**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему: "ЗАСОБИ ВИЯВЛЕННЯ ЗАГРОЗ ДЛЯ БАНКІВСЬКИХ І ФІНАНСОВИХ УСТАНОВ (ЗЛОМИ, ФІШИНГ, ШАХРАЙСТВО)"

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Артемій ДАЦЮК
*(підпис)* *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42
Артемій ДАЦЮК

Керівник: Дмитро РАБЧУН
*к.т.н.*

Рецензент: Галина ГАЙДУР
*Д-р.техн.наук, професор*

**Київ 2026**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**Навчально-науковий інститут кібербезпеки та захисту інформації**

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

**ЗАТВЕРДЖУЮ**
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дацюку Артемію Геннадійовичу

*(прізвище, ім’я, по батькові здобувача)*

1. Тема кваліфікаційної роботи “Засоби виявлення загроз для банківських і фінансових установ (зломи, фішинг, шахрайство)”,
керівник кваліфікаційної роботи РАБЧУН Д.І, к.т.н.
*(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)*

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *загроза, банківська установа, фінансова установа, злом, фішинг, шахрайство, засоби виявлення, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати кіберзагрози у сфері банківських та фінансових установ
4.2. Дослідити засоби та методи виявлення кіберзагроз у сфері банківських та фінансових установ
4.3. Визначити шляхи практичної імплементації заходів кібербезпеки у сфері банківських та фінансових установ), розробити практичні рекомендації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2026 р.

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Етапи кваліфікаційної роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Визначення об’єкту, предмету, мети та завдань дослідження. | 18.03.2026 | виконано |
| 2. | Збір та аналіз літератури. | 30.03.2026 | виконано |
| 3. | Аналіз кіберзагроз у сфері банківських та фінансових установ | 08.04.2026 | виконано |
| 4. | Засоби та методи виявлення кіберзагроз у сфері банківських та фінансових установ | 15.04.2026 | виконано |
| 5. | Рекомендації щодо практичної імплементації заходів кібербезпеки у сфері банківських та фінансових установ | 22.04.2026 | виконано |
| 6. | Формулювання висновків за результатами проведеного дослідження. | 29.04.2026 | виконано |
| 7. | Оформлення роботи. | 06.05.2026 | виконано |
| 8. | Оформлення презентації. | 11.05.2026 | виконано |
| 9. | Отримання рецензії на роботу. | 10.06.2026 | виконано |
| 10. | Захист в ЕК. | __.06.2026 | виконано |

Здобувач вищої освіти _____ Артемій ДАЦЮК
*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Дмитро РАБЧУН
*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

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

**ПОДАННЯ**
**ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**
**ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**
**на здобуття освітнього ступеня бакалавра**

Направляється здобувач Дацюк Артемій Геннадійович

до захисту кваліфікаційної роботи

за спеціальністю 125 Кібербезпека
*(код, найменування спеціальності)*
освітньої програми Управління інформаційною та кібернетичною безпекою
*(назва)*
на тему: "Засоби виявлення загроз для банківських і фінансових установ (зломи, фішинг, шахрайство)"
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**Висновок керівника кваліфікаційної роботи**

Здобувач ДАЦЮК Артемій у кваліфікаційній роботі проаналізув сучасні кіберзагрози у сфері банківських та фінансових установ, визначив ключові засоби та методи виявлення кіберзагроз у сфері банківських та фінансових установ, запропонув рекомендації щодо практичної імплементації заходів кібербезпеки у сфері банківських та фінансових установ. ДАЦЮК Артемій показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ДАЦЮКА Артемія на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2026 року

**Висновок кафедри про кваліфікаційну роботу**

Кваліфікаційна робота розглянута. Здобувач Дацюк А. Г. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

# ВІДГУК РЕЦЕНЗЕНТА
## на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ДАЦЮКА Артемія
на тему “Засоби виявлення загроз для банківських і фінансових установ (зломи, фішинг, шахрайство)”

**Актуальність.** Фінансові установи швидкими темпами впроваджують цифрові інструменти в банківській та фінансовій сфері, що підвищує попит на надійні системи захисту даних та надійні заходи кібербезпеки. У динамічному середовищі фінансової сфери виклики неминучі, починаючи від кібератак та законодавчих вимог і закінчуючи мінливими вимогами клієнтів до кібербезпеки. Надійні заходи безпеки, навчання співробітників та загальна культура безпеки – це ключові шляхи досягнення надійного стану безпеки. З огляду на зазначене дослідження проблеми вибору засобів виявлення загроз для банківських і фінансових установ є актуальним науковим завданням.

**Позитивні сторони.**

1. У роботі досліджено основні види кіберзагроз в фінансовій та банківській сферах, проаналізовано ключові засоби протидії та інструменти запобігання вторгненням, що може призвести до негативних наслідків функціонування зазначених установ, надано рекомендації удосконалення захисту та врахування розвитку технологій.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Автор опрацював значну джерельну базу: 31актуальну публікацію, більшисть з яких є англомовними.

**Недоліки.**

Доцільно було б привести реальний приклад застосування проаналізованого програмного забезпечення захисту.

Однак, вищезгадане зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

**Висновок:** Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач Дацюк Артемій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Галина ГАЙДУР
Д-р.техн.наук, професор *підпис*

# РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню засобів виявлення загроз для банківських і фінансових установ (зломи, фішинг, шахрайство). Робота складається зі вступу, трьох розділів, що містять 7 рисунків, 7 таблиць, висновків і списку використаних джерел із 31 найменування. Загальний обсяг роботи становить 70 сторінок, з яких 2 сторінки - список використаних джерел.

***Метою роботи*** є дослідження засобів виявлення загроз для банківських і фінансових установ з акцентуванням на зломи, фішинг, шахрайство.

***Об'єктом дослідження*** є засоби виявлення загроз для банківських і фінансових установ.

***Предмет дослідження*** **–** особливості застосування засобів виявлення загроз для банківських і фінансових установ.

***Методи дослідження.*** Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, системного підходу до застосування засобів виявлення кіберзагроз.

Як результат у роботі розглянуто основні види кіберзагроз, виявлено тенденції удосконалення протидії, проаналізовано основні методи штучного інтелекту, які застосовуються для виявлення кіберзагроз. Запропоновано рекомендації застосування засобів та методів для захисту від кібератак.

***Галузь застосування.*** Результаті цього дослідження, слугують цінним ресурсом для фахівців галузі для розробки більш ефективних стратегій протидії кіберзагрозам, що розвиваються, тим самим зміцнюючи стійкість та безпеку банківського та фінансового секторів.

**Ключові слова:** ЗАГРОЗА, БАНКІВСЬКА УСТАНОВА, ФІНАНСОВА УСТАНОВА, ЗЛОМ, ФІШИНГ, ШАХРАЙСТВО, ЗАСОБИ ВИЯВЛЕННЯ, МІЖНАРОДНІ СТАНДАРТИ, НАУКОВА ТА ТЕХНІЧНА ЛІТЕРАТУРА.

# ABSTRACT

The qualification work is devoted to the study of threat detection tools for banking and financial institutions (hacking, phishing, fraud). The work consists of an introduction, three sections containing 7 figures, 7 tables, conclusions and a list of sources used from 31 items. The total volume of the work is 70 sheets, of which 2 sheets are a list of sources used.

***The purpose of the work*** is to study threat detection tools for banking and financial institutions with an emphasis on hacking, phishing, fraud.

***The object of the study*** is threat detection tools for banking and financial institutions.

***The subject of the study*** is the features of the application of threat detection tools for banking and financial institutions.

***Research methods.*** To solve the above scientific problem, the work used methods of analysis and synthesis, comparison, classification, and a systematic approach to the application of cyber threat detection tools.

As a result, the work considered the main types of cyber threats, identified trends in improving countermeasures, and analyzed the main methods of artificial intelligence used to detect cyber threats. Recommendations for the use of tools and methods for protection against cyberattacks are proposed.

***Field of application.*** The results of this study serve as a valuable resource for industry professionals to develop more effective strategies to counter emerging cyberthreats, thereby strengthening the resilience and security of the banking and financial sectors.

Key words: THREAT, BANKING INSTITUTION, FINANCIAL INSTITUTION, HACKING, PHISHING, FRAUD, DETECTION TOOLS, INTERNATIONAL STANDARDS, SCIENTIFIC AND TECHNICAL LITERATURE.

# ЗМІСТ

# ВСТУП

***Актуальність теми.*** Ландшафт кібербезпеки продовжує розвиватися, і шахрайство стає дедалі серйознішою проблемою для команд безпеки. Сучасний зловмисник мотивований та націлений на отримання високого рівня вигоди від зпроєктованих кібератак. Найбільш привабливими цілями слугують банківські та фінансові установи. З огляду на зазначене дослідження проблеми анавлізу та вибору засобів виявлення загроз для банківських і фінансових установ є актуальним науковим завданням.

***Метою роботи*** є дослідження засобів виявлення загроз для банківських і фінансових установ з акцентуванням на зломи, фішинг, шахрайство.

***Об'єктом дослідження*** є засоби виявлення загроз для банківських і фінансових установ.

***Предмет дослідження*** **–** особливості застосування засобів виявлення загроз для банківських і фінансових установ.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Проаналізувати кіберзагрози у сфері банківських та фінансових установ
2. Дослідити засоби та методи виявлення кіберзагроз у сфері банківських та фінансових установ
3. Розобити практичні рекомендації вровадження заходів кібербезпеки у сфері банківських та фінансових установ.

***Методи дослідження*****.** Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, системного підходу до застосування засобів виявлення кіберзагроз.

Як результат у роботі розглянуто основні види кіберзагроз, виявлено тенденції удосконалення протидії, проаналізовано основні методи штучного інтелекту, які застосовуються для виявлення кіберзагроз. Запропоновано рекомендації застосування засобів та методів для захисту від кібератак.

***Практичне значення одержаних результатів*****.** Результати цього

дослідження, слугують цінним ресурсом для фахівців галузі для розробки більш ефективних стратегій протидії кіберзагрозам, що розвиваються, тим самим зміцнюючи стійкість та безпеку банківського та фінансового секторів.

# РОЗДІЛ 1 АНАЛІЗ ЗАГРОЗ ДЛЯ БАНКІВСЬКИХ І ФІНАНСОВИХ УСТАНОВ

## 1.1 Основні види кіберзагроз для банківських і фінансових установ

Регуляторний ландшафт кібербезпеки продовжує розвиватися в усьому світі. У 2023 році Ану Бредфорд окреслив три нові підходи: ринкова, державна та правова. Ця структура стала корисною лінзою для розуміння нових нормативних актів у 2024 році, включно з запровадженням Комісії з цінних паперів і бірж США вимог до звітності про кіберсуттєвість , DORA ЄС і Закону Китаю про безпеку даних . Ці нові правила мають міжрегіональний вплив, що вимагає глобального погляду на відповідність. Нові сфери, на які зосереджені регулятори, включають API, генеративний штучний інтелект і політику платежів за програми-вимагачі, які вимагають ретельного моніторингу [1].

Одночасно DDoS-атаки еволюціонували від переважно злочинних організацій до геополітичних інструментів, які використовують національні держави та хактивісти. Ми стали свідками рекордних атак DNS NXDOMAIN , також відомих як атаки на псевдовипадковий субдомен (PRSD) , і збільшення DDoS-атак рівня 3 і 4 (інфраструктура), націлених на фінансові установи в зонах конфлікту, разом із зростаючою поширеністю DDoS-атак рівня 7 (рівень додатків) проти програм і API. Ці тенденції спостерігалися в галузях і регіонах, підкреслюючи необхідність надійних, адаптивних заходів кібербезпеки [1].

Ландшафт кібербезпеки продовжує розвиватися, і шахрайство стає дедалі серйознішою проблемою для команд безпеки. Нещодавній звіт Akamai про веб-скрапінг, спричинений попитом клієнтів на захист, показує, що сектор фінансових послуг постраждав найбільше. Наші дані показують, що 36% виявлених підозрілих доменів були спрямовані на фінансові установи (рис. 1.1). Примітно, що 68% цих підроблених сайтів фінансових послуг використовували тактику фішингу, щоб отримати особисту ідентифікаційну інформацію, включаючи облікові дані,

сприяючи захопленню облікового запису та крадіжці особистих даних. Щоб пом'якшити ці випадки шахрайства, що зростає, потрібна міжорганізаційна співпраця [1].

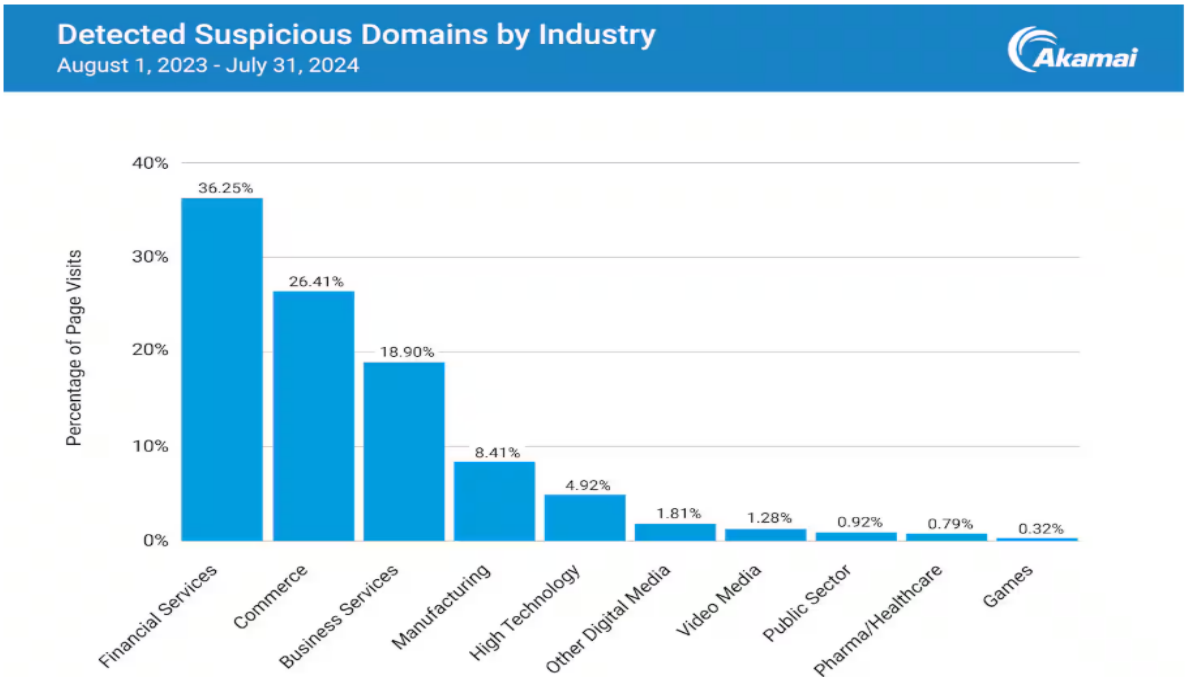


Рис. 1.1. На фінансові послуги припадає 36,3% доменів, які займаються фішингом та/або імітацією бренду [1]

Сучасний зловмисник мотивований на націлений на отримання високого рівня вигоди від зпроєктованих кібератак. Найбільш привабливими цілями слугують банківські та фінансові установи.

За даними VMware, у першій половині 2020 року кількість кібератак, націлених на фінансові установи, зросла на 238% . А за даними IBM та Ponemon Institute , середня вартість витоку даних у фінансовому секторі у 2021 році становить 5,72 мільйона доларів [2].

Найбільш поширеними сучасними атаками являються фішинг, програми-вимагачі, Ін'єкції SQL, включення локальних файлів, міжсайтові сценарії та ін'єкції OGNL Java, DDoS-атаки, атаки на ланцюги поставок, Банк Дропс.

## 1. Фішинг

Фішинг, різновид соціальної інженерії, — це метод обману змусити користувачів розкрити облікові дані для входу, щоб отримати доступ до внутрішньої мережі.

Найпоширенішою формою фішингу є фішинг електронною поштою, коли жертвам надсилається електронний лист, який видається за законне повідомлення.

Взаємодія з будь-яким із заражених посилань або вкладень у фішингових електронних листах може ініціювати встановлення зловмисного програмного забезпечення на цільовій комп'ютерній системі або завантаження підробленої веб-сторінки, яка збирає облікові дані для входу.

