Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *" Розробка та впровадження системи виявлення та запобігання кібератак у банківському секторі. "*

Виконав: студент

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Коваль В. В.
підпис (прізвище та ініціали)

Керівник *Стадник М. А.*
підпис (прізвище та ініціали)

Нормоконтроль
підпис (прізвище та ініціали)

Завідувач кафедри *Загородна Н.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

АНОТАЦІЯ

Розробка та впровадження системи виявлення та запобігання кібератак у банківському секторі.// Кваліфікаційна робота ОР «Бакалавр» // Коваль Василь Васильович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2023 // С. – 61, рис. – 10, табл. – 0, кресл. – 0, додат. – 0.

Ключові слова: КІБЕРБЕЗПЕКА, БАНКІВСЬКИЙ СЕКТОР, КІБЕРАТАКИ, ВИЯВЛЕННЯ ТА ПРОФІЛАКТИКА.

У даній роботі розглядається розробка та впровадження системи SecureBankGuard для виявлення та запобігання кібератак в банківському секторі. Практична частина охоплює два основних елементи системи: мережевий інтранет-сервіс та централізовану систему керування подіями та безпекою.

Мережевий інтранет-сервіс забезпечує контроль трафіку та захист мережі банку від зовнішніх загроз. Він використовує передові алгоритми аналізу мережевого трафіку для виявлення незвичайних активностей та атак.

Централізована система керування подіями та безпекою забезпечує збір, аналіз та кореляцію даних щодо подій безпеки. Вона використовує передові технології розпізнавання аномалій для виявлення підозрілих активностей та атак у реальному часі.

Розробка та впровадження системи SecureBankGuard допомагають банківському сектору покращити кібербезпеку, захистити мережу та дані клієнтів від загроз, та забезпечити надійність та стабільність банківської системи.

ANNOTATION

Development and implementation of a system for detecting and preventing cyberattacks in the banking sector.// Qualification work of OR "Bachelor" // Koval Vasyl Vasyliovych // Ivan Pulyuy Ternopil National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, group SBs-41 // Ternopil, 2023 // P. – 61, fig. – 10, tab. - 0, chair. – 0, add. - 0.

Keywords: CYBER SECURITY, BANKING SECTOR, CYBER ATTACKS, DETECTION AND PREVENTION.

This work considers the development and implementation of the SecureBankGuard system for detecting and preventing cyberattacks in the banking sector. The practical part covers two main elements of the system: a network intranet service and a centralized event and security management system.

The network intranet service provides traffic control and protection of the bank's network from external threats. It uses advanced network traffic analysis algorithms to detect unusual activities and attacks.

A centralized event and security management system provides security event data collection, analysis and correlation. It uses advanced anomaly detection technologies to detect suspicious activity and attacks in real time.

The development and implementation of the SecureBankGuard system helps the banking sector improve cyber security, protect the network and customer data from threats, and ensure the reliability and stability of the banking system.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IBS	Information banking system
ШІ	Штучний інтелект
APT	Advanced Persistent Threats
SWIFT	World Interbank Financial Telecommunication Society
MFA	Багатофакторна автентифікація
2FA	Двофакторна автентифікація
MitM	Man-in-the-Middle

ВСТУП

У сучасному цифровому світі банківський сектор відіграє ключову роль у світовій економіці. Однак із зростаючою залежністю від технологій і зростаючою складністю кіберзагроз забезпечення безпеки та цілісності банківських систем стало невідкладним пріоритетом. Кібератаки, націлені на фінансові установи, можуть призвести до жахливих наслідків, починаючи від фінансових втрат і закінчуючи репутаційною шкодою та ерозією суспільної довіри. Для боротьби з цією системою загроз, що постійно змінюється, розробка та впровадження надійних систем виявлення та запобігання кібератакам стали важливими для банківського сектору.

Розробка та впровадження системи виявлення та запобігання кібератакам у банківському секторі є багатогранним заходом, який охоплює різні елементи. По-перше, це передбачає створення надійної системи безпеки, що охоплює політики, процедури та протоколи, спрямовані на усунення потенційних вразливостей і встановлення проактивного захисту від кіберзагроз. Ця структура повинна охоплювати не лише технологічні аспекти, а й людський фактор, оскільки обізнаність працівників і дотримання протоколів безпеки є вирішальними для підтримки безпечного банківського середовища.

По-друге, система повинна інтегрувати передові технології та інструменти, спеціально розроблені для виявлення та запобігання кіберзагрозам. Це включає в себе розгортання систем виявлення та запобігання вторгненням (IDPS), брандмауерів, рішень для захисту кінцевих точок і систем безпеки та керування подіями (SIEM). Ці технології працюють у тандемі, щоб постійно аналізувати й ідентифікувати потенційні загрози, дозволяючи банкам швидко й ефективно реагувати на ризики, пов’язані з кібератаками.

Крім того, впровадження надійних механізмів автентифікації, таких як багатофакторна автентифікація та біометрична ідентифікація, зміцнює безпеку банківських систем, ускладнюючи доступ неавторизованих осіб до конфіденційної інформації.

Крім того, життєво важливим компонентом ефективної системи виявлення та запобігання кібератакам є постійний моніторинг і аналіз мережі, системних журналів і поведінки користувачів. Використовуючи передову аналітику та алгоритми машинного навчання, банки можуть виявляти аномалії, визначати шаблони зловмисної діяльності та оперативно реагувати на потенційні загрози. Цей проактивний підхід дозволяє банкам бути на крок попереду кіберзлочинців і мінімізувати вплив атак на їх інфраструктуру та клієнтів.

Підсумовуючи, банківський сектор стикається з постійно зростаючими кіберзагрозами, і розробка та впровадження системи виявлення та запобігання кібератакам стали першочерговими. Поєднуючи надійні системи безпеки, передові технології та постійний моніторинг і аналіз, банки можуть зміцнити свій захист, захистити дані клієнтів і зберегти довіру своїх зацікавлених сторін. Застосування проактивного підходу до кібербезпеки є не лише нормативною вимогою, але й важливою інвестицією у захист цілісності банківської галузі та глобальної фінансової екосистеми в цілому.

Метою кваліфікаційної роботи є розроблення методу для виявлення та перехоплення можливих кібератак у банківському секторі. Для досягнення цієї мети необхідно вирішити ряд завдань, які представлено нижче у вигляді списку:

- Дослідити та проаналізувати історичний вплив кібер атак на банківський сектор.
- Визначити вразливі місця та ризики, характерні для ландшафту кіберзагроз банківської галузі.
- Ознайомитись з технологіями, методологіями та найкращими практиками, які використовують фінансові установи для ефективного зниження кіберризиків.
- Запропонувати комплексну систему, яка об’єднує найсучасніші технології та адаптовані системи безпеки.

1 ІНФОРМАЦІЙНА БАНКІВСЬКА СИТЕМА

1.1 Інформаційна банківська система та її застосування

Інформаційна банківська система (IBS) є невід'ємною частиною сучасного банківського ландшафту, пропонуючи банкам і фінансовим установам інструменти для ефективного управління величезними обсягами даних і надання виняткового досвіду клієнтам. Використовуючи можливості IBS, фінансові установи можуть оптимізувати свої операції, покращити обслуговування клієнтів і приймати рішення на основі даних для довгострокового успіху.

Компоненти інформаційної банківської системи: IBS складається з кількох ключових компонентів, які працюють у тандемі, щоб забезпечити ефективне управління даними. Апаратна інфраструктура включає сервери, мережі та системи зберігання даних, які утворюють магістраль системи. Ці компоненти забезпечують доступність, надійність і масштабованість, необхідні для обробки величезних обсягів даних, створених банківськими операціями. Програмні додатки, спеціально розроблені для управління взаємовідносинами з клієнтами, керування обліковими записами, обробки транзакцій, оцінки ризиків, звітності та аналітики, становлять ядро IBS. Ці програми забезпечують необхідні функції для ефективного виконання різноманітних банківських завдань. Надійне зберігання даних і заходи безпеки забезпечують конфіденційність і цілісність конфіденційної інформації.

Застосування інформаційної банківської системи в управлінні взаємовідносинами з клієнтами: IBS революціонізує управління взаємовідносинами з клієнтами, надаючи комплексні інструменти для збору, організації та аналізу даних. Інтегруючи дані про клієнтів із кількох каналів, включаючи філії, кол-центри та цифрові платформи, банки можуть створити єдине уявлення про кожного клієнта. За допомогою IBS банки можуть ефективно керувати інформацією про клієнтів, уподобаннями та взаємодією, забезпечуючи персоналізований банківський досвід. Використовуючи можливості аналітики, банки можуть визначати потреби, уподобання та поведінку клієнтів, що дозволяє

їм адаптувати продукти та послуги для окремих клієнтів. IBS також оптимізує комунікацію з клієнтами, дозволяючи банкам відстежувати взаємодію клієнтів, надавати проактивну підтримку та проводити цільові маркетингові кампанії,

IBS відіграє вирішальну роль в управлінні рахунками, спрощуючи процеси та підвищуючи ефективність. Банки можуть використовувати систему для безпроблемного створення, обслуговування та закриття рахунків. IBS автоматизує завдання, пов’язані з обліковим записом, наприклад відкриття рахунку, оновлення інформації про клієнта та керування закриттям рахунку. Запити та оновлення балансу в реальному часі надають клієнтам точну інформацію, що дає їм змогу приймати обґрунтовані фінансові рішення. Функції відстеження історії транзакцій і звітності дозволяють легко отримати доступ до минулих дій, допомагаючи клієнтам зберігати свої рахунки та переглядати деталі транзакцій. Завдяки IBS банки можуть ефективно вирішувати завдання, пов’язані з рахунками, зменшуючи ручні зусилля, мінімізуючи помилки та підвищуючи задоволеність клієнтів (див рисунок 1.1) [1].

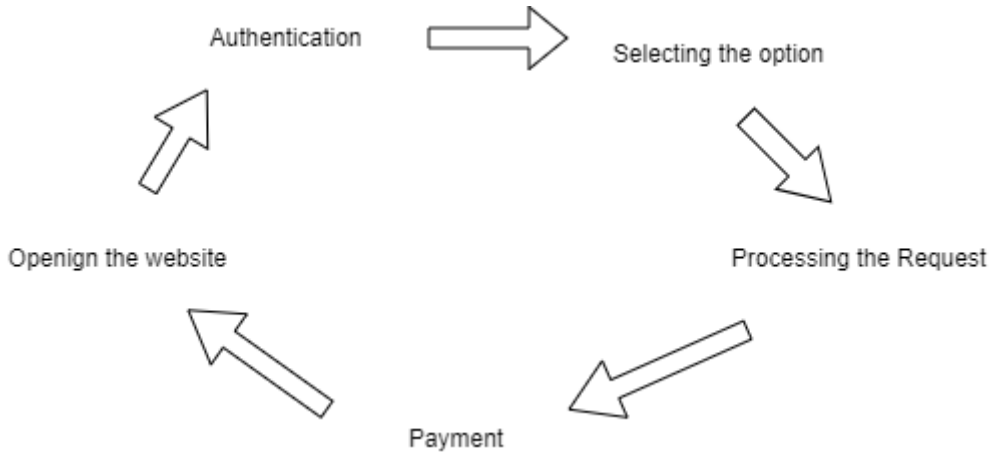

Рисунок 1.1 – Процес електронного банкінгу

Інформаційно-банківська система революціонізує обробку транзакцій шляхом автоматизації та оптимізації різноманітних банківських операцій. Банки щодня обробляють численні транзакції, включаючи депозити, зняття коштів, перекази коштів, виплату кредитів і платежі. IBS спрощує ці процеси, забезпечуючи плавні та безпечні транзакції. Це дозволяє клієнтам робити

депозити та знімати через різні канали, такі як банкомати, відділення та цифрові платформи. Перекази коштів можна ініціювати та виконувати швидко, що полегшує переміщення коштів між рахунками. Процеси управління виплатою та погашенням кредиту стають більш ефективними, зменшуючи ручні зусилля та підвищуючи точність. IBS також сприяє безпечній обробці та розрахунку платежів.

Управління ризиками є критично важливим аспектом банківських операцій, і IBS пропонує надійні рішення в цій сфері. Завдяки вдосконаленим алгоритмам і аналізу даних банки можуть використовувати IBS для оцінки кредитоспроможності, андеррайтингу кредитів і оцінки ризиків. Аналізуючи дані клієнтів, моделі транзакцій і кредитну історію, IBS допомагає банкам приймати обґрунтовані рішення щодо кредитування та ефективно керувати кредитними ризиками. Система допомагає виявляти потенційні шахрайські дії, дозволяючи банкам впроваджувати превентивні заходи та захищатися від фінансових втрат. Функції моніторингу відповідності та регулятивної звітності забезпечують дотримання галузевих норм, допомагаючи банкам уникнути штрафів і репутаційних ризиків. Загалом IBS покращує можливості управління ризиками.

IBS надає потужні можливості звітності та аналітики, що дозволяє банкам отримувати цінну інформацію з величезних обсягів даних. Система об’єднує дані з багатьох джерел створюючи комплексні звіти та інформаційні панелі. Моніторинг фінансової ефективності стає точнішим і детальнішим із переглядом ключових показників ефективності в реальному часі, аналізом прибутковості та фінансовим прогнозуванням. Використовуючи аналіз даних, банки можуть отримати глибше розуміння поведінки клієнтів, уподобань і ринкових тенденцій. Це дозволяє банкам приймати рішення на основі даних, розробляти цільові маркетингові стратегії та визначати можливості для зростання. IBS також допомагає у регулятивній звітності, автоматизації підготовки та подання звітів,

IBS відіграє ключову роль у забезпеченні онлайн- та мобільних банківських послуг. З поширенням цифрових платформ клієнти очікують зручного доступу до банківських послуг у будь-який час і в будь-якому місці. IBS надає необхідну інфраструктуру та функціональні можливості для підтримки онлайн- та

мобільних банківських операцій. Завдяки зручним інтерфейсам і безпечним з'єднанням клієнти можуть отримувати доступ до своїх рахунків 24/7, виконувати транзакції та зручно керувати своїми фінансами. Платформи онлайн-банкінгу на базі IBS дозволяють клієнтам переглядати баланси на рахунках, переказувати кошти, оплачувати рахунки та дистанційно отримувати доступ до інших банківських послуг. Мобільні банківські програми ще більше розширюють ці можливості, пропонуючи додаткові функції, такі як біометрична автентифікація, мобільні платежі, і персоналізовані сповіщення. Інформаційно-банківська система покращує загальний досвід роботи клієнтів, забезпечуючи безперебійний доступ до банківських послуг і дозволяючи клієнтам ефективно керувати своїми фінансами.

