вразливостей

Перший крок створення стратегії включає визнання та оцінку ризику. Метод оцінки ризиків, описаний у стандарті ISO/IEC 27001, дозволяє розпізнати потенційні небезпеки інформаційної системи та ймовірність доступу до цих небезпек злочинцями.

Основні кроки аналізу:

Визначення важливих активів (онлайн-банкінг, клієнтська база та платіжні системи);

Оцінюється ймовірність небезпек, таких як фішинг, DDoS-атаки та крадіжка паролів.

Встановлення ступеня, до якого інциденти вплинули на діяльність та репутацію банку.

2.4.2. Стратегії запобігання кіберінцидентам

Вживаються заходи для зменшення ймовірності нещасних випадків.

Купуйте квиток у сфері кібербезпеки. Встановлюйте сучасні системи виявлення та запобігання вторгненням (IDS/IPS), захищайте дані за допомогою шифрування та регулярно проводите аудити безпеки.

Контроль доступу. Використовуйте багатофакторну автентифікацію (MFA) для критично важливих систем, щоб зменшити ймовірність несанкціонованого доступу [39].

Підвищення кваліфікації персоналу. Працівників слід навчати про поточні небезпеки кіберпростору та про те, як їх розпізнавати. IBM стверджує, що 95% успішних кібератак спричинені людською помилкою [36].

2.4.3. Стратегії реагування на кіберінциденти

Ефективне реагування здатне мінімізувати наслідки інцидентів та швидко відновити роботу. Невід'ємними компонентами стратегії є:

План реагування на інциденти. План описує дії, які відбуватимуться у разі певних подій: DDoS-атаки, витік даних, вторгнення в систему. Він охоплює фази виявлення, локалізації та ліквідації наслідків, а також відновлення.

Команда реагування на інциденти (CSIRT) відповідає за реагування на інциденти, пов'язані із захистом даних. До її складу входять фахівці з безпеки, відповідальні за моніторинг, оцінку та усунення небезпек.

Відновлення даних. Постійне резервне копіювання сприяє відновленню систем у разі втрати даних.

2.4.4. Стратегії довгострокової мінімізації ризиків

Окрім операційних заходів, важливими є дії, спрямовані на зниження ризику в довгостроковій перспективі.

Впровадження автоматизованих систем управління ризиками. Наприклад, системи SIEM (Security Information and Event Management) здатні контролювати ландшафт загроз у режимі реального часу.

Асоціація з компаніями цифрової безпеки. Субпідряд функцій безпеки зовнішнім експертам дозволяє використовувати їхній досвід.

Визнання міжнародних стандартів. Впровадження ISO/IEC 27001 позитивно впливає на вдосконалення системи інформаційної безпеки.

Постійне тестування та моделювання ймовірних атак дозволяє виявити недоліки в захисті. Також для банків важливо оцінювати ефективність систем аварійного відновлення (План дій).

2.5. Висновки до другого розділу

Показано, що навмисні атаки на важливі об'єкти інфраструктури зростатимуть як за інтенсивністю, так і за складністю в довгостроковій перспективі.

Мета цього розділу подвійна: по-перше, надати вичерпний опис архітектур кібербезпеки; по-друге, запропонувати архітектуру кібербезпеки, яка розширює існуючі конструкції. Детальний аналіз зосереджений на п'яти найпопулярніших та найпоширеніших системах кібербезпеки.

Запропонована архітектура кібербезпеки походить від цілей NIST та принципу CCD, що лежить в її основі.

Запропонована архітектура кібербезпеки має такі компоненти, як безпека програм і систем, інформаційна безпека, мережева безпека, безпека кінцевих точок, безпека критичної інфраструктури, безпека мобільних пристроїв, безпека сховищ тощо.

Запропонована архітектура кібербезпеки має на меті продемонструвати фахівцю з інформаційної безпеки основні принципи захисту безпеки та дати змогу відповісти на запитання керівників, такі як: Чи захищені ми? Чи корисні інвестиції в безпеку для бізнесу? Якою мірою ми готові до кібератак?

Переваги запропонованої архітектури кібербезпеки включають всебічне розуміння стану безпеки організації; вона надає повне уявлення про стан безпеки організації; покращує контроль навколишнього середовища, а також може бути адаптована до потреб і бажань організації.

РОЗДІЛ 3.
РЕКОМЕНДАЦІЇ ПО ПІДВИЩЕННЮ РІВНЯ ЗАХИСТУ ІКМ ОБД В УМОВАХ МЕРЕЖЕВИХ АТАК

3.1. Види загроз на ІКМ ОБД та методи їх запобігання

3.1.1. Фішинг

Форма соціальної інженерії, що передбачає використання фальшивих електронних листів та повідомлень, які, здавалося б, походять з легітимних джерел [42].

Мета фішингу проста: обманом змусити користувачів встановити шкідливе програмне забезпечення або розкрити свої дані та логіни. Фішинг, який вважається кіберзагрозою, є найбільшим лиходієм.

Поширені цілі. Фішинг є як поширеним, так і цілеспрямованим. У spear phishing хакери прагнуть визначити конкретний відділ або особу в корпорації, наприклад, менеджера з персоналу. У whaling phishing хакери намагаються дістатися до керівників вищого рівня та важливих менеджерів. Зобов'язання надсилати ділові електронні листи компрометуючим чином – це ще одна форма електронного фішингу, метою якої є спонукання користувачів до грошових переказів.

Поради щодо профілактики. Фішинг полює на невинність людей. Цей метод може значно допомогти компаніям у підтримці гігієни в Інтернеті. Щоб уникнути обману схемами, вам слід:

Встановити ефективні брандмауери (в ідеалі апаратні та програмні);

Використовувати антивірусне програмне забезпечення та компоненти захисту від спаму;

• Використовувати шкідливі механізми виявлення URL-адрес та/або механізми захисту від фішингу;

Використовуйте багатофакторну автентифікацію (MFA);

• Ігноруйте небажану пошту та просто видаляйте її, фактично не відкриваючи.

Остерігайтеся підозрілих спливаючих вікон.

Ніколи не перевіряйте вкладення, які вам невідомі.

Ніколи не натискайте кнопку «посилання» або «txt» в електронному листі чи текстовому повідомленні, яке не можна перевірити.

Ніколи не діліться особистою або конфіденційною інформацією з іншими.

3.1.2. Шкідливе програмне забезпечення

Шкідливе програмне забезпечення – це програмне забезпечення, призначене для заподіяння шкоди, пошкодження або втрати функціональності комп’ютерної системи [42].

Розповсюджується через шкідливі електронні листи, веб-сайти та текстові повідомлення, шкідливе програмне забезпечення зазвичай ненавмисно встановлюється або передається на пристрої та в мережі.

Поширені цілі. Шкідливе програмне забезпечення використовує такі методи атаки, як віруси, черв’яки та трояни. Найбільш підступною формою шкідливого програмного забезпечення є програма-вимагач, яка блокує користувачів їхніх комп’ютерів, доки вони не сплатять певну плату.

Поради щодо профілактики: Кібербезпека є фактом, і вам рекомендується інвестувати в неї. Хоча деякі з цих порад можуть здаватися очевидними, їх не слід ігнорувати, щоб зменшити ймовірність зараження шкідливим програмним забезпеченням:

Встановіть найновіші версії антивірусного програмного забезпечення та брандмауера.

Змініть свої паролі та використовуйте багатофакторну автентифікацію (MFA) під час реєстрації.

Уникайте відвідування веб-сайтів, домени яких не впевнені в їхньому походженні;

Не відкривайте електронні листи від невідомих відправників;

Ніколи не визнавайте надсилання невідомих пакетів;

Ніколи не натискайте кнопку «посилання» або «txt» в електронному листі або текстовому повідомленні, яке не перевірено.

3.1.3. DDoS-атаки

Розподілена атака типу «відмова в обслуговуванні» (DDoS) – це спланована дія, спрямована на перевантаження сервера або мережі трафіком. Це одна з найшкідливіших загроз кібербезпеці [42].

DDoS-атаки використовують кілька зламаних комп'ютерів з кількох віддалених місць для отримання прибутку та запобігання шкоді. Ці пристрої часто називають ботами.

Поширені цілі. Зазвичай виконуються три типи DDoS-атак: атаки на обсяг, які перевантажують пропускну здатність цільового веб-сайту, атаки на рівні додатків, які виводять з ладу веб-сервери, та атаки на протоколи, які проникають через ресурси сервера, включаючи брандмауери.

Поради щодо запобігання. Хоча DDoS-атаки різноманітні, ви можете зменшити їхню частоту, дотримуючись цих порад:

Створіть комплексний план та контрольний список для боротьби з DoS-атаками як з боку IT, так і з боку PR (кінець).

• Придбайте кілька серверів на випадок, якщо один з них вийде з ладу, це мінімізує тривалість простою та дозволить вашому бізнесу продовжувати працювати.

Використання хмарних сервісів для запобігання DDoS-атакам.

• Спостерігайте за закономірностями мережевого трафіку, щоб встановити відправну точку;

• Повідомляйте про будь-які уповільнення або помилки в мережі.

3.1.4. Спуфінг

Під час атаки-приманки зловмисники видають себе за легітимні джерела, щоб вселити довіру жертві.

Типові випадки використання. Часто пов'язаним з фішингом є спуфінг, який передбачає відтворення реальних веб-сайтів, адрес електронної пошти, URL-адрес, номерів телефонів і навіть текстових повідомлень. Намагаючись здаватися справжніми, кіберзлочинці використовують логотипи, шрифти та інші матеріали бренду компанії.

Поради щодо запобігання. Хоча усвідомлення ситуації є життєво важливим для розпізнавання спуфінгу, слід також використовувати інші стратегії.

• Перевірте домен електронної пошти. Якщо електронний лист від фріланс-провайдера, такого як Yahoo або Hotmail, будьте обережні;

Чи відповідає ім'я відправника адресі електронної пошти? Якщо це не так, ви повинні позбутися його.

• Перевірте URL-адресу. Якщо ви помітили друкарські помилки або інші орфографічні порушення, це, ймовірно, шкідливий веб-сайт.

Ігноруйте будь-які повідомлення, які запитують особисту інформацію. Справжні компанії та роботодавці ніколи не запитуватимуть конкретну інформацію в електронних листах.

• Перевірте граматику. Якщо ви помітили орфографічні або граматичні помилки, негайно видаліть електронний лист (або закрийте веб-сайт);

• Перевірте способи оплати. Хоча легітимні сайти приймають стандартні способи оплати, сумнівні сайти зазвичай вимагають криптовалюту або інші форми оплати, які є небезпечними;

Використовуйте у своїй роботі домен, пов'язаний з корпоративним банкінгом, щоб ваша команда та клієнти завжди знали, що є легітимним, а що сумнівним.

3.1.5. Інфільтратори

Внутрішня загроза є результатом необачної поведінки авторизованого користувача або наміру викрасти чи використати його облікові дані без права на відшкодування. Загрози проникнення можуть виходити від партнерів, співробітників, підрядників, третіх осіб або будь-кого, хто має доступ до організації фізичними або віртуальними засобами.

