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

# КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: *"Методи та засоби забезпечення інформаційної безпеки в системах інтернет-банкінгу"*

Виконав: студент VI курсу, групи СБм-62

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

*Голда А. А.*
підпис (прізвище та ініціали)

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

Нормоконтроль *Лечаченко Т. А.*
підпис (прізвище та ініціали)

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

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
**Тернопільський національний технічний університет імені Івана Пулюя**

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2023 р.

# ЗАВДАННЯ
## НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Голда Антон Андрійович
(прізвище, ім'я, по батькові)

1. Тема роботи Методи та засоби забезпечення інформаційної безпеки в системах інтернет-банкінгу

Керівник роботи Стадник М. А., к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 16 » листопада 2023 року № 4/7-1061

2. Термін подання студентом завершеної роботи 20.12.2023

3. Вихідні дані до роботи Наукові публікації про забезпечення безпеки в банкових системах

4. Зміст роботи (перелік питань, які потрібно розробити)
Перелік умовних скорочень Вступ 1 Аналіз стану інформаційної безпеки в банківській сфері 1.1. Огляд систем загроз та захист інформації в інтернет-банкінгу 1.2. Статистичні дані щодо кіберзагроз у банківському секторі 1.3. Аналіз основних загроз інформаційній безпеці банків 1.4. Оцінка небезпек для інформаційної безпеки банку 2 Розроблення системи захисту інформації в інтернет-банкінгу 2.1. Модель порушника безпеки систем інтернет-банкінгу 2.2. Системи виявлення та моніторингу порушень безпеки 2.3. Криптографічні методи захисту конфіденційних даних 3 Комплексна система захисту банківської мережі 3.1. Розробка та впровадження системи захисту інформації 3.2. Технічні засоби захисту від загроз 3.3. Організація захищеного зберігання та обробки даних 4 Управління інформаційною безпекою в банку 4.1. Організаційні заходи збереження інформаційної безпеки 4.2. Правове регулювання захисту банківської інформації 4.3. Навчання персоналу з питань кібербезпеки 5 Охорона праці та безпека в надзвичайних ситуаціях 5.1. Охорона праці 5.2 Організація оповіщення і зв'язку у надзвичайних ситуаціях техногенного та природного характеру Висновки Список використаної літератури Додатки

5. Перелік графічного матеріалу. 1. Титулка. 2. Мета та задачі дослідження. 3. Шахрайське сповіщення 4. Основні загрози інформаційній безпеці, з якими стикаються банки 5. Види шифрування 6. Міжмережевий екран 7. Системи виявлення вторгнень (IDS) 8. Системи запобігання вторгнень (IPS) 9. Брандмауер веб-додатків 10. Висновки 11. Кількість кіберінцидентів у фінансовій галузі в усьому світі з 2013 по 2022 рік 12. Блок-схема алгоритму оцінки загроз для інформаційної безпеки банку

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Охорона праці | Осухівська Г.М., к.т.н., доцент | | |
| Безпека в надзвичайних ситуаціях | Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва | | |

7. Дата видачі завдання 14.11.2023 р.

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Ознайомлення з завданням до кваліфікаційної роботи | 14.11.2023-15.11.2023 | *Виконано* |
| 2. | Підбір наукових джерел | 16.11.2023-20.11.2023 | *Виконано* |
| 3. | Переклад та опрацювання наукових джерел | 21.11.2023-23.11.2023 | *Виконано* |
| 4. | Аналіз вразливостей інтрнет-банкінгів | 24.11.2023-27.11.2023 | *Виконано* |
| 5. | Оформлення розділу “Аналіз стану інформаційної безпеки в банківській сфері” | 28.11.2023-30.11.2023 | *Виконано* |
| 6. | Оформлення розділу “Розроблення системи захисту інформації в інтернет-банкінгу” | 01.12.2023-04.12.2023 | *Виконано* |
| 7. | Оформлення розділу “Комплексна система захисту банківської мережі” | 05.12.2023-07.12.2023 | *Виконано* |
| 8. | Оформлення розділу “Управління інформаційною безпекою в банку” | 08.12.2023-09.12.2023 | *Виконано* |
| 9. | Виконання завдання до підрозділу «Охорона праці» | 10.12.2023-11.12.2023 | *Виконано* |
| 10. | Виконання завдання до підрозділу «Безпека в надзвичайних ситуаціях» | 12.12.2023-13.12.2023 | *Виконано* |
| 11. | Оформлення кваліфікаційної роботи | 14.12.2023-15.12.2023 | *Виконано* |
| 12. | Нормоконтроль | 18.12.2023 | *Виконано* |
| 13. | Перевірка на плагіат | 20.12.2023 | *Виконано* |
| 14. | Попередній захист кваліфікаційної роботи | 21.12.2023 | *Виконано* |
| 15. | Захист кваліфікаційної роботи | 27.12.2023 | |
| | | | |
| | | | |
| | | | |

Студент _____ *Голда А. А.*
(підпис) (прізвище та ініціали)

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

# АНОТАЦІЯ

Методи та засоби забезпечення інформаційної безпеки в системах інтернет-банкінгу // Кваліфікаційна робота освітнього рівня «Магістр» // Голда Антон Андрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-62 // Тернопіль, 2023 // С. – 72, рис. – 9, табл. – 0 , кресл. – 0, додат. – 2.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМИ ІНТЕРНЕТ-БАНКІНГУ, КІБЕРЗАГРОЗИ, ЗАХИСТ ІНФОРМАЦІЇ

У роботі проаналізовано сучасний стан інформаційної безпеки в банківській сфері, виявлено основні загрози та вразливості систем інтернет-банкінгу. Запропоновано комплекс організаційних та технічних заходів для підвищення захищеності комп'ютерних мереж та інформаційних ресурсів банків.

Розроблено модель порушника безпеки систем інтернет-банкінгу. Спроектовано політику інформаційної безпеки банківської установи з урахуванням виявлених загроз.

Запропоновано використання двофакторної аутентифікації користувачів, криптографічного захисту інформації, систем виявлення вторгнень, а також навчання персоналу з питань інформаційної безпеки.

Кваліфікаційна робота має практичне значення. Її результати можуть бути використані для підвищення рівня захищеності систем інтернет-банкінгу.

# ABSTRACT

Methods and Means of Ensuring Information Security in Internet Banking Systems // Qualification work of the educational level “Master” // Golda Anton Andriiovych // Ternopil Ivan Pulyuy National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, СБм-62 group // Ternopil, 2023 // P. – 72, fig. – 9, table – 0, drawing – 0, apendix – 2.