Для одержувача, який нічого не підозрює, ці шахрайські електронні листи здаються дуже переконливими, особливо коли вони подаються з відчуттям терміновості.

Деякі фішингові атаки є повідомленнями-відповідями на наявний ланцюжок електронної пошти – тактика, відома як викрадення ланцюжка бесіди електронної пошти. Оскільки фішингові електронні листи стає все важче розпізнавати, вони є одним із найпопулярніших векторів атак кіберзлочинців. Класифікація фішингових атак представлена ра рисунку 1.2 [3].

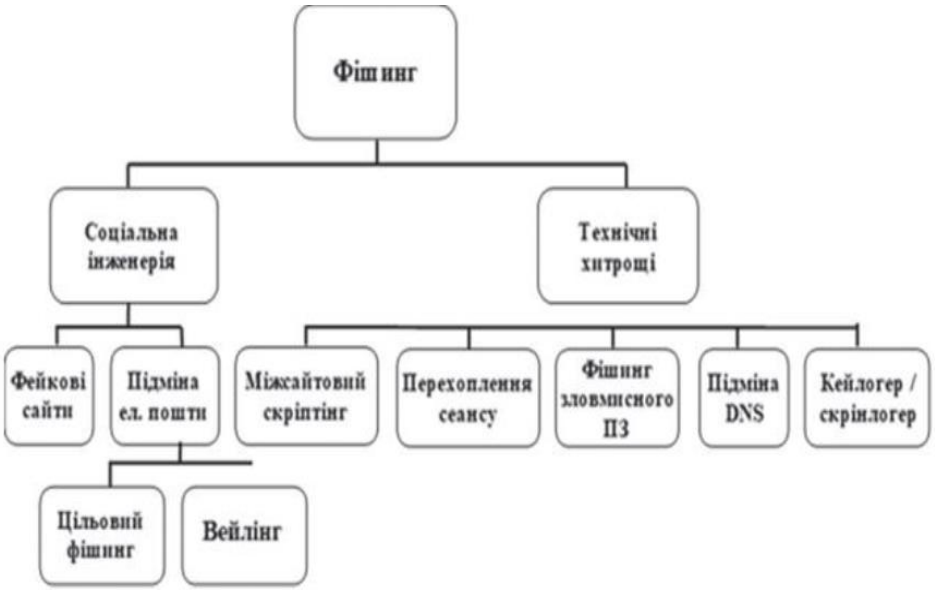


Рис. 1.2. Класифікація фішингових атак [3]

**2. Програми-вимагачі**

Програми-вимагачі та програми-вимагачі як послуга є ще одним критичним кіберризиком для фінансових послуг. Під час атаки програм-вимагачів кіберзлочинці блокують жертви з їхніх комп'ютерів, шифруючи їх за допомогою зловмисного програмного забезпечення. Збиток скасовується лише в разі сплати викупу.

Найпопулярнішим є публікація більшої частини конфіскованих конфіденційних даних на кримінальних форумах, доки не буде сплачено викуп.

Така тактика здирництва, на жаль, дуже ефективна проти фінансових установ, оскільки їхні суворі правила передбачають зразкову стійкість до кібератак і порушень даних .

У зв'язку з тим, що атаки програм-вимагачів зараз переростають у територію витоку даних, успішна атака може мати ширші наслідки для стандартів дотримання нормативних вимог .

Галузь фінансових послуг є дуже привабливою мішенню для програм-вимагачів через цінну інформацію про клієнтів, якою вони володіють. Загроза витоку цих даних у дарк-мережі та відповідна шкода репутації змушує багато організацій фінансових послуг виконувати вимоги щодо викупу.

**3. Ін'єкції SQL, включення локальних файлів, міжсайтові сценарії та ін'єкції OGNL Java**

Відповідно до щорічного звіту про безпеку Akamai , 94% спостережуваних кібератак у фінансовому секторі були спричинені такими чотирма векторами атак:

- Ін'єкції SQL (SQLi)
- Міжсайтовий сценарій (XSS)
- Включення локального файлу (LFI)
- OGNL Java Injection

**4. DDoS-атаки**

Фінансовий сектор зазнає найбільшої кількості розподілених атак типу "відмова в обслуговуванні" (DDoS).

Під час DDoS-атаки сервер жертви переповнений фальшивими запитами на з’єднання, що змушує його перебувати в мережі. DDoS-атаки є популярною кіберзагрозою для фінансових служб, оскільки їхня поверхня атак різноманітна, включаючи банківські IT-інфраструктури, облікові записи клієнтів, платіжні портали тощо. Це робить вплив DDoS-атак глибшим для фінансових установ. Кіберзлочинці можуть використовувати хаос, що виник, двома різними способами:

- Додаткові кампанії кібератак можуть бути запущені, поки групи безпеки відволікаються на DDoS-атаку.
- Кіберзлочинці можуть запропонувати виявити DDoS-атаку, якщо буде сплачено викуп. Ця стратегія, ймовірно, буде успішною, враховуючи суворі угоди SLA між фінансовими установами.

**5. Атаки на ланцюги поставок**

Під час атаки на ланцюжок постачання жертва проникає через скомпрометованого стороннього постачальника в ланцюзі постачання.

Атаки на ланцюг поставок дають змогу кібер-зловмисникам обійти заходи безпеки, створивши шляхи доступу до конфіденційних ресурсів через стороннього постачальника цільової мережі.

Оскільки, за статистикою, постачальники не сприймають кібербезпеку так серйозно, як їхні клієнти, їх компроміс зазвичай набагато легше досягти. А оскільки сторонні постачальники зберігають конфіденційні дані для всіх своїх клієнтів, один компроміс може вплинути на сотні компаній .

Для захисту від атак на ланцюжок постачання фінансовим службам рекомендується впроваджувати архітектуру нульової довіри з безпечними політиками керування привілейованим доступом . Процес зараження шкідливим програмним забезпеченням представлено на рисунку 1.3.

Складність виявлення таких атак означає, що організації повинні зосередитися на рішеннях, які можуть розглядати різні аспекти мережевих операцій, щоб виявити поточні атаки, які вже відбуваються в мережі, на додаток до потужного превентивного захисту.

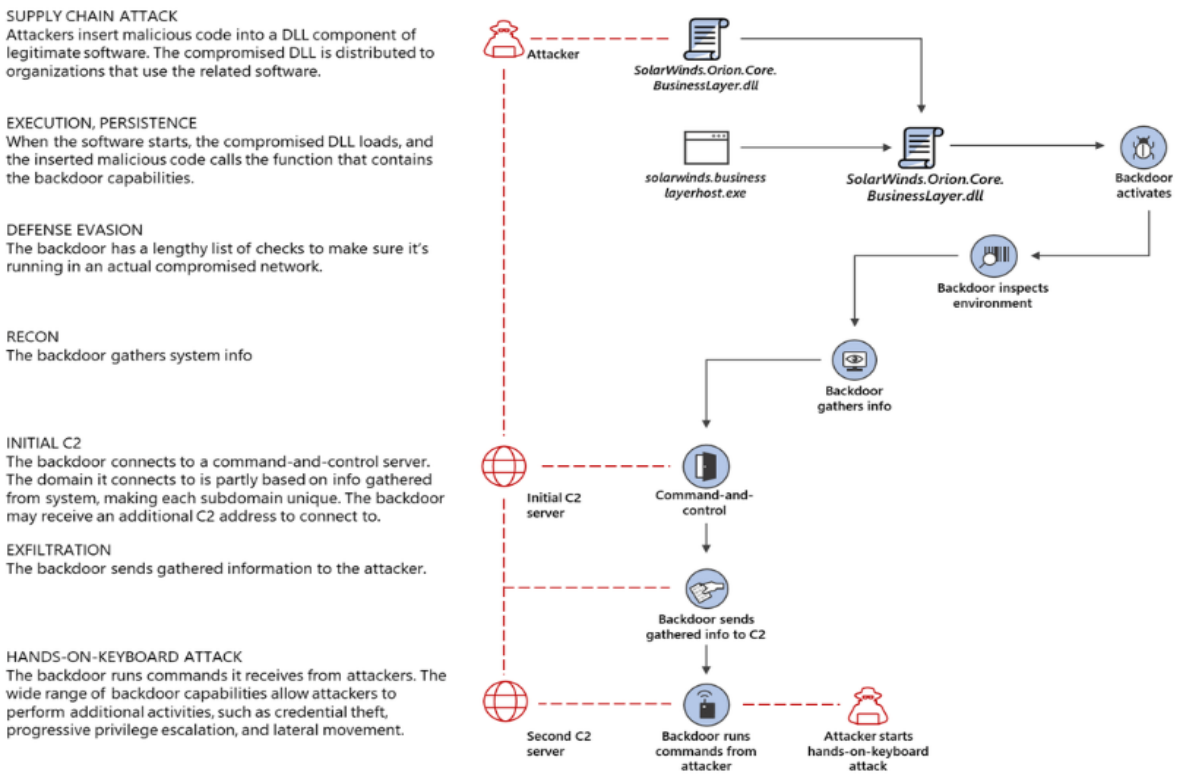


Рис. 1.3. Solorigate ланцюг зараження шкідливим програмним забезпеченням [9]

**6. Банк Дропс**

Щоб приховати своє місцезнаходження від органів влади, кіберзлочинці часто зберігають викрадені кошти на підроблених банківських рахунках (bank drops), відкритих за допомогою викрадених облікових даних клієнтів.

Серед кіберзлочинців збір облікових даних клієнта, необхідних для створення банківського скидання, називають “повним”.

Повні дані жертви можуть містити таку інформацію:

- ПІБ
- Адреса
- DOB
- Відомості про водійські права
- Кредитний рейтинг
- Деталі соціального страхування

Схеми, що сприяють звичайним банкрутствам, швидше за все, адаптуються до вимог цифрового гаманця, оскільки все більше кіберзлочинців віддають перевагу вищій анонімності криптовалюти .

У відповідь на цю кіберзагрозу фінансові установи повинні запровадити засоби контролю безпеки, зокрема для облікових даних, які зазвичай потрібні для відкриття нових рахунків.

**7. Незашифровані дані**

Зазвичай команди кібербезпеки шифрують усі дані. Тільки той, хто має відповідний ключ, може зібрати дані, що значно спрощує та робить їх передачу безпечнішою. Навіть якщо шахрай викраде інформацію, дані будуть марними без ключа.

Хакери докладають величезних зусиль, намагаючись викрасти дані щойно вони залишаються незашифрованими на банківському сервері. Зовсім недавно дослідник з кібербезпеки виявив цілу незашифровану базу даних з конфіденційною інформацією про клієнтів, що зберігалася канадською фінтех-платформою NorthOn [15].

## 1.2. Зломи банківських систем: механізми та наслідки

Кібербезпека в банківській справі стосується технологій, практик і процесів, призначених для захисту цифрових систем, даних і мереж банків від загроз кібербезпеці. Зараз банки керують величезними обсягами конфіденційної інформації, включаючи фінансові дані клієнтів, особисті дані та записи транзакцій. Заходи кібербезпеки гарантують, що ці дані захищені від злому, шахрайства, хакерства та інших форм кіберзлочинності [10].

Кібербезпека в банківській справі — це захист усієї цифрової інфраструктури банку — від систем онлайн-банкінгу до внутрішніх баз даних — від несанкціонованого доступу, витоку даних і зловмисних атак. Ефективна IT-безпека для банків має вирішальне значення для підтримки довіри, відповідності та операційної стабільності в галузі, яка стає все більшою

мішенню для кіберзлочинців [10].

Банки є одними з найбільш вразливих установ, коли мова йде про кіберзагрози. Через величезну кількість конфіденційних даних і фінансових операцій, які відбуваються щодня, вони є привабливою мішенню для хакерів. Кібербезпека є важливою для банків, щоб захистити не лише свої операції, але й конфіденційність і довіру своїх клієнтів.

Кіберзлочинці постійно адаптують свої методи під конкретні галузі, враховуючи їхню специфіку, вразливості та цінність даних. Розуміння галузевих особливостей фішингу допомагає організаціям та користувачам краще захиститися від цільових атак. Різні сектори економіки стають мішенями для різних типів фішингових схем, і кожна галузь потребує специфічних заходів захисту. На рисунку 1.4. відображено основні галузі, на які сфокусовані фішингові атаки.

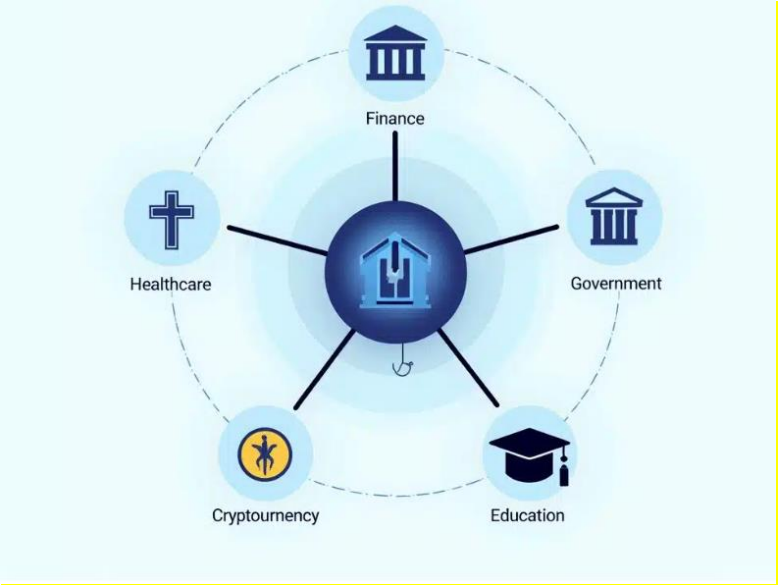


Рис. 1.4. Галузі, на які сфокусовані фішингові атаки [4]

За оцінками, понад 90% усіх успішних кібератак починаються з фішингової атаки, і цей невдалий коефіцієнт конверсії розриває фінансову індустрію.

Фішингові атаки на фінансовий сектор часто націлені на банківські реквізити клієнтів. Під конфіденційною інформацією користувачів в розрізі фішингової атаки розуміють [4]:

–логін та пароль для входу в мобільні застосунки;

–номер, термін дії, CVV2/CVC2, ПІН платіжної картки;

–одноразові паролі підтвердження операцій;

–адреса електронної пошти;

–фінансовий номер телефону;

–слово —пароль до картки, відповіді на секретні питання.

Фінансовий сектор [4]:

- Мішені атак: Банківські облікові записи, дані кредитних карток, доступи до інвестиційних платформ.
- Популярні методи: Підробка банківських вебсайтів та мобільних додатків, фальшиві повідомлення про підозрілі транзакції, фіктивні пропозиції від фінансових консультантів. Кіберзлочинці часто використовують офіційну термінологію та логотипи банків, щоб створити відчуття легітимності.
- Специфічні заходи захисту: Використання окремих пристроїв для фінансових операцій, 3D-Secure для онлайн-платежів, регулярна перевірка виписок по рахунках, використання банківських токенів та фізичних ключів безпеки.

Статистика фішингових атак у фінансовій галузі [5]:

У четвертому кварталі 2024 року APWG зафіксувала 989123 фішингових атак, порівняно з 877 536 у другому кварталі та 932 923 у третьому кварталі.

Китайські фішери надсилають потоки фішингових SMS-повідомлень завдяки новому набору для фішингу та доменним іменам .TOP.

Категорія SAAS/веб-пошти була сектором, який найбільше атакувався, а соціальні медіа-сайти йшли позаду.

Середня сума, запитувана під час атак BEC за допомогою банківських переказів у четвертому кварталі 2024 року, становила 128980 доларів США, що майже вдвічі перевищує середній показник третього кварталу.

Досить багато фішингових кампаній, які використовують QR-коди у вкладеннях електронних листів.

Спокуси та цілі різноманітні, але використання QR-коду, щоб змусити когось відвідати фішинговий сайт, швидко стає кращим методом для кіберзлочинців.