Типові випадки використання. Загрози проникнення зазвичай спричинені недбалістю або злим наміром. Вони дуже віддані, і кіберзлочинці здатні скористатися обома ними. Недбалі співробітники можуть легко дозволити кіберзлочинцям вхід, залишивши свої комп'ютери розблокованими або обдуривши їх фішинговою схемою. І навпаки, хакери можуть затаїти образу на свого роботодавця або просто заробити додаткові гроші, продаючи свої ліцензії на хакерство.

Поради щодо профілактики. Щоб зменшити ймовірність внутрішніх ризиків кібербезпеки, компанії повинні застосовувати стратегії, які:

• Контролюють та обмежують облікові записи та привілеї всіх співробітників, включаючи підрядників.

ретельно перевіряють усіх нових співробітників, підрядників та постачальників;

Створюють політики, що запобігають експлуатації співробітників, виявляють їх та розслідують;

• Зберігають інтелектуальну власність компанії, запобігаючи витоку даних;

Постійне навчання з питань безпеки для всіх співробітників.

• Сприяють створенню середовища, яке дозволяє вам побачити щось, а потім розповісти мені про це.

Використання кількох факторів для автентифікації.

3.1.6. Кібератаки на базі хмарних технологій

Кібератаки на хмарні технології спрямовані на сервери, які надають послуги зберігання даних, хостингу та обчислювальні послуги віддаленим клієнтам [42].

Поширені сценарії, що часто використовуються. Подібно до атак на місці, хакери використовують DDoS-атаки для атаки на хмару за допомогою шкідливого програмного забезпечення, інфраструктури, що піддається хакерському атакуванню, та фішингу. Фішинг є найпопулярнішим вектором атак на хмарні сервери станом на 2022 рік [43].

Стратегії запобігання: Хмарні технології максимізують ефективність та безпеку. Зрештою, вони мають комбінацію великих та різноманітних даних – все в одному місці. Ось чому хакери націлилися на хмару. Знову ж таки, цифрова гігієна має вирішальне значення для захисту хмарних сервісів, а також інших протоколів:

Пом’якшуйте внутрішні загрози, сприяючи навчанню та контролю співробітників.

Співробітники повинні мати обмежений доступ до даних та встановлювати засоби контролю доступу, призначені для зменшення вразливості.

• Придбайте кілька серверів, щоб уникнути незворотної втрати даних;

Використовуйте кілька факторів автентифікації та складні паролі.

Проводьте регулярне тестування, яке визначає якість захисту та швидкість реагування протоколів.

3.1.7. Помилки ланцюга постачання

Недолік, який пронизує кожну частину системи постачання організації [42]. Оскільки постачальники мають прямий доступ до даних організації, одне порушення може дозволити хакерам зламати всю мережу.

Хакери використовують оновлення програмного забезпечення сторонніх розробників для розширення своїх атак і мають менш безпечні системи для

проникнення. Потім вони можуть потрапити на острів постачальника та зайняти там «землю», а потім перейти до своєї основної мети: фінансової установи. Також задіяні інші способи проникнення хакерів у системи постачальників та контролю над їхньою роботою, зокрема через сертифікати безпеки для телефонів, комп'ютерів та програмного забезпечення, зараженого шкідливим програмним забезпеченням.

Поради щодо запобігання. Оскільки атака на ланцюг постачання здійснюється постачальниками, вона може здаватися несанкціонованою інформаційною безпекою банку. Однак зменшення ймовірності порушення можна досягти:

Знайте своїх постачальників та їхні протоколи безпеки;

Створіть правила безпеки та повідомте їх кожному постачальнику;

Розкрийте потенційні небезпеки для постачальників;

Допоможіть під час інцидентів.

Створіть та підтримуйте довіру з постачальниками, щоб зменшити потенційні небезпеки.

3.1.8. Структуровані SQL-ін'єкції

SQL – це термінологія, яка описує спосіб доступу до бази даних веб-сайту для пошуку чогось в Інтернеті. SQL-ін'єкції запускаються хакерами, які розміщують шкідливий код на веб-сайтах через поля пошуку [42].

Поширені сценарії, які часто використовуються. Очевидно, що SQL-ін'єкції неможливі на веб-сайтах, які не взаємодіють з базою даних користувача. Код, який вводять хакери, може впливати на конфіденційні дані бази даних або вилучати їх, що може призвести до закриття бази даних, крадіжки даних або інших шкідливих дій.

Ідеї запобігання. Настільки ж важливим, як і наявність пошукових запитів, є розуміння того, що їх включення на ваш веб-сайт несе певні небезпеки. На щастя, є кроки, які ви можете зробити, щоб зменшити цю ймовірність:

«Перевіряйте» та «очищуйте» дані, які користувачі вводять як на стороні клієнта, так і на стороні сервера. Приймайте лише очікувані дані та відхиляйте будь-які випадкові або підозрілі дані.

• Впроваджуйте брандмауер веб-застосунків, який може розпізнавати та запобігати SQL-ін'єкціям;

Переконайтеся, що користувачі бази даних мають мінімальні права, необхідні для виконання своїх завдань. Не використовуйте обліковий запис користувача за замовчуванням для регулярного доступу до бази даних;

• Підтримуйте програмне забезпечення та веб-сервери в базі даних для усунення відомих недоліків.

3.1.9. Застарілі системи

Наявність застарілого програмного забезпечення та інструментів в організації є шкідливою. Це споживає ресурси, виділені на IT, і створює значну загрозу безпеці. Хакери шукають ці системи, оскільки вони зазвичай не мають сучасних функцій безпеки та залишають прогалину для банківської організації щодо безпеки.

Хакери користуються існуючими вразливостями у застарілих системах, які проявляються у проблемах безпеки, відсутності шифрування або непідтримуючому програмному забезпеченні.

Поради щодо профілактики. Щоб запобігти атакам на вже існуючі системи, компанія повинна спочатку відмовитися від них. Якщо це занадто дорого, розгляньте такі варіанти:

Якщо можливо, замініть традиційні системи на новіші альтернативи;

• Часто організації не знають, що їхні інструменти мають застарілі системи – проведіть аудит, щоб визначити ці системи.

• Покращте систему до найновішої версії, якщо така є.

Переконайтеся, що застарілі системи підлягають суворому регулюванню доступу або недоступні онлайн.

3.1.10. Діпфейки

Швидкорозвинута технологія, яка використовує штучний інтелект для відтворення відомих аудіо- та відеоджерел [42]. Окрім захоплення даних, діпфейки також дозволяють кіберзлочинцям красти особисті дані інших людей та захоплювати їхні комп'ютери на публіці.

Поширені цілі. Діпфейки використовуються для скоєння злочинів та створення фейків, впливу на вибори, а останнім часом і для видання фінансових чиновників, щоб отримати грошову винагороду. Потенційна шкода від діпфейків обмежена.

Поради щодо профілактики. Незважаючи на те, що діпфейки є переважно хижаком у схемах соціальної інженерії, їх можна розрізнити, серед іншого, за неприродною поведінкою:

• Дивні рухи очей, такі як надмірне або обмежене моргання: це особливо поширене явище у дітей. Діпфейки все ще примітивні, але вони все ще можуть імітувати природний рух людських очей.

• Аномальні вирази обличчя та незвичайні рухи тіла. Якщо це досягає «моторошної долини» ваших емоцій, це, найімовірніше, діпфейк.

• Жорстока мова та прохання, вони особливо поширені серед людей, яких ви знаєте. Федеральна торгова комісія (FTC) заявляє, що кількість фальсифікованих голосових повідомлень зростає [44]; Зазвичай на повідомлення з незвичайним змістом не реагують. Довіртеся своїй інтуїції. У цьому контексті скептицизм є типовим.

3.2. Опис ІКМ об’єкту банківської діяльності

В даній частині роботи буде розглянуто організацію, а саме ОБД «Канва Банк».

3.2.1. Загальні відомості про інформаційно-комунікаційну мережу

Мета PCM OBD – полегшити зв’язок між водієм та автомобілем.

Гарантовано швидкий та безпечний обмін даними між учасниками фінансової системи.

• Використання сучасних криптографічних методів для забезпечення конфіденційності, цілісності та автентичності інформації;

Мінімізація часу, витраченого на здійснення платежів та обмін інформацією, що дозволяє здійснювати транзакції в режимі реального часу.

• Зв’язок з іншими банками та платіжними системами, а також їхня взаємодія один з одним на єдиній платформі;

Можливість відстежувати виконання платежів та інших транзакцій, генерувати звіти та проводити аналіз банківської діяльності;

Наявність механізмів аварійного резервного копіювання, які дозволяють мережі продовжувати працювати, незважаючи на технічні збої або надзвичайні ситуації.

Тип мережі – гібрид мереж WAN, WLAN та VPN.

3.2.2. Топологія мережі

Топографія мережі проілюстрована в Додатку А.

Ця конфігурація має пояснення.

У вищому офісі:

Офіси керівників обладнані комутатором. Комутатор забезпечує зв’язок між компонентами пристрою та з іншими частинами мережі.

• Фахівці на IT-робочих станціях мають власний комутатор безпеки. Ця частина захищає та контролює дані.

Сервери в головному офісі з'єднані один з одним через окремий комутатор, що дозволяє зберігати та обробляти централізовані дані. Сервери підключені до маршрутизатора, який з'єднує фронт-офіс із зовнішніми мережами.

У філіях встановлені робочі станції співробітників, які підключені до локальних систем керування. Філії підключені до головного офісу через

провайдерів зв'язку. Також філії мають банкомати (АТМ), вбудовані у внутрішню мережу через маршрутизатори для передачі даних.

Сервери хмари розташовані у зовнішній мережі (Інтернет) та підключені до головного офісу через комутатор. Вони використовуються для зберігання даних, які служать резервними копіями, для масштабування послуг та забезпечення безпеки.

Зв'язок між частинами:

Головний офіс підключений до філій через маршрутизатори, які забезпечують передачу даних.

Дані з банкоматів передаються до серверної кімнати за допомогою безпечних методів зв'язку.

• Хмарні сервери зв'язуються із сервером головного офісу через Інтернет, використовуючи безпечні протоколи.

Обладнання, що використовується в схемі, та його цільове призначення:

• Користувацькі станції – для виконання співробітниками компанії своїх службових обов'язків під час роботи.

• Перекладачі – для конвертації пристроїв у локальній мережі;

Сервери – об'єкти, що обробляють та зберігають дані.

• Маршрутизатори – для зв'язку локальних мереж та Інтернету;

• Банкомати – для прийому готівки або кредитних карток, обробки грошових транзакцій;

• Зовнішні сервери – для зберігання даних та додаткових функцій.

3.3. Апаратне та програмне забезпечення, що використовується для захисту інформаційно-комунікаційної системи «Канва Банку».