Keywords: INFORMATION SECURITY, INTERNET BANKING SYSTEMS, CYBER THREATS, INFORMATION PROTECTION

The paper analyzes the current state of information security in the banking sector, identifies the main threats and vulnerabilities of Internet banking systems. A set of organizational and technical measures to improve the security of computer networks and information resources of banks is proposed.

A model of a security breacher of Internet banking systems is developed. The information security policy of a banking institution is designed taking into account the identified threats.

The use of two-factor user authentication, cryptographic protection of information, intrusion detection systems, as well as training of personnel on information security issues is proposed.

The qualification work is of practical importance. Its results can be used to increase the level of security of Internet banking systems.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АТС – автоматична телефонна станція

БД – база даних

ДСК – довідково-сервісний центр

ЕЦП – електронно-цифровий підпис

ІБ – інтернет–банкінг

ІКС – інформаційно-комунікаційна система

ІР – інтернет-протокол

КЗІ – криптографічний захист інформації

МАС – міжмережевий екран

МБ – мобільний банкінг

ОС – операційна система

ОТР – одноразовий тимчасовий пароль

ПЗ – програмне забезпечення

СКБД – система керування базами даних

ТЗІ – технічний захист інформації

ФБ – фішинг-бот

ЧД – чат-додаток

ШІ – штучний інтелект

# ВСТУП

Актуальність теми дослідження. Сучасні інформаційні технології докорінно змінили сферу банківських послуг, зробивши їх більш мобільними, доступними та зручними для клієнтів. Одним із проявів цих змін стало стрімке поширення інтернет-банкінгу – системи дистанційного банківського обслуговування через мережу Інтернет. Інтернет-банкінг надає користувачам можливість цілодобово виконувати платежі, переглядати залишки на рахунках, відкривати депозити, обмінюватися фінансовими документами з банком та іншими операціями, не відвідуючи відділення. Популярність цього сервісу зростає з кожним роком. За даними дослідницької компанії Berg Insight, у 2018 році кількість активних користувачів інтернет-банкінгу в Європі досягла близько 172 мільйонів осіб. В Україні частина громадян, які користуються послугами інтернет-банкінгу, також демонструє стійку тенденцію до зростання.

Водночас, поряд із зручністю та ефективністю, інтернет-банкінг несе і певні ризики у сфері інформаційної безпеки. Передача конфіденційних даних через відкриті канали зв’язку, а також зберігання цієї інформації в електронному вигляді створює можливості для кіберзлочинців. Злами банківських рахунків, крадіжка грошей, несанкціонований доступ до персональних даних клієнтів – це далеко не повний перелік загроз, з якими можуть зіткнутися користувачі інтернет-банкінгу. Тому питання забезпечення належного рівня інформаційної безпеки ця система є вкрай актуальною.

Аналіз останніх досліджень і публікацій. Проблемам інформаційної безпеки в інтернет-банкінгу присвячено чимало наукових публікацій. також, теоретичні та практичні аспекти забезпечення безпеки електронних банківських систем досліджували такі вітчизняні науковці, як Н.В. Вовчак, І.В. Сало, Т.Б. Кушнір, С.В. Клименко, О.Є Маслак та ін. Зарубіжний досвід розвитку інтернет-банкінгу висвітлено у роботах Д. Лаудона, К. Трейсі, Е. Оз, Х. Йен.

Водночас, за значною кількістю наукових напрацювань, проблема комплексного забезпечення інформаційної безпеки в системах інтернет-банкінгу

залишається не вирішеною остаточно. Це пов'язано зі стрімким розвитком інформаційних технологій та постійною появою нових кіберзагроз. Тому пошук ефективних методів та засобів захисту інформації в інтернет-банкінгу є актуальним науковим завданням.

Мета і завдання дослідження. Методом дослідження є підвищення рівня інформаційної безпеки в системах інтернет-банкінгу шляхом удосконалення існуючих та розробки нових методів і засобів захисту даних.

Для поставленої мети в досягненні результату такі основні завдання:

– проаналізувати сучасний стан забезпечення інформаційної безпеки в системах інтернет-банкінгу;

– дослідити існуючі загрози та вразливість інтернет-банкінгу з точки зору інформаційної безпеки;

– систематизувати та узагальнити існуючі методи і засоби захисту інформації в інтернет-банкінгу;

– запропонувати удосконалення та нові підходи до забезпечення інформаційної безпеки в системах інтернет-банкінгу;

– експериментально перевірити ефективність запропонованих методів і засобів захисту інформації;

– розробити рекомендації щодо практичного впровадження результатів дослідження.

Об'єкт дослідження – процеси забезпечення інформаційної безпеки в системах інтернет-банкінгу.

Предмет дослідження – методи та засоби захисту інформації в системах інтернет-банкінгу.

Методи дослідження. Теоретичною основою дослідження є фундаментальні положення інформаційної безпеки, теорії інформації, системного аналізу та теорії згідно рішень.

# 1 АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БАНКІВСЬКІЙ СФЕРІ

## 1.1 Огляд систем загроз та захист інформації в інтернет-банкінгу

Розвиток онлайн-банкінгу та мобільного банкінгу, а також інноваційних інтерфейсів банківських послуг підвищує рівень маркетингових стратегій, банківських установ, що дозволяє краще взаємодіяти зі своїми клієнтами, доносити до них інформацію про послуги та зробити їх швидшими та простішими для використання.

Пандемія COVID-19 та війна в Україні суттєво вплинули на фінансовий сектор, змушуючи розширювати набір онлайн-послуг не лише для українців на території України, але і за кордоном. Це викликало зростання вимог споживачів і збільшення ризиків, пов'язаних із збереженням безпеки персональних даних та розвитком ефективних, безпечних методів ідентифікації клієнтів без їх фізичної присутності.

Внаслідок пандемії COVID-19 нам довелося перейти на віддалену роботу. Співробітники банківських установ зуміли підтримати необхідний рівень продуктивності, створивши можливість безпечного обміну даними між колегами на відстані.

Підвищення рівня діджиталізації призводить до зростання загроз кібератак, викрадання особистих даних та інших форм незаконної фінансової діяльності. Таким чином, для банків надзвичайно важливо використовувати технології, що забезпечують вищий рівень кіберстійкості.

Інтернет-банкінг набуває все більшої популярності серед користувачів завдяки своїй зручності та швидкості. Проте поряд із перевагами, інтернет-банкінг несе і певні ризики, пов'язані із безпекою та конфіденційністю даних. Тому банки приділяють значну увагу розробці надійних систем захисту інформації.