Причини, чому кіберзлочинці можуть захотіти використовувати QR-коди:

- QR-код, імовірно, сканується за допомогою телефону, який часто гірше захищений від шкідливих веб-сайтів або навіть зовсім незахищений.
- Телефони також, ймовірно, є персональними пристроями, які надають зловмисникам прямий шлях до конфіденційних особистих облікових записів. Наприклад, банківські програми часто встановлюються на одному пристрої.
- QR-коди з першого погляду неможливо визначити як шкідливі.
- Посилання в електронних листах зазвичай аналізуються фільтрами електронної пошти, тоді як QR-коди можна вставляти як зображення, яке багато фільтрів електронної пошти ігноруватимуть.
- Використання QR-кодів в інших програмах, наприклад банківських, може викликати певний рівень довіри.

У поєднанні з іншими відомими методами фішингу QR-коди надають злочинцям потужний інструмент для збору імен користувачів і паролів, розповсюдження зловмисного програмного забезпечення та інших шкідливих дій.

Оскільки будь-який сканер QR-коду повинен показувати вам URL-адресу перед переходом за посиланням, фішери часто поєднують використання QR-кодів із скороченнями URL-адрес, щоб ще більше приховати справжнє призначення.

Зловмисники можуть навіть вставляти QR-коди в професійно розроблені документи, що імітують HR-портали, оновлення заробітної плати, податкові перевірки або служби електронного підпису (наприклад, DocuSign , Adobe), що підвищує сприйману легітимність фішу [6].

**Black Basta**

Компанія ReliaQuest виявила, що група програм-вимагачів Black Basta проводить масову електронну розсилку спаму та голосового фішингу (вішингу) для розгортання програм-вимагачів. Атака починається, з того, що користувач отримує велику кількість спаму. Зловмисник імітує IT-підтримку, пропонуючи допомогу та інструктуючи користувача завантажити інструмент віддаленого доступу, який надає зловмиснику початковий доступ. Компанія рекомендує організаціям проінформувати користувачів, щоб підвищити обізнаність про цю кампанію, запровадити правила прямого проксі-сервера, щоб блокувати нещодавно зареєстровані домени та налаштувати білий список застосунків лише для затверджених інструментів віддаленого моніторингу та керування (RMM) [7].

***Статистика програм-вимагачів у фінансовій галузі***

Як пише видання HelpNetSecurity, платежі на користь операторів ренсомвер зменшилися, попри збільшення кількості атак, завдяки покращенню кіберстійкості, діям правоохоронних органів і наявності дешифраторів. За даними фірми Chainalysis, що займається аналізом блокчейнів, у 2023 році кількість атак програм-вимагачів, пов'язаних із платежами, зменшилася на 46%. Зусилля правоохоронних органів, такі як збій роботи ботнету Qakbot у 2023 році та проникнення до LockBit у 2024 році, підірвали довіру та порушили діяльність у спільнотах програм-вимагачів. Крім того, афера з виходом групи ALPHV/BlackCat, яка раніше захопила 30% усіх платежів ренсомвер, ще більше дестабілізувала екосистему програмвимагачів. Ця тенденція відображає зростаюче небажання жертв платити викуп і підкреслює важливість постійних скоординованих зусиль між приватним сектором і правоохоронними органами для протидії загрозам програм-вимагачів. Для ефективного захисту від програм-вимагачів команди аналізу загроз повинні знати про найпопулярніші варіанти програм-вимагачів, націлених на фінансові системи [8].

Сучасні 11 найпоширеніших типів програм-вимагачів змушують фінансові установи оновити свої плани реагування на інциденти, щоб усунути кожну з цих активних загроз [1]:

1. Ресурси програм-вимагачів Sodinokibi;

2. Ресурси програм-вимагачів Conti V2;
3. Ресурси програм-вимагачів Lockbit;
4. Ресурси Clop Ransomware;
5. Ресурси програм-вимагачів Egregor;
6. Ресурси програм-вимагачів Avaddon;
7. Ресурси програм-вимагачів Ryuk;
8. Ресурси програм-вимагачів Darkside;
9. Ресурси програм-вимагачів SunCrypt;
10. Ресурси програм-вимагачів Netwalker;
11. Ресурси програми-вимагача Phobos.

CERT-UA попередила про значне зростання кількості кібератак, пов'язаних з діяльністю фінансово мотивованого угруповання UAC-0006. З 20 травня 2024 року фахівці зафіксували дві масштабні кампанії з розповсюдження шкідливого програмного забезпечення SMOKELOADER. Наразі бот-мережа UAC-0006 налічує декілька сотень заражених комп'ютерів. Існує висока ймовірність, що найближчим часом зловмисники активізують шахрайські схеми з використанням систем дистанційного банківського обслуговування [7].

Передбачається продовження атак програм-вимагачів, які базувались на техніках успіху в 2024 році. Тактика просунулася від подвійного вимагання до потрійного вимагання (часто з DDoS-атаками) і навіть до чотириразового вимагання (тобто зловмисники безпосередньо зв'язуються з клієнтами жертви, співробітниками та іншими пов'язаними особами, щоб повідомити їх про те, що їхню конфіденційну інформацію було зламано). Організації, які платять викупи, ймовірно, знову стануть мішенню. Щоб захистити себе, компаніям необхідно покращити свої рішення для резервного копіювання та інтенсифікувати навчання співробітників, щоб зменшити ці ризики [1].

Очікується збільшення атак на пристрої Інтернету речей (IoT), які часто не мають надійного захисту. Зловмисники можуть використовувати багато пристроїв, і ці атаки, як правило, відбуваються швидко після виявлення

вразливостей. Це підкреслює необхідність посилення заходів безпеки та стандартизованих протоколів як на рівні споживача, так і на рівні організації. Дуже важливо постійно оновлювати засоби захисту, а також розуміти свій вплив на Інтернет речей [1].

Особливо цікавою подією став бекдор XZ Utils (CVE-2024-3094), який використовував уразливість у цій широко використовуваній бібліотеці з відкритим кодом. Цей зловмисник грав у довгу гру, роблячи внесок у проєкт XZ протягом майже двох років, щоб завоювати довіру, доки їм не вдалося вставити зловмисне програмне забезпечення у середовище з відкритим кодом . Ця довга гра мала відгомони кампанії Volt Typhoon , яка проникла в DSL-маршрутизатори в Сполучених Штатах з метою порушити зв'язок [1].

Значна кількість зловмисного програмного забезпечення скористалося старими уразливими місцями, як-от Log4Shell , деяким з яких понад десять років, і навіть деяким без належного призначення CVE . Досвідчений актори ботнету можуть розширити свій набір інструментів, включивши в нього зловмисне програмне забезпечення на основі Golang, оскільки його складніше обфускати, а будь-яка особа, яка має доступ до кредитної картки, може запустити повномасштабне програмне забезпечення-вимагач або DDoS-атаку так само легко, як купити пару взуття в Інтернеті [1].

Виявлення вразливостей, що впливають на фінансову галузь

- У березні 2021 року в плагіні WordPress було виявлено вразливість , яка спрощувала сліпі ін'єкції SQL на основі часу. Потенційно це могло вплинути на 600 000 користувачів.
- У квітні 2021 року компанія Trend Micro виявила вразливість XSS, яка впливає на веб-сайти електронної комерції.
- У серпні 2021 року було виявлено вразливість Local File Inclusion (LFI) для версії BIQS – програмного забезпечення, яке використовується в автошколах для виставлення рахунків.
- У серпні 2021 року було виявлено вразливість OGNL, яка дозволяла зловмисникам впроваджувати довільний код на серверах Atlassian Confluence .

- Видалення ін’єкційних атак зі списку було сміливим і суперечливим кроком у спільноті безпеки API, але існує менша загроза ін’єкційних атак на кінцеві точки API.
- Інжекція тепер по суті є частиною API8:2023 | Неправильна конфігурація безпеки . Належна конфігурація безпеки повинна включати механізми захисту веб-додатків і API, які повинні сканувати та запобігати ін’єкціям за замовчуванням.
- GraphQL розвивається як технологія API. За своєю суттю це мова запитів, яка може знову відкрити двері для зростання ін’єкційних атак, тому розробникам API, які покладаються на GraphQL, слід і надалі залишатися пильними [8].

***Статистика DDoS-атак у фінансовій галузі***

У фінансовому секторі у 2024 році кількість DDoS-атак зросла на 30%. Особливо важливою тенденцією 2024 року стало величезне збільшення DDoS-атак рівня 7, націлених на Азіатсько-Тихоокеанський регіон і Японію (APJ). Дослідники Akamai виявили, що кількість DDoS-атак рівня 7 в APJ зросла в п’ять разів із січня 2023 року по червень 2024 року (рис. 1.5). Траєкторія зростання цього типу сильної атаки викликає занепокоєння.

Також примітним був той факт, що сплески DDoS-атак узгоджувалися з часом важливих геополітичних подій. У 2024 році відбулися великі вибори в трьох країнах регіону APJ — Індії, Індонезії та Тайвані — і ми спостерігали зростання DDoS-атак приблизно під час цих подій.

Зростання кількості атак можна пояснити зростанням хактивізму, спрямованого проти країн або галузей промисловості, які, на думку хактивістів, суперечать їхній ідеології та переконанням. Це спостереження підкреслює необхідність для організацій не лише захищатися від кіберзлочинців, які прагнуть отримати прибуток, але й захищатися від хактивістів, які керуються політичними планами та можуть атакувати будь-коли.

Очевидно, DDoS-атаки є серйозною проблемою, але багато організацій в APJ все ще недостатньо підготовлені до них. Це реальні загрози, до яких слід

ставитись серйозно. DDoS-атаки спрямовані не лише на комерційні підприємства, але й на критичні інфраструктури, банківські системи, комунальні служби. Якщо DDoS-атаки будуть успішними, їхній вплив, швидше за все, буде відчутним у нашому повсякденному житті [1].

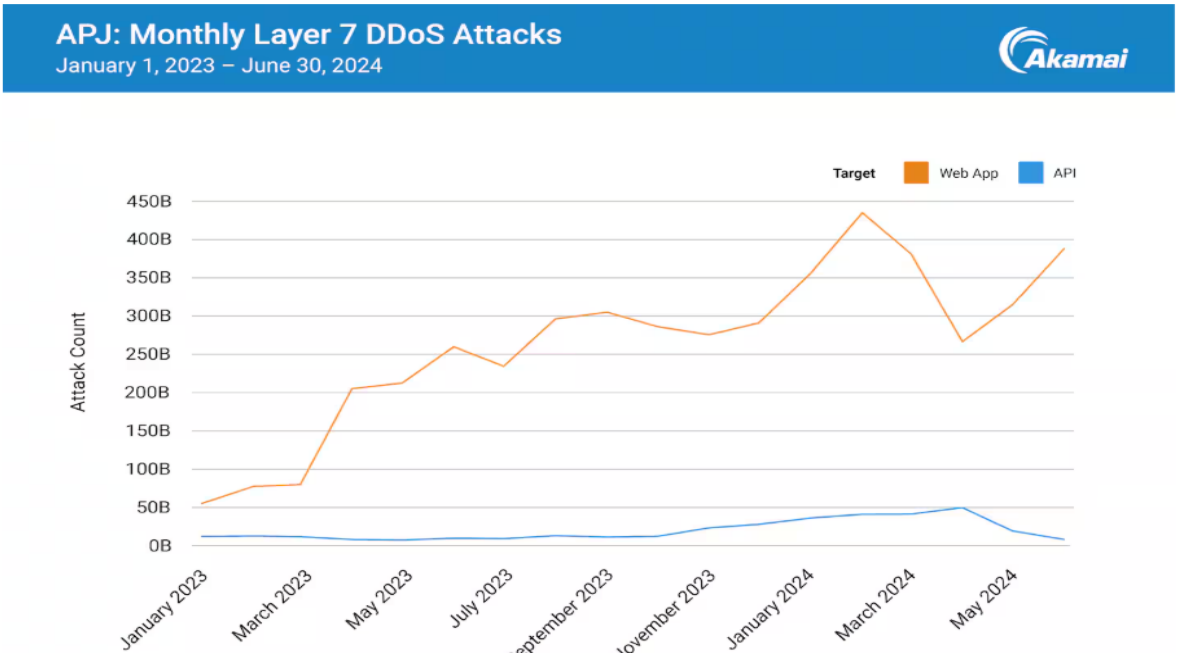


Рис. 1.5: Динаміка DDoS-атак рівня 7 в APJ із січня 2023 року до червня 2024 року [1]

Платіжні процеси не завжди класифікуються як фінансові установи, оскільки це зазвичай приватні компанії або сторонні постачальники, найняті банками для обробки платежів. Але, в очах кіберзлочинців, їх зв'язок із даними приватних банків групує їх до однієї категорії.

У 2023 році двома основними кіберзагрозами платіжним процесам були атаки під час входу через пароль і DoS-атаки.

Багатовекторні DDoS-атаки зросли на 80% у 2024 році порівняно з тим самим періодом 2023 року. Це DDoS-атаки, які складаються з кількох кампаній, щоб перевантажити команди безпеки.

***Статистика атак на ланцюг поставок у фінансовій галузі***

З атак на ланцюги поставок, проаналізованих Агентством Європейського Союзу з кібербезпеки , 66% скомпрометованих постачальників або не знали, або не повідомили про те, що їх зламали. Ця статистика підкреслює

занепокоєння дефіциту кіберстійкості серед постачальників і відчайдушну потребу в програмі управління ризиками постачальника, щоб усунути цей дефіцит.

Відповідно до звіту Агентства кібербезпеки Європейського Союзу (ENISA), 50% спостережуваних атак на ланцюг поставок були пов'язані з такими розширеними постійними загрозами (APT):

- APT29
- APT41
- Талій
- Лазаря
- TA413
- TA428

Очікується, що з 2020 по 2021 рік кількість атак на ланцюги поставок зросте в чотири рази

Агентство Європейського Союзу з кібербезпеки (ENISA ) прогнозує, що у 2025 році кількість атак на ланцюги поставок зросте в 4 рази порівняно з 2024 роком.

***Статистика банківського падіння(bank drops) у фінансовому секторі***

Середній діапазон цін на дані Fullz у Dark Web становить 15–60 доларів США за запис.

Згідно зі звітом Armor Dark Market Report , середні діапазони цін на fullz-дані, які продаються в темній мережі, такі:

- Загальні дані Fullz: $15-$60
- Business Fullz Data: $35-$60

Загальні повні дані можуть включати:

8. Ім'я
9. DOB
10. Адреса
11. Дівоче прізвище матері
12. SSN

13. Номер водійського посвідчення

Повні бізнес-дані можуть включати:

- Номери банківських рахунків
- EIN
- DOB
- SSN
- Бізнес сертифікати
- Імена посадових осіб

Як захиститися від кіберзагроз фінансових послуг

У багатьох випадках кібератаки повторюють ту саму послідовність атак, оскільки різні фінансові організації мають загальні вразливості безпеки .

***Захист даних клієнтів***

Дані клієнтів є основою банківських операцій. Від особистої інформації, як-от номерів соціального страхування та адрес, до конфіденційних фінансових даних, банки зберігають скарбницю даних, які, якщо їх розкриють, можуть призвести до крадіжки особистих даних, шахрайства та значних фінансових втрат для людей.

Кібербезпека відіграє вирішальну роль у захисті цієї інформації від несанкціонованого доступу. Шифрування, брандмауери та безпечний контроль доступу – це лише деякі із заходів, які впроваджують банки, щоб забезпечити захист даних клієнтів. Якщо банк не в змозі захистити ці дані, фінансові втрати, підрив довіри та репутація є серйозними.

***Збереження довіри та репутації клієнтів***

Довіра є основою банківських відносин. Клієнти очікують, що фінансова установа належним чином оброблятиме їх особисту та фінансову інформацію. Будь-яке порушення може порушити цю довіру, що призведе до втрати клієнтів і довгострокової шкоди репутації.

Кібератаки чи викрадання даних можуть швидко потрапити в заголовки газет, і сприйняття банку громадськістю може змінитися миттєво. Суворі заходи кібербезпеки мають вирішальне значення для підтримки довіри та

забезпечення безпеки клієнтів під час проведення транзакцій і обміну конфіденційною інформацією зі своїм банком.