Дотримання нормативних актів є критично важливим аспектом банківських операцій, і IBS відіграє вирішальну роль у забезпеченні дотримання нормативних вимог. Система містить нормативні вказівки та автоматизує процеси моніторингу відповідності. Інтегруючи дані з різних джерел, IBS дозволяє банкам проводити регулярні перевірки на відповідність, гарантуючи, що транзакції клієнтів відповідають нормативним стандартам. Крім того, IBS полегшує створення нормативних звітів, спрощуючи процес звітування та зменшуючи ручні зусилля. Маючи можливість відстежувати та аналізувати дані в режимі реального часу, банки можуть миттєво виявляти будь-які прогалини у відповідності та вживати необхідних заходів для виправлення [2].

IBS дозволяє банкам отримувати цінну інформацію про поведінку та вподобання клієнтів за допомогою розширених можливостей аналітики. Аналізуючи дані клієнтів, історію транзакцій і демографічну інформацію, банки можуть сегментувати свою клієнтську базу та розробляти цільові маркетингові стратегії. IBS надає інструменти для сегментації клієнтів на основі різних критеріїв, таких як вік, дохід, моделі витрат і використання продукту. Це дозволяє банкам пропонувати персоналізовані рекомендації щодо продуктів, індивідуальні акції та можливості цільового перехресного продажу. Розуміючи потреби та вподобання клієнтів, банки можуть підвищити задоволеність клієнтів.

У міру розвитку технологій інформаційно-банківська система готова зазнавати подальших розробок і вдосконалень. Інтеграція нових технологій, таких як штучний інтелект (ШІ), машинне навчання та блокчейн, може революціонізувати можливості IBS. Чат-боти та віртуальні помічники на основі штучного інтелекту можуть надавати персоналізовану підтримку клієнтів і ще більше оптимізувати взаємодію з клієнтами. Алгоритми машинного навчання можуть постійно аналізувати шаблони даних і виявляти аномалії, покращуючи виявлення шахрайства та управління ризиками. Технологія блокчейн має потенціал для підвищення безпеки, прозорості та ефективності транзакцій, відкриваючи шлях для швидших і безпечніших транскордонних платежів.

Безпека даних і запобігання шахрайству є першочерговими проблемами для банків, і IBS пропонує надійні рішення в цій сфері. Система включає розширені заходи безпеки для захисту конфіденційних даних клієнтів, такі як шифрування, контроль доступу та системи виявлення вторгнень. Завдяки централізації зберігання даних і застосуванню суворих протоколів безпеки IBS знижує ризик витоку даних і несанкціонованого доступу. Крім того, IBS використовує розширену аналітику та алгоритми машинного навчання для ідентифікації та виявлення шахрайських дій у режимі реального часу. Він аналізує моделі транзакцій, поведінку клієнтів і історичні дані для виявлення аномалій і потенційних шахрайських транзакцій, що дозволяє банкам негайно вжити заходів і зменшити фінансові втрати.

IBS відіграє ключову роль у стимулюванні розробки продуктів та інновацій у банківській галузі. Використовуючи дані про клієнтів і інформацію, зібрану за допомогою системи, банки можуть виявляти прогалини в своїх пропозиціях продуктів і розробляти нові рішення, які задовольняють постійні потреби клієнтів. IBS дозволяє банкам відстежувати вподобання клієнтів, аналізувати ринкові тенденції та визначати нові можливості. Ця інформація допомагає банкам запроваджувати нові продукти, вдосконалювати існуючі та випереджати конкурентів. Крім того, IBS сприяє швидкому створенню прототипів і тестуванню нових продуктів, що дозволяє банкам швидко й ефективно виводити інновації на ринок.

Інформаційно-банківська система змінила банківську галузь, зробивши революцію в управлінні даними, операційній ефективності та клієнтському досвіді. Додатки для управління взаємовідносинами з клієнтами, керування рахунками, обробки транзакцій, управління ризиками, звітності та аналітики, відповідності та онлайн-/мобільного банкінгу змінили спосіб проведення банківських операцій. Використовуючи можливості IBS, банки можуть оптимізувати процеси, покращити обслуговування клієнтів, зменшити ризики та приймати рішення на основі даних. З розвитком технологій інформаційно-банківська система й надалі відіграватиме центральну роль у формуванні майбутнього банківської справи, надаючи можливість установам відповідати очікуванням клієнтів, стимулювати інновації та орієнтуватися у постійно мінливому ландшафті фінансової галузі [3].

1.2 Історичний огляд кібератак у банківській сфері

За останні роки банківський сектор зазнав значної цифрової трансформації, спричиненої технологічним прогресом і зростанням попиту на зручні фінансові онлайн-послуги. Ця зміна принесла численні переваги, такі як покращена ефективність, доступність і покращений досвід клієнтів. Однак, поряд із цими перевагами, банківський сектор став привабливою мішенню для кіберзлочинців через величезну кількість конфіденційних фінансових і особистих даних, з якими він працює. Кібератаки в банківському секторі стали свідками постійного зростання як частоти, так і складності, створюючи значні загрози для фінансових установ, їхніх клієнтів і загальної стабільності світової економіки.

Протягом останніх років банківський сектор був сценою безлічі кібератак, які насували загрозу фінансовій безпеці і приватності користувачів. Згідно з даними, у 2019 році було зафіксовано приблизно 2 000 кібератак, у 2020 році ця цифра зросла до близько 4 500, а в 2021 році їх було вже понад 6 000. Це лише загальна статистика, і варто відзначити, що складність кібератак також зросла протягом цього періоду. Зловмисники використовують все більш витончені техніки, включаючи фішинг, розповсюдження шкідливих програм і атаки на

інфраструктуру фінансових установ. У період з 2020 по 2021 рік Україна посідає друге місце по кількості цілеспрямованих кібер атак на різні сфери діяльності (див рисунок 1.2) [4].

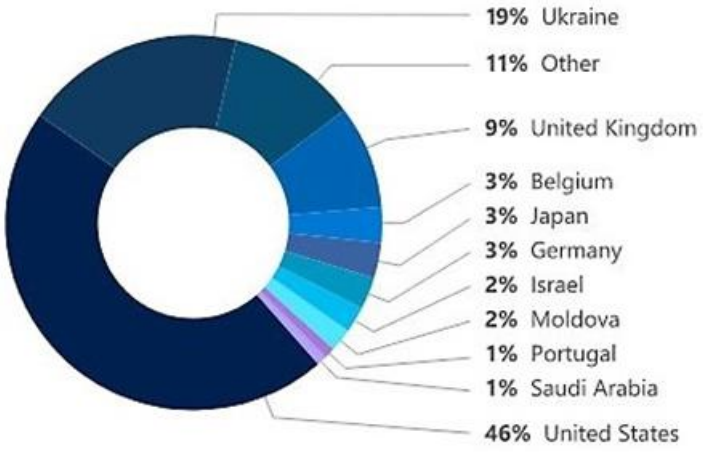

Рисунок 1.2 – Статистика кібератак у світі згідно даних Microsoft 2020-2021

У своєму річному звіті за 2022 рік Microsoft висвітлила найпоширеніші галузі для атак хакерів саме в Україні (див рисунок 1.3) [5].

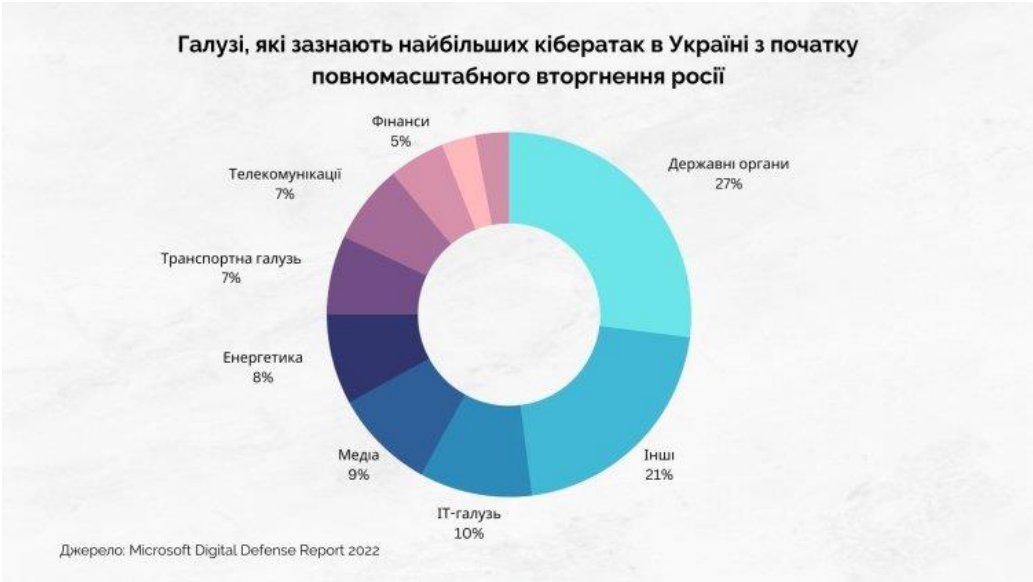

Рисунок 1.3 – Статистика кібератак в Україні

Банківський сектор пережив значну цифрову трансформацію, спричинену прогресом технологій та зміною очікувань клієнтів. Традиційні банківські

послуги, які колись переважно надавалися через фізичні відділення, перейшли в цифрову сферу. Клієнти тепер мають доступ до широкого спектру онлайнових і мобільних банківських послуг, включаючи керування рахунками, перекази коштів і онлайн-платежі. Крім того, фінансові установи використовують взаємопов'язані системи для оптимізації своїх операцій, сприяння транскордонним трансакціям і покращення співпраці з іншими зацікавленими сторонами галузі. Цифровізація та взаємозв'язок банківського сектору проклали шлях до більшої зручності та ефективності, але вони також створили нові ризики та вразливі місця.

Атаки зловмисного програмного забезпечення є звичайною та постійною загрозою для банківського сектору. Кіберзлочинці використовують різні форми шкідливого програмного забезпечення, наприклад трояни, програми-вимагачі та кейлоггери, щоб отримати несанкціонований доступ до банківських систем, компрометувати дані клієнтів або ініціювати шахрайські транзакції. Шкідливі програми можуть поширюватися через фішингові електронні листи, шкідливі завантаження або скомпрометовані веб-сайти, використовуючи вразливості програмного забезпечення або обманом змушуючи користувачів установлювати заражені програми. Потрапивши в систему, програми можуть залишатися непоміченими, дозволяючи зловмисникам збирати конфіденційну інформацію, маніпулювати транзакціями або навіть контролювати банківську інфраструктуру.

Фішингові атаки залишаються поширеним методом, який використовують кіберзлочинці для нападу на банківський сектор. Фішинг передбачає використання оманливих електронних листів, повідомлень або телефонних дзвінків, які здаються законними, щоб змусити користувачів оманою розкрити конфіденційну інформацію, як-от облікові дані для входу чи особисту інформацію. Методи соціальної інженерії, такі як видавання себе за іншу особу, психологічні маніпуляції або використання довіри, часто використовуються, щоб зробити ці атаки більш переконливими. Спонукаючи нічого не підозрюючих осіб до розголошення конфіденційної інформації, зловмисники можуть отримати несанкціонований доступ до банківських рахунків, сприяти крадіжці особистих даних або проводити шахрайські операції.

За останні роки банківський сектор став особливо уразливим перед кібератаками. Відомі приклади включають атаку WannaCry, яка відбулася у 2017 році і поширилася по всьому світу, а також атаку на Central Bank of Bangladesh у 2016 році, яка призвела до втрати майже 81 мільйона доларів. Окрім того, у 2020 році спостерігалося значне зростання кібератак у зв'язку з пандемією COVID-19, коли багато людей перейшли на роботу з дому і більше використовували онлайн-банкінг.

Одним із способів боротьби з цими загрозами є вдосконалення кібербезпеки у банківському секторі. Банки вкладають значні зусилля в удосконалення захисту своїх систем і даних клієнтів. Вони використовують передові технології шифрування, багатофакторну аутентифікацію, системи виявлення вторгнень і постійно моніторять свої мережі на випадки несправедливого поведінки або незвичайних активностей.

Загальноприйнятою практикою є також регулярне навчання персоналу щодо кібербезпеки та усвідомлення ризиків фішингу та інших атак. Створення свідомого підходу до кібербезпеки серед співробітників може допомогти запобігти багатьом атакам, які використовують соціальну інженерію.

Для клієнтів також важливо бути пильними та брати заходи для захисту своїх особистих даних. Необхідно уникати відкриття підозрілих електронних листів, особливо тих, які запитують конфіденційну інформацію. Користувачам слід встановлювати оновлення програмного забезпечення, використовувати сильні паролі та багатофакторну аутентифікацію, а також уважно перевіряти адреси веб-сайтів перед введенням будь-якої особистої інформації.

Крім того, ефективне співробітництво між банками, правоохоронними органами та кібербезпековими компаніями також є важливим для виявлення, припинення та розслідування кібератак. Інформаційний обмін та спільні зусилля можуть допомогти виявити нові загрози та швидко реагувати на них.

Атаки DDoS стали все поширенішими в останні роки. За даними статистики, зібраної різними джерелами, було помітне збільшення кількості DDoS-атак на банківські установи протягом останніх п'яти років. Наприклад, в 2019 році було зафіксовано понад 8 000 DDoS-атак на банківські установи у всьому світі. У 2020

році ця кількість зросла до 10 000 атак. За останні роки, із загостренням кібербезпекових загроз та зростанням компетенції кіберзлочинців, кількість DDoS-атак на банківські сектори продовжує збільшуватись.

Щодо інсайдерських загроз, важко надати конкретні числові дані про кількість таких атак на банківські установи. Однак, відомо, що інсайдерські загрози залишаються серйозною проблемою для цього сектора. За оцінками кібербезпекових експертів, близько 30% усіх кіберінцидентів у банківській галузі пов'язані з інсайдерами, які використовують свій авторизований доступ для незаконних цілей.

Такі атаки як Advanced Persistent Threats (APT), виявляються все частіше у банківському секторі. Хакерські групи, фінансовані державами або організовані організації кіберзлочинців, використовують APT для шпигунства, викрадення цінної фінансової інформації та маніпулювання транзакціями. На протязі останніх років було зафіксовано зростання кількості APT-атак на банківські установи.

Джекпотинг банкоматів став особливо актуальним явищем протягом останніх років. За даними з кібербезпекових джерел, перший випадок джекпотингу банкомату був зафіксований у 2010 році. З тих пір кількість таких атак значно зросла. У період з 2010 по 2022 рік, зареєстровано понад 4 500 випадків джекпотингу банкоматів у різних країнах світу. Ці атаки призвели до серйозних фінансових втрат для банків та порушення довіри громадськості до безпеки банкоматів.

Щодо криптоджекінгу, цей вид кібератак став особливо поширеним у останні роки, разом зі зростанням популярності криптовалют. Даних про точну кількість криптоджекінг-атак на банківські мережі недостатньо, оскільки багато з них можуть залишатись непоміченими або неповідомленими. Проте, за оцінками експертів, кількість таких атак зростає. З впровадженням додаткових заходів безпеки і підвищення свідомості про цю загрозу, банки докладають зусиль для запобігання криптоджекінгу та захисту своїх систем від несанкціонованого майнінгу криптовалют.