В більшості випадків причиною крадіжки грошей клієнтів онлайн банку є фішинговий електронний лист (рисунок 1.1), котрий намагається змусити користувача натискати на шкідливі посилання або на перший погляд безпечного прикріплення. Такі вкладення надзвичайно часто виявляються пасткою для кіберзловмисників, які намагаються отримати несанкціонований доступ до фінансових рахунків осіб, що піддаються обману.

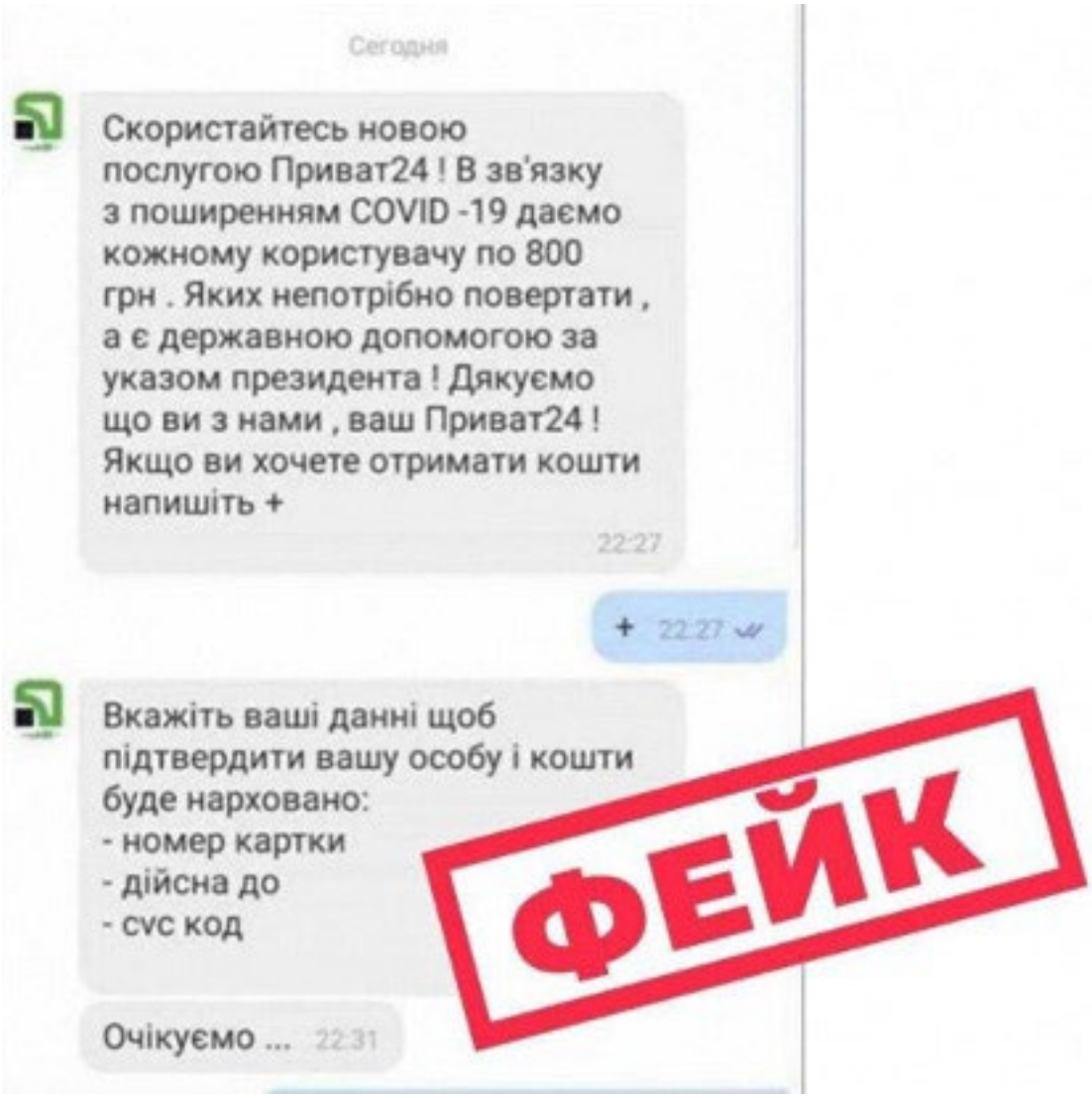


Рисунок 1.1 – Шахрайське сповіщення

Зловмисники все частіше не лише намагаються викрадати особисті дані, але й аналізують поведінку користувачів, їх фінансові звички, графіки транзакцій та залишки. Зокрема, кіберзлочинці можуть обирати користувачів із значними сумами грошей, залишаючись непомітними завдяки детальному вивченню цих

даних. Попри те, що будь-хто може стати жертвою, бізнесмени та підприємці частіше потрапляють під атаки.

Ще однією загрозою є кейлогери (keyloggers) - шкідливі програми, які фіксують натискання клавіш на клавіатурі. Вони дозволяють зловмисникам отримувати конфіденційні дані користувачів, такі як логіни і паролі до систем інтернет-банкінгу. Кейлогери можуть потрапляти на пристрій жертви разом із зараженими файлами або через експлойти (exploits) в програмному забезпеченні.

Ще одним поширеним методом є атака типу "людина посередині". В цьому випадку зловмисники вдаються до перехоплення трафіку між користувачем та сервером банку. Це дозволяє їм отримувати реквізити платежів та навіть змінювати їх для перенаправлення коштів на власні рахунки.

Окрім крадіжки грошей, існує загроза витоку конфіденційних даних клієнтів, таких як особиста інформація, номери рахунків, кредитна історія тощо. Ці дані можуть бути використані для подальших зловмисних дій, включаючи крадіжку особистості.

З боку самих банків однією з найбільших загроз є DDoS атаки на сервери та інфраструктуру банку. Такі атаки можуть призвести до тимчасової недоступності систем інтернет-банкінгу, що негативно впливає на репутацію банку та завдає збитків через неможливість обслуговування клієнтів.

Для протидії зазначеним загрозам банки використовують комплексні системи інформаційної безпеки, що включають:

– Сучасне антивірусне програмне забезпечення використовує не лише сигнатурний аналіз для виявлення відомого шкідливого коду, але й евристичний аналіз та машинне навчання. Це дозволяє виявляти нові, раніше невідомі загрози шляхом аналізу поведінки програм. Kaspersky Endpoint Security містить такі технології як System Watcher для аналізу активності процесів та Automatic Exploit Prevention для запобігання експлуатації вразливостей.