***Відповідність Регламенту***

Банки повинні дотримуватися суворого захисту даних, а стандарти дотримання кібербезпеки у фінансовій галузі суворо регулюються. Такі закони, як Загальний регламент захисту даних (GDPR) у Європі та Каліфорнійський закон про конфіденційність споживачів (CCPA) у США встановлюють суворі вказівки щодо того, як банки мають обробляти та захищати дані клієнтів.

Недотримання цих правил може призвести до великих штрафів, юридичних наслідків і втрати ліцензій на діяльність. Впроваджуючи надійні методи кібербезпеки, банки захищають себе від кіберзагроз і забезпечують відповідність цим критичним нормативним вимогам.

***Запобігання фінансовим втратам***

Успішна кібератака може призвести до значних фінансових втрат для банків. Це може включати крадіжки коштів безпосередньо з рахунків, витрати, пов’язані з простоєм системи, або високу ціну на ремонт пошкоджених систем. Крім того, банки можуть нести відповідальність за компенсацію клієнтам, які постраждали від шахрайства або крадіжки особистих даних через кіберзлом.

Банки можуть мінімізувати фінансові ризики, пов’язані з кіберзлочинністю, інвестуючи в передові рішення з кібербезпеки. Механізми проактивного захисту, такі як моніторинг загроз у реальному часі, багатофакторна автентифікація та виявлення загроз на основі ШІ, можуть запобігти атакам до того, як вони призведуть до дорогих наслідків.

***Захист критичної інфраструктури***

Інфраструктура банківського сектору, включаючи платформи онлайн-банкінгу, банкомати та системи обробки платежів, є основною мішенню для кіберзлочинців. Успішна атака на ці системи може призвести до збоїв у роботі, через що клієнти не зможуть отримати доступ до своїх коштів або здійснювати транзакції.

Кібербезпека допомагає банкам захистити цю критично важливу інфраструктуру, запобігаючи несанкціонованому доступу, виявляючи аномалії та пом’якшуючи потенційні загрози. Постійний моніторинг і тестування безпеки гарантують, що ці основні служби залишаються безпечними та повноцінними, запобігаючи збоям, які можуть завдати шкоди репутації та фінансовій стабільності банку.

***Забезпечення безперервності бізнесу***

Кібератаки можуть спричинити значні збої в роботі банку, що призведе до збою системи, втрати даних і навіть зупинки послуг. Ці перерви можуть бути дорогими з точки зору фінансових втрат і негативного впливу на досвід клієнтів.

Впровадження комплексних заходів кібербезпеки допомагає банкам захиститися від таких збоїв. Наявність надійного плану реагування на інциденти, регулярне резервне копіювання та використання рішень для аварійного відновлення гарантують, що банки зможуть швидко відновитися після атаки та продовжувати безперебійне обслуговування клієнтів.

***5 ЕФЕКТИВНИХ РІШЕНЬ КІБЕРБЕЗПЕКИ ДЛЯ БАНКІВ***

Для боротьби з цими загрозами банки повинні впроваджувати комбінацію технологічних рішень і найкращих практик. Ось п’ять ефективних рішень кібербезпеки для банків:

***1. Багатофакторна автентифікація (MFA)***

MFA додає додатковий рівень безпеки, крім паролів, вимагаючи від користувачів підтверджувати свою особу за допомогою додаткових методів, таких як біометрія або одноразові паролі. Це значно знижує ризик несанкціонованого доступу.

***2. Наскрізне шифрування***

Шифрування даних гарантує, що навіть якщо кіберзлочинці перехоплять конфіденційні дані, вони не зможуть їх прочитати або використовувати. Банки повинні використовувати надійні методи шифрування для даних у стані спокою та передачі.

***3. Виявлення загроз на основі ШІ***

Штучний інтелект (ШІ) може допомогти виявляти загрози та реагувати на них у режимі реального часу, аналізуючи величезні обсяги даних на наявність аномальних моделей. ШІ особливо ефективний у боротьбі з фішинговими та шахрайськими атаками.

***4. Архітектура нульової довіри***

Модель Zero Trust передбачає, що всі користувачі, пристрої та мережі за своєю суттю не заслуговують довіри. Банки можуть запобігти несанкціонованому доступу та витоку даних, вимагаючи перевірки на кожному етапі. Для ефективного впровадження такої моделі надзвичайно важливо мати надійну мережеву архітектуру безпеки, яка гарантує безпеку кожної точки доступу та з'єднання в системі.

***5. Системи управління інцидентами та подіями безпеки (SIEM).***

Системи SIEM збирають і аналізують дані безпеки з багатьох джерел, щоб надавати сповіщення в реальному часі про потенційні загрози. Це забезпечує швидший час реакції та мінімізує шкоду від кібератак.

Щоб глибше зрозуміти, як банки створюють надійні системи безпеки, перегляньте цей посібник із безпеки мережі .

Наведені нижче засоби контролю безпеки можуть усунути більшість ризиків, що сприяють витоку даних у секторі фінансових послуг:

- **Управління ризиками третіх сторін (TPRM)** – Програма керування ризиками третіх сторін визначатиме вразливі місця для всіх сторонніх хмарних служб, щоб запобігти атакам на ланцюг поставок.
- **Багатофакторна автентифікація** . Впровадження політики MFA на всіх кінцевих точках, у тому числі на мобільних пристроях, дуже ускладнить для суб'єктів загрози скомпрометувати привілейовані облікові дані – критичний крок перед крадіжкою конфіденційної інформації для фінансових компаній.

- **Брандмауер** . Регулярно оновлюваний брандмауер здатний виявляти та блокувати спроби впровадження шкідливого програмного забезпечення.
- **Керування поверхнею атак** . Рішення для керування поверхнею атак, здатне виявляти витік даних, значно зменшить шанси успішного злому даних як усередині, так і в мережі постачальника.
- **Вивчення TTP (Tactics, Techniques, & Procedures)** – Зловмисники часто використовують подібні стратегії атак через подібні вразливості в галузі. Вивчення поширених шаблонів підозрілої діяльності може допомогти вам перехопити спробу атаки до того, як буде впроваджено будь-який шкідливий код.
- **Оцінки безпеки** . Ця функція підтримує моніторинг у реальному часі нових ризиків безпеці, створених цифровою трансформацією. У поєднанні з інструментом керування поверхнею атак рейтинги безпеки допомагають виявити найкращі заходи безпеки для багатьох поширених типів атак, включаючи атаки зловмисного програмного забезпечення та компрометацію даних клієнтів.
- **Регулярне резервне копіювання даних** . Маючи під рукою чисту резервну копію системи, ви зможете відновити безперервність роботи під час атаки програм-вимагачів.
- **Стратегія виявлення та реагування на кіберзагрози** – задокументована стратегія керування кіберзагрозами, які, найімовірніше, вплинуть на вашу організацію. Ви можете дізнатися більше про таку програму в нашій публікації про виявлення кіберзагроз і реагування на них.

Можливо, найбільш тривожним є те, що кіберзлочинці зараз використовують штучний інтелект (ШІ) для створення більш складних векторів атак. Інструменти на основі штучного інтелекту дозволили створювати дуже переконливі фішингові кампанії, глибокі фейки та інші новітні тактики. Це впровадження штучного інтелекту призвело до значного збільшення успішних атак. Щоб боротися з цією загрозою, організації повинні культивувати культуру

скептицизму та навчання на всіх рівнях у поєднанні з надійними процесами перевірки конфіденційних запитів.

### *НАЙКРАЩІ ПРАКТИКИ КІБЕРБЕЗПЕКИ В БАНКІВСЬКІЙ СПРАВІ*

Хоча рішення є важливими, впровадження найкращих практик є не менш важливим для забезпечення довгострокової безпеки. Представляємо ключові стратегії:

*Регулярне навчання співробітників*: співробітники часто є першою лінією захисту від кіберзагроз. Важливо регулярно навчати персонал розпізнавати спроби фішингу, повідомляти про підозрілу активність і дотримуватися протоколів безпеки.

*Проведення регулярних аудитів*: звичайні аудити безпеки допомагають банкам виявляти вразливі місця у своїх системах і процесах, дозволяючи їм усунути ці недоліки до того, як ними скористаються зловмисники.

*Оновлення програмного забезпечення*: застаріле програмне забезпечення є одним із найпростіших способів для хакерів проникнути в систему. Банки повинні переконатися, що все програмне забезпечення, особливо патчі безпеки, оновлені, щоб закрити відомі вразливості.

*Запровадження політики надійних паролів*: заохочення надійних унікальних паролів і їх регулярне оновлення допомагає мінімізувати ризик атак грубої сили.

*Розробка плану реагування на інциденти*: банки повинні мати надійний план реагування на інциденти, щоб мінімізувати збитки та швидко відновити послуги у разі кібератаки.

### Висновки до розділу 1

За результатами проведеного аналізу доведено, що основними загрозами кібербезпеки в фінансовій сфері являються фішинг, програми-вимагачі, DDoS-атаки, ін’єкції SQL, включення локальних файлів, міжсайтові сценарії та ін’єкції OGNL Java, атаки на ланцюги поставок, Банк Дропс. Загрози стають більш витонченими та

відповідно до статистичного аналізу провідних компаній, які проводять аналітичні дослідження зростають за кількістю та успішностю, що вимагає від фінансових установ посилювати захист тавпроваджувати новітні технології кібербезпеки.

Основними векторами захисту визначаються: захист даних клієнтів, збереження довіри та репутації клієнтів, відповідність регламенту захисту, запобігання фінансовим втратам, захист критичної інфраструктури банківських установ, забезпечення безперервності бізнесу.

Основними ефективними рішеннями в фінансовій сфері визнано запровадження багатофакторної автентифікації (MFA), наскрізного шифрування, виявлення загроз на основі ШІ, запровадження архітектури нульової довіри, побудова систем управління інцидентами та подіями безпеки (SIEM). Найкращими практиками кібербезпеки в фінансовій сфері вважаємо: регулярне навчання співробітників, проведення регулярних аудитів, оновлення програмного забезпечення, запровадження політики надійних паролів, розробка плану реагування на інциденти.

# РОЗДІЛ 2 ЗАСОБИ ТА МЕТОДИ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

## 2.1. Засоби виявлення та запобігання кіберзагроз

Основними засобами, що спрямовані запобіганню кіберзагроз, які покращують безпеку та зміцнюють критичну інфраструктуру в банківському та фінансовому секторах являються компоненти технічних, правових, регулятивних та організаційних заходів. Ключовими визначено технічні заходи: сегментація мережі, шифрування, системи виявлення вторгнень та виправлення вразливостей. Нетехнічні заходи, які складаються з організаційних, правових та регуляторних заходів, таких як навчання співробітників, планування реагування на інциденти, обмін розвідувальною інформацією про загрози та дотримання нормативних вимог. Організаційні заходи спрямовані на забезпечення розуміння різноманітних стратегій, які можна використовувати для зменшення кіберризиків. На рисунку 3.1 показано контрзаходи проти кіберзагроз.

**Технічні заходи**

Технічні контрзаходи – це інструменти та методи, призначені для захисту систем і даних від кіберзагроз. Вони є важливими для захисту цілісності інформаційних систем, мереж і даних від несанкціонованого доступу та кібератак. Їх можна класифікувати за кількома вимірами залежно від їхніх основних функцій та варіантів використання. У таблиці 2.1. наведено технічні засоби контролю.

У таблиці 2.2. наведено рейтинг технічних засобів контролю для банківських та фінансових послуг на основі їх ефективності та важливості. Шифрування вважається найефективнішим та найважливішим технічним засобом контролю для банківських та фінансових послуг, оскільки воно допомагає захистити конфіденційні дані та запобігти несанкціонованому доступу.

Багатофакторна автентифікація (MFA) та сегментація мережі також дуже ефективні у запобіганні несанкціонованому доступу до систем та даних.

| ЗАХОДИ ПРОТИ КІБЕРЗАГРОЗ | | |
|---|---|---|
| **Технічні контрзаходи** | **Правові та регуляторні контрзаходи** | **Організаційні контрзаходи** |
| Шифрування | Правила захисту даних | Планування реагування на інциденти |
| Багатофакторна автентифікація (MFA) | Нормативні акти фінансової галузі | Управління ризиками та оцінка |
| Сегментація мережі | Стандарти кібербезпеки | Політика та процедури безпеки. |
| Брандмауер та системи запобігання вторгненням (IPS) | Закони про кібербезпеку | Регулярні аудити та тестування на проникнення |
| Звичайне оновлення безпеки | Обов'язкові повідомлення про порушення | Управління ризиками третіх сторін |
| Безпека кінцевих точок | Вимоги до кіберстрахування | Навчання з підвищення обізнаності щодо безпеки |
| Управління безпекою інформації та подіями (SIEM) | Міжнародне співробітництво | Призначення головного спеціаліста з інформаційної безпеки (CISO) |
| Інструменти запобігання втраті даних (DLP) | | Створення Центру операцій безпеки (SOC) |
| Зашифрований зв'язок | | Перевірки біографічних даних співробітників |
| Виявлення аномалій | | Обмін інформацією про загрози |
| Технології обману | | Управління ризиками постачальників |
| | | Планування забезпечення безперервності бізнесу та аварійного відновлення (BCDR) |
| | | Фізична безпека |

Рис. 2.1. Заходи проти кіберзагроз (складено на основі [18])

Брандмауери та системи запобігання вторгненням (IPS), регулярне оновлення систем безпеки, безпека кінцевих точок та управління інформацією та подіями безпеки (SIEM) також є важливими технічними засобами контролю для банківських та фінансових послуг. Інструменти запобігання втратам даних (DLP), зашифрований зв'язок, технології виявлення аномалій та обману також є важливими технічними засобами контролю, які можуть допомогти запобігти та виявити кібератак. Загалом, ефективність та важливість цих технічних засобів контролю може відрізнятися залежно від конкретних потреб та ризиків кожної

організації. Тому для банківських та фінансових послуг важливо оцінити свої ризики кібербезпеки та впровадити комплексну стратегію кібербезпеки, яка включає поєднання технічних засобів контролю, політик та процедур для зменшення ризиків.

Таблиця 2.1.

**Технічні засоби контролю**

| **Засіб контролю** | **Опис засобу** | **Приклад технічного захисту** |
|---|---|---|
| Аутентифікація та контроль доступу | Технології, які перевіряють користувачів та контролюють доступ до системи та даних | Багатофакторна автентифікація Зашифрований зв'язок |
| Безпека мережі. | Контрзаходи в зосереджені на захисті цілісності та функціональності мережі | Сегментація мережі Брандмауер та системи запобігання вторгненням (IPS) |
| Захист даних | Контрзаходи, які в першу чергу зосереджені на захисті даних від несанкціонованого доступу або втрати. | Шифрування<br>Регулярне оновлення безпеки<br>Інструменти запобігання втраті даних (DLP) |
| Захист кінцевих точок | Забезпеченні безпеки кінцевих точок у мережі для запобігання несанкціонованому доступу та захисту від загроз. | Безпека кінцевих точок |
| Моніторинг безпеки та реагування. | Контрзаходи допомагають виявляти, аналізувати та реагувати на події та інциденти безпеки. | Інформація про безпеку та управління подіями (SIEM)<br>Виявлення аномалій Технології обману |

Таблиця 2.2.