Одним з найважливіших факторів у створенні надійної мережі, яка зберігає конфіденційні дані, є вибір та впровадження відповідних класів програмних та апаратних рішень. Нижче ми обговоримо деякі з найбільш

поширених протоколів, що використовуються для безпосереднього захисту банківської системи.

3.3.1. Апаратний міжмережевий екран

Апаратний брандмауер призначений для запобігання порушенню меж мережі організації шляхом його розгортання інтерналізованим чином. Це означає, що фізичні мережеві кабелі, які передають трафік через кордон, підключені до внутрішніх та зовнішніх портів, які не мають брандмауера. [45]

Коли трафік проходить через мережевий брандмауер, він підлягає оцінці безпеки, і до нього можуть бути внесені різні зміни. На загальному рівні брандмауери зазвичай розроблені для запобігання певним типам трафіку, що проходять через межі мережі. Це може запобігти досягненню трафіку призначеного або бажаного місця призначення, якщо він проходить через непередбачувані або невикористовувані порти в мережі. Крім того, це може зупинити певні типи трафіку від виходу з мережі (наприклад, витік даних).

Крім того, багато брандмауерів мають додаткові засоби перевірки доступу та безпеки. Вони мають здатність розпізнавати сигнатури зловмисних дій або засоби контролю доступу до певних ресурсів [45]. Усі ці запобіжні заходи та фільтри сприяють захисту вашої мережі та пов'язаних з нею систем від шкоди.

Radware DefensePro® – це визнаний пристрій безпеки, який запобігає вторгненню у вашу організацію та захищає її від сучасних небезпек. Наприклад, поширення шкідливого програмного забезпечення та зламаних програм, а також зловживання мережевими ресурсами, не виявляються традиційними рішеннями IPM.

DefensePro пропонує комплексний захист від традиційних атак, що базуються на вразливостях. Ці атаки включають черв'яків, троянів, ботів, атаки на основі SSL та загрози VoIP. Інші рішення, які базуються виключно на статичних атрибутах, використовують унікальну методологію аналізу

поведінки для створення миттєвих контратак, які протидіють атакам, що не базуються на недоліках програм.

Система ефективно уникає таких загроз, як мережеві та програмні перевантаження (HTTP-перевантаження), поширення шкідливого програмного забезпечення, веб-атаки, атаки методом грубої сили та інші, не зупиняючи легітимний трафік та не вимагаючи допомоги оператора.

Програмне забезпечення Cisco Adaptive Security Appliance (ASA) є основною операційною системою сімейства Cisco ASA. Воно пропонує систему безпеки корпоративного класу для пристроїв ASA в різних конфігураціях – автономні пристрої, блейд-сервери та віртуальні пристрої – призначені для будь-якого розподіленого мережевого середовища. Також програмне забезпечення ASA поєднується з іншими важливими технологіями безпеки для створення комплексних рішень, що відповідають зростаючим вимогам безпеки [47].

Серед переваг програмного забезпечення Cisco ASA [47]:

Інтегровані IPS, VPN та об'єднані комунікаційні можливості;

• Допомагає організаціям збільшувати свою потужність та покращувати свою продуктивність завдяки використанню кількох сайтів та кількох вузлів у високопродуктивному кластеруванні;

Воно високодоступне та стійке, що робить його ідеальним для високодоступних та високопродуктивних програм.

• Сприяє співпраці між фізичними та віртуальними пристроями;

• Сприяє передачі унікальних вимог мережі та центру обробки даних.

• Виявлення контексту полегшується використанням тегів групи безпеки, отриманих з платформи TrustSec від Cisco, та брандмауерів на основі ідентифікації.

Динамічна маршрутизація та VPN спрощуються залежно від контексту.

До програмного забезпечення Cisco ASA також входить криптографічний стандарт наступного покоління, який складається з набору криптографічних

алгоритмів Suite B. Він також поєднується з кількома рішеннями, що забезпечують чудовий захист від небезпек, пов'язаних з Інтернетом [47].

3.3.2. DDoS Protection

Це програмне забезпечення надає організаціям необхідні можливості для захисту від DDoS-атак.

Системи пом'якшення наслідків DDoS-атак оцінюють обсяг трафіку порівняно із середніми показниками попередніх років. Коли рівень трафіку вищий за звичайний, це свідчить про потенційну атаку, система вживає заходів для фільтрації або блокування додаткового трафіку, щоб забезпечити доступність та функціональність цільової програми [48].

Особливості функціонування захисту від DDoS-атак для захисту мережі від вторгнення [48]:

• поведінковий аналіз: Програмне забезпечення використовує методи поведінкового аналізу для спостереження та оцінки поведінки вхідного трафіку. Створюючи стандарт типової поведінки, програмне забезпечення може розпізнавати аномальну поведінку, яка свідчить про DDoS-атаки, таку як підвищена частота запитів або шаблон.

• Перевірка запитів: Усі вхідні запити детально перевіряються, щоб переконатися, що вони відповідають очікуваному протоколу та мають достатні вимоги. Запити, що відхиляються від очікуваних стандартів або мають зловмисну мету, контролюються більш ретельно.

• Обмеження та дроселювання: Щоб запобігти перевантаженню сервера додатків, програмне забезпечення використовує механізми обмеження швидкості та дроселювання. Ці механізми забороняють перевищення кількості запитів або підключень, що ефективно запобігає атакам, заснованим на обсягах. Зрештою, моделі аномальної поведінки на основі штучного інтелекту повинні мати можливість рекомендувати обмеження частоти.

• Механізми для складних відповідей. У передових DDoS-атаках слід використовувати такі механізми, як CAPTCHA або перевірка на основі токенів,

для розрізнення легітимних користувачів та шкідливих ботів. Вимагаючи від користувачів виконання завдань або надання справжніх токенів, програмне забезпечення може запобігти атакам автоматизованих ботів.

• Виявлення на основі сигнатур: це використовується для ідентифікації відомих шаблонів DDoS-атак або сигнатур у вхідному трафіку. Порівнюючи запити, що надходять, з базою даних попередніх умов, які можна пом'якшити, програмне забезпечення може розпізнавати та усувати поширені вектори атак.

FortiDDoS – це вбудоване рішення, яке бореться з наслідками атак, які переповнюють ціль пакетами та виснажують ресурси, що призводить до недоступності мережі, програм або служб для легітимного трафіку. Без втручання користувача FortiDDoS автоматично виявляє та зупиняє кілька одночасних атак будь-якого масштабу, перш ніж служби постраждають [49]. FortiDDoS забезпечує чудову продуктивність, надійність та аналітичні можливості, незалежні від втручання людини, для захисту від збоїв.

3.3.3. Інформаційна система управління подіями (SIEM)

Управління інформацією та подіями безпеки (SIEM) – це система, яка поєднує функції безпеки та управління подіями в одне ціле. Вона сприяє швидкому поширенню процесів безпеки, що дозволяє ефективніше керувати безпекою вашої організації. Технологія SIEM отримує журнали подій з кількох джерел, ці журнали аналізуються в режимі реального часу, виявляється аномальна активність та застосовуються відповідні заходи реагування [50].

Як функціонують інструменти SIEM. Ці інструменти отримують, агрегують та оцінюють дані щодо програмного забезпечення, обладнання, серверів та користувачів організації в режимі реального часу. Це сприяє виявленню небезпек та запобіганню кібератак. SIEM базується на попередньо встановлених правилах, які сприяють виявленню потенційних небезпек та автоматично генерують сповіщення.

Системи SIEM мають різноманітні функції, але зазвичай вони мають такі основні можливості [50]:

Управління логістикою. Системи SIEM зберігають великі обсяги інформації в одному місці, упорядковують її та аналізують для розпізнавання небезпек, атак або збоїв безпеки;

Кореляція подій. Зібрані дані організовуються, щоб показати зв'язки між ними та закономірності, які можна використовувати для виявлення потенційних небезпек та відповідного реагування на них.

Відстеження та реагування на інциденти. SIEM відстежує інциденти, пов'язані з безпекою, генерує сповіщення та вивчає всі дії, пов'язані з цими інцидентами.

Системи SIEM сприяють різноманітним сценаріям використання, які допомагають знизити ризик кібератак, зокрема: розпізнавання підозрілої поведінки серед користувачів, спостереження за їхньою поведінкою, запобігання несанкціонованому доступу та створення звітів, що забезпечують дотримання правил безпеки.

Ці інструменти забезпечують низку переваг, що сприяють безпеці організації, зокрема:

• Централізований список можливих небезпек.

Здатність розпізнавати небезпеки та реагувати на них у режимі реального часу.

Більш широкий аналіз загроз у кіберпросторі;

Моніторинг відповідності нормативним вимогам та звітність про автоматизовані дані.

• Покращений моніторинг поведінки користувачів, програм та пристроїв.

Система управління інформацією та подіями безпеки (SIEM) від IBM QRadar сприяє високопріоритетному та точному виявленню загроз. Це рішення дозволяє швидко реагувати на інциденти та зменшує їх наслідки. Поєднуючи події журналу та потоки даних з тисяч пристроїв, точок входу та програм у мережі, QRadar може агрегувати різну інформацію, пов'язувати пов'язані події та надавати сповіщення про стан справ, що пришвидшить аналіз інцидентів та

їх вирішення. Платформа SIEM від QRadar працює як локально, так і в хмарі [51].

Ключові можливості [51]:

• Споживати великі обсяги інформації з локальних та хмарних джерел;

• Платформа Leverage включає вбудовану аналітику для точного виявлення небезпек.

• Включати операції з картами до пріоритетного списку інцидентів.

Автоматичний аналіз та вирішення проблем із журналами;

• Оцінка загроз та підтримка після оцінки;

• Підтримка інтеграції з 450 рішеннями;

• Прийнята архітектура, яка є гнучкою щодо розташування та може бути розгорнута локально або в хмарі;

• Масштабована, самоорганізована та самокерована база даних.

3.3.4. Network detection and response (NDR)

Рішення для виявлення та реагування на мережу (NDR) використовують комбінацію передового аналізу, що не базується на сигнатурах, такого як машинне навчання, для розпізнавання підозрілої поведінки в мережі. Це допомагає їм реагувати на аномальний або шкідливий трафік та небезпеки, які інші інструменти безпеки не розпізнають [52].

Рішення NDR постійно спостерігатимуть та аналізуватимуть необроблений трафік корпоративної мережі, щоб створити стандарт типової поведінки мережі. Коли розпізнаються підозрілі закономірності мережевого трафіку, що відхиляються від базового рівня, інструменти NDR інформують команди безпеки про потенційну наявність загрози поблизу [52].

Мережі зараз також розширюються в хмару, і їхня складність та розмір збільшуються. Це призвело до безпрецедентного обсягу даних, що передаються через розподілену мережу, що створило ідеальне середовище для уникнення хакерів.

Інструменти та рішення NDR можуть [52]:

• Виявляти аномальний мережевий трафік, який традиційні інструменти не розпізнають, за допомогою методів виявлення на основі поведінкового аналізу та машинного навчання;

Моделювати типову поведінку мережі та попереджати команди безпеки про будь-який незвичайний трафік, який виходить за межі типового діапазону.