– Міжмережеві екрани, такі як Cisco ASA, дозволяють налаштувати детальні правила фільтрації трафіку на основі IP адрес, портів та мережевих протоколів. Це дає можливість блокувати підключення з підозрілих діапазонів

IP, закривати вразливі порти, забороняти небезпечні протоколи. Також можна використовувати контекстний аналіз для розгляду всієї сесії з'єднання.

– Системи виявлення вторгнень, такі як Snort, аналізують весь мережевий трафік в режимі реального часу та порівнюють його із сигнатурами атак. Це дозволяє виявляти спроби мережевих атак, експлуатації вразливостей, поширення шкідливого ПЗ. Системи типу IPS можуть не лише попереджати, але й блокувати загрози шляхом переривання сесії з'єднання.

– SSL/TLS сертифікати забезпечують шифрування трафіку між користувачами і серверами інтернет банкінгу. Використовуються надійні алгоритми шифрування з відкритим ключем, такі як RSA та Diffie-Hellman. Для симетричного шифрування даних застосовують AES з довжиною ключа мінімум 128 біт. Обов'язково слід відключати слабкі алгоритми типу RC4, MD5, SHA1.

– Для надійної аутентифікації користувачів інтернет банкінгу доцільно використовувати дво- або багатофакторну аутентифікацію. Це може включати поєднання паролів, одноразових паролів з OTP токенів, сканування біометричних даних (відбитки пальців, обличчя), підтвердження через мобільний додаток або пуш-повідомлення. Це значно ускладнює підбір облікових даних зловмисниками.

## 1.2 Статистичні дані щодо кіберзагроз у банківському секторі

За даними аналітичної компанії Positive Technologies, у 2023 році фінансовий сектор посідав друге місце за кількістю кібератак після державного сектору. На фінансові організації припадало 18% усіх атак [36]. Найпоширенішими типами атак на фінансові установи є цільові атаки (89%), веб-атака (82%), шкідливе ПЗ (76%) та botnet-атаки (58%), згідно звіту компанії Carbon Black [37].

За оцінками Juniper Research, збитки від шахрайства у мобільному і онлайн-банкінгу досягнуть 362 млрд доларів за 5 років [38]. 78% фінансових

організацій зіткнулися з витоками даних за останні 5 років, згідно дослідження Ponemon Institute [39]. В середньому витік зазнавали 6 разів.

Фішингові атаки на фінансові організації зросли на 15% у 2023 році в порівнянні з 2019 роком, згідно звіту компанії VMware Carbon Black [37].

Середні втрати від інцидентів, пов'язаних з фішингом, склали 1,2 млн доларів для фінансової організації, згідно IBM Security [40]. 81% кібератак на фінансові організації мали на меті крадіжку грошей, 76% - крадіжку даних, а 29% - завдання репутаційної шкоди компанії, згідно дослідження LexisNexis Risk Solutions [41].

За даними аналітичної компанії Positive Technologies, найбільш атакованими банківськими системами є платіжні системи (69% атак), backend-системи (46%), CRM-системи (42%), POS-термінали (39%) та API для мобільних додатків (37%). Найпоширеніші вектори атак на банки - це атаки з використанням шкідливих файлів (90% випадків), фішинг (86%), експлуатація вразливостей ПЗ (75%) та зараження через веб-ресурси (73%) [36].

За оцінками компанії Accenture, втрати банків від кібершахрайства у 2019 році склали 42 млрд доларів, а до 2025 року можуть досягти 300 млрд [42].

У 2020 році 41% фінансових організацій в США зазнали фінансових збитків від кібератак, середній розмір яких склав 7,5 млн доларів. 78% атак на фінансові організації мали виток конфіденційних даних, а 25% призвели до простою бізнес-процесів, за даними RiskRecon [43].

Найдорожчою кібератакою для банку став злам бангладеського Bank SWIFT-системи у 2016 році, який приніс зловмисникам 81 млн доларів. У 2018 році хакери викрали 14 млн доларів з рахунків в банку Chile's Banco de Chile за допомогою вірусу QakBot.

У 2020 році група Lazarus здійснила атаку на банківську мережу в Індії, викравши 10 млн доларів з рахунків Cosmos Bank. За перше півріччя 2021 року кількість цільових атак на фінансові організації зросла на 238% у порівнянні з аналогічним періодом 2020 року, випереджаючи усі інші галузі, згідно звіту Positive Technologies [36].

Фінансові компанії в середньому витрачають близько 28 млн доларів щорічно на заходи із забезпечення кібербезпеки, згідно Statista [44]. Це один з найвищих показників серед усіх галузей економіки. Більш ніж 80% банків планують збільшити інвестиції у кібербезпеку у найближчі 2-3 роки, щоб протистояти зростаючим кіберзагрозам, згідно звіту Deloitte [45].

У 2023 році хакери здійснили DDoS-атаку на український monobank, яку вдалося відбити досить швидко, що вже свідчить, про зростання безпеки інтернет банкінгу.

Отже, статистика свідчить про зростання кіберзагроз у фінансовому секторі (рисунок 1.2). Найбільш уразливими ланками є працівники, клієнти та незахищені дані. Тому банки активно вкладають кошти у підвищення кібербезпеки.