**Рейтинг технічних засобів контролю для банківських та фінансових послуг**

| Технічні засоби | Опис засобу |
|---|---|
| Шифрування | Банки використовують шифрування для захисту конфіденційних даних як під час передачі, так і в стані зберігання. Шифрування гарантує, що доступ до даних та їх читання можуть отримати лише уповноважені особи, запобігаючи несанкціонованому доступу та порушенням даних. |
| Багатофакторна автентифікація (MFA) | MFA вимагає від користувачів надання кількох форм ідентифікації перед доступом до конфіденційних систем або даних. Це може включати паролі, біометричні дані або апаратні токени, що ускладнює для зловмисників отримання несанкціонованого доступу за допомогою викрадених облікових даних. |
| Сегментація мережі | Сегментація мережі передбачає розділення різних частин мережі для обмеження несанкціонованого доступу та потенційного поширення атаки. |
| Брандмауер та системи запобігання вторгненням (IPS) | Брандмауери та IPS захищають внутрішню мережу банків від несанкціонованого доступу та спроб вторгнення. Вони контролюють вхідний та вихідний мережевий трафік, блокуючи шкідливу активність та запобігаючи несанкціонованому доступу до конфіденційних даних. |
| Регулярне оновлення безпеки | Банки повинні підтримувати свої системи та програмне забезпечення в актуальному стані, регулярно застосовуючи оновлення та патчі безпеки. Це допомагає закрити відомі вразливості, які можуть використовувати зловмисники. |
| Безпека кінцевих точок | Впровадження рішень безпеки кінцевих точок, таких як антивірусне та антивірусне програмне забезпечення, допомагає захистити окремі пристрої від таких загроз, як шкідливе програмне забезпечення, програми-вимагачі та цілеспрямовані атаки |
| Інформація про безпеку та управління подіями (SIEM) | Системи SIEM збирають, аналізують та співвідносять дані з різних джерел для виявлення та реагування на потенційні інциденти безпеки. Вони забезпечують моніторинг та сповіщення в режимі реального часу, що дозволяє банкам швидко реагувати на кіберзагрози. |
| Інструменти запобігання втраті даних (DLP) | Інструменти DLP контролюють та запобігають несанкціонованій передачі конфіденційних даних як всередині, так і за межі організації. |
| Зашифрований зв'язок | Використання зашифрованих каналів зв'язку, таких як Secure Sockets Layer (SSL) або Transport Layer Security (TLS), захищає конфіденційні дані під час передачі та запобігає несанкціонованому доступу або перехопленню. |
| Виявлення аномалій | Впровадження систем виявлення аномалій на основі машинного навчання допомагає виявити незвичайні закономірності в мережевому трафіку, поведінці користувачів або транзакціях, які можуть свідчити про потенційні загрози. |
| Технології обману | Технології обману створюють системи-приманки, такі як honeypots, які заманюють зловмисників і дозволяють організаціям вивчати їх тактику, методи та процедури (TTP) без ризику для реальних систем або даних. |

**Правові та регуляторні заходи**

Правові та регуляторні заходи відіграють важливу роль у формуванні ландшафту кібербезпеки. Вони розроблені для забезпечення дотримання встановлених правил, інструкцій та стандартів, що регулюють захист даних, конфіденційність та кібербезпеку в банківському та фінансовому секторах. Ці заходи можна розділити на кілька вимірів, як показано в таблиці 2.3, кожен з яких зосереджений на певному аспекті правових та регуляторних заходів контролю кібербезпеки.

Таблиця 2.3.

**Правові та регулятивні засоби контролю**

| **Засіб контролю** | **Опис засобу** | **Приклад технічного захисту** |
|---|---|---|
| Захисту даних | Заходи, спрямовані на захист персональних та конфіденційних даних. | Правила захисту даних |
| Регулювання фінансової галузі | Нормативні акти, спеціально розроблені для фінансового сектору. | Регулювання фінансової галузі. |
| Рамкові положення та найкращі практики | Заходи, що забезпечують структуровані підходи та рекомендації щодо кібербезпеки. | Рамкові положення кібербезпеки |
| Правові санкції та зобов'язання | Закони та вимоги, що накладають юридичні зобов'язання на суб'єкти господарювання щодо підтримки певного рівня кібербезпеки | Закони про кібербезпеку<br>Обов'язкові повідомлення про порушення<br>Вимоги до кіберстрахування |
| Міжнародна співпраця | Заходи, що передбачають співпрацю та узгодження між різними країнами або міжнародними організаціями. | Міжнародна співпраця |

У таблиці 2.4 наведено рейтинг правових та регуляторних заходів для банківських та фінансових послуг на основі їхньої ефективності та важливості. Правила захисту даних та правила фінансової галузі вважаються найефективнішими та найважливішими правовими та регуляторними заходами для банківських та фінансових послуг, оскільки вони забезпечують чіткі рекомендації та стандарти кібербезпеки. Структури та закони про кібербезпеку також є важливими правовими та регуляторними заходами, які можуть допомогти встановити стандарти та вимоги кібербезпеки для галузі. Правила

захисту даних та обов'язкові повідомлення про порушення також є важливими правовими та регуляторними заходами, які можуть допомогти захистити конфіденційні дані та забезпечити своєчасне повідомлення про інциденти кібербезпеки. Вимоги щодо кіберстрахування та міжнародна співпраця також є важливими правовими та регуляторними заходами, які можуть допомогти пом'якшити фінансові та репутаційні ризики, пов'язані з інцидентами кібербезпеки.

Таблиця 2.4.

**Правові та регуляторні засоби**

| **Правові та регуляторні засоби** | **Опис** |
|---|---|
| Правила захисту даних | Банки повинні дотримуватися правил захисту даних, таких як Загальний регламент захисту даних (GDPR) у ЄС, Закон про конфіденційність споживачів Каліфорнії (CCPA) у США та аналогічні закони в інших юрисдикціях. Ці правила встановлюють суворі вимоги щодо того, як банки збирають, обробляють та зберігають персональні дані, гарантуючи захист конфіденційної інформації від несанкціонованого доступу та неправильного використання. |
| Нормативні акти фінансової галузі | Банки також повинні дотримуватися специфічних для фінансової галузі норм, таких як Стандарт безпеки даних індустрії платіжних карток (PCI-DSS), який встановлює стандарти безпеки для обробки даних власників карток, та Закон про банківську таємницю (BSA), який вимагає від банків повідомляти про підозрілу діяльність правоохоронним органам. |
| Стандарти кібербезпеки | Різні стандарти кібербезпеки, такі як стандарти кібербезпеки NIST та стандарт ISO/IEC 27001, надають банкам рекомендації та найкращі практики щодо впровадження надійних заходів кібербезпеки. |
| Закони про кібербезпеку | Національні та міжнародні закони про кібербезпеку накладають штрафи та санкції на банки, які не впроваджують належних заходів безпеки або своєчасно не повідомляють про інциденти безпеки. |
| Обов'язкові повідомлення про порушення | Закони багатьох юрисдикцій вимагають від банків повідомляти клієнтів та органи влади у разі порушення безпеки даних, забезпечуючи прозорість та заохочуючи проактивні заходи кібербезпеки. |
| Вимоги до кіберстрахування | Регулятори можуть вимагати від банків мати поліси кіберстрахування, які допомагають покривати фінансові втрати, спричинені кібератаками, та можуть стимулювати організації підтримувати надійні методи безпеки. |
| Міжнародне співробітництво | Уряди та фінансові регулятори повинні співпрацювати в глобальному масштабі для обміну інформацією про загрози, передовим досвідом та правовими рамками для ефективної боротьби з кіберзагрозами |

Загалом, ефективність та важливість цих правових та регуляторних заходів може відрізнятися залежно від конкретних потреб та ризиків кожної організації. Тому для банківських та фінансових послуг важливо дотримуватися

відповідних правил та стандартів, а також впроваджувати комплексну стратегію кібербезпеки, яка включає поєднання правових та регуляторних заходів, технічних заходів контролю, політик та процедур для пом'якшення ризиків.

**Організаційні контрзаходи**

Організаційні контрзаходи зосереджені на формуванні культури безпеки у фінансовій установі. Це включає регулярні програми навчання та підвищення обізнаності співробітників, чітке інформування про політику безпеки та зобов'язання вищого керівництва надавати пріоритет кібербезпеці. Крім того, впровадження планів реагування на інциденти, управління безперервністю бізнесу та проведення регулярних оцінок ризиків мають вирішальне значення для ефективного реагування на потенційні кіберзагрози та їх пом'якшення. Організаційні контрзаходи можна розділити на чотири виміри на основі спільних тем та цілей кожного контрзаходу, що перетинаються, як показано в таблиці 2.5.

Таблиця 2.5.

**Організаційні контрзасоби**

| Контрзасіб | Опис | Приклад технічного захисту |
|---|---|---|
| Управління ризиками та інцидентами | Проактивному плануванні та своєчасному реагуванні на потенційні інциденти безпеки, одночасно керуючи ризиками та пом'якшуючи їх керівництво та регулярне тестування для забезпечення відповідності вимогам та стану кібербезпеки. | Планування реагування на інциденти Управління ризиками та оцінка Управління ризиками третіх сторін Управління ризиками постачальників Створення Центру операцій безпеки (SOC) Спеціаліст з безпеки (CISO) Регулярні аудити та тестування на проникнення |
| Навчання з питань безпеки та підвищення обізнаності | Навчання працівників компетенціям для боротьби з кіберзагрозами та підкреслює важливість заходів щодо забезпечення безпеки персоналу та обміну інформацією про загрози. | Це інтегрує навчання з підвищення обізнаності щодо безпеки. Перевірки біографічних даних працівників Обмін інформацією про загрози |
| Безперервність бізнесу та фізична безпека. | Забезпечення операційної стійкості в умовах інцидентів безпеки та захисті фізичних активів. | Планування забезпечення безперервності бізнесу та відновлення після аварій (BCDR) Фізична безпека |

У таблиці 2.6 наведено рейтинг організаційних контрзаходів на основі їхньої ефективності та важливості.

Таблиця 2.6.

## Рейтинг організаційних контрзаходів

| Організаційні контрзаходи | Опис |
|---|---|
| Планування реагування на інциденти | Наявність чітко визначеного плану реагування на інциденти дозволяє банкам швидко та ефективно керувати та пом'якшувати наслідки кібератаки. |
| Управління ризиками та оцінка | Банки повинні проводити регулярні оцінки ризиків, щоб виявити потенційні вразливості та слабкі місця у своїх системах і процесах, відповідно визначаючи пріоритети та реагуючи на ризики. |
| Політика та процедури безпеки. | Впровадження чіткої та комплексної політики та процедур безпеки гарантує, що всі співробітники знають про свої обов'язки щодо кібербезпеки та знають, як реагувати на потенційні загрози. |
| Регулярні аудити та тестування на проникнення | Банки повинні регулярно проводити внутрішні та зовнішні аудити безпеки та тести на проникнення, щоб виявити вразливості у своїх системах та забезпечити ефективність заходів безпеки. |
| Управління ризиками третіх сторін | Банки повинні оцінювати стан безпеки сторонніх постачальників та партнерів, забезпечуючи дотримання ними тих самих стандартів безпеки для запобігання потенційним атакам на ланцюг поставок. |
| Навчання з підвищення обізнаності щодо безпеки | Забезпечення постійного навчання співробітників з питань безпеки допомагає їм розуміти ризики, свої ролі та обов'язки у підтримці кібербезпеки, розпізнавати потенційні загрози та дотримуватися найкращих практик. |
| Призначення головного спеціаліста з інформаційної безпеки (CISO) | Призначення спеціального CISO гарантує наявність старшого керівника, відповідального за нагляд за стратегією та впровадженням кібербезпеки. |
| Створення Центру операцій безпеки (SOC) | SOC – це централізований підрозділ, відповідальний за моніторинг, виявлення та реагування на інциденти безпеки. Спеціальний SOC може значно покращити здатність організації керувати кіберзагрозами та реагувати на них. |
| Перевірки біографічних даних співробітників | Проведення ретельних перевірок біографічних даних співробітників, особливо тих, хто має доступ до конфіденційних даних або критично важливих систем, може допомогти зменшити ризик внутрішніх загроз. |
| Обмін інформацією про загрози | Банки повинні брати участь у галузевих ініціативах щодо обміну інформацією про загрози, таких як Центр обміну та аналізу інформації про фінансові послуги (FS-ISAC), щоб бути в курсі останніх загроз та вразливостей, що впливають на сектор. |
| Управління ризиками постачальників | Банки повинні впроваджувати комплексну програму управління ризиками постачальників, яка оцінює стан безпеки сторонніх постачальників та постійно контролює їх дотримання вимог безпеки |
| Планування забезпечення безперервності бізнесу та аварійного відновлення (BCDR) | Розробка та підтримка планів BCDR гарантує, що банки можуть швидко відновитися після кіберінциденту, мінімізуючи час простою та фінансові втрати. |
| Фізична безпека | Банки також повинні враховувати заходи фізичної безпеки, такі як системи контролю доступу та камери спостереження, щоб запобігати несанкціонованому доступу до своїх об'єктів та крадіжці або втручанню в критично важливу інфраструктуру |

Планування реагування на інциденти вважається найефективнішим та найважливішим організаційним контрзаходом для банківських та фінансових послуг, оскільки воно допомагає забезпечити своєчасне та ефективне реагування на інциденти кібербезпеки. Управління та оцінка ризиків, політики та процедури безпеки, регулярні аудити та тестування на проникнення, а також управління ризиками третіх сторін також є важливими організаційними контрзаходами, які можуть допомогти виявити та пом'якшити ризики кібербезпеки. Навчання з питань безпеки, призначення головного директора з інформаційної безпеки (CISO), створення Центру операцій безпеки (SOC), перевірка біографічних даних співробітників, обмін інформацією про загрози, управління ризиками постачальників, планування забезпечення безперервності бізнесу та відновлення після аварій (BCDR), а також фізична безпека також є важливими організаційними контрзаходами, які можуть допомогти запобігти кібератакам та виявити їх. Загалом, ефективність та важливість цих організаційних контрзаходів може відрізнятися залежно від конкретних потреб та ризиків кожної організації. Тому для банківських та фінансових послуг важливо впроваджувати комплексну стратегію кібербезпеки, яка включає поєднання організаційних контрзаходів, технічних заходів контролю, політик та процедур для пом'якшення ризиків.

## 2.2. Методи штучного інтелекту для виявлення кіберзагроз

Одним із найперспективніших напрямків є дослідження вторгнень зі застосування методів штучного інтелекту (ШІ). Найцінніша характеристика системи ШІ – це здатність автоматично навчатися відповідно до введених даних. Виявлена характеристика може додати більше гнучкості системі виявлення вторгнення, оскільки має доступ до постійного оновлення бази даних можливих атак. Маються на увазі не тільки системи вторгнення (IDS), а й інтелектуальна система вторгнень (IIDS), яка здатна створювати атакуючі

блоки, вивчаючи нові атаки на основі базового досвіду [19].

Більшість систем виявлення вторгнень (IDS) здійснюють моніторинг системи шляхом перегляду для специфічних “сигнатур” поведінки. Однак, використовуючи сучасні методи, майже неможливо розробити достатньо повні бази даних, щоб попередити всі атаки.

**Методи штучного інтелекту**

1. Підхід нейронних мереж.

Правильно спроєктовані та реалізувані нейронні мережі мають потенціал для вирішення багатьох проблем з виявлення вторгнень. В оснві полягають процеси вивчення типових характеристик користувачів системи (нормальну та анормальну повідінку) та визначення статистично значущих відхилень від їхньої встановленої поведінки.

*Контрольована модель навчання*

Ліппман і Каннінгем [12] запропонували модель-систему, яка шукала в мережевому трафіку ключові слова, специфічні для атаки. Мульти-рівень perceptron використовувався для виявлення атак на хост UNIX та атак для отримання root-привілей на сервері. Система намагалася виявити наявність атаки за допомогою класифікації входів на два виходи: нормальний та атакуючий. Системі вдалося виявити 80% атак. Головним досягненням цієї системи була її здатність також виявляти старі та нові атаки, не включені в навчальні дані.

*Неконтрольована модель навчання*

Л. Жирарден виконав кластеризацію мережевого трафіку, щоб виявляти атаки. Для асоціації атаки було обрано візуальний підхід [13]. Були використані самоорганізуючі карти (SOM). Проєктував мережеві події у відповідному 2D-простір для візуалізації, потім адміністратор мережі аналізував їх. Втручання були вилучені з огляду шляхом виділення відхилень від норми з візуальними метафорами мережевого трафіку. Основний недолік цього підходу є його необхідність інтерпретації мережевого трафіку адміністратором або іншою уповноваженою особою виявляти атаки.

*Гібридні мережі*

Кілька дослідників об'єднали Multi -Layer Perceptron (MLP) і Self – Організація Map (SOM) у своїй спробі створити систему виявлення вторгнень. Досліджували застосування MLPмодель і SOM для виявлення неправильного використання. Мережі вдалося виявити атаки, для яких її було навчено.

Bivens вважає, що мережевий трафік можна ефективно моделювати за допомогою штучної нейронної системи мережі, тому MLP було обрано для вивчення даних мережевого трафіку. Ця система залишається системою виявлення на основі хоста, оскільки вона розглядає дії користувача.