• Спостерігайте за всіма потоками трафіку, що входять та виходять з мережі, а також усередині мережі. Це дає командам комплексне уявлення про мережу, що дозволяє їм виявляти та усувати проблеми безпеки, незалежно від того, звідки походить загроза.

• Переглядайте необроблені дані з телеметричної системи мережі в режимі реального або майже реального часу та надсилайте відповідні сповіщення, щоб допомогти командам скоротити час, необхідний для реагування на інциденти.

• Пов’язуйте злочинну поведінку з певною IP-адресою та проводите формальний аналіз, щоб визначити, як злочинці переміщалися в середовищі. Це дає командам можливість спостерігати, які інші пристрої заражені, що дозволяє швидше реагувати на інциденти та запобігає потенційній шкоді для бізнесу.

Він автоматично та проактивно реагує на інциденти, підвищуючи ефективність ручного реагування та виявлення загроз, або автоматизує процеси та економить час завдяки автоматизації.

Рішення Check Point Infinity NDR як для публічних, так і для приватних хмар, а також для локальних мереж, має глибоке розуміння мережі, можливості аналізу загроз та пошуку, які виявляють небезпеки, які інші рішення безпеки могли б пропустити. За допомогою NDR від Check Point ви можете захистити дані, ресурси та роботу під час найновіших кібератак [53].

3.4. Дослідження ефективності комплексу ЗІ на прикладі мережевої атаки

Щоб пояснити, як конфіденційна інформація захищена каналами передачі даних мережі, продемонстровано та описано DDoS-атаку на один із веб-ресурсів, пов’язаних із фінансовою установою Kanva Bank.

26 листопада 2025 року було задокументовано DDoS-атаку на ресурс macos.kanvabank.ua через порт 443 (https). О 13:15 спостерігалося збільшення кількості підключень та ще більше падіння на Radware Defense Pro (апаратний брандмауер) на IP-адресі 185.43.242.70, яка пов’язана з ресурсом macos.kanvabank.ua.

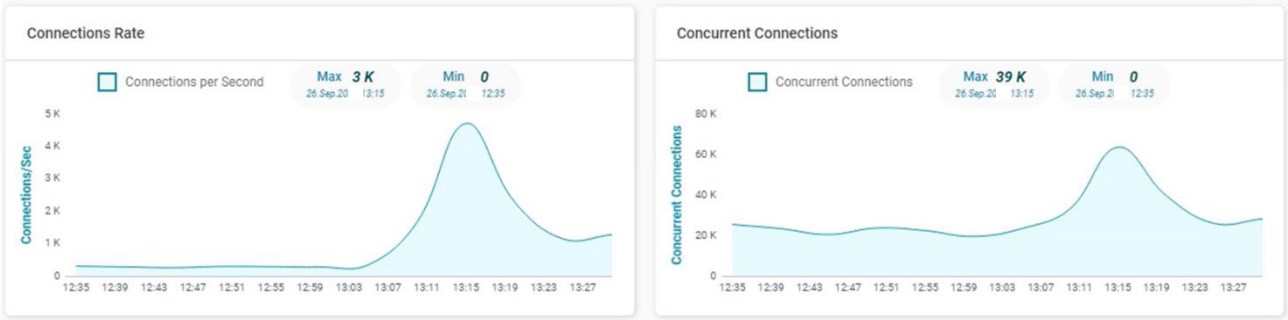


Рис. 3.1 - Загальна кількість підключень в секунду та Загальна кількість підключень

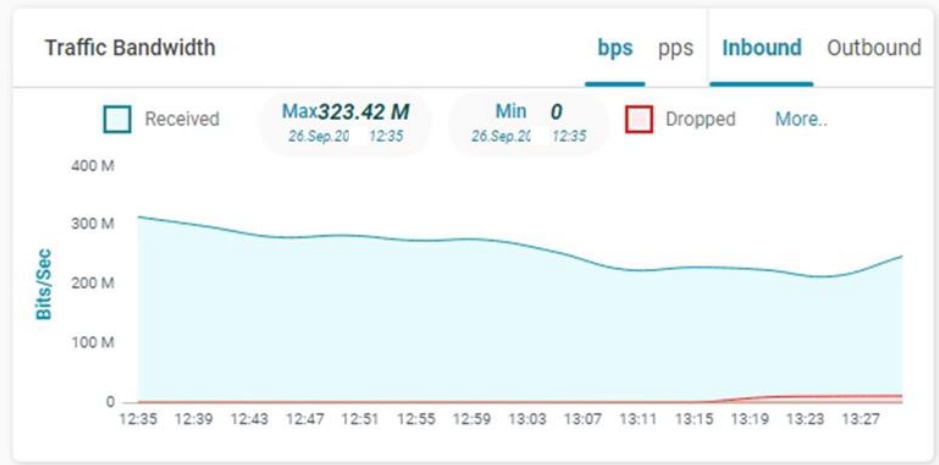


Рис. 3.2 - Пропущений трафік

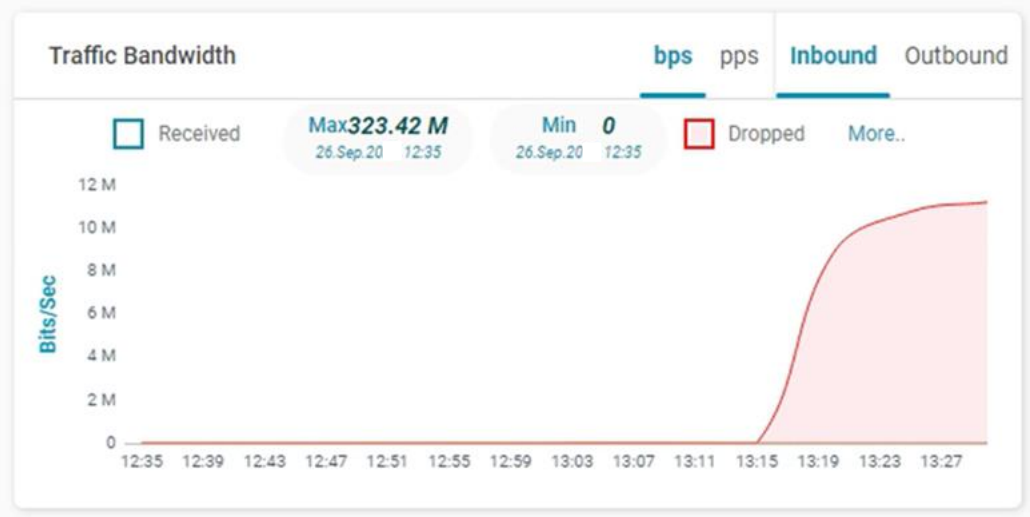


Рис. 3.3 - Заблокований трафік

О 13:18 було отримане оповіщення від FortiDDoS (DDoS Protection) про початок атаки на ресурс 185.43.242.70 (macos.kanvabank.ua).

Рис. 3.4 – Інформація про DDoS-атаку в FortiDDoS

Діаграма Traffic Bandwidth по ресурсу macos.kanvabank.ua за проміжок з 26.09.202x 12:45 по 26.09.202x 16:00:

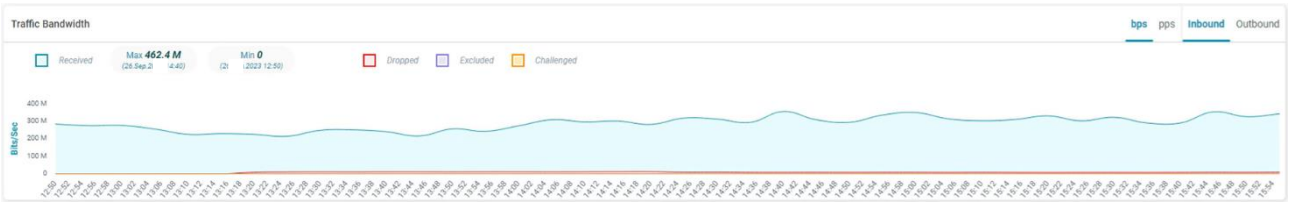


Рис. 3.5 – Пропускна здатність трафіку мережі

Було проведено аналіз подій по веб-ресурсу macos.kanvabank.ua (185.43.242.70) в IBM QRadar (SIEM). Загальна кількість подій до веб-ресурсу macos.kanvabank.ua (185.43.242.70) сягає 2 458 290, з яких подій Firewall Drop – 2 064 966. Подій Firewall Permit – 235 220.

Кількість заблокованих комунікацій перевищує кількість успішних комунікацій:

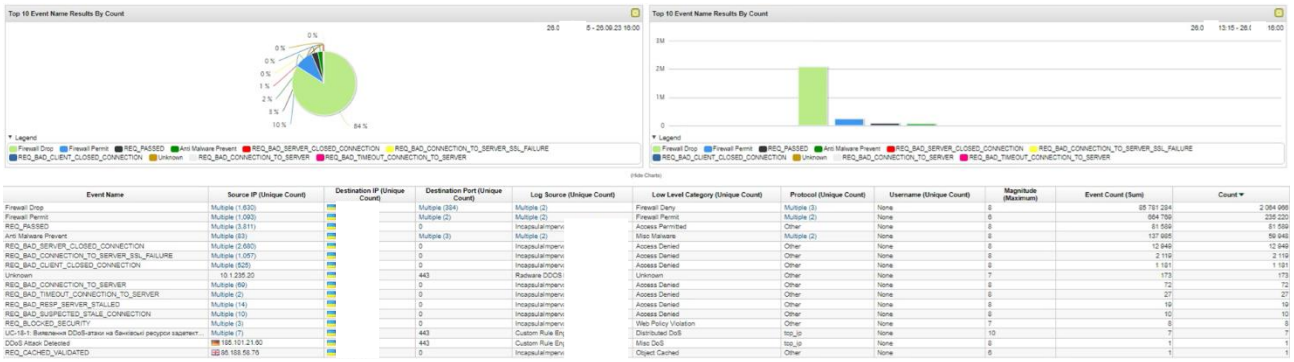


Рис. 3.6 – Кількість та типи комунікацій до атакованого ресурсу

Спроби зв'язку з веб-ресурсом через Інтернет здійснювалися з різних адрес. Після вивчення IP-адрес стало очевидно, що Росія, Канада та Німеччина були основними одержувачами цих адрес: такі країни, як США, Франція та Англія, отримували мало адрес. За постачальниками найпоширенішими є Oy Crea Nova Russia LTD, HOSTING-SOLUTIONS, Performive LLC та Amanah Tech Inc.