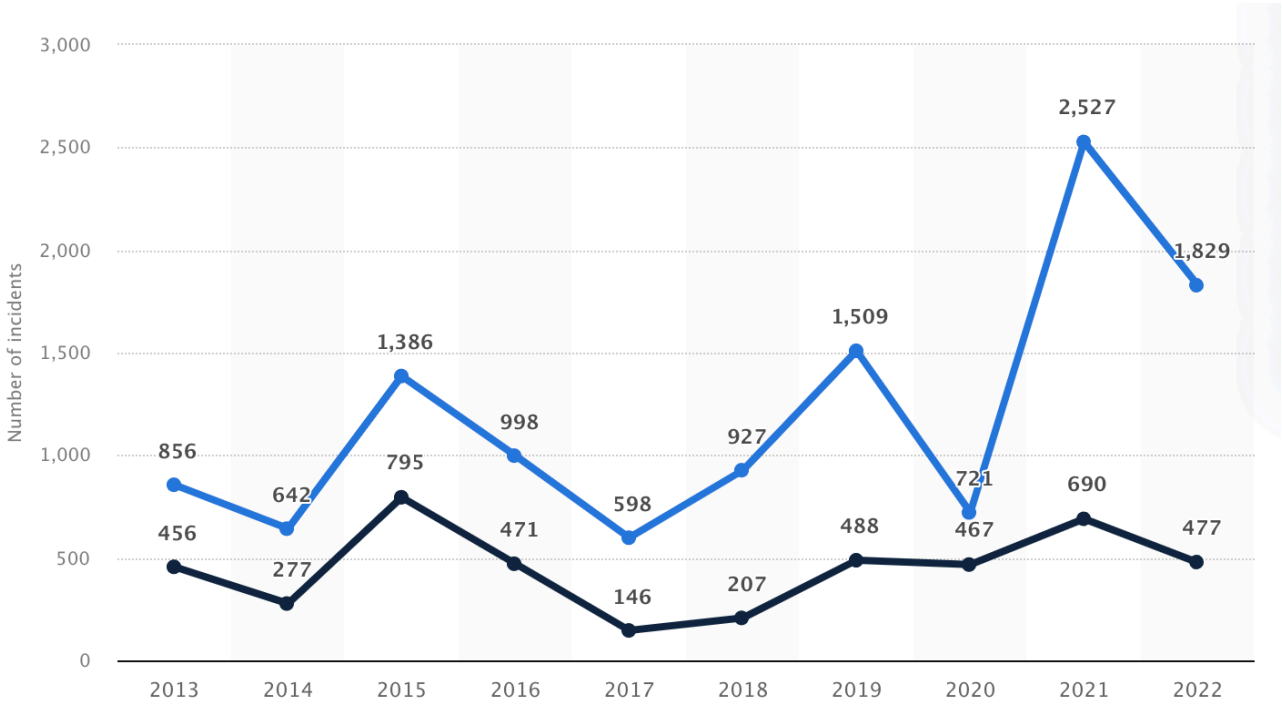


Рисунок 1.2 – Кількість кіберінцидентів у фінансовій галузі в усьому світі з 2013 по 2022 рік [44]

### 1.3 Аналіз основних загроз інформаційній безпеці банків

Інформаційна безпека є критично важливою для банківської сфери, оскільки вона оперує великими масивами конфіденційних даних та грошових коштів. Банки піддаються численним кіберзагрозам, які можуть призвести до витоку персональних даних клієнтів, фінансових втрат та порушення репутації.

Основні загрози інформаційній безпеці, з якими стикаються банки наведені на рисунку 1.3.


Рисунок 1.3 – Основні загрози інформаційній безпеці, з якими стикаються банки

Фішинг є однією з найпоширеніших кіберзагроз для банків. Його мета - виманити у користувача конфіденційні дані, такі як логіни, паролі, PIN-коди тощо. Найчастіше фішинг проводиться через електронні листи або сайти-підробки, схожі на справжні ресурси банку. Якщо користувач вводить свої дані на шахрайському сайті або в листі, вони потрапляють до зловмисників. Після

отримання доступу до рахунку жертви зловмисники можуть викрасти гроші різними методами: перевести на інший рахунок, зробити покупки онлайн, зняти готівкою через банкомат тощо. Ці атаки можуть завдати банку значних фінансових збитків.

Іноді хакери не викрадають гроші, а шифрують дані на банківських серверах та вимагають викуп за розшифрування. Наприклад, у 2022 році хакерська група LockBit атакувала системи банку США First Bank та виклала в Dark Web вкрадені дані після відмови заплатити викуп.

Розподілені атаки на відмову в обслуговуванні (DDoS) паралізують роботу веб-ресурсів та серверів банку шляхом навантаження на них шквалу запитів. Це призводить до простоїв систем інтернет-банкінгу, мобільних додатків, сайтів. Клієнти втрачають доступ до послуг банку.

Віруси, трояни, програми-вимагачі тощо можуть потрапляти на пристрої клієнтів чи працівників банку та компрометувати їх. Зловмисне ПЗ здатне красти паролі, банківські реквізити, контролювати систему тощо. Це створює загрозу витоку даних та шахрайських операцій.

Працівники банку, які мають законний доступ до систем і інформації, можуть навмисно чи ненавмисно порушити політики безпеки: розголосити дані, пошкодити систему, підробити документи тощо. Інсайдерські загрози складно попередити та виявити.

Неправильна конфігурація серверів, хмарних сервісів, мережевого обладнання та ПЗ може призвести до вразливостей. Наприклад, слабкі паролі адміністратора, застаріле ПЗ, ліберальна політика доступу. Хакери активно сканують мережі на наявність таких дірок.

Передача конфіденційних даних та трафіку без шифрування створює ризик перехоплення та витоку інформації зловмисниками. Особливо вразливий трафік між офісами, філіалами, банкоматами та серверами банку.

Якщо зловмисники отримають фізичний доступ до пристроїв клієнта чи працівника банку, вони можуть скомпрометувати її: встановити шпигунське ПЗ,

переналаштувати, підключитись до мережі тощо. Це може відкрити хакерам шлях у корпоративну мережу банку.

Шахраї можуть застосовувати маніпуляції та психологічний тиск для отримання конфіденційної інформації від персоналу чи клієнтів банку. Наприклад, телефонні дзвінки від імені техпідтримки або прохання допомогти з мотивацією альтруїзму.

Для ефективного захисту потрібен комплексний підхід, що включає технічні рішення, політики, навчання персоналу та клієнтів. Безперервний моніторинг, аудит безпеки та вчасне реагування є запорукою мінімізації ризиків та наслідків кібератак на банки.

Проведений детальний аналіз звітів Держспецзв'язку та ряду ІТ-компаній щодо кіберінцидентів за останні роки [15]. Виявлено, що основними загрозами для банківської сфери є цільові атаки з використанням шкідливого ПЗ, фішинг, інсайдери та DDoS. Розроблено модель потенційного порушника, що включає 5 типів зловмисників: зовнішні хакери, хактивісти, кібершахраї, колишні та нинішні працівники, конкуренти. Детально опрацьовано їх мотивацію, наявні ресурси, ймовірні цілі атак та методи реалізації загроз. На основі цього розроблено систему захисту, яка поєднує технологічні (антивірус, фаєрволи, шифрування трафіку тощо) та організаційні (політики безпеки, аудити, навчання персоналу тощо) заходи протидії [15].

## 1.4 Алгоритм оцінки загроз для інформаційної безпеки банку

Оцінка небезпек для інформаційної безпеки банку - це важливий процес, який допомагає ідентифікувати потенційні загрози, яким піддається банк у сфері інформаційної безпеки. Цей процес допомагає банку розробити стратегії і заходи для зменшення ризику і вдосконалення захисту інформації клієнтів та власної інформації банку.