*Підхід на основі правил*

Агарвал [14] запропонували двоетапну структуру від загального до конкретного для вивчення правил. Заснована модель для вивчення моделей класифікаторів на наборі даних, який має дуже різні класи розподіли в навчальних даних. Система класифікувала атаки на 4 основні групи:

Зондування – збір інформації;

Відмова в обслуговуванні (DOS) – заперечувати законні запити до системи;

User-to-Root (U2R) – несанкціонований доступ до локальних користувачів або root,

Remote-to-Local (R2L) – несанкціонований локальний доступ з віддаленого пристрою.

Система виявила зондування та виявлення атак DOS дуже добре73,2% і 96,6% відповідно. Було виявлено 6,6% атак U2R і 10,7% R2L. Помилкові тривоги були створені на рівні менше 10% для всіх категорії атак, за винятком U2R – для цього було повідомлено про неприйнятно високий рівень 89,5% помилкової тривоги категорії.

*Підхід на основі дерева рішень*

Левін створює набір локально оптимальних дерев рішень, з яких оптимальні підмножини дерев вибирається для прогнозування нових випадків [20]. 10% даних від навчання та тестування використовується база даних KDD Cups. Дані випадково відбираються з всього набір навчальних даних.

Багатокласовий підхід виявлення використовується для виявлення різних атак категорій в наборі даних KDD. Так само, як Агарвал і Джоші [14] Левін намагається класифікувати дані на чотири основні категорії: зондування, DOS, U2R та R2L.Остаточні дерева дають дуже високі показники виявлення для всіх класів, включаючи R2L увесь набір навчальних даних. Зокрема, 84,5% виявлення для зондування, 97,5% для DOS,11,8% для U2R і 7,32% для R2L. Помилкові тривоги автор не обговорює.

**Висновки до розділу 2**

Отже, доведено що фінансові та банківські установи мають бути надійно захищені завдяки застосували багаторівневому підходу до кібербезпеки, поєднуючи технічні засоби контролю, правові та регуляторні заходи, а також організаційні контрзаходи, що дозволить ефективно реагувати на загрози, також сприяти формуванню культури безпеки, підвищуючи їхню готовність до боротьби з кіберінцидентами та відновлення після них. Співпраця між різними зацікавленими сторонами, постійна пильність, навчання співробітників та стратегічне управління ризиками мають вирішальне значення для підтримки безпечного операційного середовища для банківського та фінансового сектору.

Доведено необхідність створення комплексної основи для керування створенням та застосуванням ефективних захисних стратегій у банківському та фінансовому секторах. Визначені контрзаходи пропонують організаціям засоби для посилення їхньої безпеки, проактивного виявлення та реагування на загрози, а також мінімізації збитків, що виникають внаслідок кібератак.

Фахівці з кібербезпеки докладають зусиль для використання штучного інтелекту в області виявлення вторгнень, щоб створити системи, здатні до виявлення невідомих атак і вивчення нових сигнатур атак самостійно. В основі вирішення проблеми форматування набору даних і техніки оптимізації полягає бібліотека атак, яка має бути використана за допомогою нейронних мереж, оскільки вони здатні навчатися. Навчені нейронні мережі можуть приймати рішення швидко,

що дає можливість використовувати їх для виявлення кіберзагроз в реальному часі.

# РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ ЗАСОБІВ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ ДЛЯ БАНКІВСЬКИХ І ФІНАНСОВИХ УСТАНОВ (ЗЛОМИ, ФІШИНГ, ШАХРАЙСТВО)

## 3.1. Рекомендації щодо засобів виявлення та попередження вторгнень для банківських і фінансових установ

Регулятор платіжних систем (PSR) наголошує, що шахрайство з платіжними системами (APP) становило 40% усіх збитків від шахрайства у 2022 році. Крім того, PSR встановив нові вимоги для банків та платіжних компаній, які мають набути чинності з 2024 року. Згідно з новими правилами, фінансові установи будуть зобов'язані компенсувати жертві втрачені кошти у співвідношенні 50/50 [22].

Це є частиною зусиль PSR, спрямованих на забезпечення достатніх заходів захисту клієнтів. З набранням чинності нових вимог фінансові установи стикаються з нагальною потребою покращити свій захист від шахрайства та забезпечити безпеку своїх клієнтів.

Існує багато хороших варіантів, деякі з яких розроблені для великих підприємств та банків, а інші підтримують різноманітні типи бізнесу, від електронної комерції до онлайн-платежів та платіжних шлюзів.

*Як вибрати програмне забезпечення для виявлення шахрайства*

Ключові орієнтири щодо вибору програмного забезпечення для виявлення шахрайства.

Вимоги бізнесу

Перш ніж вибирати програмне рішення для виявлення шахрайства, важливо уважно вивчити потреби бізнесу чи організації. Чітке визначення конкретних потреб бізнесу є вирішальним кроком для того, щоб знайти правильне рішення серед багатьох доступних варіантів. Кожен бізнес стикається з різними проблемами шахрайства, тому універсальне рішення може не підійти всім.

*Вартість*

В разі розуміння що потрібно, не витрачається забагато на функції програмного забезпечення, які не потрібні, через ризики шахрайства, з якими стикається бізнес. Важливо враховувати довгострокові потреби бізнесу: спроба заощадити гроші спочатку може створити каскад проблем у майбутньому.

Моделі ціноутворення передбачають багато різних варіантів серед постачальників: фіксовані плани підписки, за транзакцію, а також гнучкі плани ціноутворення залежно від розміру бізнесу та галузі, річного обсягу продажів.

*Функціональність та особливості*

Моніторинг транзакцій у режимі реального часу: моніторинг транзакцій у режимі реального часу має вирішальне значення для виявлення шахрайських моделей та аномалій у даних транзакцій, що передбачає використання передових аналітичних інструментів та алгоритмів. Це дозволяє фінансовим установам виявляти шахрайство та афери в режимі реального часу та до того, як будь-які гроші залишать рахунок жертви.

Співвідношення хибнопозитивних та істинно позитивних сповіщень, засновані на актуальних інструментах, забезпечують оптимальний рівень схвалення.

Поведінкова та транзакційна аналітика: пріоритетність рішень для виявлення шахрайства за допомогою поведінкової аналітики для виявлення незвичайної поведінки для розслідування.

Можливості штучного інтелекту/машинного навчання та рівень автоматизації: ШІ може підвищити операційну ефективність та зменшити кількість хибнопозитивних результатів. Крім того, він пропонує адаптивні можливості для виявлення типологій шахрайства, що розвиваються, та боротьби з шахрайством у більших масштабах.

Досвід користувача: зручний інтерфейс підвищує зручність використання, підвищує ефективність, сприяє адаптивності та полегшує співпрацю між різними відділами.

Підтримка клієнтів: Передбачає переманетний зв'язок з постачальником

програмного забезпечення, якщо виникнуть труднощі або необхідніть поставити додаткові запитання. Постачальник повинен мати змогу пояснити, яку технічну підтримку можна очікувати, який середній час відповіді та інші відповідні умови.

Можливості інтеграції: Одним із найважливіших моментів, які слід враховувати, є середній час інтеграції та її простота. Один із варіантів – провести дослідження, переглянувши розділи обговорень на таких веб-сайтах, як Gartner Peer Insights, Capterra, G2crowd та FinancesOnline. Актуальним є моніторинг відгуків, щоб зрозуміти площину помилок та проблеми.

Масштабованість: Клієнти цінують швидку реакцію на випадки шахрайства. Необхідний інструмент, який здатний обробляти великі обсяги транзакцій та складні сценарії для компаній, що працюють по всьому світу, або з заможними особами, і який може швидко масштабуватися без шкоди для точності.

Відповідність стандартам безпеки: обране рішення для виявлення шахрайства має відповідати вимогам безпеки організації, які відрізнятимуться залежно від сектору бізнесу.


Рис. 3.1. Програмні рішення для виявлення шахрайства

**Програмні рішення для виявлення шахрайства** (рис.3.1) [22]

1. Salv Bridge – платформа для співпраці, збільшення повернення коштів до 80%
2. Ризик шахрайства споживачів Mastercard – виявлення шахрайства в режимі реального часу для банків

3. Виявлення схем шахрайства та аномалій EBA CLEARING (FPAD)
4. Swift GPI – Сервіс оплати за зупинку та відкликання
5. Cifas – провідна служба запобігання шахрайству у Великій Британії
6. Feedzai – моніторинг транзакцій у режимі реального часу та запобігання шахрайству
7. Verafin – рішення корпоративного рівня для боротьби з фінансовими злочинами
8. ComplyAdvantage – виявлення ризиків шахрайства та боротьби з відмиванням коштів за допомогою штучного інтелекту
9. Стійкий штучний інтелект – виявлення шахрайства для банків та фінтех-компаній
10. HAWK: AI – виявлення шахрайства на основі штучного інтелекту
11. Unit21 – моніторинг транзакцій у режимі реального часу
12. SEON – виявлення шахрайства за допомогою штучного інтелекту
13. Sift – програмне забезпечення для виявлення шахрайства

**Salv Bridge**

Salv Bridge – це платформа для співпраці, яка, серед різних застосувань, продемонструвала ефективність у виявленні шахрайства в режимі реального часу. В рамках платформи команди з боротьби з фінансовими злочинами з різних установ отримують доступ до ефективних банківських попереджень, що дозволяє їм об’єднати зусилля та працювати як єдина команда. Великі банківські групи, фінтех-компанії та VASP повідомляють про збільшення успішності повернення коштів до 80% .

Найновіші функції включають Бібліотеку спільних сценаріїв — кураторську, анонімізовану базу даних перевірених сценаріїв моніторингу та правил. Це рішення виходить за рамки виявлення шахрайства, усуваючи розрив між запобіганням на основі ризиків та відкликанням продукції у разі підтвердженого шахрайства.

Ось деякі ключові особливості Salv Bridge:

- Дозволяє повернути кошти на основі високого рівня підозри та до повідомлення жертви.

- Зменшує тривалу затримку, спричинену очікуванням підтвердження (тобто повідомлення про жертву), що зазвичай робить кошти непідйомними.
- Співпраця, що забезпечується Salv Bridge, підвищує ефективність контролю платежів у режимі реального часу.
- Підкріплено вдосконаленим шифруванням, яке гарантує, що ні Salv, ні будь-яка третя сторона не зможе отримати доступ до конфіденційної інформації, що передається на платформі.

**Ризик шахрайства споживачів MASTERCARD**

Система захисту від шахрайства споживачів Mastercard – це рішення для запобігання шахрайству, яке використовується лише банками.

Mastercard використовує штучний інтелект та дані про платежі в режимі реального часу для виявлення шахрайства, перш ніж гроші залишать рахунок клієнта. Таким чином, банки можуть виявляти підозрілі транзакції в режимі реального часу, купуючи собі можливість вимагати додаткової перевірки. Рішення було створено саме для боротьби з шахрайством у додатках, коли шахрай видає себе за друга, члена родини або компанію та обманом змушує особу здійснити переказ від її імені.

**Виявлення схем шахрайства та аномалій EBA CLEARING (FPAD)**

EBA CLEARING – це загальноєвропейський постачальник платіжної інфраструктури, який у вересні 2023 року запустив пілотний проект з виявлення шахрайства (FPAD) з дев'ятьма банками у шести країнах.

FPAD охоплює широкий спектр інструментів запобігання та виявлення шахрайства в режимі реального часу, включаючи перевірку IBAN/імені, пропонуючи аналітичне уявлення з точки зору централізованої інфраструктури. Аналітичний пілотний проект має на меті розробити моделі для виявлення схем шахрайства у співпраці з користувачами, підвищуючи адаптивність системи до загроз, що змінюються. FPAD має на меті забезпечити комплексні можливості розслідування після транзакцій, а також функції оцінки ризиків транзакцій та рахунків.

**SWIFT GPI - сервіс оплати за зупинку та відкликання**

Swift GPI , що розшифровується як Global Payments Innovation (Глобальні інновації в платежах), – це ініціатива, розроблена спеціально для транскордонних платежів.

Swift GPI – сервіс “Зупинка та відкликання платежів” – це рішення для запобігання шахрайству, призначене для банків та фінансових установ, яке дозволяє їм ініціювати, здійснювати та реагувати на відкликання платежів, а також перенаправляти кошти назад клієнту.

Swift GPI Tracker відстежує платежі та запобігає шахрайству в режимі реального часу. У свою чергу, автоматизація забезпечує швидше відкликання платежів, а також зменшує зусилля та витрати на ручний пошук і робоче навантаження, пов'язане зі зупинкою платежу.

**CIFAS**

Cifas – провідна служба запобігання шахрайству у Великій Британії, яка керує двома найбільшими базами даних про шахрайство в країні. Служба надає обширні дані та розвідувальні дані про шахрайство, обслуговуючи різноманітну мережу з понад 600 організацій-членів у 14 секторах.

Бази даних Cifas щодо шахрайства, включаючи Національну базу даних про шахрайство та Внутрішню базу даних про шахрайство, пропонують обмін даними в режимі реального часу та онлайн для захисту організацій від шахрайства та афер. Сервіс вирішує такі проблеми, як шахрайство з особистими даними, захоплення облікових записів, неправдиві заяви, фальшиві заявки.

**FEEDZAI**

Feedzai — це комплексна платформа для запобігання шахрайству, адаптована як для роздрібних і корпоративних банків, так і для фінтех-компаній, постачальників платіжних послуг та еквайрів.

Платформа сприяє точній оцінці ризиків для клієнтів, розпізнаючи ранні сигнали ризику та виявляючи моделі шахрайства. Вона виявляє аномалії користувачів та запобігає крадіжці облікових даних, маніпуляціям під чужим ім'ям. Шахрайство з транзакціями ефективно відстежується за кількома каналами з акцентом на взаємодію з клієнтами в режимі реального часу, що дозволяє моделям

оцінки поведінкових та транзакційних моделей виявляти нові випадки шахрайства. Платформа забезпечує високий рівень деталізації, коли йдеться про виявлення шахрайства та афер з авторизованими push-платежами (APP).

**Verafin**

Verafin надає рішення корпоративного рівня для боротьби з фінансовими злочинами, допомагаючи фінансовим установам покращити свої зусилля у сфері боротьби з відмиванням коштів/фінансуванням тероризму та боротьбою з шахрайством. Verafin використовує цільову аналітику для виявлення фінансових злочинів, моніторингу транзакцій по кількох каналах та автоматичного аналізу профілів клієнтів та їхньої історії поведінки.

Verafin інтегрує міжінституційні, сторонні та відкриті джерела даних, щоб мінімізувати хибнопозитивні результати та генерувати високоякісні сповіщення. Платформа FRAML від Verafin охоплює широкий спектр шахрайських сценаріїв. Використовуючи штучний інтелект та машинне навчання, платформа генерує надійні сповіщення, що дозволяє вам проактивно виявляти шахрайство за кількома каналами. Станом на 2023 рік 92,14% клієнтів Verafin знаходяться або працюють у США.

**Comply advantage**

ComplyAdvantage пропонує фінансовим установам послуги з виявлення шахрайства та боротьби з відмиванням коштів на основі штучного інтелекту. Використовуючи моніторинг у режимі реального часу, компанії можуть виявляти шахрайську діяльність з мінімальним впливом на своїх клієнтів. Платформа охоплює понад 50 сценаріїв шахрайства незалежно від типу платежу, з можливістю виявлення шахрайства на етапі до транзакції. Модель машинного навчання ComplyAdvantage, навчена на історичних даних, пов'язує шахрайські облікові записи, які можуть контролюватися однією особою або організацією, що призводить до виявлення організованого шахрайства.

**Resistant AI**

Resistant AI – це програмне забезпечення для виявлення шахрайства, призначене для банків та фінтех-компаній. Воно використовує штучний інтелект

для розширення існуючих точок взаємодії з ризиками, від адаптації до постійного моніторингу, а також підвищує ефективність внутрішніх команд з управління ризиками та комплаєнсу.

Стійкий штучний інтелект надає рішення для виявлення та запобігання шахрайству, включаючи шахрайство з додатками та афери, зокрема, зосереджуючись на виявленні шахрайства з документами. Програмне забезпечення інтегрує профілювання ідентифікації та поведінки для виявлення потенційних шахраїв, зменшуючи кількість ручних перевірок, а також спроб серійного шахрайства.