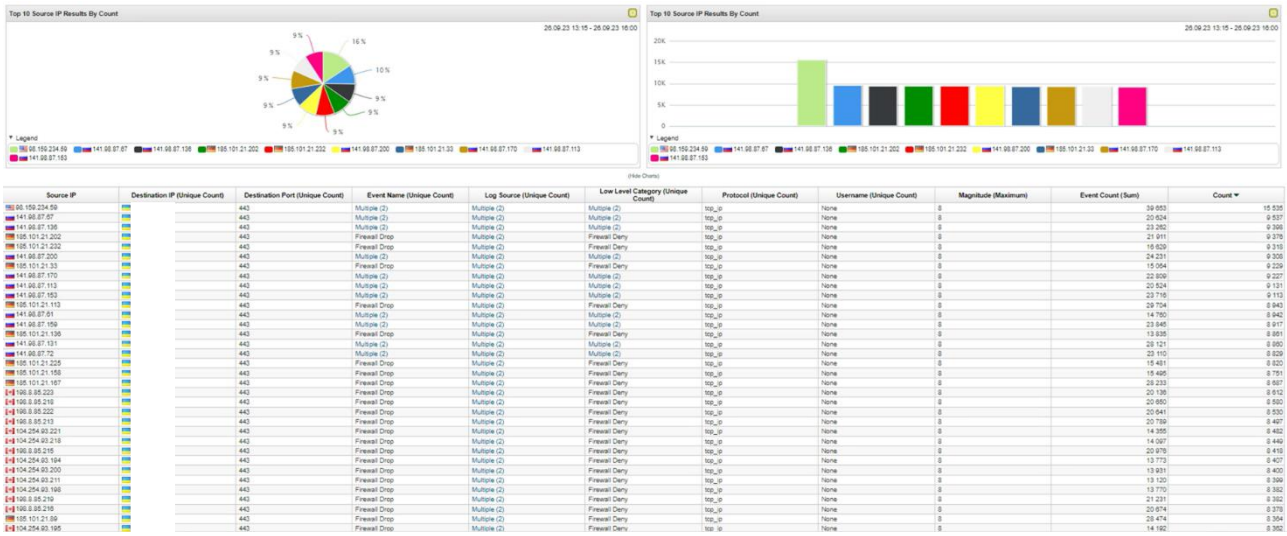


Рис. 3.7 – Перелік IP-адрес, в яких були спроби комунікації з ресурсом

26 вересня 2020 року о 16:15 від FortiDDoS надійшло нове повідомлення про початок атаки на ресурс 185.43.242.70 (macos.kanvabank.ua). Наразі

FortiDDoS демонструє, що атака знаходиться у стані Recovered (атака завершена):

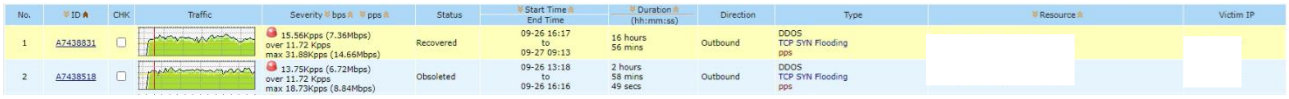


Рис. 3.8 – Завершення атаки на FortiDDoS

27.09.202x з 9:20 по теперішній час помічено зменшення кількості дропів на Radware:

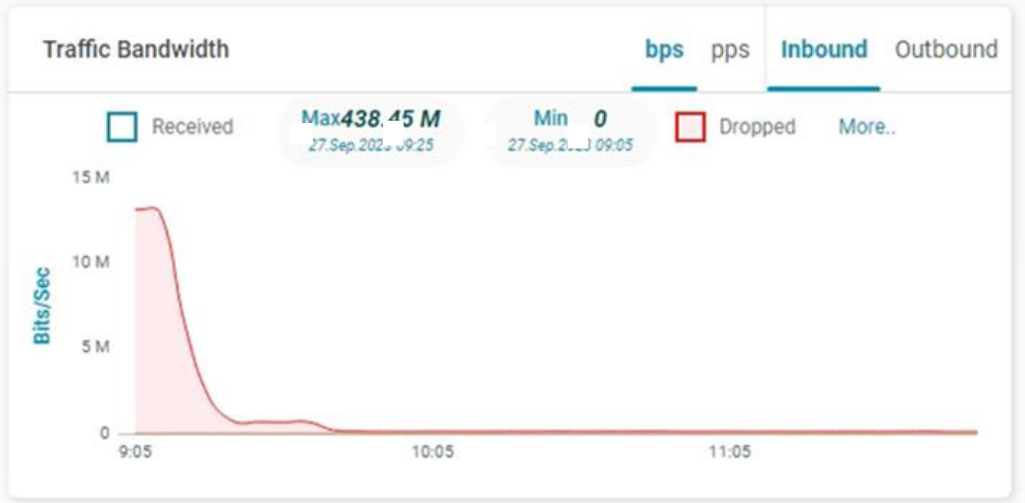


Рис. 3.9 - Завершення атаки на Radware

IPv4-адреси з найбільшою кількістю запитів на перевірку Check Point NDR та Cisco ASA були цензуровані. Загалом 107 адрес, які брали участь в DDoS-атаках, було заблоковано від продовження атак на мережу.

3.4. Висновки до третього розділу

З невдалої спроби атаки на мережу OBD банку Kanva можна зробити висновок, що PCM та системи безпеки в ній побудовані, налаштовані та обрані на рівні, який запобігає негативному впливу зловмисників на критичний ресурс, що несе конфіденційну інформацію.

Обране апаратне та програмне забезпечення запобігало доступу неавторизованих осіб до конфіденційної інформації. Було проведено дослідження різних небезпек, які можуть негативно вплинути на банківську систему та негативно вплинути на бізнес.

На основі отриманої інформації було визначено десять найбільших небезпек та ризиків. Було описано методи та принципи використання, щоб легше розпізнати та запобігти їх виникненню. Крім того, було надано пропозиції щодо конкретного запобігання кожній загрозі.

ВИСНОВКИ

У процесі підготовки необхідної роботи було виконано такі завдання:

Досліджено функції інформаційно-комунікаційних мереж у банківських установах.

Виявлено складові створення системи кібербезпеки для передачі секретних даних у фінансовій установі;

• Оцінено та застосовано рекомендації щодо підвищення ступеня безпеки цифрового зв'язку банківської організації в умовах цифрових атак.

1. У першій частині статті описано та пояснено різні формати банківських мереж, що використовуються організаціями по всьому світу та в Україні, ці організації запозичили свій досвід з цих мереж. Було наголошено на важливості безпеки системи передачі даних у фінансовій установі. Було описано популярні та значущі тенденції в IT, які стосуються банківської справи та повинні враховуватися при впровадженні нових технологій.

2. У другому розділі розглянуто різні концепції архітектур кібербезпеки та наведено конкретний приклад однієї з них, в якому детально розглянуто її особливості. Було розкрито ідею представлення завадостійкості під час передачі цифрової приватної інформації. Було задокументовано види збитків, пов'язаних з потенційними кіберзлочинами, метод їх оцінки та рекомендації щодо їх мінімізації.

3. У третьому розділі перераховано та детально описано можливі небезпеки для інформаційно-комунікаційних мереж фінансової установи. Також запропоновано методи зменшення їх поширеності та мінімізації. Описано предмет дослідження, представлено загальну інформацію про склад та організацію мережі. Додано звіт, у якому детально описано атаку та реакцію на неї систем інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Dr. Nirmalarajah Asokan. Banking Networks, Protocols and Formats You Should Know About. [Електронний ресурс]. – Режим доступу: https://agicap.com/en/article/banking-networks-protocols-formats/

2. H. D. Lin, “True reason for breakdown of Facebook and Yahoo,” Business Weekly, vol.1320, pp.70‑71, 2013

3. C. Lozano-Garzon, C. Ariza-Porras, S. Rivera-Diaz, H. Riveros-Ardila, and Y. Donoso, “Mobile network QoE-QoS decision making tool for performance optimization in critical web service,” International Journal of Computers Communications Control, vol.7, no.5, pp.892‑899, 2012

4. Y. K. Lin and L. C. LouisYeng, “Evaluation of network reliability for computer networks with multiple sources”, Mathematical Problems in Engineering, vol.2012, Article ID 737562, p.18, 2012

5. Gartner Survey of Over 2,000 CIOs Reveals the Need to Accelerate Time to Value from Digital Investments. [Електронний ресурс]. – Режим доступу: https://www.gartner.com/en/newsroom/press-releases/2022-10-18-gartner-survey-of-over-2000-cios-reveals-the-need-to-accelerate-time-to-value-from-digital-investments

6. Banking Technology Trends to Watch in 2025. [Електронний ресурс]. – Режим доступу: https://kissflow.com/solutions/banking/banking-technologies/

7. Ткач А.І., Ткач І.І. Інформаційні системи в фінансово-кредитних установах: Курс лекцій. Тернопіль: ТНЕУ, 2008. – 120с.

8. Інструкція про міжбанківський переказ грошей в Україні в національній валюті, затверджена постановою Правління Національного банку України від 17.03.2004 р. № 110. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1035-06#Text

9. Закон України "Про захист персональних даних". [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

10. NIST Special Publication 800-53 – Security and Privacy Controls for Information Systems and Organizations. [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

11. ISO/IEC 27001:2013 – Information security management systems. [Електронний ресурс]. – Режим доступу: https://www.iso.org/contents/data/standard/05/45/54534.html

12. Податковий кодекс України – положення щодо фінансових звітів та конфіденційності. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2755-17#Text

13. Möller, D. P., NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices, pp. 231-271, Cham: Springer Nature Switzerland, 2023

14. Aphane, M. P., Cybersecurity Awareness on Cybercrime Among the Youth in Gauteng Province. International Journal of Social Science Research and Review, 6(8), 23-32, 2023

15. Carcary, M., Doherty, E., and Conway, G., A framework for managing cybersecurity effectiveness in the digital context. In European Conference on Cyber Warfare and Security, pp. 78-86, Academic Conferences International Limited, 2019

16. Almuhammadi, S., and Alsaleh, M., Information security maturity model for NIST cyber security framework. Computer Science & Information Technology (CS & IT), 7(3), 51-62, 2017

17. Le, N. T., and Hoang, D. B., Capability maturity model and metrics framework for cyber cloud security. Scalable Computing, 2017

18. Sulistyowati, D., Handayani, F., and Suryanto, Y., Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. JOIV: International Journal on Informatics Visualization, 4(4), pp. 225-230, 2017

19. Curtis, P. D., and Mehravari, N., Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. In 2015 IEEE

international symposium on technologies for homeland security (hst), pp. 1-6, IEEE, 2015

20. Qadir, S., and Quadri, S. M. K., Information availability: An insight into the most important attribute of information security. Journal of Information Security, 7(3), pp. 185-194, 2016

21. Samonas, S., and Coss, D., The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3), 2014

22. HIZA, D., Assessing the Significance of Cia Triad Security Model in Establishing ICT Security Controls in The Public Sector (Doctoral dissertation, Institute of Accountancy Arusha (IAA)), 2022

23. Usman, M., Jan, M. A., He, X., and Chen, J., A survey on representation learning efforts in cybersecurity domain. ACM Computing Surveys (CSUR), 52(6), pp. 1-28, 2019

24. Obrst, L., Chase, P., and Markeloff, R., Developing an Ontology of the Cyber Security Domain. In STIDS, pp. 49-56, 2012

25. Collier, Z. A., Linkov, I., and Lambert, J. H., Four domains of cybersecurity: a risk-based systems approach to cyber decisions. Environment Systems and Decisions, 33, pp. 469-470, 2013

26. Sabillon, R., Serra-Ruiz, J., Cavaller, V., and Cano, J., A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In 2017 International Conference on Information Systems and Computer Science (INCISCOS), pp. 253-259, IEEE, 2017

27. Wang, H., Lau, N., and Gerdes, R. M., Examining cybersecurity of cyberphysical systems for critical infrastructures through work domain analysis. Human factors, 60(5), pp. 699-718, 2018

28. Pfleeger C. P., Pfleeger S. L. Security in Computing. New Jersey: Prentice Hall, 2003. 746 p.

29. Nieles M., Dempsey K., Pillitteri V. Y. An Introduction to Information Security. National Institute of Standards and Technology Special Publication 800-12 Revision 1, June 2017. 101 p.