Атаки програм-вимагачів стають все більш поширеними в банківському секторі, спричиняючи значні збої та фінансові втрати. Програми-вимагачі – це

різновид зловмисного програмного забезпечення, яке шифрує файли жертви або блокує їх із їхніх систем, вимагаючи викупу в обмін на ключ розшифровки. Ці атаки можуть паралізувати банківські операції, скомпрометувати дані клієнтів і завдати шкоди репутації. Кіберзлочинці можуть спеціально націлюватися на банки, очікуючи більших платежів викупу через критичний характер їхніх послуг. Розуміючи різні типи кібератак, спрямованих на банківський сектор, організації можуть розробити надійні стратегії захисту та впровадити проактивні заходи безпеки для ефективного пом'якшення цих загроз.

Одним із помітних випадків, який підкреслив уразливість банківського сектору, був злом банківської системи SWIFT у 2016 році. Зловмисники зламали мережу SWIFT (Суспільство всесвітньої міжбанківської фінансової телекомунікації), яка використовується фінансовими установами в усьому світі для безпечного обміну повідомленнями та грошові перекази. Кіберзлочинці надсилали шахрайські повідомлення, щоб ініціювати несанкціоновані перекази коштів із кількох банків, що призвело до значних фінансових втрат. Цей інцидент підкреслив необхідність посилених заходів безпеки в системі SWIFT і спонукав фінансові установи переглянути власні протоколи безпеки.

Кампанії Carbanak і Cobalt Group, які діяли з 2013 по 2018 рік, були націлені на численні банки по всьому світу. Ці групи кіберзлочинців використовували складні методи, зокрема фішингові електронні листи та зловмисне програмне забезпечення, щоб отримати несанкціонований доступ до банківських мереж. Опинившись усередині, вони провели широку розвідку, маніпулювали внутрішніми системами та ініціювали шахрайські транзакції, що призвело до збитків на сотні мільйонів доларів. Справи Carbanak і Cobalt Group підкреслили важливість комплексних заходів безпеки, таких як надійна фільтрація електронної пошти, регулярне оновлення системи та вдосконалене виявлення загроз, для виявлення та запобігання таким атакам.

У 2016 році кіберзлочинці здійснили добре скоординовану атаку на банк Бангладеш, намагаючись викрасти майже 1 мільярд доларів. Зловмисники зламали системи банку та отримали доступ до мережі SWIFT. Вони надсилали шахрайські запити на переказ до Федерального резервного банку Нью-Йорка,

намагаючись переказати кошти на різні рахунки. Хоча більшість спроб транзакцій було заблоковано, зловмисникам вдалося викрасти 81 мільйон доларів. Цей випадок підкреслив необхідність надійних механізмів автентифікації, ефективного розподілу обов'язків і постійного моніторингу для виявлення та запобігання несанкціонованим переказам коштів.

Lazarus Group, спонсорована державою хакерська група, яка, як вважають, пов'язана з Північною Кореєю, привернула світову увагу завдяки гучній кібератаці на Sony Pictures у 2014 році. Хоча ця атака була спрямована на індустрію розваг, Lazarus Group також була причетна до кібератак на фінансові установи. Вони використовували різні методи, в тому числі фішинг, атаки на водопою та експлойти нульового дня, щоб скомпрометувати банківські мережі та здійснювати фінансове шпигунство. Діяльність Lazarus Group підкреслює важливість атрибуції, міжнародного співробітництва та надійного захисту кібербезпеки для протидії спонсорованим державою загрозам у банківському секторі.

Атака програми-вимагача NotPetya у 2017 році мала значний вплив на українські банки, порушивши їх роботу та спричинивши повсюдний фінансовий хаос. Спочатку зловмисники націлилися на механізми оновлення програмного забезпечення, що дозволяло їм поширювати зловмисне програмне забезпечення під виглядом законного оновлення. Потрапляючи в банківські мережі, зловмисне програмне забезпечення швидко поширюється, шифруючи критичні системи та приводячи їх у непрацездатний стан. Ця атака продемонструвала необхідність надійних процесів керування виправленнями, сегментації мережі та безпечних механізмів резервного копіювання та відновлення для пом'якшення впливу атак програм-вимагачів.

Ці відомі інцеденти підкреслюють еволюцію кібератак у банківському секторі, починаючи від складних цільових кампаній і закінчуючи великомасштабними руйнівними інцидентами. Фінансові установи повинні вчитися на цьому досвіді та постійно зміцнювати свої позиції безпеки для захисту від нових загроз і захисту своїх активів і клієнтів. Збереження довіри клієнтів є надзвичайно важливим для банків, оскільки клієнти довіряють їм свою особисту

та фінансову інформацію. Кібератаки можуть підірвати цю довіру, особливо якщо дані клієнтів скомпрометовані або фінансові операції проводяться шахрайським шляхом. Клієнти можуть втратити впевненість у безпеці онлайн-банківських послуг, що призведе до зниження цифрового впровадження або переходу до більш безпечних постачальників фінансових послуг. Відновлення довіри та репутації може бути складним і трудомістким, вимагаючи відкритого спілкування, оперативного реагування на інциденти та проактивних заходів безпеки, щоб переконати клієнтів у безпеці їхніх даних.

Впровадження надійних механізмів автентифікації має важливе значення для захисту від несанкціонованого доступу до банківських систем. Багатофакторна автентифікація (MFA) збільшує рівень безпеки, потребуючи від користувачів надання кількох форм ідентифікації, таких як паролі, біометричні дані або апаратні маркери. MFA значно знижує ризик компрометації облікового запису, навіть якщо паролі зламано або спроби атаки соціальної інженерії. Фінансові установи повинні заохочувати клієнтів увімкнути MFA для своїх облікових записів і також розглянути можливість впровадження MFA для внутрішнього доступу до системи.

Сегментація банківської мережі на окремі зони на основі чутливості даних і функцій може допомогти стримати вплив кібератаки. Впроваджуючи сегментацію мережі, банки можуть обмежити несанкціонований рух у своїх системах, гарантуючи, що зловмисники не зможуть легко перетнути мережу та отримати доступ до критично важливих активів. Крім того, слід запровадити жорсткі засоби контролю доступу, щоб обмежити привілеї користувачів за принципом найменших привілеїв. Регулярні перевірки доступу та механізми моніторингу можуть допомогти виявити та запобігти спробам несанкціонованого доступу. Впровадження моніторингу в реальному часі та можливостей аналізу загроз дозволяє фінансовим установам виявляти кіберзагрози та оперативно реагувати на них. Розширені інструменти моніторингу безпеки можуть ідентифікувати аномальну поведінку мережі, індикатори компрометації або потенційні інциденти безпеки. Завдяки інтеграції каналів розвідки про загрози банки можуть бути в курсі останніх загроз і вразливостей, що стосуються їх галузі. Постійний

моніторинг і розвідка про загрози дозволяють проактивно шукати загрози, раннє виявлення кіберзагроз і оперативне реагування на інциденти.

Співпраця між державним і приватним секторами має вирішальне значення для боротьби з кіберзагрозами в банківському секторі. Уряди, регуляторні органи та фінансові установи повинні налагодити міцні партнерські стосунки для обміну інформацією, розвідувальними даними та передовим досвідом. Державно-приватне партнерство може сприяти обміну розвідувальними даними про загрози, своєчасному сповіщенню про нові загрози та скоординованому реагуванню на кіберінциденти. Ця співпраця дає змогу отримати більш повне розуміння ландшафту загроз і покращує колективну здатність запобігати, виявляти та ефективно реагувати на кібератаки. Центри обміну та аналізу інформації (ISAC) відіграють важливу роль у сприянні співпраці та обміні інформацією в окремих галузях. Банківський сектор може отримати вигоду від участі в спеціальних ISAC з кібербезпеки, які об'єднують фінансові установи, правоохоронні органи та експертів з кібербезпеки. ISAC сприяють обміну інформацією про загрози, звітами про інциденти та найкращими практиками, характерними для банківського сектора. Приєднавшись до ISAC і беручи активну участь у них, фінансові установи можуть залишатися в курсі останніх загроз і використовувати колективні знання для зміцнення своїх засобів захисту.

Кібернетичні загрози в банківському секторі не обмежені географічними кордонами, і міжнародна співпраця є важливою для ефективної боротьби з ними. Уряди, регуляторні органи та правоохоронні органи повинні співпрацювати на міжнародному рівні для розслідування кіберзлочинів, обміну даними про загрози та затримання кіберзлочинців. Для сприяння транскордонному співробітництву в боротьбі з кібератаками слід створити рамки міжнародного співробітництва, такі як двосторонні угоди, договори про взаємну правову допомогу та платформи обміну інформацією. Тісна співпраця в міжнародному масштабі зміцнює колективну відповідь на кіберзагрози та забезпечує більш безпечну глобальну банківську екосистему.

Оскільки банківський сектор продовжує розвиватися, кібератаки залишатимуться постійною загрозою. Фінансові установи повинні передбачати й

адаптуватися до цих нових викликів, використовуючи технологічні досягнення, співпрацюючи з колегами галузі та інвестуючи в надійні заходи кібербезпеки. Захищаючись на випередження, фінансові установи можуть підвищити свою стійкість, захистити активи клієнтів і зберегти довіру до цифрового банківського ландшафту.

2 ВИДИ КІБЕРАТАК ТА СИСТЕМИ ЇХ ВИЯВЛЕННЯ

2.1 Фішингові атаки

Фішингові атаки бувають різних форм, кожна з яких спрямована на оману людей і отримання несанкціонованого доступу до конфіденційної інформації. Найпоширенішим типом є фішинг електронної пошти, коли зловмисники надсилають шахрайські електронні листи, видаючи себе за законних осіб. Фішинг — це цілеспрямований підхід, який пристосовує повідомлення до конкретних жертв. Смішинг відбувається за допомогою текстових повідомлень, тоді як вішинг передбачає телефонні дзвінки. Pharming перенаправляє користувачів на шахрайські веб-сайти, використовуючи вразливі місця DNS.

Останніми роками кількість фішингових атак зросла, що становить серйозну загрозу для окремих осіб і організацій. Лише в першому кварталі 2021 року було виявлено понад 245 000 унікальних фішингових веб-сайтів, що на 25% більше, ніж у попередньому кварталі. Google повідомила про блокування понад 100 мільйонів фішингових електронних листів, пов’язаних із шахрайством щодо COVID-19, щодня у 2020 році. Найчастіше зловмисники видавали себе за працівників Google або Amazon (див рис 2.1) [6].

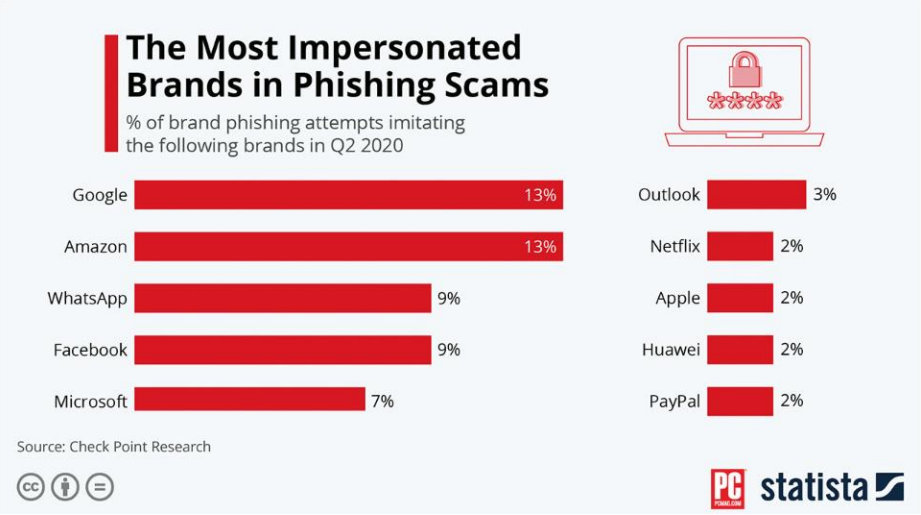

Рисунок 2.1 Статистика pcmag

Мобільні платформи також стали однією з головних мішеней, 28% фішингових атак у четвертому кварталі 2020 року були спрямовані спеціально на мобільні пристрої. Фінансовий сектор залишається найбільш цільовою галуззю, на яку припадає 25% усіх зафіксованих фішингових атак. Адаптація тактики фішингу під час пандемії COVID-19 сприяла збільшенню атак на 13,7% у 2020 році порівняно з попереднім роком. Згідно із статистики що надав сайт Verizon.com на сферу фінансів припадає 1829 випадків фішингових атак серед яких 477 призвели до витоку даних (див. рис 2.2) [7].

	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	16,312	694	489	15,129	5,199	376	223	4,600
Accommodation (72)	254	4	2	248	68	4	1	63
Administrative (56)	38	8	14	16	32	8	11	13
Agriculture (11)	66	1	5	60	33	0	3	30
Construction (23)	87	7	1	79	66	4	1	61
Education (61)	496	63	15	418	238	28	8	202
Entertainment (71)	432	13	3	416	93	10	1	82
Finance (52)	1,829	70	30	1,729	477	38	18	421
Healthcare (62)	522	28	15	479	433	23	15	395
Information (51)	2,105	45	110	1,950	380	23	19	338
Management (55)	9	1	0	8	9	1	0	8
Manufacturing (31–33)	1,814	37	24	1,753	259	18	15	226
Mining (21)	25	2	0	23	13	2	0	11
Other Services (81)	143	7	2	134	100	6	1	93
Professional (54)	1,396	176	54	1,166	421	85	32	304
Public Administration (92)	3,270	87	110	3,073	582	48	39	495
Real Estate (53)	83	15	5	63	59	10	2	47
Retail (44–45)	404	62	44	298	191	33	28	130
Transportation (48–49)	349	13	25	311	106	8	13	85
Utilities (22)	117	12	6	99	33	3	3	27
Wholesale Trade (42)	96	42	22	32	53	23	11	19
Unknown	2,777	1	2	2,774	1,553	1	2	1,550
Total	16,312	694	489	15,129	5,199	376	223	4,600

Рисунок 2.2 – Статистика Verizon

Ці статистичні дані підкреслюють зростаючу загрозу, яку представляють фішингові атаки, і наголошують на необхідності надійних заходів безпеки, навчання користувачів і передових технологій виявлення. Організації та окремі особи повинні бути пильними, щоб зменшити ризики, пов’язані з цією поширеною формою кіберзлочинності.