**Hawk:AI**

Hawk:AI — це програмне забезпечення для виявлення шахрайства на базі штучного інтелекту, яке використовує штучний інтелект для вдосконалення застарілих систем на основі правил, яким часто важко адаптуватися до нових норм. Його обробка транзакцій у режимі реального часу дозволяє комплексно виявляти шахрайство в різних каналах та методах оплати.

Платформа пропонує низку рішень, від перевірки платежів та клієнтів, оцінки ризиків клієнтів, моніторингу транзакцій до запобігання шахрайству. Використовуючи машинне навчання у великих обсягах транзакцій, Hawk AI ефективно зменшує кількість хибнопозитивних сповіщень та збільшує виявлення істинно позитивних результатів. Програмне забезпечення розроблено для використання як традиційними, так і цифровими банками, платіжними компаніями та фінтех-компаніями.

**UNIT 21**

Unit 21 пропонує комплексні рішення для виявлення шахрайства клієнтам, починаючи від стартапів і закінчуючи компаніями зі списку Fortune 500, включаючи як традиційні банки, так і цифрові банки, платіжні компанії та фінтех-компанії.

Unit21 надає платформу для прийняття рішень щодо ризиків, шахрайства та відповідності на основі даних, зосереджуючись на виявленні та запобіганні шахрайству. Це досягається за допомогою моніторингу транзакцій у режимі

реального часу та розслідувань шахрайства на основі машинного навчання. Рішення Unit21 для боротьби з шахрайством пропонує єдине уявлення про дії та транзакції клієнтів, щоб зменшити втрати від шахрайства через захоплення облікових записів, шахрайство з платежами та зловживання платформою.

**SEON**

SEON пропонує оптимізований підхід до виявлення шахрайства. Використовуючи понад 50 соціальних сигналів та даних цифрового сліду, SEON застосовує штучний інтелект та машинне навчання для динамічного адаптування до методів оцінки ризиків різних підприємств. Адаптивний підхід підвищує його здатність ефективно виявляти та запобігати шахрайським транзакціям.

SEON пропонує послуги широкому колу підприємств: банкам, iGaming, онлайн-кредитуванню, електронній комерції, платіжним шлюзам, криптокомпаніям тощо.

**Sift**

Sift — це програмне забезпечення для виявлення шахрайства з уніфікованим та зручним інтерфейсом. Програмне забезпечення використовує запатентовану технологію для надання підключених даних та інтелектуальної автоматизації, спрямованої на запобігання захопленню облікових записів та мінімізацію впливу шахрайства на клієнтів. Sift використовується широким колом компаній, включаючи фінтех-компанії, постачальників цифрових товарів і послуг, а також торговельні майданчики. Завдяки своїй налаштовуваній логіці, Sift надає гнучкий сервіс із провідними в галузі функціями та можливостями.

Отже, основні характеристики, які мають бути в програмного забезпечення для виявлення шахрайства:

- Моніторинг транзакцій у режимі реального часу
- Співвідношення хибнопозитивних та істиннопозитивних сповіщень
- Поведінкова та транзакційна аналітика
- Можливості штучного інтелекту/машинного навчання та рівень автоматизації

Основні засоби виявлення фішингу представлено в таблиці 3.1.

Таблиця 3.1.

**Поширені засоби виявлення фішингу [23]**

| Утиліта | Опис | Переваги | Недоліки |
|---|---|---|---|
| GoldFish | Баєсова фільтрація спаму | Може бути натренований на кожного користувача;<br>Уникає помилкових спрацювань (FP). | Нестійкий до техніки «байєсівського отруєння»;<br>Можна обійти трохи змінюючи слова. |
| Браузери Site Adviser Netcraft | Чорні списки | Швидкий аналіз | Повільне оновлення списків;<br>Хибні спрацювання (FP). |
| SpoofGuard PwdHash | Інтегровані в браузер рішення;<br>Вивчає ознаки фішингу, такі як заплутані URL-адреси на веб-сторінках;<br>Збільшує сповіщення;<br>Метод евристики | PwdHash запобігає крадіжці паролів;<br>SpoofGuard захищає від неавторизованих IP та MAC-адрес | Ненадійність;<br>Захоплений пароль можна використовувати на цільовому сайті |
| EarthLink toolbar | Комбінація евристики, користувальницької оцінки та ручної перевірки | Перевіряє інформацію про реєстрацію домену | Не захищає від атак |
| eBay tool | Евристика та чорні списки | Захищає користувачів eBay | Недоліки чорних списків |

У 2025 році банківські і фінансові установи змущені будуть застосовувати криптографічну гнучкість, як аспект “квантової безпеки”. Штучний інтелект все глибше впроваджується в бізнес-операції, зусилля щодо захисту ШІ повинні бути в авангарді стратегій установ. Але слід враховувати два аспекти безпеки штучного інтелекту: захисту систем штучного інтелекту та захисту від атак, керованих штучним інтелектом. Кіберзлочинці вчаться використовувати штучний інтелект, щоб зробити свої атаки більш обхідними, ефективнішими та результативнішими [12].

## 3.2. Рекомендації щодо покращення безпеки банківських і фінансових установ

Світова економіка увійшла у 2024 рік з імпульсом на тлі супутніх вітрів

— послаблення тиску на ланцюги поставок, стримування інфляції — та зустрічних вітрів — геополітичної напруженості, посилення регуляторного контролю. Ці фактори випробовують стійкість бізнес-моделей фінансових послуг (ФП) та спонукають лідерів сектору досліджувати інноваційні шляхи створення цінності, одночасно керуючи новими ризиками кібербезпеки та проблемами конфіденційності.

Командам безпеки потрібно зосередитися на хвилі революційних технологій, що розвиваються, зокрема генеративному штучному інтелекті, необхідності автоматизації, зміцненні бази даних фірм і тенденціях до вбудованих фінансів.

З одного боку, поширення цифрових технологій розмиває глобальні кордони, що ускладнює узгодження ініціатив щодо зростання зі змінними регуляторними вимогами. Зі зростанням попиту на безперебійний та персоналізований досвід зростають і проблеми забезпечення комплексної безпеки та конфіденційності даних, що робить управління цифровою ідентифікацією складнішим, ніж будь-коли.

Одночасно, експоненціальне зростання обсягів даних та зростаюче впровадження хмарних систем розширили поле для кібератак, підкреслюючи прогалини в управлінні вразливостями та здатності своєчасно реагувати на інциденти.

Основна увага приділяється посиленому діалогу з питань ризиків між керівниками кіберпроектів та бізнесу, щоб забезпечити готовність до майбутніх дій та узгодити стратегії, що ґрунтуються на стійкості, інноваціях, безпеці та довірі.

Тому пропонується план успішного та відповідального подолання викликів у умовах постійно мінливого ландшафту загроз та нормативних актів.

***1. Орієнтування в глобальних кордонах, регуляторному середовищі***

Оскільки сектор фінансових послуг продовжує масштабувати технологічні інновації, регуляторні органи реагують новими стандартами кібербезпеки, щоб збалансувати зростання з управлінням. Найскладнішим

завданням для сучасних фахівців з безпеки є калібрування їхньої регуляторної звітності для світу, де кордони дедалі більше відсутні, зберігаючи при цьому засоби контролю безпеки, які можна адаптувати до місцевих вимог.

***Ключові виклики***

Орієнтування в різноманітних регуляторних ландшафтах – Збалансування дотримання вимог у постійно мінливому регуляторному просторі кібербезпеки та конфіденційності є важливим завданням для багатонаціональних фінансових компаній, особливо коли ці правила можуть суттєво відрізнятися в різних юрисдикціях.

Адаптація до національних інтересів та інформаційного суверенітету – національні інтереси надихнули на появу різноманітних регуляторних вимог щодо суверенітету даних, що ускладнює глобальне надання послуг. Підтримка глобальної доступності та дотримання місцевих норм вимагає значних інвестицій у місцеву інфраструктуру та масштабних операційних модифікацій.

Дотримання вимог безпеки ланцюга поставок – Оскільки ланцюги поставок простягаються через континенти, вразливості зростають через різні вимоги до кіберконтролю та прозорості. Забезпечення безпеки та дотримання вимог для кожної залученої організації вимагає ретельної перевірки та нагляду, що може призвести до збільшення складності та витрат.

Звітність про інциденти в глобальному контексті – Різні вимоги до звітності про інциденти в різних юрисдикціях вимагають гнучких та ефективних механізмів звітності, які можуть враховувати мінливі вимоги щодо кібербезпеки, забезпечуючи при цьому оперативне та точне розкриття інформації.

Дотримання правил конфіденційності – Окрім дотримання нових правил розкриття інформації про кібербезпеку Комісії з цінних паперів і бірж США (SEC) та Закону про цифрову операційну стійкість (DORA) в ЄС, сектор фінансових послуг намагається впровадити заходи контролю конфіденційності, які є одночасно узгодженими на глобальному рівні та адаптованими до місцевих норм, щоб відповідати глобальним законам про конфіденційність,

таким як Загальний регламент про захист даних (GDPR) у Європі та Закон Каліфорнії про конфіденційність споживачів (CCPA) у США. Досягнення балансу між захистом даних клієнтів та операційною гнучкістю залишається ключовим завданням.

***Ключові можливості***

Побудова стійкої системи дотримання нормативних вимог – Вирішення транскордонних складнощів вимагає складного та гнучкого підходу до дотримання нормативних вимог, який дозволяє швидко адаптуватися до нових правил, одночасно підвищуючи операційну стійкість у глобальному масштабі.

Посилення заходів щодо суверенітету даних – інвестування в місцеві центри обробки даних та хмарні технології з регіональними варіантами зберігання даних може допомогти компаніям-фінансовим компаніям адаптуватися до місцевих норм та ефективно виконувати вимоги щодо суверенітету даних у різних юрисдикціях.

Посилення безпеки ланцюга поставок – компанії, що займаються фінансовим забезпеченням, можуть зміцнити свою операційну основу від кіберзагроз та регуляторних змін, впроваджуючи надійні процеси перевірки безпеки та постійного моніторингу у своїх ланцюгах поставок.

Використання технологій для автоматизації дотримання вимог – передові технології, такі як штучний інтелект та блокчейн, можуть дозволити сектору автоматизувати виснажливі завдання дотримання вимог, знизити ризики людських помилок та підвищити ефективність звітності про інциденти та управління конфіденційністю.

Встановлення глобальних стандартів конфіденційності – установи фінансового забезпечення можуть отримати свою перевагу, очолюючи розробку та впровадження високих глобальних стандартів конфіденційності даних. Це має не лише сприяти культурі безпеки та довіри клієнтів, але й встановити орієнтир для всієї екосистеми.

Центральним питанням для сектору фінансового забезпечення є те, як найефективніше орієнтуватися в сучасному бізнес-ландшафті, щоб забезпечити

стійкість та безперервність бізнесу. Хоча багатонаціональні компанії часто є лідерами у впровадженні нових тенденцій, менші фірми часто можуть бути менш підготовленими до вирішення цих складнощів. Завдяки партнерству фірми можуть скористатися спільними знаннями та покращити свою безпеку у відповідь на мінливі глобальні регуляторні вимоги, не винаходячи велосипеда.

***2. Покращення безпеки за допомогою автоматизації***

Цифрові програми поширюються величезними темпами. Зі зростаючим переходом до хмарних систем та віддаленої роботи обсяг даних, що потребують захисту, стрімко зростає. Як наслідок, розширюється область кібератак, створюючи більше сповіщень та подій сортування, якими повинні керувати керівники кібербезпеки фінансових установ. Отже, як команди безпеки можуть постійно виявляти загрозу за загрозою та визначати, яким пріоритетам приділяти першочергову увагу? Один із найефективніших способів зробити це – автоматизація.

***Ключові виклики***

Обмеження ресурсів та перевантаження даними – галузь кібербезпеки стикається з подвійною проблемою: стрімким зростанням кіберзагроз та критичною нестачею кваліфікованих фахівців з кібербезпеки. Ця нестача ускладнює управління, виявлення та реагування на загрози під час обробки величезних обсягів даних. В результаті центри операцій безпеки (SOC) перевантажені величезним обсягом сповіщень, які необхідно аналізувати та контролювати.

Обсяг вразливостей – Швидкий розвиток технологій та виявлення недоліків програмного забезпечення залишають компанії, що займаються фінансовими послугами, з вразливостями, що робить визначення пріоритетів та їх виправлення складним завданням. Оскільки зрілі організації працюють над створенням надійних програм реагування, обмеження потужностей перешкоджають ефективному та своєчасному усуненню недоліків.

Ведення інвентаризації активів – Зріла інвентаризація управління активами стала необхідною умовою для багатьох процесів кібербезпеки,

забезпечуючи охоплення можливостей, володіння активами та критичної важливості ресурсів. Установи фінансового забезпечення часто стикаються із застарілими або неповними даними про активи, що перешкоджає ефективності процесів управління ризиками та безпеки.

Своєчасне пом'якшення наслідків інцидентів – Зростаюча кількість сповіщень та складні міжплатформні взаємозалежності сприяють затримкам у пом'якшенні наслідків кіберінцидентів. Центри захисту даних (SOC) справляються з цим робочим навантаженням, що призводить до затримок в оцінці та реагуванні на кожен інцидент, потенційно посилюючи наслідки порушень.

***Ключові можливості***

Управління вразливостями за допомогою машинного навчання – організаціям, що займаються фінансовими послугами, рекомендується оновити свої програми управління вразливостями, щоб комплексно усунути вузькі місця. Автоматизація може допомогти визначити пріоритети, призначити та усунути вразливості високої та низької критичності за допомогою рішень «політика як код».

Автоматизовані робочі процеси управління активами – вдосконалені автоматизовані процеси виявлення можуть ефективніше перевіряти метадані активів та права власності, забезпечуючи постійне оновлення інвентаризації активів у режимі реального часу та гарантуючи точне застосування протоколів безпеки.

Проактивні засоби контролю реагування на інциденти – Організації повинні наголошувати на проактивних засобах контролю для автоматичного блокування та реагування на потенційні мережеві загрози. Впровадження передових автоматизованих заходів стримування та блокування може обмежити поширення шкідливої активності, тим самим мінімізуючи вплив інцидентів безпеки.

Автоматизоване традиційне сортування аналітиків 1-го рівня – використовуйте машинне навчання (ML) для співвіднесення подій з кількох

джерел телеметрії, щоб зменшити кількість хибнопозитивних результатів та швидше передати важливі питання аналітикам 2-го рівня.

У міру оцифрування операційних моделей, SOC повинні автоматизувати та модернізувати свої процеси, щоб йти в ногу з часом. Завдяки автоматизації безпеки, фінансові установи можуть захистити екосистему третіх сторін, оцінити вразливості та виявити слабкі зв'язки в екосистемах постачальників та постачальників. Використовуючи штучний інтелект та машинне навчання, сектор може централізувати критично важливі процеси безпеки для зон високого ризику, що дозволяє командам безпеки досягати більш гнучкого та ефективного часу реагування.

### *3. Процес ідентичності має бути індивідуальним, а не інституційним*

Сьогодні межа між безпекою між бізнесом та споживачем (B2C) та бізнесом для бізнесу (B2B) значно розмилася. З огляду на перетин бізнес-моделей, вкрай важливо, щоб організації, що займаються фінансовими послугами, розглядали ідентифікацію не ізольовано, а з цілісної точки зору. Це важливий фактор для створення моделі управління ідентифікацією та доступом, яка охоплює новий рівень стійкості, придатний для федеративних, приватних, публічних або багатохмарних обчислювальних середовищ.

***Ключові виклики***

Стратегії управління ідентифікацією та доступом клієнтів (CIAM) – Зі зростанням цифрового банкінгу та фінансових послуг зростає потреба в надійних рішеннях CIAM, які не лише підтримують безперебійний досвід роботи з клієнтами, але й захищають ідентичність клієнтів та зміцнюють довіру.

Виявлення та запобігання шахрайству – Сектор фінансових послуг постійно стикається зі складними схемами шахрайства. Це дедалі більше посилює потребу в аналітиці ідентифікації та аналізі поведінки для виявлення аномальних моделей доступу та транзакцій.