30. Шаров В. О., Нікуліна О. М. Дворівнева концепція для моделювання єдиної завадостійкої передачі цифрових даних. Вісник Національного технічного університету «Харківський політехнічний інститут»: сб. наук. пр. Темат. вип.: Системний аналіз, управління та інформаційні технології. Харків: НТУ «ХПІ», 2024, №1 (11), с. 70-75.

31. Шаров В. О., Нікуліна О. М., Северин В. П. Моделювання та аналіз кодерів завадостійких каскадних кодів для динамічних систем. Вісник Національного технічного університету «Харківський політехнічний інститут»: сб. наук. пр. Темат. вип.: Системний аналіз, управління та інформаційні технології. Харків: НТУ «ХПІ», 2023, № 1 (9). С. 64–69.

32. Шаров В. О., Нікуліна О. М., Лошкарьова С. Є. Розробка гнучкої моделі завадостійкої передачі даних для управління динамічними системами. Інформаційні технології: наука, техніка, технологія, освіта, здоров’я: Тези доповідей XXXI міжнародної науково-практичної конференції MicroCAD-2023. Харків: НТУ «ХПІ», 2023. С. 1048

33. Лосев Ю. І., Шматков С. І. Основи теорії передачі інформації. Харків: ХНУ ім. В. Н. Каразіна, 2013. 290 с.

34. Yue Tang, Tian Mao, Bing Jiang, Design and Experiment of Multi-resolution Composite Digital Array Antenna. Journal of Radars. 2016, 5 (3). P. 265.

35. Банкет В. Л., Іващенко П. В., Іщенко М. О. Завадостійке кодування в телекомунікаційних системах. Одеса: ОНАЗ ім. О. С. Попова, 2011. 100 с.

36. IBM. "Cost of a Data Breach Report 2023.". [Електронний ресурс]. – Режим доступу: https://10guards.com/ru/blog/2024/01/07/ibm-cost-of-a-data-breach-report-2023-reveals-huge-business-data-breach-costs/

37. European Commission. "General Data Protection Regulation (GDPR).". [Електронний ресурс]. – Режим доступу: https://gdpr-info.eu/

38. ISO/IEC 27005:2018. "Information security risk management.". [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/75281.html

39. NIST. "Multi-Factor Authentication Best Practices.". [Електронний ресурс]. – Режим доступу: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication

40. SANS Institute. "Incident Response Plan Template.". [Електронний ресурс]. – Режим доступу: https://www.sans.org/white-papers/1516/

41. Gartner. "SIEM Solutions for Financial Institutions.". [Електронний ресурс]. – Режим доступу: https://www.gartner.com/reviews/market/security-information-event-management

42. Banking's Top 10 Cybersecurity Threats. [Електронний ресурс]. – Режим доступу: https://register.bank/media/top-cybersecurity-threats-banking/

43. Most common security incidents in the cloud and on-premises worldwide in 2024. [Електронний ресурс]. – Режим доступу: https://www.statista.com/statistics/1320178/common-cloud-security-attacks-worldwide/

44. That panicky call from a relative? It could be a thief using a voice clone, FTC warns. [Електронний ресурс]. – Режим доступу: https://www.npr.org/2023/03/22/1165448073/voice-clones-ai-scams-ftc

45. What is a Hardware Firewall? [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-a-hardware-firewall/

46. Radware Defense Pro. [Електронний ресурс]. – Режим доступу: http://www.infobezpeka.com/products/apatnye/?view=395

47. Cisco Secure Firewall ASA. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html

48. 13 Best DDoS Protection Software in the Market 2024. [Електронний ресурс]. – Режим доступу: https://www.indusface.com/blog/best-ddos-protection-software/

49. DDoS Protection. [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/products/ddos/fortiddos

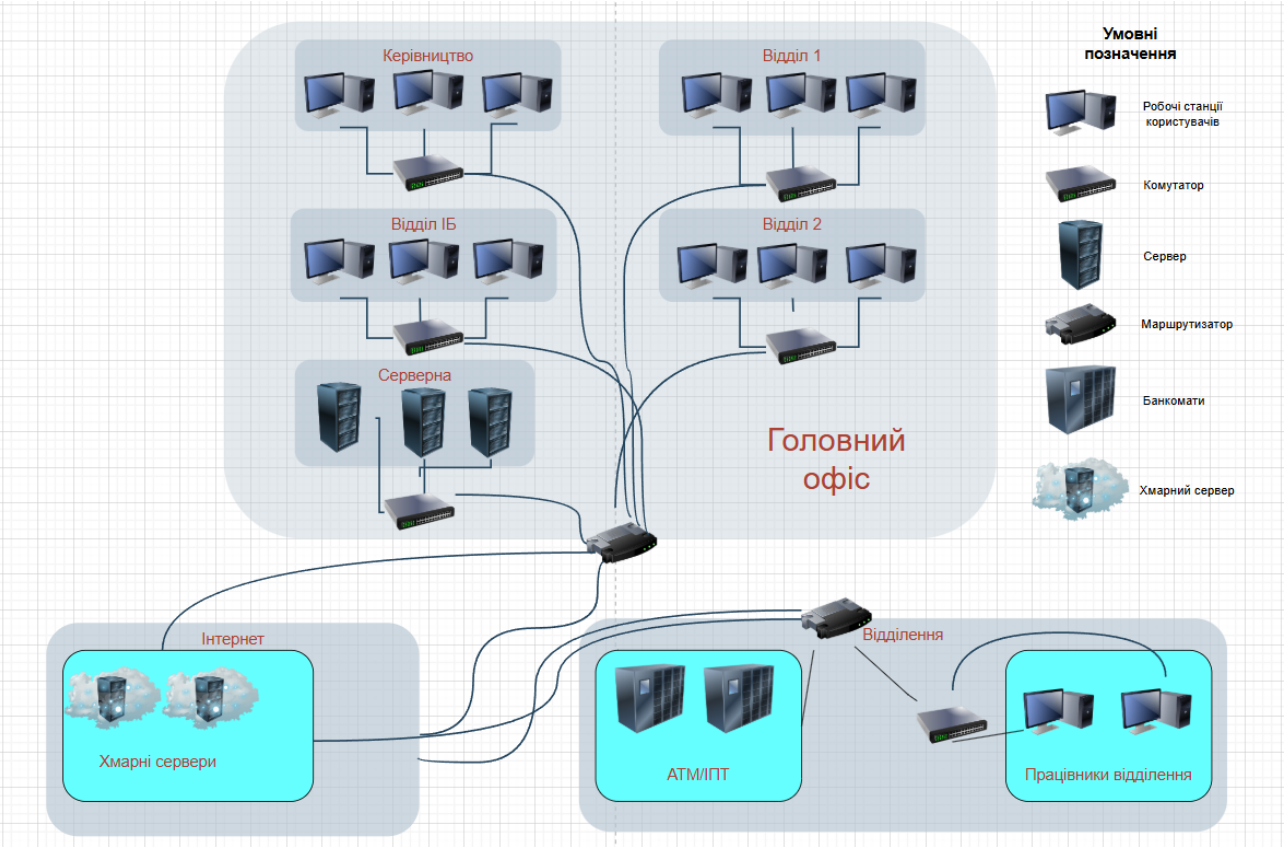
50. Що таке SIEM? [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem

51. IBM QRadar SIEM. [Електронний ресурс]. – Режим доступу: https://csc-ua.com/qradar-siem/

52. What Is Network Detection and Response? [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/security/what-is-network-detection-response.html

53. What is Network Detection and Response (NDR)? [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-network-detection-and-response-ndr/

ДОДАТОК А


Керівництво
Відділ 1
Відділ ІБ
Відділ 2
Серверна
Головний офіс
Умовні позначення
Робочі станції користувачів
Комутатор
Сервер
Маршрутизатор
Банкомати
Хмарний сервер
Інтернет
Хмарні сервери
Відділення
АТМ/ІПТ
Працівники відділення

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

Презентація до кваліфікаційної роботи магістра

УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ МЕРЕЖЕВИХ КАНАЛІВ БАНКІВСЬКОЇ УСТАНОВИ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Євген НАГАЄВ

Керівник: д.т.н., професор Олександр ТУРОВСЬКИЙ

Київ - 2025

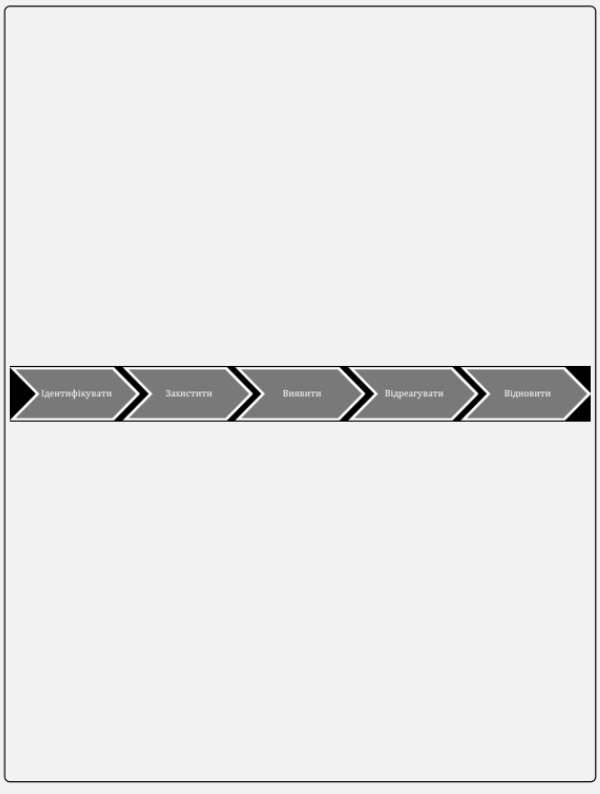
АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

- Актуальність роботи визначається високою критичністю банківських інформаційно-комунікаційних мереж та необхідністю захисту конфіденційних даних, що передаються мережевими каналами.
- Мета роботи - підвищення ефективності захисту мережевих каналів банківської установи від несанкціонованого доступу до конфіденційної інформації.
- Завдання: дослідити особливості роботи банківських мереж, розкрити елементи побудови системи кібербезпеки та сформувати рекомендації щодо підвищення рівня захисту в умовах мережевих атак.
- Об’єкт дослідження - інформаційні мережі банківських установ. Предмет - системи кібербезпеки мережевих каналів передачі конфіденційних даних.