У 2017 році яскравим прикладом масштабної фішингової атаки став випадок із сервісом Google Docs. Кіберзлочинці надсилали начебто законні електронні листи, які нібито походять від контактів, запрошуючи одержувачів отримати

доступ до спільного документа в Google Docs. Натискання наданого посилання перенаправляло користувачів на шахрайську сторінку входу, яка імітувала інтерфейс Google. Вводячи свої облікові дані, жертви мимоволі передавали інформацію свого облікового запису зловмисникам. Ця атака використала довіру користувачів до комунікаційних платформ і хмарних сервісів, вплинувши на значну кількість користувачів.

Зменшення ризиків, пов'язаних із фішинговими атаками, потребує багатогранного підходу, який охоплює як технологічні заходи, так і обізнаність користувачів:

- Розгортання надійних рішень безпеки електронної пошти, які поєднують фільтри спаму, антивірусні сканери та аналіз вмісту, може значно зменшити кількість фішингових електронних листів, які надходять до скриньок вхідних повідомлень користувачів. Розширені платформи аналізу загроз можуть ідентифікувати та блокувати відомі індикатори фішингу, шкідливі посилання та підозрілі вкладення;
- Впровадження надійних механізмів автентифікації, таких як 2FA або MFA, збільшує рівень безпеки. Вимагаючи від користувачів додаткового підтвердження, крім пароля, наприклад унікального коду або біометричних даних, ризик несанкціонованого доступу через викрадені облікові дані значно мінімізується;
- Проведення регулярних тренінгів і програм підвищення обізнаності для співробітників є життєво важливим у боротьбі з фішинговими атаками. Ці ініціативи мають ознайомити користувачів з найновішими методами фішингу, поширеними попереджувальними знаками та способами повідомляти про ймовірні спроби фішингу. Імітовані фішингові кампанії також можуть допомогти посилити навчання, надаючи приклади з реального світу та дозволяючи користувачам відчути спроби фішингу в контрольованому середовищі.
- Розгортання рішень веб-фільтрації, які аналізують і блокують доступ до відомих фішингових веб-сайтів, може запобігти випадковому доступу користувачів до шахрайських доменів. Крім того, впровадження інструментів аналізу URL-адрес, які оцінюють репутацію та безпеку веб-посилань, вбудованих

в електронні листи чи повідомлення, може допомогти користувачам ідентифікувати потенційно шкідливі URL-адреси.

- Створення ефективного плану реагування на інциденти забезпечує оперативне та скоординоване реагування на інциденти фішингу. Це включає в себе процедури швидкої ідентифікації та ізоляції скомпрометованих облікових записів, сповіщення постраждалих осіб і проведення судових розслідувань для визначення масштабу атаки. Заохочення користувачів негайно повідомляти про ймовірні спроби фішингу сприяє своєчасній реакції та пом'якшенню.
- Бути в курсі нових методів і тенденцій фішингу має вирішальне значення для проактивного захисту. Участь в ініціативах з обміну інформацією про загрози, підписка на галузеві сповіщення безпеки та моніторинг платформ розвідки з відкритим кодом (OSINT) можуть надати цінну інформацію про розвиток тактики фішингу. Ця інформація допомагає організаціям адаптувати свої засоби захисту та завчасно блокувати нові загрози.

2.2 Атаки шкідливих програм

Атаки зловмисного програмного забезпечення охоплюють різні типи шкідливого програмного забезпечення, призначеного для проникнення в системи, компрометації даних і отримання несанкціонованого доступу. До поширених типів зловмисного програмного забезпечення належать троянські програми, програми-вимагачі, шпигунські програми, черв'яки та ботнети.

Троянські коні — це оманливі програми, які виглядають законними, але містять шкідливий код. Вони можуть викрасти конфіденційну інформацію, надати зловмисникам віддалений доступ або розмістити інше зловмисне програмне забезпечення.

Програми-вимагачі шифрують файли або блокують цілі системи, вимагаючи викуп за їх звільнення. Ці атаки стають дедалі витонченішими та спрямовані на окремих осіб, підприємства та критичну інфраструктуру.

Шпигунське програмне забезпечення таємно збирає інформацію користувача без згоди, відстежуючи такі дії, як натискання клавіш, перегляд веб-

сторінок і конфіденційні дані. Ця інформація може бути використана в зловмисних цілях.

Черв'яки — це зловмисне програмне забезпечення, що самовідтворюється, яке поширюється мережами, використовуючи вразливі місця для зараження кількох систем. Вони можуть перевантажувати мережі, скомпрометувати дані або запускати інші шкідливі дії.

Бот-мережі — це мережі скомпрометованих пристроїв, які контролюються центральним сервером. Інфіковані пристрої або «боти» можуть використовуватися для DDoS-атак, розповсюдження спаму або скоординованої зловмисної діяльності.

У звіті SonicWall Cyber Threat Report зафіксовано збільшення глобального обсягу зловмисного програмного забезпечення на 62% у 2020 році з понад 56,9 мільярдами атак зловмисного програмного забезпечення.

Відповідно до звіту Verizon про розслідування витоку даних, у 2020 році кількість атак програм-вимагачів зросла на 150%.

Звіт CyberEdge Group про захист від кіберзагроз за 2021 рік показав, що 68% організацій зазнали успішної атаки зловмисного програмного забезпечення у 2020 році.

McAfee повідомила про збільшення кількості нових зразків шкідливого програмного забезпечення на 26%, досягнувши 1,3 мільйона на день.

У звіті Symantec про загрози інтернет-безпеці зазначено, що у 2020 році кількість атак Інтернету речей зросла на 350%, націлених на розумні пристрої.

Ці статистичні дані підкреслюють зростаючу загрозу атак зловмисного програмного забезпечення та потребу в надійних заходах кібербезпеки, регулярних оновленнях, навчанні користувачів і комплексних механізмах виявлення загроз і реагування. Організації повинні віддати перевагу проактивним стратегіям безпеки, щоб зменшити ескалацію ризику, який створює зловмисне програмне забезпечення. Поради щодо боротьби з атаками зловмисного програмного забезпечення:

- Використовуйте надійне антивірусне та антишкідливе програмне забезпечення, оновлюйте його для регулярного сканування та видалення зловмисного програмного забезпечення.
- Оновлюйте програмне забезпечення, операційні системи та вбудоване програмне забезпечення за допомогою останніх виправлень безпеки.
- Будьте обережні, завантажуючи файли або натискаючи посилання, особливо з невідомих або ненадійних джерел.
- Увімкніть брандмауери та системи виявлення/попередження вторгнень для моніторингу та блокування підозрілого мережевого трафіку.
- Застосуйте політику надійних паролів і багатофакторну автентифікацію для підвищення безпеки.
- Регулярно створюйте резервні копії важливих даних і безпечно зберігайте резервні копії в автономному режимі або в окремому місці.
- Розкажіть співробітникам про ризики зловмисного програмного забезпечення та про те, як розпізнавати потенційні інциденти безпеки та повідомляти про них.

2.3 Атаки соціальної інженерії

Атаки соціальної інженерії використовують людську психологію та змушують людей розголошувати конфіденційну інформацію або виконувати дії, що ставлять під загрозу безпеку. Ці атаки покладаються на психологічні маніпуляції, а не на технічну вразливість. Атаки соціальної інженерії можуть приймати різні форми і часто є цілеспрямованими та персоналізованими.

Фішинг — це поширений метод соціальної інженерії, коли зловмисники надсилають шахрайські електронні листи, повідомлення або створюють підроблені веб-сайти, які видають себе за законні організації чи окремих осіб. Мета полягає в тому, щоб обманом змусити одержувачів розкрити особисту інформацію, таку як облікові дані для входу, дані кредитної картки або номери соціального страхування. Фішингові атаки часто використовують терміновість, страх або привабливі пропозиції, щоб спонукати жертв негайно вжити заходів.

Передтекстування передбачає створення фальшивого сценарію або приводу для маніпулювання особами, щоб вони надали конфіденційну інформацію. Зловмисники можуть видаватися за довірену особу, наприклад, за колегу, персонал служби підтримки IT або представника служби підтримки клієнтів. Встановлюючи довіру та надійність, зловмисники переконують жертв розкрити конфіденційну інформацію, таку як паролі чи номери облікових записів.

Зловмисники можуть залишати заражені USB-накопичувачі чи інші фізичні носії інформації в публічних місцях або надсилати привабливі посилання чи завантаження, які містять зловмисне програмне забезпечення. Цікавість або бажання отримати халяву можуть змусити нічого не підозрюючи жертви поставити під загрозу свою безпеку, взаємодіючи з приманкою.

Атаки Quid pro quo включають пропозицію вигоди або послуги в обмін на конфіденційну інформацію. Зловмисники можуть видавати себе за персонал технічної підтримки та пропонувати допомогу або обіцяти винагороду в обмін на облікові дані для входу або доступ до системи. Жертва несвідомо надає необхідну інформацію, дозволяючи зловмиснику отримати несанкціонований доступ.

На протязі останніх декількох років бізнеси активно збільшують свої витрати на різного роду програмне забезпечення аби як найбільше знизити ризик атаки соціальною інженерією (див рис 2.3) [8].

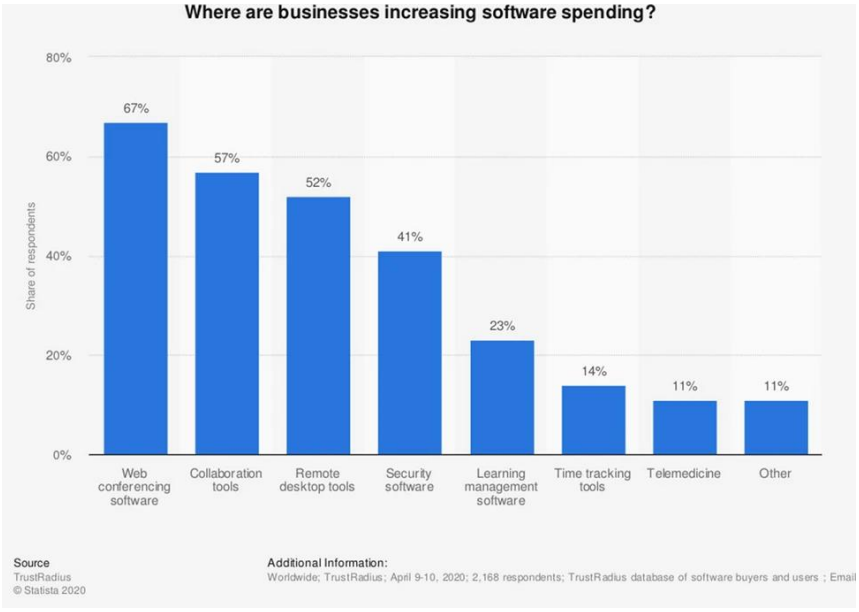

Рисунок 2.3 – Графік збільшення витрат на програмне забезпечення

Проте якісне програмне забезпечення не може знизити ризик такої атаки, боротьба з атаками соціальної інженерії вимагає поєднання технічних засобів захисту та навчання користувачів:

- Навчання з питань безпеки: регулярно навчайте співробітників і користувачів про різні форми атак соціальної інженерії та про те, як їх розпізнавати та реагувати на них. Навчіть їх важливості перевірки автентичності запитів на конфіденційну інформацію.
- Попередження про фішинг: навчіть користувачів бути обережними під час взаємодії з електронними листами, повідомленнями чи веб-сайтами. Заохочуйте їх уважно перевіряти адресу електронної пошти відправника, шукати підозрілі посилання та скептично ставитися до термінових або незвичайних запитів.
- Багатофакторна автентифікація: запровадьте багатофакторну автентифікацію (MFA), щоб додати додатковий рівень безпеки. MFA вимагає від користувачів додаткового підтвердження, наприклад унікального коду, надісланого на їхні мобільні пристрої, разом із звичайними обліковими даними для входу.
- Надійні спам-фільтри: розгорніть розширені спам-фільтри та рішення для захисту електронної пошти, які можуть ідентифікувати та блокувати шкідливі електронні листи або спроби фішингу. Ці фільтри можуть запобігти потраплянню підозрілих повідомлень до скриньки вхідних повідомлень користувачів.
- Повідомлення про інциденти: встановіть чіткі канали для повідомлення про ймовірні спроби соціальної інженерії. Заохочуйте користувачів повідомляти про будь-які підозрілі електронні листи, повідомлення чи телефонні дзвінки відповідній групі IT або відділу безпеки.
- Заходи фізичної безпеки: повідомте співробітникам про ризики фізичної безпеки, наприклад про небезпеку підключення ненадійних USB-накопичувачів або надання конфіденційної інформації неавторизованим особам.
- Постійне тестування: проводьте регулярні імітовані фішингові кампанії, щоб оцінити обізнаність користувачів і швидкість реагування. Це дозволяє організаціям визначати області для вдосконалення та проводити цільове

навчання осіб, які можуть бути більш сприйнятливими до атак соціальної інженерії.

2.4 Атаки MitM

Атаки Man-in-the-Middle (MitM) — це тип кібератак, коли зловмисник перехоплює спілкування між двома сторонами без їх відома. Ці атаки використовують вразливі місця в каналах зв'язку для підслуховування, викрадення конфіденційної інформації або маніпулювання даними. Атаки MitM можуть відбуватися в різних контекстах, включаючи мережі Wi-Fi, веб-перегляд і онлайн-транзакції.

Останніми роками атаки MitM значно зросли, створюючи дедалі більшу загрозу для окремих осіб і організацій. Звіт Verizon про розслідування витоку даних за 2021 рік показав, що 35% зломів пов'язані з використанням викрадених облікових даних, що вказує на можливість атак MitM. Крім того, у звіті Symantec про загрози безпеці в Інтернеті за 2021 рік зазначено, що кількість нових варіантів зловмисного програмного забезпечення для мобільних пристроїв зросла на 54%, що створює можливості для атак MitM на мобільні пристрої.

Робоча група з боротьби з фішингом (APWG) повідомила про збільшення кількості фішингових атак на 65% у першому кварталі 2021 року, підкреслюючи актуальність атак MitM для компрометації облікових даних користувачів. Національний інститут стандартів і технологій (NIST) також підкреслив зростання атак MitM, пов'язаних з Wi-Fi, особливо в публічних мережах, що призводить до перехоплення даних і несанкціонованого доступу.

Ці статистичні дані підкреслюють зростаючий ландшафт атак MitM, що вимагає надійних заходів безпеки для захисту конфіденційної інформації. Впроваджуючи превентивні заходи, тримаючи в курсі нових методів атак і навчаючи користувачів, організації можуть посилити свій захист від атак MitM і захистити свої цифрові комунікації. Поради щодо боротьби з атаками MitM:

- Безпечні канали зв'язку: використовуйте протоколи шифрування, такі як SSL/TLS, щоб встановити безпечні канали зв'язку. Шифрування гарантує, що

дані, що передаються між сторонами, залишаються конфіденційними та захищеними від перехоплення чи модифікації.