Дотримання нормативних вимог та управління ідентифікацією (IM) – З

огляду на суворі нормативні вимоги, включаючи принцип «знай свого клієнта» (KYC), боротьбу з відмиванням грошей (AML) та конфіденційність (наприклад, GDPR, CCPA), багато фінансових установ мають труднощі з управлінням цифровою ідентифікацією, забезпечуючи при цьому дотримання вимог.

Розширення прав доступу та управління ними – споживачі та працівники фінансових послуг взаємодіють з різними цифровими платформами, що призводить до розширення прав доступу та збільшення вразливостей безпеки. Управління правами доступу стає складним та схильним до помилок, що робить цей сектор головною мішенню для крадіжки особистих даних та шахрайства.

Управління поверхнею атак, орієнтованою на ідентифікацію – відсутність стандартизованого підходу до автентифікації в установах фінансових послуг ускладнює взаємодію з користувачем та протоколи безпеки. Різноманітні методи призводять до плутанини, послаблення заходів безпеки та збільшення кіберризиків.

Зростання кількості діпфейків – легкість, з якою зловмисники можуть змінювати контент, загрожує бізнесу практично в кожній галузі та секторі. Державні та приватні організації в усьому світі повинні підтримувати відповідну обчислювальну потужність, судово-медичні алгоритми, процеси аудиту та кваліфікований персонал для боротьби з цією загрозою.

**Ключові можливості**

Покращення безпеки та вражень – Балансування зручності з безпекою за допомогою таких інструментів, як біометрична автентифікація, єдиний вхід (SSO) та багатофакторна автентифікація (MFA), може покращити враження клієнтів, що призведе до підвищення залученості та лояльності.

Моніторинг безпеки – Фінансові установи можуть використовувати аналітику ідентифікаційних даних для виявлення шахрайства та захисту клієнтів і активів. Такий проактивний підхід може слугувати ключовою перевагою на ринку, залучаючи клієнтів, які надають пріоритет конфіденційності даних. Окрім шахрайства, критично важливо пов’язати

привілейований доступ, внутрішні загрози та нелюдські ідентичності з традиційними процесами реагування на інциденти безпеки за допомогою розширеного виявлення та реагування (XDR).

Трансформація, що підживлюється регуляторними нормами – впровадження ефективних рішень для управління обміном повідомленнями, які автоматизують процеси дотримання вимог та зменшують регуляторні ризики, може зміцнити довіру клієнтів, що призведе до збільшення їх утримання та залучення.

Автоматизоване управління правами доступу – оптимізація та автоматизація управління правами доступу може допомогти підвищити операційну ефективність, зменшити кількість людських помилок та пом'якшити внутрішні загрози. Установи фінансового забезпечення можуть використовувати передові технологічні рішення для управління та адміністрування ідентифікацією (IGA), щоб забезпечити безпечний, сумісний та зручний для користувача досвід управління доступом.

Єдина ідентифікація – впровадження широкого спектру рішень для обміну миттєвими повідомленнями та співпраця над загальногалузевими стандартами автентифікації можуть посилити захист сектору від кіберзагроз та стимулювати інновації.

**Висновки до розділу 3**

Постійна боротьба з шахрайством вимагає радикально нового підходу з боку банківських і фінансових установ. Хоча існує безліч рішень для боротьби з шахрайством, кожен бізнес повинен чітко розуміти необхідні функції та свої обов'язки щодо забезпечення дотримання законів і нормативних актів.

Запропоновано актуальні програмні рішення для боротьби з шахрайством в банківських та фінансових установах: Salv Bridge, ризик шахрайства споживачів Mastercard, виявлення схем шахрайства та аномалій EBA CLEARING (FPAD), Swift GPI, Cifas, Feedzai, Verafin, ComplyAdvantage,

Стійкий штучний інтелект, HAWK: AI, Unit21, SEON, Sift.

Визнано, що основними характеристики, які мають бути в програмного забезпечення для виявлення шахрайства є: моніторинг транзакцій у режимі реального часу: співвідношення хибнопозитивних та істиннопозитивних сповіщень; поведінкова та транзакційна аналітика; можливості штучного інтелекту/машинного навчання та рівень автоматизації.

Проаналізовано вектори успішного та відповідального подолання викликів у банківських і фінансових установах в умовах постійно мінливого ландшафту кіберзагроз та нормативних актів. Вони сфокусовані на трьох площинах: 1. Орієнтуванні в глобальних кордонах та регуляторному середовищі, що передбачає адаптацію до національних інтересів та інформаційного суверенітету, дотримання вимог безпеки ланцюга поставок, звітність про інциденти в глобальному контексті, дотримання правил конфіденційності, чого можна досягнути за рахунок побудови стійкої системи дотримання нормативних вимог, посилення заходів щодо суверенітету даних, посилення безпеки ланцюга поставок, використання технологій для автоматизації дотримання вимог, встановлення глобальних стандартів конфіденційності.

Покращення безпеки за допомогою автоматизації що передбачає обмеження ресурсів та перевантаження даними, врахування обсягу вразливостей, ведення інвентаризації активів, своєчасне пом’якшення наслідків інцидентів за рахунок управління вразливостями за допомогою машинного навчання,

автоматизованих робочих процесів управління активами, проактивних засобів контролю реагування на інциденти, автоматизованому традиційному сортуванню аналітиків

Процес ідентичності має бути індивідуальним, а не інституційним що передбачає стратегії управління ідентифікацією та доступом клієнтів (CIAM), виявлення та запобігання шахрайству, дотримання нормативних вимог та управління ідентифікацією (IM), розширення прав доступу та управління ним,

управління поверхнею атак, орієнтованою на ідентифікацію, зростання кількості діпфейків за рахунок покращення безпеки та вражень, моніторингу безпеки, трансформації, що підживлюється регуляторними нормами, автоматизованого управління правами доступу, єдиної ідентифікації.

# ВИСНОВКИ

У кваліфікаційній роботі проведено аналіз та практичне дослідження засобів виявлення загроз для банківських і фінансових установ (зломи, фішинг, шахрайство), що дало змогу узагальнити основну проблематику та сформувати наступні висновки.

Доведено, що основними загрозами кібербезпеки в фінансовій сфері являються фішинг, програми-вимагачі, DDoS-атаки, ін'єкції SQL, включення локальних файлів, міжсайтові сценарії та ін'єкції OGNL Java, атаки на ланцюги поставок, Банк Дропс.

Підтверджена доцільність основних векторів захисту банківськимх і фінансових установ: захист даних клієнтів, збереження довіри та репутації клієнтів, відповідність регламенту захисту, запобігання фінансовим втратам, захист критичної інфраструктури банківських установ, забезпечення безперервності бізнесу.

Акцентовано на важливості застосування ефективних рішень в банківської і фінансовій сфері, які базуються на запроваджені багатофакторної автентифікації (MFA), наскрізному шифруванні, виявленні загроз на основі ШІ, запровадженні архітектури нульової довіри, побудові систем управління інцидентами та подіями безпеки (SIEM). Найкращими практиками кібербезпеки в фінансовій сфері вважаємо: регулярне навчання співробітників, проведення регулярних аудитів, оновлення програмного забезпечення, запровадження політики надійних паролів, розробка плану реагування на інциденти.

Доведено що фінансові та банківські установи мають бути надійно захищені завдяки застосували багаторівневому підходу до кібербезпеки, поєднуючи технічні засоби контролю, правові та регуляторні заходи, а також організаційні контрзаходи, що дозволить ефективно реагувати на загрози, також сприяти формуванню культури безпеки, підвищуючи їхню готовність до боротьби з кіберінцидентами та відновлення після них. Співпраця між різними зацікавленими сторонами, постійна пильність, навчання співробітників та стратегічне управління ризиками мають вирішальне значення для підтримки

безпечного операційного середовища для банківського та фінансового сектору.

Підтверджено, що фахівці з кібербезпеки докладають зусиль для використання штучного інтелекту в області виявлення вторгнень, щоб створити системи, здатні до виявлення невідомих атак і вивчення нових сигнатур атак самостійно. В основі вирішення проблеми форматування набору даних і техніки оптимізації полягає бібліотека атак, яка має бути використана за допомогою нейронних мереж, оскільки вони здатні навчатися. Навчені нейронні мережі можуть приймати рішення швидко, що дає можливість використовувати їх для виявлення кіберзагроз в реальному часі.

Запропоновано актуальні програмні рішення для боротьби з шахрайством в банківських та фінансових установах: Salv Bridge, ризик шахрайства споживачів Mastercard, виявлення схем шахрайства та аномалій EBA CLEARING (FPAD), Swift GPI, Cifas, Feedzai, Verafin, ComplyAdvantage, Стійкий штучний інтелект, HAWK: AI, Unit21, SEON, Sift.

Визнано, що основними характеристики, які мають бути в програмного забезпечення для виявлення шахрайства є: моніторинг транзакцій у режимі реального часу: співвідношення хибнопозитивних та істиннопозитивних сповіщень; поведінкова та транзакційна аналітика; можливості штучного інтелекту/машинного навчання та рівень автоматизації.

Проаналізовано вектори успішного та відповідального подолання викликів у банківських і фінансових установах в умовах постійно мінливого ландшафту кіберзагроз та нормативних актів. Вони сфокусовані на трьох площинах: 1. Орієнтуванні в глобальних кордонах та регуляторному середовищі, що передбачає адаптацію до національних інтересів та інформаційного суверенітету, дотримання вимог безпеки ланцюга поставок, звітність про інциденти в глобальному контексті, дотримання правил конфіденційності, чого можна досягнути за рахунок побудови стійкої системи дотримання нормативних вимог, посилення заходів щодо суверенітету даних, посилення безпеки ланцюга поставок, використання технологій для автоматизації дотримання вимог, встановлення глобальних стандартів

конфіденційності.

Покращення безпеки за допомогою автоматизації передбачає обмеження ресурсів та перевантаження даними, врахування обсягу вразливостей, ведення інвентаризації активів, своєчасне пом’якшення наслідків інцидентів за рахунок управління вразливостями за допомогою машинного навчання, автоматизованих робочих процесів управління активами, проактивних засобів контролю реагування на інциденти, автоматизованому традиційному сортуванню аналітиків.

Процес ідентичності має бути індивідуальним, а не інституційним що передбачає стратегії управління ідентифікацією та доступом клієнтів (CIAM), виявлення та запобігання шахрайству, дотримання нормативних вимог та управління ідентифікацією (IM), розширення прав доступу та управління ним, управління поверхнею атак, орієнтованою на ідентифікацію, зростання кількості діпфейків за рахунок покращення безпеки та вражень, моніторингу безпеки, трансформації, що підживлюється регуляторними нормами, автоматизованого управління правами доступу, єдиної ідентифікації.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The Year in Review 2024: Today's Insights, Tomorrow's Outlook. URL:https://www.akamai.com/blog/security-research/2024-december-today-insights-tomorrow-outlook-2025

2. The 6 Biggest Cyber Threats for Financial Services in 2025. URL: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services

3. Що таке фішинг і як від нього захиститись? URL: https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html

4. Як розпізнати та захиститися від фішингу в інтернеті: інструкція на 2025 рік. URL: https://www.grivnya.in.ua/bezpeka/phishing-security/

5. Phishing Activity Trends Reports. URL: https://apwg.org/trendsreports/

6. QR codes sent in attachments are the new favorite for phishers. URL: https://www.malwarebytes.com/blog/news/2025/04/qr-codes-sent-in-attachments-are-the-new-favorite-for-phishers

7. CYBER DIGEST Огляд подій в сфері кібербезпеки, травень 2024. URL: https://ufss.com.ua/wp-content/uploads/2024/06/Cyber-digest_May_2024_UA.pdfURL

8. OWASP Top 10 API Security Risks: The 2023 Edition Is Finally Here. URL: https://www.akamai.com/blog/security/owasp-top-10-api-security-risks-2023-edition

9. Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers URL: https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

10. Cybersecurity in Banking: Threats, Solutions & Best Practices. URL: https://www.esecurityplanet.com/cloud/cyber-security-in-banking/

11. Planquart J. (2001). Application of Neural Networks to Intrusion Detection. SANS Institute. URL: http://www.sans.org/reading_room/whitepapers/detection/336.php?portal=59ce6bc816da952ccdc3c878029b635a.

12. Sabhnani M. and G. Serpen (2003). Application of Machine Learning Algorithms to KDDIntrusion Detection Dataset within Misuse Detection Context. Procedings of the International Conference on Machine Learning, Models, Technologies and Applications (MLMTA 2003), Las Vegas, NV

13. Agarwal R. and M. Joshi (2000). PNrule: A New Framework for Learning Classifier Models inData Mining. Technical Report TR 00 -015, Department of Computer Science, University ofMinnesota.

14. The State of Cybersecurity in Banking 2024. URL: https://startups.epam.com/blog/cyber-security-in-banking

15. Darem A. A., Alhashmi A. A., Alkhaldi T. M., Alashjaee A. M., Alanazi S. M. and Ebad S. A. Cyber Threats Classifications and Countermeasures in Banking and Financial Sector in IEEE Access. 2023. vol. 11. pp. 125138-125158, doi: 10.1109/ACCESS.2023.3327016. URL: https://www.researchgate.net/publication/374942247_Cyber_Threats_Classifications_and_Countermeasures_in_Banking_and_Financial_Sector

16. Novikov D., Yampolskiy R., Reznik L. Traffic Analysis Based Identification of Attacks. Traffic Analysis Based Identification of Attacks. *International Journal of Computer Science and Applications, Technomathematics Research Foundation.* 2008. Vol. 5, No. 2, pp 69 – 88.

17. Levin I. “KDD -99 Classifier Learning Contest LLSoft's Results Overview.” SIG KDDExplorations. 2000. vol. 1.

18. 13 Best fraud detection software solutions in 2024. URL: https://salv.com/blog/fraud-detection-software-solutions/

19. Штонда Р., Черниш Ю., Терещенко Т., Терещенко К., Цикало Ю., Поліщук С. Класифікація та методи виявлення фішингових атак. *Кібербезпека: освіта, наука, техніка*. 2024. Том 4. № 24. С. 69-80. URL:https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/591/464

20. The State of Cybersecurity in Banking 2024. URL: https://startups.epam.com/blog/cyber-security-in-banking

21. Cyber threats impacting the financial sector in 2024 - focus on the main actors.

URL: https://t7f4e9n3.delivery.rocketcdn.me/wp-content/uploads/2025/02/Cyber-threats-impacting-the-financial-sector-in-2024_-focus-on-the-main-actors-TLPCLEAR.pdf

22. Cyber threats impacting the financial sector in 2024 – focus on the main actors. URL:https://blog.sekoia.io/cyber-threats-impacting-the-financial-sector-in-2024-focus-on-the-main-actors/

23. Cybersecurity considerations 2024: Financial services sector. URL:https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2024-financial-services-sector.html

24. Cybersecurity and Financial SystemResilience Report. URL:https://www.federalreserve.gov/publications/files/cybersecurity-report-202407.pdf

25. Two-thirds of financial institutions faced cyberattacks in 2024. URL:https://www.securitymagazine.com/articles/101524-two-thirds-of-financial-institutions-faced-cyberattacks-in-2024

26. Digital threat report 2024 for the banking financial services and insurance (bfsi) sector a collaborative effort of sisa, cert-in & csirt-fin. 1 digital threat report 2024 digital threat report 2024 for the banking financial services and insurance (bfsi) sector. URL:https://www.csk.gov.in/documents/digital-threat-report-2024.pdf

27. 2024 Report on Cybersecurity and Resilience. URL:https://www.fdic.gov/regulations/resources/cybersecurity/2024-cybersecurity-financial-system-resilience-report.pdf

28. Global Cybersecurity Outlook 2025 INSIGHT REPORT JANUARY 2025. URL:https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

29. Cyber Security Threats To Financial Services In 2024. URL:https://www.firesand.co.uk/articles-research/posts/2024/march/9-top-cyber-security-threats-to-financial-services-in-2024/

30. The biggest data breaches of 2024 in financial services. URL:https://www.americanbanker.com/list/the-biggest-data-breaches-of-2024-in-financial-services

31. Cyber Security in Banking: How We Address Rising Challenges. URL:https://www.techmagic.co/blog/cybersecurity-in-banking