СТРУКТУРА МАГІСТЕРСЬКОЇ РОБОТИ

- Перший розділ присвячено протоколам і форматам банківських мереж, надійності передавання даних, тенденціям IT-технологій, банківським інформаційним системам і типам конфіденційних даних.
- Другий розділ розкриває архітектури кібербезпеки, концепцію завадостійкого передавання цифрових даних, оцінку потенційних збитків та стратегії мінімізації ризиків.
- Третій розділ містить рекомендації щодо захисту ІКМ ОБД від фішингу, шкідливого ПЗ, DDoS-атак, спуфінгу, хмарних атак, атак на ланцюги поставок та SQL-ін’єкцій.
- Практична частина включає опис мережі «Канва Банк» та комплекс засобів: апаратний міжмережевий екран, DDoS Protection, SIEM і NDR.

ПРОТОКОЛИ ТА ФОРМАТИ БАНКІВСЬКИХ МЕРЕЖ



- Для банківських мереж розглянуто H2H-з’єднання, EBICS, SWIFT, PSD2/Open Banking та ISO 20022.
- H2H забезпечує прямий захищений обмін між банком і клієнтською інфраструктурою; EBICS орієнтований на стандартизований банківський обмін у Європі.
- SWIFT використовується як глобальна мережа фінансових повідомлень, PSD2 формує API-доступ, а ISO 20022 задає уніфікований формат фінансових повідомлень.

ТИПИ КОНФІДЕНЦІЙНИХ ДАНИХ У БАНКІВСЬКІЙ МЕРЕЖІ

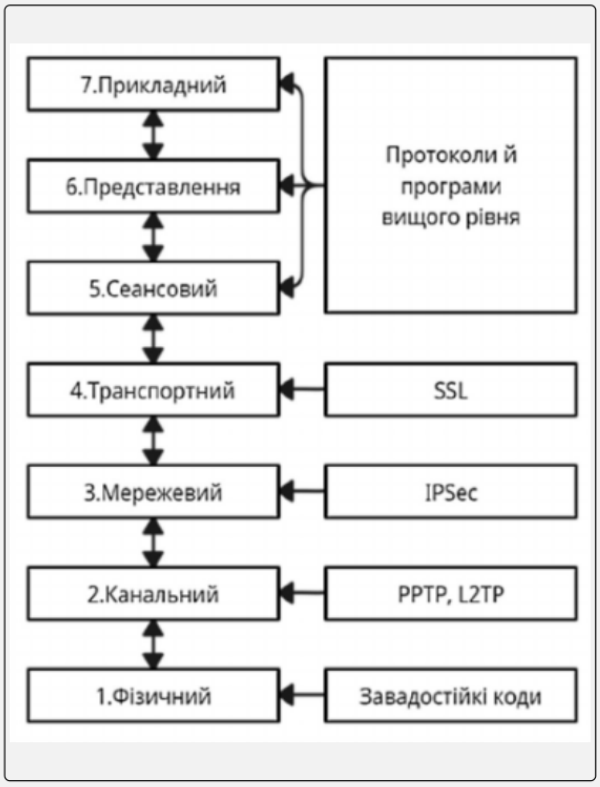
Домени можливостей NIST	Сертифікація CISSP	Сертифікація GSEC	Архітектура з відкритим кодом	Розшифрована зона
Контроль доступу	Безпека та управління ризиками	Активна оборона	Шаблони безпеки IT-послуг	Безпека мережі
Оцінка безпеки	Безпека активів	Криптографія	IT шаблони рівня додатків	Хмарна безпека
Обізнаність і навчання	Інженерія безпеки	Захищена мережева архітектура	Шаблони IT-інфраструктури	Безпека програм
Управління ризиками	Комунікаційна та мережева безпека	Обробка інцидентів і реагування	Центральна служба безпеки	Безпека критичної інфраструктури
Ситуаційна обізнаність	Керування ідентифікацією та доступом	Безпека Linux	Управління	Безпека кінцевого користувача
Управління активами	Оцінка безпеки та тестування	Політика безпеки		Аварійне відновлення
Захист медіа	Операції безпеки	Безпека веб-підключень		Інформаційна безпека
Технічне обслуговування	Безпека розробки ПЗ			Безпека зберігання
Персональна безпека				Мобільна безпека
Аудит та звітність				
Захист системи та зв'язку				
Ідентифікація та автентифікація				

- До критичних даних віднесено персональні дані клієнтів, фінансову інформацію, історію транзакцій, кредитні дані, дані співробітників і технічні параметри IT-інфраструктури.
- Найвищий рівень конфіденційності мають реквізити карток, банківські рахунки, транзакційна історія та регуляторна інформація.
- Порушення конфіденційності таких даних призводить до фінансових втрат, репутаційних ризиків і правових наслідків для банківської установи.

АРХІТЕКТУРА КІБЕРБЕЗПЕКИ БАНКІВСЬКОЇ МЕРЕЖІ

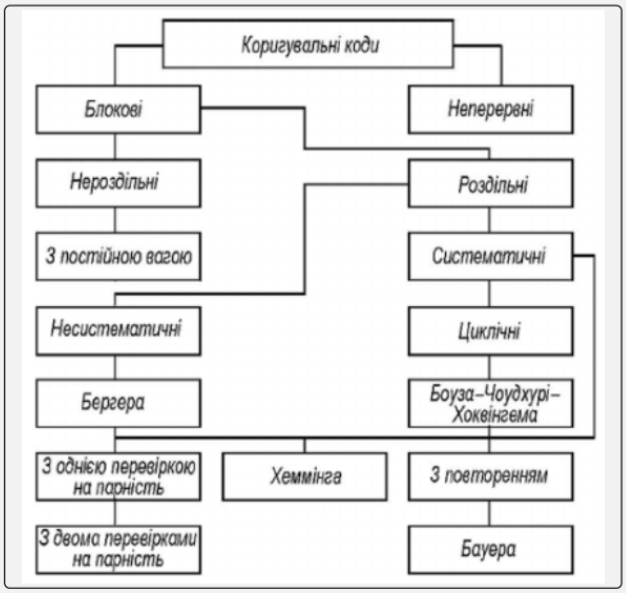
- Основою архітектури кібербезпеки є забезпечення конфіденційності, цілісності та доступності інформації.
- У роботі виділено домени: мережева безпека, безпека кінцевих точок, безпека критичної інфраструктури, хмарна безпека, безпека користувача, управління ризиками та відповідністю.
- Комплексна архітектура дозволяє оцінювати захист не окремих вузлів, а всієї банківської інформаційно-комунікаційної мережі.

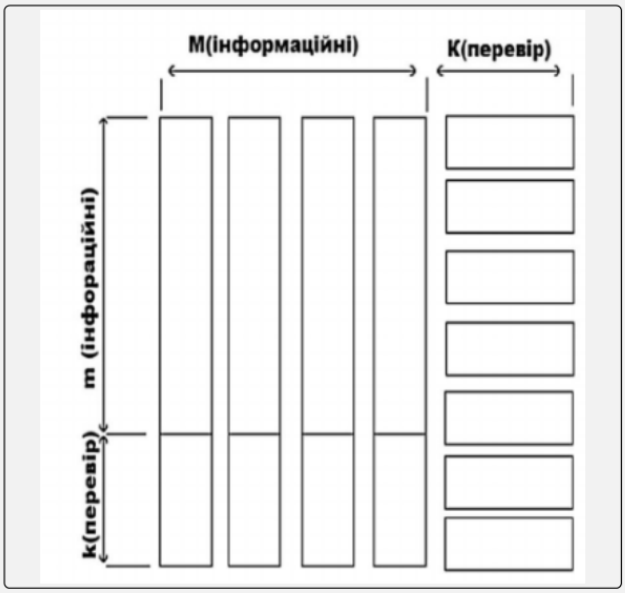
КОНЦЕПЦІЯ ЗАВАДОСТІЙКОГО ПЕРЕДАВАННЯ ЦИФРОВИХ ДАНИХ



- У роботі розглянуто концепцію моделювання завадостійкої передачі цифрових даних через мережеві канали.
- Модель враховує вплив каналів, алгоритмів обробки сигналів, функцій кодування/декодування та характеристик середовища передавання.
- Мета концепції - підвищення стійкості банківського обміну до спотворення, втрат і несанкціонованого впливу на передані дані.

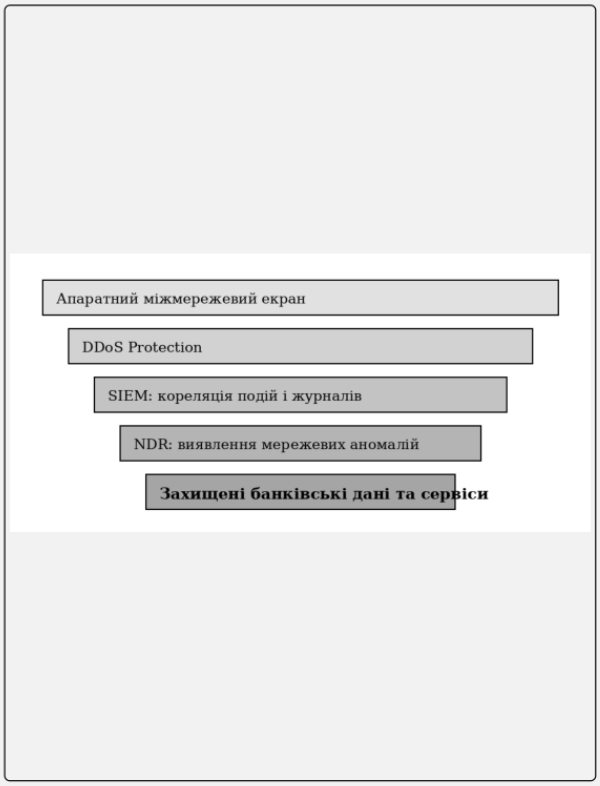
МАТЕМАТИЧНЕ ПРЕДСТАВЛЕННЯ ТА РІВНІ КОНЦЕПЦІЇ





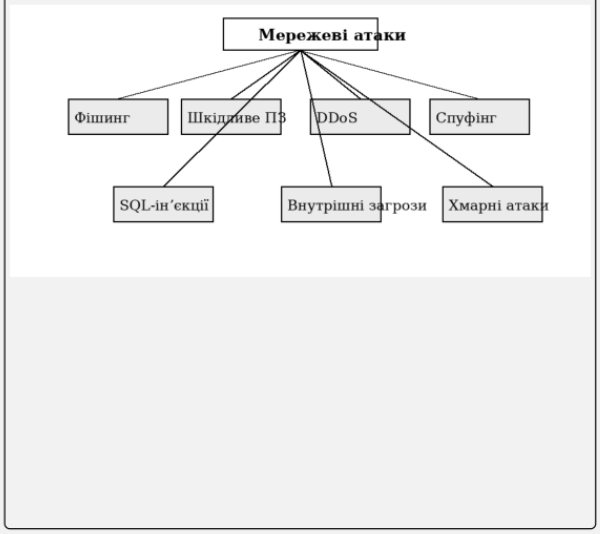
- У роботі використано формалізовані залежності для оцінювання параметрів передавання, а також подано структурні рівні концепції захищеної передачі цифрових даних.