- Перевірте цифрові сертифікати: перевірте автентичність цифрових сертифікатів, які використовуються в безпечному зв'язку. Переконайтеся, що сертифікати видані перевіреними органами та не були підроблені.
- Уникайте загальнодоступних мереж Wi-Fi: будьте обережні, підключаючись до незахищених або загальнодоступних мереж Wi-Fi, оскільки вони більш вразливі до атак MitM. Замість цього використовуйте віртуальні приватні мережі (VPN) або захищені стільникові мережі для передачі конфіденційної інформації.
- Двофакторна автентифікація (2FA): запровадьте 2FA або MFA, щоб додати додатковий рівень безпеки. Це вимагає від користувачів додаткового підтвердження, наприклад унікального коду, надісланого на їхній мобільний пристрій, разом із звичайними обліковими даними для входу.
- Оновлюйте програмне забезпечення: регулярно оновлюйте програмне забезпечення, операційні системи та програми, щоб виправити вразливості системи безпеки, якими можуть скористатися зловмисники для полегшення атак MitM.
- Системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS): розгортайте рішення IDS/IPS для моніторингу мережевого трафіку та виявлення підозрілих дій, що вказують на атаки MitM. Ці системи можуть подавати сповіщення та вживати профілактичних заходів для блокування або пом'якшення зловмисного трафіку.
- Обізнаність і освіта користувачів: розкажіть користувачам про ризики, пов'язані з атаками MitM, і про те, як розпізнати попереджувальні знаки. Заохочуйте їх бути пильними під час обміну конфіденційною інформацією в Інтернеті та перевіряти автентичність веб-сайтів і цифрових сертифікатів.

2.5 Розподілені атаки на відмову в обслуговуванні (DDoS)

Розподілені атаки на відмову в обслуговуванні (DDoS) призначені для перевантаження цільової системи, мережі або веб-сайту потоком трафіку, що робить їх недоступними для звичайних користувачів. Ці атаки використовують обмеження інфраструктури або програмного забезпечення, щоб вичерпати доступні ресурси, такі як пропускна здатність, обчислювальна потужність або пам’ять. DDoS-атаки можуть бути дуже руйнівними та часто включають мережу скомпрометованих пристроїв, відомих як ботнет, якими керує зловмисник.

Зловмисники створюють ботнет, заражаючи шкідливим програмним забезпеченням велику кількість комп’ютерів, серверів або пристроїв Інтернету речей. Ці скомпрометовані пристрої стають частиною мережі, контрольованої зловмисником, готовою до скоординованих атак.

Потік трафіку – зловмисник ініціює DDoS-атаку, даючи команду бот-мережі надіслати величезний обсяг трафіку до цільової системи чи мережі. Цей потік трафіку споживає доступні ресурси та вичерпує можливості для обробки законних запитів. Оскільки цільова система намагається впоратися з потоком трафіку, вона перевантажується, що призводить до зниження продуктивності або повної недоступності. Це запобігає доступу звичайних користувачів до служб або ресурсів, розміщених у цільовій системі.

Деякі атаки DDoS використовують методи посилення, щоб максимізувати вплив атаки. Зловмисники використовують уразливості в певних службах, таких як DNS, NTP або memcached, щоб генерувати значно більші обсяги трафіку, спрямованого до цілі.

Для зменшення шкоди від атак DDoS вимагається поєднання превентивних заходів і стратегій реагування:

Моніторинг і аналіз трафіку: запровадьте інструменти моніторингу трафіку, які можуть виявляти аномальні стрибки або шаблони в мережевому трафіку. Це дозволяє завчасно ідентифікувати потенційні DDoS-атаки та полегшує швидке реагування.

Масштабована інфраструктура: проектуйте системи та мережі з урахуванням масштабованості. Маючи здатність обробляти збільшений трафік, організації можуть краще протистояти DDoS-атакам, не зазнаючи значних збоїв у роботі.

Мережі доставки вмісту (CDN): використовуйте CDN для географічного розподілу мережевого трафіку між кількома серверами та центрами обробки даних. CDN можуть допомогти поглинати та пом'якшувати атаки DDoS, розподіляючи навантаження трафіку та відфільтровуючи зловмисні запити.

Обмеження та фільтрація швидкості: використовуйте механізми обмеження швидкості та методи фільтрації трафіку, щоб ідентифікувати та блокувати підозрілий або зловмисний трафік. Це допомагає відрізнити законні запити користувачів від трафіку, створеного DDoS-атакою.

Системи виявлення та запобігання вторгненням (IDPS): розгортайте рішення IDPS, які можуть виявляти та блокувати DDoS-атаки в реальному часі. Ці системи відстежують мережевий трафік, виявляють шкідливі шаблони та автоматично вживають контрзаходи для пом'якшення впливу атаки.

План реагування на інциденти: розробіть комплексний план реагування на інциденти, який містить конкретні дії, які необхідно вжити у випадку DDoS-атаки. Цей план має окреслювати ролі та обов'язки, протоколи зв'язку та кроки для відновлення та відновлення послуг.

Останніми роками DDoS-атаки стають все більш поширеними та витонченими. Зловмисники постійно вдосконалюють свою тактику, тому для організацій вкрай важливо залишатися пильними. Нижче наведено деякі статистичні дані, що підкреслюють зростаючий маштаб DDoS-атак:

Згідно зі звітом NETSCOUT Threat Intelligence Report 2020, кількість DDoS-атак зросла на 25% порівняно з попереднім роком, досягнувши рекордного рівня (див рис 2.4) [9].

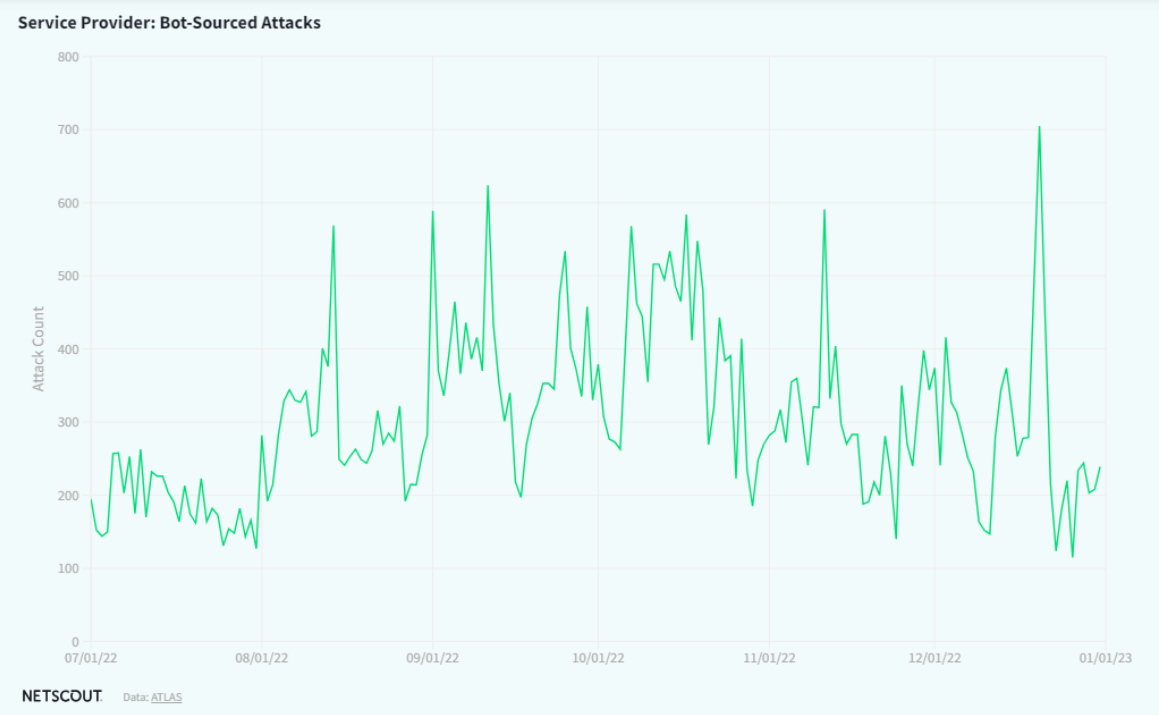

Рисунок 2.4 – Статистика NETSCOUT

Найбільша DDoS-атака за всю історію, як повідомляє Cloudflare, сталася в лютому 2020 року, досягнувши пікового обсягу трафіку в 2,5 терабіт на секунду (Tbps).

Згідно зі звітом Nexusguard про загрози за другий квартал 2020 року, кількість атак посилення, типу DDoS-атак, зросла на 15% у першій половині 2020 року.

Ці статистичні дані підкреслюють значну загрозу, яку становлять атаки DDoS, і потребу організацій у впровадженні надійних стратегій запобігання таким атакам. Впроваджуючи профілактичні заходи, такі як моніторинг трафіку, масштабована інфраструктура та ефективні плани реагування, організації можуть мінімізувати вплив DDoS-атак і забезпечити доступність своїх послуг навіть у разі атаки.

2.6 Атаки SQL інєкції

Атаки SQL Injection націлені на веб-програми, які використовують базу даних для зберігання та отримання даних. Ці атаки використовують уразливості в

обробці додатком введення користувача, що дозволяє зловмиснику виконувати зловмисні оператори SQL. Впроваджуючи шкідливий код у запити до бази даних програми, зловмисники можуть маніпулювати базою даних, витягувати конфіденційну інформацію, змінювати дані або навіть отримати неавторизований доступ до основної системи.

Зловмисники виявляють веб-програми, які мають уразливі місця в механізмах перевірки вхідних даних. Ці вразливості можуть включати погано написаний код, відсутність обробки вхідних даних або неправильне використання параметризованих запитів. Зловмисники вводять спеціально створені дані в поля введення програми, такі як форми входу або вікна пошуку. Ці дані зазвичай містять інструкції SQL або фрагменти, які зловмисник хоче виконати. Введений зловмисником SQL-код об'єднується з законним SQL-запитом, який виконує програма. Ця маніпуляція може призвести до ненавмисної поведінки, що дозволить зловмиснику отримати, змінити або видалити дані з бази даних. Під час успішних атак SQL-ін'єкцій зловмисники можуть отримати конфіденційну інформацію, таку як сенсативну інформацію користувача, дані кредитної картки або інші конфіденційні дані, що зберігаються в базі даних.

Атаки SQL Injection залишаються значною загрозою, коли зловмисники постійно використовують вразливі веб-програми. Ось деякі статистичні дані, що демонструють зростання атак SQL Injection.

Звіт Verizon про розслідування витоку даних за 2021 рік показав, що атаки SQL Injection спричинили 4% усіх проаналізованих у звіті зламів.

Згідно з індексом кіберзагроз Imperva, атаки SQL Injection становили 19% усіх атак веб-додатків у третьому кварталі 2020 року.

У звіті Positive Technologies виявлено, що вразливості SQL Injection були присутні в 29% веб-додатків, перевірених у 2020 році, підкреслюючи постійну поширеність цієї вразливості.

Ці статистичні дані демонструють постійний ризик, пов'язаний з атаками SQL Injection. Впроваджуючи методи безпечного кодування, проводячи регулярні оцінки вразливостей і використовуючи механізми захисту, такі як WAF,

організації можуть значно знизити ризик атак SQL Injection і захистити свої веб-додатки та бази даних від компрометації.

Запобігання атакам SQL Injection вимагає поєднання безпечних практик кодування, перевірки введених даних і постійних заходів безпеки:

- Реалізуйте надійні механізми перевірки вхідних даних, які перевіряють і дезінфікують введені користувачем дані, щоб запобігти впровадженню шкідливого коду SQL. Використовуйте параметризовані запити або підготовлені оператори, щоб відокремити код SQL від введення користувача.
- Переконайтеся, що облікові записи користувачів бази даних, які використовує програма, мають обмежені привілеї та права доступу. Обмежте доступ до конфіденційних даних і операцій, щоб мінімізувати потенційний вплив успішної атаки SQL Injection.
- Оновлюйте фреймворки веб-додатків, бібліотеки та системи керування базами даних за допомогою останніх виправлень безпеки. Це допомагає захистити від відомих уразливостей, якими зловмисники можуть скористатися для атак SQL Injection.
- Запровадьте WAF для моніторингу та фільтрації вхідного трафіку до веб-програми. WAF можуть виявляти та блокувати спроби впровадження SQL, аналізуючи шаблони та поведінку запитів.
- Навчіть розробників дотримуватись методів безпечного кодування, таких як використання підготовлених операторів або параметризованих запитів, уникнення динамічної конструкції SQL і використання перевірки вхідних даних і кодування вихідних даних.

3 ВПРОВАДЖЕННЯ СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ У БАНКІВСЬКОМУ СЕКТОРІ

3.1 Виявлення та запобігання вторгненням

Зі зростанням залежності від цифрових технологій і онлайн-транзакцій банківський сектор став привабливою мішенню для кіберзлочинців, які прагнуть скористатися вразливими місцями та отримати несанкціонований доступ до критично важливих фінансових систем і даних клієнтів. Наслідки успішних кібератак у банківському секторі можуть бути руйнівними, призвести до фінансових втрат, репутаційної шкоди та підірвати довіру клієнтів.

У відповідь на цю ескалацію загроз існує нагальна потреба в розробці та впровадженні надійних систем, які можуть ефективно виявляти та запобігати кібератакам у банківському секторі. Ця кваліфікаційна робота зосереджена на розробці та впровадженні такої системи під назвою «SecureBankGuard», яка спрямована на посилення заходів безпеки в банківському секторі та захисту від складних кіберзагроз.

Основна мета SecureBankGuard — створити проактивну багаторівневу структуру безпеки, яка охоплює розширене виявлення загроз, надійні механізми автентифікації та комплексний моніторинг безпеки. Завдяки інтеграції передових технологій і найкращих практик SecureBankGuard прагне мінімізувати ризик кібератак, захистити облікові записи клієнтів і зберегти цілісність критично важливих банківських систем.

Завдяки розробці та впровадженню SecureBankGuard ця робота має на меті зробити внесок у загальну безпеку банківського сектору, допомагаючи банкам і фінансовим установам зміцнити свій захист від кіберзагроз. Застосовуючи проактивний і комплексний підхід до кібербезпеки, SecureBankGuard дає змогу банківському сектору захищати активи клієнтів, зберігати конфіденційність і підтримувати довіру та впевненість своїх клієнтів.

Система виявлення та запобігання вторгненням (IDPS) від SecureBankGuard — це багаторівневе рішення безпеки, призначене для

моніторингу мережі на наявність підозрілих дій і ефективного запобігання кібератакам у банківському секторі. Система використовує комбінацію виявлення на основі сигнатур, виявлення аномалій на основі поведінки, попередження в реальному часі та автоматичні механізми реагування для забезпечення надійного захисту.