Алгоритм оцінки загроз для інформаційної безпеки банку можна подати у вигляді блок-схеми (рисунок 1.4).

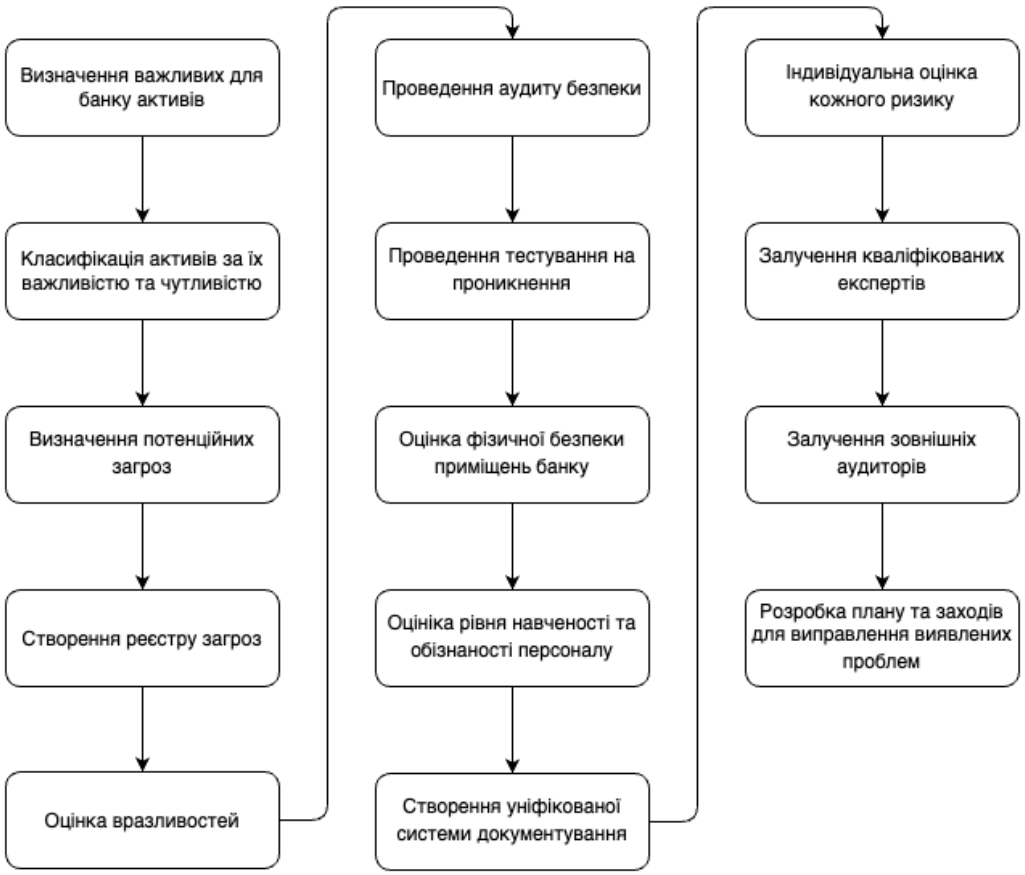


Рисунок 1.4 – Блок-схема алгоритму оцінки загроз для інформаційної безпеки в системах інтернет-банкінгу

Дана схема включає в себе наступні кроки:

– Визначення важливих для банку активів. Ідентифікація активів - це перший та дуже важливий крок у процесі оцінки загроз для інформаційної безпеки банку. Вони включають в себе усю інформацію, ресурси та компоненти, які є важливими для функціонування банку і можуть підлягати ризику:

1) фінансові дані клієнтів, особиста інформація клієнтів, внутрішні документи банку, технічна документація та інша конфіденційна інформація;

2) інформаційні системи та обладнання, які використовуються в банку. Це можуть бути сервери, комп'ютери, мережева інфраструктура, програмне забезпечення та інше;

3) процеси та послуги банку критичні для його функціонування. Зокрема, операції з клієнтами, обробка платежів, управління резервами.

4) персонал, який має доступ до важливих активів банку, інформації та систем, включаючи адміністраторів, працівників служби підтримки, менеджерів та інших працівників [24].

– Класифікація активів за їх важливістю та чутливістю. Це допоможе визначити, які активи потребують найвищого рівня захисту. Результатом даного кроку буде реєстр активів банку, в якому буде вказана вся інформація про ідентифіковані активи, включаючи їхню класифікацію та відповідальних за них працівників. Цей процес допоможе банку зрозуміти, які активи потребують захисту та які загрози можуть вплинути на них. На основі ідентифікації активів банк може розробити стратегію і заходи для забезпечення їхньої безпеки та захисту від можливих ризиків.

– Визначення потенційних загроз, які можуть вплинути на інформаційну безпеку банку. Ідентифікація загроз - це наступний важливий крок у процесі оцінки небезпек для інформаційної безпеки банку. Це можуть бути технічні загрози, такі як віруси і хакерські атаки, негативний вплив природних катастроф, економічні зміни, а також загрози з боку персоналу, такі як внутрішні погрози. Загрози представляють собою потенційні події або ситуації, які можуть призвести до порушень безпеки інформації банку. Ідентифікація загроз допомагає банку розпізнати, які конкретні ризики існують і як їх виявити та контролювати.

Кроки для ідентифікації загроз:

1) оцінка зовнішнього середовища, в якому діє банк, щоб визначити загрози, які можуть виникнути;

2) перегляд внутрішніх факторів, які можуть становити загрозу, включаючи дії або бездіяльність співробітників, недостатню кваліфікацію, внутрішні шахрайства;

3) визначення конкретних типів загроз, які можуть впливати на інформаційну безпеку банку. Серед них: кіберзлочинність, соціальна інженерія, природні лиха, технічні несправності, внутрішні загрози;

4) визначення можливих наслідків, які можуть виникнути внаслідок кожного типу загрози. Це може бути втрата даних, порушення конфіденційності, недоступність систем та послуг, фінансові втрати, репутаційні проблеми і інше;

5) оцінка ймовірності виникнення кожної загрози. Визначення ймовірності допоможе визначити, які загрози потребують найбільшого уваги.

– Створення реєстру загроз, в якому буде вказана вся інформація про ідентифіковані загрози, їхні типи, потенційні наслідки та ймовірність. На цьому кроці необхідно розглянути можливі взаємозв'язки між різними загрозами та активами банку, оскільки одна загроза може впливати на декілька активів або навпаки. Створення реєстру допомагає банку краще розуміти, з якими ризиками він має справу, і розробляти стратегії та заходи для їхнього управління та мінімізації.