ОЦІНКА ЗБИТКІВ І СТРАТЕГІЇ МІНІМІЗАЦІЇ РИЗИКІВ



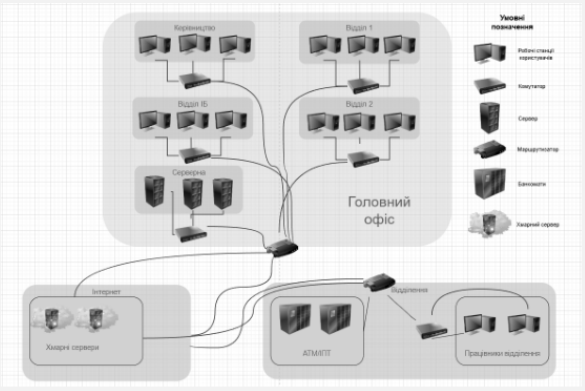
- Потенційні збитки від кіберінцидентів включають прямі фінансові втрати, простої сервісів, витрати на відновлення, штрафи та репутаційні наслідки.
- Мінімізація ризиків передбачає запобігання інцидентам, швидке реагування, довгострокове вдосконалення політик безпеки та постійний моніторинг.
- Пріоритет надається багаторівневому захисту мережевих каналів і сервісів банківської установи.

ОСНОВНІ МЕРЕЖЕВІ ЗАГРОЗИ ДЛЯ ІКМ ОБД



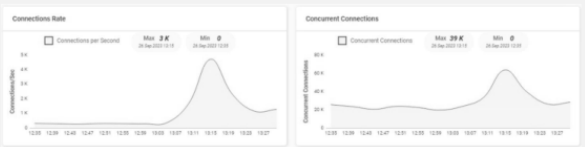
- У роботі розглянуто фішинг, шкідливе програмне забезпечення, DDoS-атаки, спуфінг, внутрішні загрози, атаки на хмарні технології, атаки на ланцюги поставок, SQL-ін'єкції та діпфейки.
- Найбільш критичними для банківської мережі є DDoS-атаки, компрометація облікових записів, фішинг і порушення роботи застарілих систем.
- Захист має включати як технічні засоби, так і навчання персоналу та контроль дотримання політик безпеки.

ОПИС ІКМ ОБ’ЄКТУ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ «КАНВА БАНК»



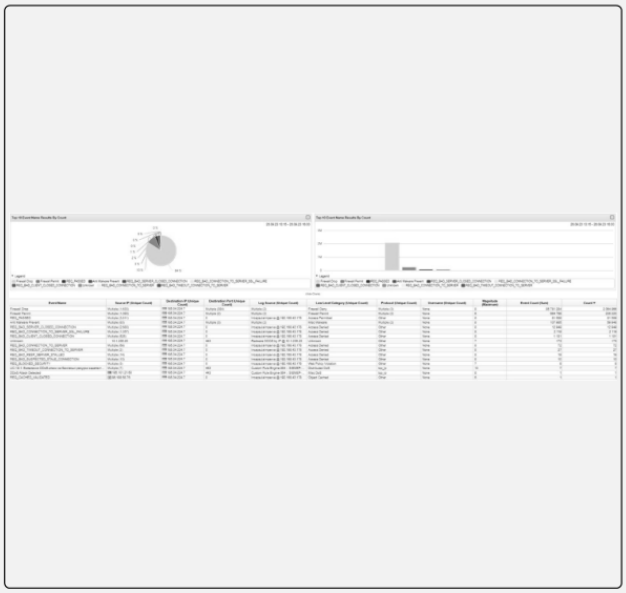
- Інформаційно-комунікаційна мережа банку включає серверну інфраструктуру, робочі станції, сегменти обслуговування клієнтів, мережеві шлюзи та засоби захисту периметра.
- Сегментація мережі дозволяє відокремити критичні банківські сервіси від користувацьких зон та зовнішніх каналів зв’язку.
- Захист будується навколо контролю трафіку, моніторингу подій, виявлення аномалій і протидії відмові в обслуговуванні.

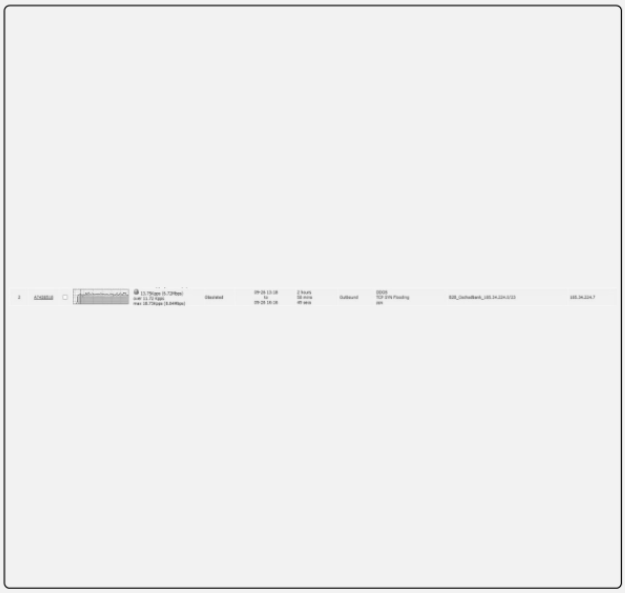
АПАРАТНИЙ МІЖМЕРЕЖЕВИЙ ЕКРАН ТА DDOS PROTECTION



- Апаратний міжмережевий екран використовується для фільтрації трафіку, контролю доступу, сегментації мережі та блокування небажаних з’єднань.
- DDoS Protection забезпечує виявлення аномального зростання трафіку, фільтрацію шкідливих потоків і підтримання доступності банківських сервісів.
- Комбінація firewall + anti-DDoS формує перший технічний бар’єр проти атак на мережеві канали.

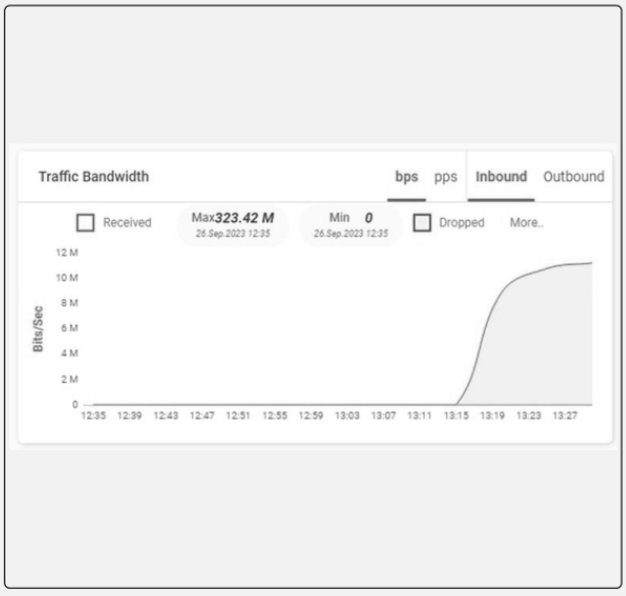
SIEM ТА NDR ЯК ЗАСОБИ МОНІТОРИНГУ І ВИЯВЛЕННЯ ІНЦИДЕНТІВ





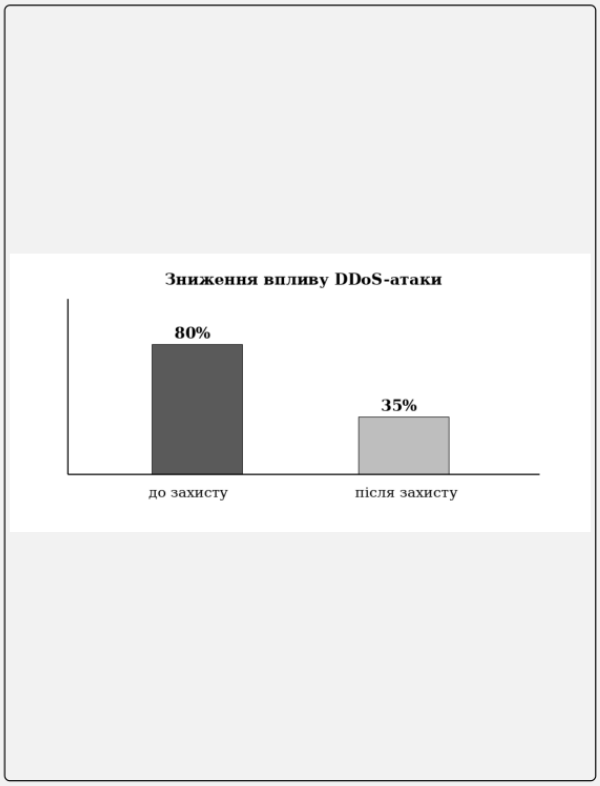
- SIEM централізує збір і кореляцію подій безпеки, а NDR аналізує мережеву поведінку та виявляє аномалії, які можуть свідчити про атаку або компрометацію.

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ КОМПЛЕКСУ ЗАХИСТУ НА ПРИКЛАДІ DDOS-АТАКИ



- Порівняння графіків демонструє різке зростання шкідливого трафіку під час атаки та подальше зменшення навантаження після спрацювання засобів захисту.

ОЦІНКА РЕЗУЛЬТАТИВНОСТІ ЗАПРОПОНОВАНОГО КОМПЛЕКСУ ЗАХИСТУ



- Запропонований комплекс поєднує периметровий захист, anti-DDoS, SIEM-моніторинг, NDR-виявлення мережевих аномалій та організаційні заходи реагування.
- Очікуваний ефект полягає у зниженні впливу мережевих атак, скороченні часу виявлення інцидентів і підвищенні доступності банківських сервісів.
- Комплекс забезпечує не лише блокування атак, а й аналітичну основу для подальшого вдосконалення політики кібербезпеки.

ВИСНОВКИ

- У роботі досліджено особливості функціонування інформаційно-комунікаційної мережі банківської установи при передаванні конфіденційних даних.
- Проаналізовано архітектури кібербезпеки, домени захисту, методи оцінювання збитків і стратегії мінімізації ризиків від кіберінцидентів.
- Розглянуто основні загрози для ІКМ ОБД: фішинг, шкідливе ПЗ, DDoS, спуфінг, хмарні атаки, атаки на ланцюги поставок, SQL-ін’єкції та діпфейки.
- Запропоновано комплекс засобів захисту для «Канва Банк»: апаратний міжмережевий екран, DDoS Protection, SIEM та NDR, що підвищує стійкість мережевих каналів до атак.