SecureBankGuard підтримує обширну та актуальну базу даних відомих сигнатур атак, яка постійно оновлюється завдяки співпраці з галузевими експертами, спільнотами безпеки та каналами аналізу загроз. Це комплексне сховище сигнатур охоплює широкий спектр відомих загроз, включаючи зловмисне програмне забезпечення, експлойти та відомі моделі атак. Коли мережевий трафік проходить через SecureBankGuard, він порівнює вхідні пакети з базою даних підписів, миттєво виявляючи збіги. Цей метод виявлення на основі сигнатур дозволяє системі швидко ідентифікувати та блокувати добре відомі та загальновизнані атаки, забезпечуючи ефективний захист від поширених загроз.

Окрім виявлення на основі сигнатур, SecureBankGuard використовує розширені алгоритми машинного навчання та аналітику поведінки для виявлення аномалій у мережевому трафіку та поведінці користувачів. Система встановлює базову лінію, вивчаючи типові моделі мережевої активності та взаємодії користувачів у банківському середовищі. Постійно відстежуючи мережевий трафік і дії користувачів, він може виявити відхилення від встановленого базового рівня, які можуть вказувати на ненормальну або зловмисну поведінку. Ці аномалії можуть включати незвичайні передачі даних, спроби неавторизованого доступу або підозрілі дії, що вказують на розширені постійні загрози (APT) або атаки нульового дня. Завдяки такому поведінковому підходу SecureBankGuard має можливість виявляти раніше невідомі або нові загрози,

SecureBankGuard надає можливість попередження в режимі реального часу, щоб оперативно повідомляти персонал служби безпеки про можливі спроби вторгнення. Коли система визначає дію, яка відповідає відомій сигнатурі атаки, або виявляє аномалію в поведінці мережі, вона генерує негайні сповіщення. Ці сповіщення надсилаються кількома каналами, наприклад електронною поштою, SMS або через інтеграцію з існуючими системами керування інцидентами

безпеки. Отримуючи сповіщення в режимі реального часу, служби безпеки можуть швидко досліджувати потенційні загрози та реагувати на них, скорочуючи часове вікно для використання зловмисниками вразливостей.

Щоб підвищити ефективність системи та мінімізувати час реагування, SecureBankGuard можна налаштувати для впровадження автоматизованих дій реагування, коли виконуються певні умови. На основі попередньо визначених політик і протоколів безпеки система може вжити негайних заходів для пом'якшення впливу атаки. Наприклад, він може автоматично блокувати підозрілий мережевий трафік, ізолювати скомпрометовані кінцеві точки або ініціювати контрзаходи для нейтралізації загрози. Ці автоматизовані дії реагування допомагають стримати атаку, обмежити її поширення та зменшити потенційну шкоду для банківських систем і даних клієнтів. Дії реагування ретельно визначені, щоб гарантувати їх відповідність політиці безпеки банку та толерантності до ризику, забезпечуючи настроюваний та адаптивний механізм захисту.

SecureBankGuard використовує підхід постійного вдосконалення, щоб з часом покращити свої можливості виявлення. Система збирає та аналізує дані про виявлені загрози, результати реагування та мінливий ландшафт загроз. Ці дані використовуються для підвищення ефективності механізмів виявлення як на основі сигнатур, так і на основі поведінки. Використовуючи алгоритми машинного навчання, SecureBankGuard може адаптувати та вдосконалювати свої моделі виявлення, забезпечуючи стійкість проти нових загроз і векторів атак, що розвиваються. Постійне вдосконалення дає змогу системі випереджати досвідчених противників і завчасно захищати банківське середовище.

Завдяки комплексним можливостям виявлення та запобігання вторгненням SecureBankGuard є надійною системою захисту банківського сектора. Поєднуючи виявлення відомих загроз на основі сигнатур і виявлення аномалій на основі поведінки нових загроз, система пропонує цілісний підхід до безпеки. Попередження в режимі реального часу забезпечують оперативне реагування на інциденти, а автоматизовані дії реагування пом'якшують вплив атак. Завдяки постійному вдосконаленню завдяки аналізу даних і машинному навчанню

SecureBankGuard підтримує високий рівень захисту від нових кіберзагроз, захищаючи банківські системи, інформацію про клієнтів і цілісність фінансового сектора в цілому.

3.2 Двофакторна автентифікація (2FA) і багатофакторна автентифікація (MFA)

3.2.1 Двофакторна автентифікація (2FA)

SecureBankGuard надає пріоритет реалізації надійних механізмів автентифікації для забезпечення безпечного доступу до критично важливих банківських систем і програм. Він виходить за рамки традиційної автентифікації на основі пароля та об’єднує методи двофакторної автентифікації (2FA) і багатофакторної автентифікації (MFA), щоб забезпечити додатковий рівень безпеки та запобігти несанкціонованому доступу.

SecureBankGuard вимагає від користувачів надавати два різні фактори автентифікації під час процесу входу. Ці фактори, як правило, діляться на три категорії: на основі знань, на основі володіння та на основі приналежності.

Фактор, заснований на знаннях: цей фактор включає щось, що користувач знає, наприклад пароль, PIN-код або відповіді на таємні запитання. Щоб продовжити автентифікацію, користувач повинен правильно ввести певну інформацію, пов’язану з його обліковим записом.

Фактор володіння: SecureBankGuard включає фактори володіння, щоб додати додатковий рівень безпеки. Користувачі повинні мати фізичний або віртуальний маркер, згенерований мобільним додатком. Фізичними маркерами можуть бути смарт-карти, USB-токени або апаратні ключі безпеки, тоді як віртуальні маркери зазвичай генеруються за допомогою мобільних додатків. Ці маркери є унікальними для кожного користувача та використовуються в поєднанні з фактором на основі знань для автентифікації.

Фактор, заснований на приналежності: SecureBankGuard також використовує фактори, засновані на приналежності, які залежать від

біометричних характеристик користувача. Це включає в себе сканування відбитків пальців, розпізнавання обличчя, тощо. Використовуючи біометричну автентифікацію, система забезпечує використання унікальних фізичних атрибутів користувача як додаткового фактора автентифікації [10].

3.2.2 Багатофакторна автентифікація (MFA)

На додаток до 2FA, SecureBankGuard підтримує багатофакторну автентифікацію (MFA), яка дозволяє використовувати додаткові фактори автентифікації крім мінімально необхідних двох. Це додає додатковий рівень безпеки та робить неавторизованим особам ще більш складним доступ.

SecureBankGuard інтегрується з передовими технологіями біометричної автентифікації, щоб забезпечити високобезпечний метод автентифікації. Унікальні біометричні атрибути користувачів, такі як відбитки пальців, риси обличчя або голосові моделі, фіксуються та порівнюються із зареєстрованими біометричними шаблонами для перевірки. Це гарантує, що тільки авторизовані особи з перевіреними біометричними даними можуть отримати доступ до банківських систем і програм.

SecureBankGuard використовує дані геолокації для перевірки фізичного місцезнаходження користувача під час спроб входу. Аналізуючи IP-адресу користувача, GPS-координати або інформацію про мережу Wi-Fi, система може порівняти поточне місцезнаходження з очікуваним або відомим розташуванням користувача. Якщо буде виявлено спробу входу з незнайомого або підозрілого місця, можуть знадобитися додаткові фактори автентифікації для підтвердження особи користувача.

SecureBankGuard використовує методи ідентифікації пристрою для розпізнавання та автентифікації пристрою користувача. Він аналізує специфічні атрибути пристрою, такі як відбитки пальців пристрою, MAC-адреси або характеристики апаратного забезпечення, щоб переконатися, що доступ надається лише надійним і авторизованим пристроям. Це запобігає доступу

неавторизованих користувачів до конфіденційної інформації, навіть якщо вони мають дійсні облікові дані для входу.

SecureBankGuard включає в себе можливості адаптивної автентифікації для динамічного налаштування необхідного рівня автентифікації на основі різних факторів ризику, поведінки користувачів і контекстної інформації. Це гарантує, що процес автентифікації адаптований до конкретних обставин кожної спроби входу.

Наприклад, якщо користувач зазвичай входить із надійного пристрою та знайомого місця, SecureBankGuard може дозволити спрощений процес автентифікації з меншою кількістю факторів. Однак, якщо спроба входу здійснена з невідомого пристрою або незвичайного місця, система може запропонувати додаткові фактори для забезпечення вищого рівня гарантії. Цей адаптивний підхід збалансовує безпеку та зручність для користувача, забезпечуючи легкий досвід виконання рутинних завдань і водночас посилюючи безпеку, коли цього вимагають фактори ризику.

Концепція SecureBankGuard розроблена для повної інтеграції з існуючими банківськими системами та користувацькими інтерфейсами, забезпечуючи плавну та зручну автентифікацію. Він надає безпечні API та параметри інтеграції, які дозволяють легко розгортати в банківській інфраструктурі, не порушуючи існуючі робочі процеси.

Система пропонує зручний інтерфейс, який проводить користувачів через процес автентифікації, надаючи чіткі інструкції та підказки для кожного необхідного фактора. Він підтримує різні канали автентифікації, включаючи веб-інтерфейси, мобільні додатки, коди на основі SMS або апаратні маркери, що дозволяє користувачам вибирати найбільш зручний і безпечний спосіб доступу до своїх облікових записів.

Впроваджуючи двофакторну автентифікацію (2FA), багатофакторну автентифікацію (MFA) і адаптивну автентифікацію, SecureBankGuard підвищує безпеку банківського сектору, значно знижуючи ризик несанкціонованого доступу та компрометації рахунку. Цей комплексний підхід до автентифікації забезпечує захист критично важливих фінансових систем, облікових записів

клієнтів і конфіденційних даних, зміцнюючи довіру та впевненість між клієнтами, одночасно пом’якшуючи потенційний вплив кіберзагроз [11].

3.3 Інформація про безпеку та керування подіями (SIEM)

Впровадження SecureBankGuard системи управління інформацією про безпеку та подій (SIEM) є критично важливим компонентом для забезпечення виявлення та реагування на кіберзагрози в банківському секторі. Система SIEM діє як центральний центр для збору, аналізу та кореляції даних, пов’язаних із безпекою, з різних джерел, що забезпечує комплексний моніторинг і проактивне керування інцидентами.

Система SIEM від SecureBankGuard збиратиме та об’єднуватиме журнали та дані про події безпеки з різних джерел, включаючи мережеві пристрої, сервери, бази даних, програми та пристрої безпеки. Вона фіксує широкий діапазон журнальної інформації, такої як дії користувача, системні події, журнали автентифікації, журнали брандмауера та дані мережевого трафіку. Завдяки централізації цих даних система SIEM забезпечує цілісне уявлення про безпеку всієї банківської інфраструктури, забезпечуючи ефективний моніторинг і аналіз.

Система SIEM використовує вдосконалені методи кореляції для аналізу та виявлення потенційних інцидентів безпеки. Вона співвідносить події з різних джерел даних, використовуючи правила, алгоритми та шаблони поведінки для виявлення аномалій, моделей зловмисної діяльності та індикаторів компрометації. Цей процес кореляції дозволяє системі SIEM виявляти складні методи атак, як-от розширені постійні загрози (APT), інсайдерські загрози та скоординовані атаки, які можуть охоплювати кілька систем або часових проміжків.

Щоб покращити свої можливості виявлення, система SIEM SecureBankGuard інтегрується із зовнішніми джерелами аналізу загроз. Ці джерела включають галузеві канали, комерційні постачальники інформації про загрози та бази даних загроз з відкритим кодом. Збираючи та аналізуючи інформацію про загрози в реальному часі, система SIEM розширює свій аналіз, ідентифікуючи відомі сигнатури атак, нові загрози та вразливості нульового дня.

Ця інтеграція гарантує, що банківський сектор залишається в курсі останніх загроз і може проактивно захищатися від них.

Система SIEM від SecureBankGuard забезпечуватиме можливості оповіщення в режимі реального часу, щоб оперативно повідомляти команди безпеки про потенційні інциденти безпеки. Коли стається певна подія або підозріла активність, система SIEM генерує сповіщення на основі попередньо визначених правил, порогових значень або алгоритмів виявлення аномалій. Ці сповіщення надсилаються призначеному персоналу або в центри безпеки (SOC) через різні канали, включаючи електронну пошту, SMS або інтеграцію з платформами реагування на інциденти.

Отримавши сповіщення, служби безпеки можуть продовжити розслідування інцидентів і розпочати ефективне реагування на інциденти. Система SIEM надає детальну інформацію про подію, зокрема її джерело, серйозність, уражені системи та відповідні журнали. Ця контекстна інформація дає змогу аналітикам безпеки визначати пріоритети та ефективно реагувати на інциденти, скорочуючи середній час виявлення (MTTD) і середній час відповіді (MTTR). Спрощуючи реагування на інциденти, система SIEM допомагає пом’якшити потенційний вплив порушень безпеки та мінімізує час простою в роботі.

Система SIEM від SecureBankGuard включає надійні можливості судового аналізу, що дозволяє проводити ретельне розслідування та аналіз інцидентів безпеки. Він підтримує контрольний журнал подій безпеки та журналів, фіксуючи детальну інформацію про дії, зміни та взаємодії користувачів. Цей контрольний журнал служить цінним ресурсом для судово-медичного аналізу після інцидентів, визначення першопричини та збору доказів для юридичних і нормативних цілей.

Система SIEM також полегшує звітування про відповідність, створюючи комплексні звіти, які демонструють дотримання галузевих норм, стандартів безпеки та внутрішньої політики. Ці звіти містять детальний огляд інцидентів безпеки, тенденцій загроз, показників відповідності та ключових показників продуктивності (KPI). Звітність про відповідність допомагає банківському

сектору продемонструвати свою відданість безпеці та дотриманню нормативних вимог під час аудитів, оцінок та перевірок.

Система SIEM від SecureBankGuard забезпечить постійний моніторинг і вдосконалення стану безпеки в банківському секторі. Вона постійно збиратиме й аналізуватиме події безпеки, мережевий трафік і поведінку користувачів для виявлення потенційних загроз і підозрілих дій. Система SIEM використовує алгоритми машинного навчання, аналітику поведінки та методи виявлення аномалій, щоб адаптувати та розвивати свої можливості виявлення. Постійно вивчаючи нові дані та враховуючи нові дані про загрози, система SIEM покращує свою здатність ідентифікувати нові кіберзагрози та реагувати на них.

Регулярний аналіз показників продуктивності системи SIEM, таких як рівень виявлення, помилкові спрацьовування та ефективність реагування на інциденти, дозволяє постійно вдосконалювати та налаштовувати систему. Система SIEM від SecureBankGuard забезпечує ефективність і адаптивність у виявленні та реагуванні на кіберзагрози в банківському секторі, постійно вдосконалюючи свої алгоритми, правила та механізми кореляції.

Таким чином, впровадження SecureBankGuard надійної системи безпеки інформації та керування подіями (SIEM) забезпечує комплексні можливості моніторингу, аналізу та реагування для захисту банківського сектора від кіберзагроз. Завдяки збору та агрегації журналів, кореляції та аналізу подій, інтеграції розвідки про загрози, попередженню в режимі реального часу, криміналістичному аналізу, звітності про відповідність, а також постійному моніторингу та вдосконаленню система SIEM посилює загальну безпеку банківського сектору, захищає критично важливі активи та дані , і допомагає зберегти довіру та впевненість клієнтів [12].