– Оцінка вразливостей - це наступний важливий етап у процесі оцінки небезпек для інформаційної безпеки банку. Вразливості - це слабкі точки або недоліки в системах, процесах або заходах безпеки, які можуть бути використані зловмисниками для порушення інформаційної безпеки. Ідентифікація вразливостей допомагає визначити, де саме системи банку можуть бути найбільш вразливими на атаки та зловмисний доступ. Для реалізації цього кроку потрібно використовувати спеціалізовані інструменти та програми для сканування і аналізу інформаційних систем банку з метою виявлення потенційних вразливостей. Це може включати в себе перевірку на наявність застарілих програм, слабкі точки в мережевій інфраструктурі та інше.

– Проведення аудиту безпеки, включаючи огляд політик безпеки, процедур аутентифікації та авторизації, управління доступом. Аудит допомагає виявити вразливості в організаційних аспектах інформаційної безпеки.

– Проведення тестування на проникнення, щоб визначити, наскільки вразливості дійсно ефективні і чи є можливість отримання несанкціонованого доступу до систем та даних банку. Необхідно перевірити всі програмні продукти, які використовуються в банку, на предмет наявності вразливостей, інформація

про які може бути відома на діловому рівні. Після виявлення вразливостей, слід вимагати від виробників програмного забезпечення їх виправлення.

– Оцінка фізичної безпеки приміщень банку, а також контроль доступу до обладнання та серверів.

– Оцінка рівня навченості та обізнаності персоналу щодо безпеки та визначення можливих вразливостей, які можуть виникнути внаслідок недоліків у навчанні та вимогах безпеки. Потрібно врахувати вразливості, які можуть виникнути внаслідок діяльності третіх сторін, таких як підрядники або постачальники.

– Створення уніфікованої системи документування, в якій буде вказана вся інформація про виявлені вразливості, включаючи їхні характеристики та потенційні наслідки.

– Індивідуальна оцінка кожного ризику - це процес визначення ступеня небезпеки і визначення ймовірності виникнення небезпеки для інформаційної безпеки банку, а також оцінка наслідків, які можуть виникнути внаслідок цієї небезпеки. Оцінка ризику допомагає банку приймати обґрунтовані рішення щодо прийняття відповідних заходів безпеки та блокування ресурсів для зменшення ризику до прийнятного рівня.

Кроки для оцінки ризику:

1) після ідентифікації загроз та вразливостей банку потрібно поєднати ці дві інформації, щоб визначити, які вразливості можуть бути використані загрозами для створення ризику;

2) оцінка ймовірністі виникнення кожної загрози на основі історичних даних, аналізу середовища та інших факторів;

3) визначення можливих наслідків, які можуть виникнути внаслідок кожної загрози. Це може включати фінансові втрати, втрату репутації, порушення законодавства, втрату даних та інше. Для цього потрібно використати шкалу або систему рейтингу. Ризик розраховується як добуток ймовірності і наслідків. Наприклад, якщо ймовірність виникнення загрози

дорівнює 0,7 (70%) і наслідки відповідають рейтингу 4 (на шкалі від 1 до 5), то ризик дорівнює 0,7 * 4 = 2,8;

4) розподіл ризиків на категорії за їхнім рівнем серйозності або важливості. Наприклад, можна визначити ризики як високі, середні і низькі. Потрібно з'ясувати, які ризики є прийнятними для банку, а які необхідно зменшувати або уникати.

– Залучення кваліфікованих експертів для аналізу інформаційної безпеки та впровадження необхідних заходів захисту є важливим кроком. Залучення експертів у галузі інформаційної безпеки може бути важливим для забезпечення високого рівня захисту інформації та вирішення складних проблем. Експерти можуть надати цінні поради, використовувати свої знання та досвід для ідентифікації та вирішення загроз, а також допомогти банку у розробці та впровадженні ефективних стратегій і заходів безпеки.

Залучення незалежних консультантів або фахівців з інформаційної безпеки може допомогти визначити слабкі точки та ризики в існуючих системах та заходах безпеки. Вони можуть надати рекомендації щодо удосконалення безпеки.

– Залучення зовнішніх аудиторів для перевірки систем і процесів безпеки допоможе отримати об'єктивну оцінку стану інформаційної безпеки банку. Аудитори можуть виявити вразливості та рекомендувати заходи для їх виправлення. Багато компаній спеціалізуються на наданні послуг інформаційної безпеки, таких як виявлення загроз, моніторинг безпеки, реагування на інциденти та інше. Банк може укласти угоду з такими службами для забезпечення надійного захисту. Експерти можуть проводити навчання та семінари для персоналу банку, допомагаючи підвищити рівень обізнаності та навичок щодо інформаційної безпеки. Банк може вступити в партнерство з організаціями, які спеціалізуються на інформаційній безпеці, для обміну досвідом та інформацією про загрози. Експерти можуть допомогти у розробці стратегії та політики інформаційної безпеки, а також у впровадженні та моніторингу цих документів [20].

– Розробка плану та заходів для виправлення виявлених проблем та підвищення рівня безпеки інформації. Потрібно сформувати рішення щодо прийняття відповідних заходів для управління ризиками, розробити план дій для зменшення ризику. Цей план може включати в себе впровадження технічних та організаційних заходів, навчання персоналу та інші заходи безпеки. Після впровадження заходів моніторингу ризиків потрібно розглянути можливі зміни в середовищі, періодично оновляти оцінку ризиків та плани дій.

## 1.5 Правове регулювання захисту банківської інформації

Захист банківської інформації в Україні нормується переліком нормативно-правових актів, найважливішими з яких можна назвати:

Закон України "Про банки і банківську діяльність" визначає зобов’язання банками забезпечення конфіденційності банківської інформації та даних, пов'язаних з діяльністю та фінансовим станом клієнта, які стали відомими банку під час обслуговування клієнта та взаємодії з ним під час надання банківських послуг. Закон також встановлює відповідальність за порушення вимог щодо розкриття та використання банківської інформації.

Закон України "Про захист персональних даних" визначає правові основи захисту персональних даних в Україні під час їх обробки. Згідно закону, банки як володільці персональних даних клієнтів зобов'язані вживати організаційні та технічні заходи для захисту даних від незаконної обробки та доступу, а також запобігати випадковій втраті, знищенню чи пошкодженню даних.