Для кращої візуалізації було спроєктовано теоретично блок-схему того як відбуватиметься управління нашою системою (див. рис. 3.1)

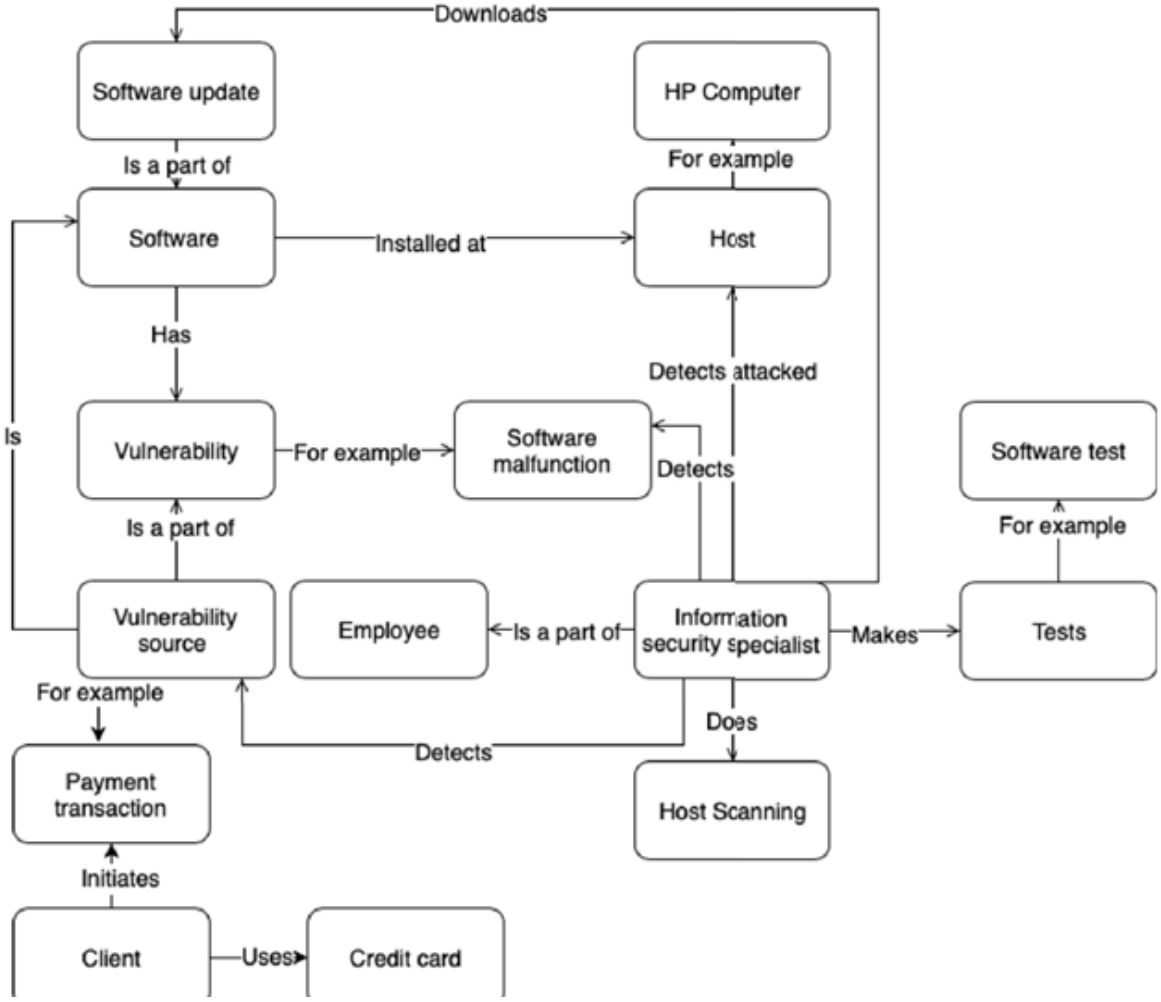

Рисунок 3.1 – Схема управління системою

Таким чином наш спеціаліст з інформаційної безпеки матиме повний доступ до системи, що в свою чергу дозволить йому моніторити систему в режимі реального часу та своєчасно зреагувати на любі ризики несанкціонованого доступу чи любих інших вразливостей. Людина що відповідатиме за інформаційну безпеку зможе вчасно оновити систему у разі виявляння любих вразливостей нульового дня. Розробка та впровадження надійної системи виявлення та запобігання кібератакам у банківському секторі, такої як SecureBankGuard, має величезне значення в сучасному цифровому середовищі.

Усуваючи обмеження існуючих систем і використовуючи передові технології, SecureBankGuard пропонує комплексну багаторівневу систему безпеки. Вона містить розширені механізми виявлення загроз, які аналізують шаблони, поведінку та індикатори компрометації для завчасного виявлення потенційних кіберзагроз. Крім того, SecureBankGuard використовує надійні

механізми автентифікації, такі як двофакторна автентифікація (2FA) і багатофакторна автентифікація (MFA), щоб забезпечити безпечний доступ до облікових записів клієнтів і захистити від несанкціонованого доступу.

Крім того, інтеграція системи безпеки та керування подіями (SIEM) у SecureBankGuard забезпечує моніторинг у реальному часі, кореляцію подій та аналіз подій безпеки та журналів. Це дозволяє оперативно виявляти потенційну небезпеку та зреагувати на неї, мінімізуючи вплив кібератак і спрощуючи судово-медичний аналіз для розслідування інцидентів і звітування про відповідність. Однак важливо визнати, що ландшафт загроз постійно змінюється, а кіберзлочинці постійно розробляють нові вектори атак і методи. Таким чином, безперервний моніторинг і вдосконалення SecureBankGuard разом із регулярними оновленнями та покращеннями є важливими для забезпечення його ефективності перед обличчям нових загроз.

Реалізація SecureBankGuard забезпечить банківський сектор комплексною системою виявлення та запобігання кібератакам. Використовуючи розширені механізми виявлення загроз, надійні заходи автентифікації та надійну систему SIEM, SecureBankGuard дає банкам і фінансовим установам можливість проактивно захищати свою інфраструктуру, підтримувати довіру клієнтів і підтримувати безпеку та стабільність банківського сектора у все більш цифровому світі.

3.4 Розробка та впровадження системи виявлення та запобігання кібератак на основі облікових засобів

При розробці систем запобігання кібератак у банківському секторі важко просимулювати будь яку атаку на апаратну або ж мережеву частину банку, адже для цього потрібно мати доступ до спеціального обладнання чи складної мережевої системи банку. Проте роботу користувача банківської системи можна просимулювати та проаналізувати поведінку облікового запису. Для аналізу кібербезпеки в банківській сфері в роботі використовувалась постанова

Національного банку України №95 про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України.

3.4.1 Техніки безпеки щодо облікових засобів

У моїй системі реалізовані різні техніки безпеки щодо облікових засобів, які допомагають захистити користувачів і їхні облікові записи. Одна з таких технік - це аналіз активності користувачів в їхніх облікових записах. Я створив функцію, яка аналізує запити користувача (див. лістинг 3.1).

Лістинг 3.1 – Логування запиту користувача

```
def log_user_activity(user_id, action):
    current_time = get_current_time()  # Отримати поточний час
    log_entry = {
        'user_id': user_id,
        'action': action,
        'timestamp': current_time
    save_log_entry(log_entry)  # Зберегти запис у лог-файлі або базі даних
def get_user_logs(user_id):
    user_logs = retrieve_user_logs(user_id)  # Отримати логи для певного користувача
    return user_logs
```

Після чого нам повертаються логи де вказано що зробив користувач та дані облікового запису(див. рис. 3.2).

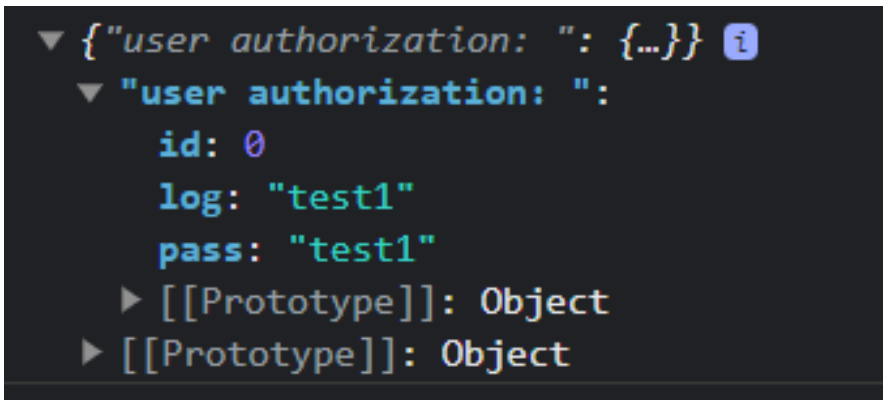

Рисунок 3.2 Логи користувача

Також якщо користувач не використовує систему протягом 10 хвилин або залишає її без дії, система автоматично виходить з облікового запису користувача

і вимагає повторної авторизації при наступному доступі (див. лістинг 3.2). Це дозволяє попередити несанкціонований доступ до облікового запису, якщо користувач, наприклад, залишив комп'ютер без нагляду.

Лістинг 3.2 – Блокування екрану

```
const mouseMove = document.querySelector("mouse");
    const tenMinutes = 10 * 60 * 1000;
    mouseMove.addEventListener("move", () => {
      if (mouseMove.move() === tenMinutes) {
        const screen = document.querySelector("screen");
        screen.lock();}});
```

3.4.2 Права та обов’язки облікових засобів.

У кожній системі облікові засоби мають певні права та обов'язки. Одним з головних обов'язків облікових засобів є регулярна зміна паролю не рідше, ніж кожні 30 днів (див. лістинг 3.2). Система автоматично нагадуватиме користувачам про необхідність зміни паролю, щоб зменшити ризик його неправомірного використання третіми особами.

Лістинг 3.3 – Зміна паролю

```
    const timeChangePassword = new Date().getTime(); // Отримання поточного часу в мілісекундах
    const thirtyDaysInMilliseconds = 30 * 24 * 60 * 60 * 1000; // 30 днів у мілісекундах
    const currentDate = new Date().getTime();
    if (currentDate - timeChangePassword >= thirtyDaysInMilliseconds) {
       window.alert("Настав час змінити пароль");
       changePassword();
    }
```

Якщо ж користувач був відсутній у мережі протягом 90 днів або його звільнили то такий обліковий запис видаляється.

3.4.3 Журнали логування

Система веде журнали логування, щоб фіксувати дії користувачів та забезпечити контроль за роботою мережі. Це необхідно для точного визначення причин проблем, що виникають у роботі мережі. Додатково, для запобігання спробам DDoS-атаки, встановлено обмеження на кількість спроб входу до мережі з одного облікового запису (див. лістинг 3.4). Якщо користувач невдало спробує ввійти в обліковий запис 5 разів, система сприймає це як аномальну активність і блокує доступ користувача.

Лістинг 3.4 – Обмеження доступу

```
let failedLoginAttempts = 0;
const maxFailedAttempts = 5;

function login(username, password) {
  if (checkCredentials(username, password)) {
    // Успішний вхід
    failedLoginAttempts = 0; // Скидаємо лічильник невдалих спроб
  } else {
    // Невдалий вхід
    failedLoginAttempts++;
    if (failedLoginAttempts >= maxFailedAttempts) {
      blockUser();
      return;
    }
  }
}
```

Крім того, користувачам обмежений доступ до встановлення будь-якого програмного забезпечення, що допомагає запобігти потраплянню шкідливих програм та втраті даних.

У моїй системі банківської безпеки я реалізував заходи щодо захисту електронної пошти. Ось як ці вимоги були втілені у моїй системі:

Встановлено міжмережевий екран (WAF), який контролює доступ до сервера електронної пошти. Цей екран дозволяє обмежити зовнішній доступ до

сервера тільки з довірених IP-адрес або мереж, що забезпечує надійний контроль над доступом до електронної пошти (див рис 3.3).

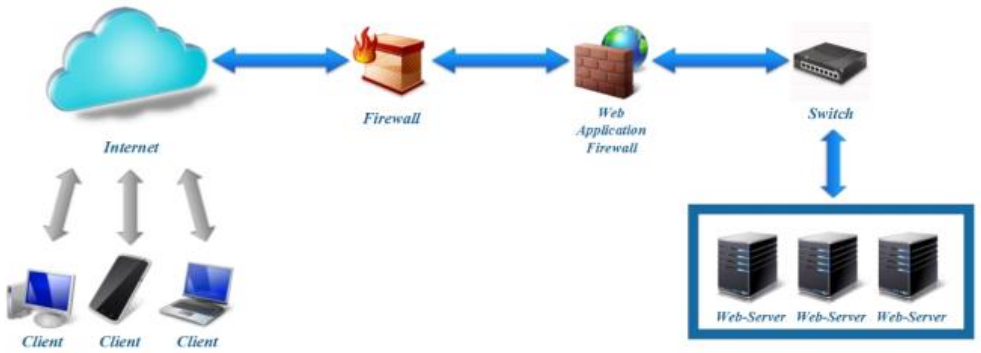

Рисунок 3.3 – Розгортання WAF

Блокування отримання спам-повідомлень: У системі використовується механізм фільтрації, який блокує отримання вхідних повідомлень від серверів мережі Інтернет, що розсилають спам. Цей механізм використовує різні алгоритми та правила для виявлення та блокування небажаних повідомлень, забезпечуючи чисту електронну пошту для користувачів.

У системі встановлений процес постійного моніторингу вразливостей сервера застосувань електронної пошти та клієнтського програмного забезпечення доступу до сервера. Цей процес регулярно перевіряє систему на наявність вразливостей та шукає оновлення, які усувають виявлені проблеми. Це забезпечує високий рівень безпеки сервера електронної пошти.

Запобігання кібератакам і захист банківських систем - постійний процес, і ці заходи є лише деякими засобами забезпечення безпеки. Система повинна бути постійно оновлювана та адаптована до нових загроз для максимального захисту банку та його клієнтів.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при кровотечах.

Навіть при розробці систем виявлення кібератак потрібно знати як діяти при будь-якій надзвичайній ситуації. Стихійні лиха, аварії і катастрофи, вибухи снарядів можуть викликати масові ураження. Унаслідок цього можливі різні травми – струси, переломи, кровотечі, стискання окремих частин тіла, поранення живота, грудної клітини, голови. Ураження людей може бути викликане уламками зруйнованих ударною хвилею споруд, і поєднувати поранення, переломи, опіки, кровотечі.

При наданні домедичної допомоги ураженому спочатку здійснюють тимчасову зупинку кровотечі, потім накладають пов’язки при пораненнях і опіках, далі здійснюють іммобілізацію при переламах кісток та, якщо необхідно, штучне дихання і закритий масаж серця.

В першу чергу домедичну допомогу надають ураженим, що мають небезпечну для життя артеріальну кровотечу. Необхідно також визначити черговість виконання прийомів надання домедичної допомоги, особливо при тяжкій комбінованій травмі – не можна, проводити іммобілізацію при відкритому переломі кістки з артеріальною кровотечею, поки вона не зупинена, не введений протибольовий засіб, а рана не закрита стерильною пов'язкою.

Кровотечу зупиняють накладанням джгута, тиснучої пов'язки або пальцевим притискуванням судин.

Якщо відсутня зовнішня кровотеча, а потерпілий відчуває різку слабкість, запаморочення, втрачає свідомість, шкірні покрови у нього бліді, то це свідчить про можливу внутрішню кровотечу. Для забезпечення термінової лікарняної допомоги необхідно терміново доставити потерпілого в медичний заклад. Щоби не допустити при цьому знекровлення мозку потерпілого, потрібно покласти його на ноші з припіднятими вверх кінцівками.

Не дозволяється промивати рану, видаляти із неї чужорідні тіла і торкатися руками, оскільки цим можна ускладнити пошкодження і викликати зараження рани.

Неприпустимо:

- промивати рану водою;
- лити у рану спиртові або будь-які інші розчини;
- обробляти йодом саму рану;
- прикладати вату безпосередньо до рани.

Потрібно звернутися до лікаря, якщо:

- рана розміром більше 1,0-1,5 см;
- велика кровотеча з рани;
- у потерпілого немає щеплення проти правця;
- рана розташована на пальцях кисті або стопи;
- рана сильно болить;
- виникло почервоніння і набряк шкіри навколо рани, підвищилася температура тіла;
- при будь-яких укушених або забруднених землею ранах.

Якщо кров повільно сочиться із пошкоджених судин то це капілярна кровотеча, яка зупиняється накладанням давлючої пов'язки.

Якщо із рани безперервно витікає струмінь темно-червоної крові, то це венозна кровотеча, яку зупиняють шляхом придання підвищеного стану пошкодженій частині тіла і накладенням тугої давлючої пов'язки або джгута при пошкодженні великих вен.

Якщо із рани витікає яскраво-червона кров, то це артеріальна кровотеча, яку зупиняють пальцевим притискуванням, накладанням давлючої пов'язки, джгута або закрутки. Давлюча пов'язки – це накладання декількох шарів стерильної марлі або бинта, які щільно прибинтовують. При кровотечах із ран голови притискують скроневу артерію попереду вуха, на рівні брови. При кровотечах із ран обличчя або губ притискують нижню щелепну артерію по середині нижньої щелепи напроти малого корінного зуба. Кровотечу із ран голови і обличчя можна також

зупинити шляхом притискування одної із сонних артерій, збоку від гортані, до шийних хребців.

Кровотечу із плечової артерії можна зупинити вдавлюванням тугого валика із вати у підпахвову впадину. Кровотечу із ран на нозі зупиняють шляхом притискування стегнової артерії всередині пахового згину.

Сильну артеріальну і венозну кровотечу тимчасово зупиняють за допомогою джгута або закрутки. Джгут на кінцівку накладається тоді, коли туга пов'язка не дає ефекту або потрібно швидко зупинити сильну кровотечу із великих судин [13].

Перед накладанням джгута обов'язкове пальцеве притискання артерії. Для зупинки кровотечі максимальним згинанням кінцівки і фіксації її в цьому положенні підкладається прокладка із тканини, вати або марлі. Джгут беруть за середину, злегка розтягують і обертають ним кінцівку так, щоби наступні оберти розташувалися поруч з першими і з'являлася широка давлюча поверхня. Для уникнення омертвіння кінцівки необхідно накладати джгут або закрутку не більш ніж на 1,5-2 год, а у холодний час і при променевих (радіаційних) ураженнях – не більше як на 1 годину. Під джгут (закрутку) підкладають записку з часом його накладення або записують на самій пов'язці .

Якщо з моменту накладання джгута або закрутки минуло більше 1-2 год., то необхідно повільно послабити джгут (закрутку) – до появи рожевого кольору і відновлення чутливості. Опісля 5-10 хвилин при повному розслаблені джгута (закрутки) і не відновлення кровотечі можна вважати її зупиненою. При цьому розслаблений джгут (закрутку) не знімають. Другим надійним способом є зупинка кровотечі із ран кінцівок згинанням їх у суглобах з наступною фіксацією. В область суглобного згинання попередньо кладуть валик із марлі або вати.

При цьому необхідно:

- артерію притиснути пальцями або кулаком вище місця поранення кінцівки;

- до накладення джгута тримати кінцівку у піднятому положенні;

- завести джгут за кінцівку (підклавши під джгут серветку, хустинку) і розтягнути з максимальним зусиллям;

- зробити перший виток джгута і перевірити пульс (його не повинно бути);

- накласти наступні витки джгута з меншим зусиллям;

- закріпити джгут і вкласти записку із зазначенням часу накладення джгута.

Неприпустимо:

- гаяти час на звільнення постраждалої кінцівки від одягу;

- маскувати джгут під одяг (джгут повинен бути добре помітним!);

- негайно не накласти джгут правильно у разі посиніння кінцівки та появи набряку;

- у холодну пору року не вкрити кінцівку, на яку накладено джгут, для запобігання відмороження.

Оптимальний термін надання домедичної допомоги – до 30 хв. після отримання ушкодження. При виклику швидкої медичної допомоги (номер телефону 103) слід повідомити диспетчеру наступну інформацію:

- точне знаходження місця події, її адресу або місце розташування;

- назву населеного пункту або найближчих пересічних вулиць (перехресть або доріг);

- орієнтири;

- свої прізвище, ім'я, по батькові;

- що відбулося (ДТП, пожежа, вибух);

- число потерпілих;

- характер ушкоджень (болі в грудині, важке дихання, відсутність пульсу, кровотеча) [14].

4.2 Вимоги пожежної безпеки при гасінні комп’ютерів.

Пожежна безпека є важливим аспектом, коли мова йде про комп’ютерну техніку. Електричні пожежі можуть становити значний ризик через наявність електричного струму під напругою та можливість швидкого поширення. Дотримання належних вимог пожежної безпеки є життєво важливим для зниження ризику пожежі, захисту життя та збереження майна.

Під час боротьби з електричними пожежами вкрай важливо вибрати відповідні вогнегасники. Вогнегасники ВВК - 2 дуже ефективні при гасінні електричних пожеж. Під час виділення вуглекислого газу витісняється кисень,

придушуючи вогонь. Для ефективної боротьби з електричними пожежами особи, відповідальні за пожежну безпеку, мають пройти відповідну підготовку щодо правильного використання вогнегасників. Це навчання включає розуміння конкретних прийомів і заходів безпеки, необхідних під час роботи з електричними пожежами. Важливо підкреслити необхідність дотримання дистанції та обережності, щоб запобігти ураженню електричним струмом і забезпечити безпеку людей, які намагаються загасити вогонь.

Протипожежні ковдри є цінним інструментом для гасіння невеликих електричних пожеж. Вони виготовлені з вогнетривких матеріалів і можуть швидко розгортатися, прикриваючи полум'я. Протипожежні ковдри перекривають подачу кисню та ефективно гасять вогонь. Використовуючи протипожежні ковдри, важливо переконатися, що ковдра повністю покриває полум’я та прилеглі зони, щоб запобігти повторному спалаху вогню [15].

Встановлення аварійних вимикачів живлення в безпосередній близькості від комп’ютерів має вирішальне значення. Ці вимикачі дозволяють швидко і негайно відключити джерело живлення в разі пожежі. Відключивши джерело живлення, можна стримати поширення вогню, зменшивши ймовірність подальших збитків і забезпечивши безпеку осіб, які беруть участь у гасінні пожежі.

Регулярні перевірки комп’ютерної техніки є життєво важливими для виявлення та усунення потенційної небезпеки пожежі. Ці перевірки включають ретельні огляди на наявність несправної проводки, забруднених вентиляторів, пошкодженого обладнання чи будь-яких інших електричних проблем, які можуть збільшити ризик пожежі. Швидкий ремонт або заміна несправних компонентів має важливе значення для підтримки пожежної безпеки при роботі із комп’ютерами.

Важливо також впровадити автоматичні системи пожежогасіння, які спеціально розроблені для гасіння пожежі спричинені за допомогою електрики. Для офісу з комп'ютерами використовують автоматичну систему пожежогасіння, яка не залишає залишкових слідів та не завдає шкоди обладнанню. Один з найкращих варіантів для таких умов - система пожежогасіння на основі газу FM-200 (гексафторпропану). FM-200 є безбарвним і беззапаховим газом, який відноситься до групи газових засобів пожежогасіння, відомих як газові агенти.

FM-200 є ефективним гасителем пожежі, який швидко гасить вогонь, запобігаючи поширенню вогню і забезпечуючи мінімальний вплив на оточуюче середовище та електронну техніку. Він дозволяє негайно втрутитися у випадку пожежі і гасити її шляхом витіснення кисню з вогню, тим самим гасячи його. Крім того, FM-200 не залишає залишкових слідів, що дозволяє швидко повернутися до нормального режиму роботи після активації системи пожежогасіння [16].

Встановлення систем пожежної сигналізації, які включають датчики диму та датчики тепла, має вирішальне значення для раннього виявлення електричних пожеж. Ці системи можуть швидко виявляти наявність диму або аномальний рівень тепла, запускаючи звукові сигнали та сповіщаючи мешканців про потенційну небезпеку. Раннє виявлення дає змогу швидко діяти та підвищує ефективність заходів із гасіння пожежі.

Необхідно проводити регулярні тренування та навчання, щоб переконатися, що всі особи в приміщеннях знайомі з планом евакуації та можуть належним чином реагувати під час надзвичайних ситуацій. Надання всебічного навчання пожежній безпеці та програм інформування для працівників або окремих осіб, які працюють поблизу електричних приладів, має важливе значення. Ці програми мають охоплювати заходи запобігання пожежі, розпізнавання потенційної небезпеки пожежі, належне використання вогнегасників, процедури евакуації та загальні протоколи пожежної безпеки. Підвищуючи обізнаність і знання, люди можуть зробити свій внесок у створення безпечнішого середовища та ефективно реагувати в разі виникнення пожежі.

Встановлення відносин співпраці з місцевою пожежною службою є дуже корисним для пожежної безпеки в офісах. Пожежні служби можуть надати експертні поради та рекомендації під час оцінки безпеки, гарантуючи, що установки відповідають усім необхідним стандартам пожежної безпеки. Участь у регулярній комунікації та залученні пожежних служб до тренінгів і тренувань може покращити можливості реагування на надзвичайні ситуації та сприяти скоординованому підходу до пожежної безпеки.

ВИСНОВКИ

У розробці та впровадженні системи виявлення та запобігання кібератак у банківському секторі були розглянуті ключові аспекти, пов'язані з інформаційною банківською системою, видами кібератак та методами їх виявлення. Історичний огляд кібератак в банківській сфері підкреслив необхідність постійного удосконалення захисту від цих загроз.

Зокрема, розглянуто фішингові атаки, атаки шкідливих програм, атаки соціальної інженерії, атаки MitM, розподілені атаки на відмову в обслуговуванні (DDoS) та атаки SQL-ін'єкції. Ці атаки можуть спричинити серйозні фінансові збитки та порушити довіру клієнтів до банківських установ.

У розділі про впровадження системи виявлення та запобігання кібератак у банківському секторі розглянуто ефективні методи боротьби з цими загрозами. Виявлення та запобігання вторгненням, двофакторна автентифікація (2FA) та багатофакторна автентифікація (MFA), а також інформація про безпеку та керування подіями (SIEM) є важливими компонентами системи захисту банківської інформації.

Розробка та впровадження системи виявлення та запобігання кібератак у банківському секторі є критично важливою для забезпечення безпеки клієнтів та збереження довіри до банківських установ. Реалізація такої системи допоможе зменшити ризик фінансових втрат і захистити конфіденційні дані клієнтів, що є невід'ємною умовою стабільної та надійної діяльності банківського сектору.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Saeid Khajeh dangolani, The Impact of Information Technology in Banking System (A Case Study in Bank Keshavarzi IRAN), 2011.
2. Mircea Georgescu and Victor Jeflea, The Particularity of the Banking Information System, Volume 20, 2015, pp 268-276.
3. Banphot Vatanasombut, Magid Igbaria, Antonis C. Stylianou, Waymond Rodgers, Information & Management, Volume 45, Issue 7, November 2008, Pages 419-428.
4. Microsoft Digital Defense Report OCTOBER 2021, Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi#page=47
5. Microsoft Digital Defense Report 2022, Retrieved from https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022
6. Verizon's 2019 Data Breach Investigations Report, Retrieved from https://www.pcmag.com/news/google-and-amazon-are-impersonated-the-most-in-phishing-scams.
7. Financial and Insurance (NAICS 52), Retrieved from https://www.verizon.com/business/resources/reports/dbir/2023/industries-intro/financial-services-data-security-breaches/
8. Venkatesha Sushruth, K. Rahul Reddy & B. R. Chandavarkar, Social Engineering Attacks During the COVID-19 Pandemic, 06 February 2021.
9. NETSCOUT DDoS THREAT INTELLIGENCE REPORT / 5TH ANNIVERSARY EDITION, Retrieved from https://www.netscout.com/threatreport/ddos-threat-intelligence-report/#netscout-visibility.
10. Uzma Afzal, Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools, 2013.

11. Gustavo González-Granadillo ,Susana González-Zarzosa and Rodrigo Diaz, Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures, 12 July 2021.
12. IOP Publishing Ltd, Implementation of Information Security System in Service and Trade, 2019.
13. Порядок надання домедичної допомоги постраждалим при рані кінцівки, в тому числі ускладненій кровотечею, https://zakon.rada.gov.ua/laws/show/z0759-14/paran2#n2.
14. ДОЛІКАРСЬКА ДОПОМОГА ПРИ КРОВОТЕЧАХ, 12 БЕРЕЗНЯ 2022, http://www.oblses.ck.ua/index.php?option=com_content&view=article&id=2710:dolikarska-dopomoha-pry-krovotechakh&catid=41:2013-05-13-02-14-47&Itemid=57
15. ПРАВИЛА НАКЛАДАННЯ ДЖГУТА І КОМПРЕСІЙНИХ ПОВ'ЯЗОК, 28 червня 2022, https://velykomykh.otg.dp.gov.ua/novini-ta-podiyi/novini/domedichna-dopomoga-pri-krovotechah
16. Наказ про затвердження Інструкції з гасіння пожеж на енергетичних об'єктах України, 22.12.2011 № 863, https://zakon.rada.gov.ua/laws/show/z0013-12#Text