Закон України "Про електронні документи та електронний документообіг" регулює питання електронного документообігу, в тому числі в банківській сфері. Закон визначає вимоги щодо забезпечення цілісності, автентичності та збереження електронних документів шляхом використання електронного цифрового підпису та засади використання електронних довірчих послуг.

Закон України "Про електронну комерцію" встановлює правові основи надання інформаційних послуг в електронній комерції. Зокрема, визначає

обов'язок провайдерів інформаційних послуг вживати заходів щодо захисту інформації від незаконного доступу, знищення, модифікації, блокування та інших незаконних дій.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" визначає основні засади забезпечення захисту інформації в ІТС, права та обов'язки володільців і розпорядників інформації щодо захисту інформації, а також відповідальність за порушення законодавства у цій сфері.

Закон України "Про телекомунікації" встановлює зобов'язання операторів телекомунікацій вживати технічних і організаційних заходів для забезпечення: цілісності телекомунікаційної мережі; захисту інформації з обмеженим доступом під час надання телекомунікаційних послуг; захисту від несанкціонованого доступу до телекомунікаційних мереж.

Також оператори мають забезпечувати конфіденційність інформації, отриманої в процесі діяльності.

Закон України "Про Національний банк України" визначає повноваження НБУ у сфері банківського регулювання та нагляду. Зокрема, НБУ уповноважений встановлювати вимоги до банків щодо захисту електронних банківських документів, інформації про клієнтів, а також інших видів банківської інформації.

Стандарт PCI DSS (Payment Card Industry Data Security Standard) є міжнародним стандартом безпеки даних індустрії платіжних карток, який є обов'язковим для організацій, що приймають, обробляють, зберігають або передають дані держателів платіжних карток.

Стандарт складається з 12 вимог щодо: налаштування мережі і систем, захисту даних, аудиту та моніторингу, тестування системи безпеки, керування доступом тощо. Всі банки в Україні, які працюють з платіжними картками, мають проходити аудит та сертифікацію на відповідність PCI DSS.

Стандарт ISO 27001 визначає вимоги до систем менеджменту інформаційної безпеки. Він є загальновизнаною міжнародною нормою у цій сфері. Стандарт містить 114 контрольних цілей та заходів у таких сферах:

Сертифікація банку на відповідність ISO 27001 є добровільною, проте демонструє дотримання банком найкращих міжнародних практик у сфері управління інформаційною безпекою.

Окремо слід відзначити вимоги щодо захисту банківської інформації, які містяться в законодавстві про протидію легалізації злочинних доходів та фінансуванню тероризму. Зокрема Закон України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення" містить низку вимог до банків щодо захисту інформації, яка стосується фінансових операцій клієнтів, а також інформації, отриманої в процесі ідентифікації клієнтів.

Для гарантування незмінності та прозорості фінансових транзакцій пропонується інтеграція приватного блокчейну між банком та клієнтами. Кожна транзакція буде записуватися в розподілений реєстр у вигляді блоків, пов'язаних криптографічно. Це убезпечить від несанкціонованих змін даних з боку зловмисників. На основі блокчейну можлива також реалізація смарт-контрактів для автоматизації банківських операцій за заздалегідь заданими правилами.

Отже, питання захисту банківської інформації та інформаційної безпеки банків є предметом пильної уваги законодавця та регуляторів. Банки зобов'язані дотримуватися значного обсягу нормативних вимог у цій сфері та проходити регулярні перевірки контролюючих органів. Відповідність законодавству є обов'язковою умовою здійснення банківської діяльності в Україні [4,8,11,15].

# 2 РОЗРОБЛЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНТЕРНЕТ-БАНКІНГУ

## 2.1 Модель порушника безпеки систем інтернет-банкінгу

Побудова адекватної моделі потенційних загроз є надзвичайно важливим етапом у проектуванні комплексної системи кібербезпеки інтернет-банкінгу. Така модель дозволяє врахувати можливі способи, методи та мотивацію атак з боку зловмисників. Серед основних типів порушників слід виділити зовнішніх хакерів, колишніх працівників, конкурентів, кіберзлочинців, зловмисних інсайдерів, скріпт-кідді, хактивістів та навіть кібертерористів. Вони можуть застосовувати широкий арсенал методів - від фішингу до складних APT-атак. Метою є крадіжка грошей, даних, завдання фінансових збитків або репутаційної шкоди. Врахування всього спектру загроз дає змогу спроектувати ефективну систему протидії можливим атакам.

Серед основних типів порушників безпеки систем інтернет-банкінгу можна виділити:

– Це особи або групи, які зламують системи інтернет-банкінгу з метою збагачення, демонстрації своїх можливостей, або просто задля розваги чи виклику. Вони можуть застосовувати різноманітні методи вторгнення - від сканування мережі та експлуатації вразливостей до фішингових атак та використання шкідливого ПЗ. Їх мотивація полягає у крадіжці грошей з банківських рахунків, отриманні особистих даних клієнтів або порушенні роботи системи. (Зовнішні хакери)

– Це особи, які раніше працювали в банку та мали доступ до внутрішніх систем і конфіденційної інформації. Після звільнення вони можуть використовувати отримані знання та дані для злому системи або продажу цієї інформації стороннім особам. Такі інсайдери становлять серйозну загрозу, оскільки добре обізнані про внутрішні процедури та налаштування систем банку.

– Це інші банки чи фінансові установи, які бачать ваш банк конкурентом і намагаються отримати несанкціонований доступ до ваших систем для збору інформації, порушення роботи або нанесення репутаційної шкоди. Вони можуть проводити складні цілеспрямовані кібератаки, вербувати ваших працівників або поширювати неправдиву інформацію. Метою є послаблення позицій конкурента на ринку.

– Організовані злочинні угруповання, які спеціалізуються на кібератаках з метою фінансового збагачення. Вони можуть мати в розпорядженні значні ресурси, досвідчених хакерів і розвинену інфраструктуру для проведення складних атак на фінансові установи. Їх метою є максимальне розкрадання грошових коштів з рахунків та систем банку.

– Працівники банку, які умисно порушують політики безпеки зсередини. Вони можуть красти дані, проводити несанкціоновані операції, надавати доступ стороннім особам або заражати системи шкідливим ПЗ. Такі інсайдери складно виявити, а їх дії можуть завдати значної шкоди.

– Молоді та недосвідчені хакери, які часто атакують системи заради хвастощів, а не для отримання фінансової вигоди. Вони використовують готові інструменти та поширені методи, такі як DDoS-атаки, сканування портів, експлуатація типових вразливостей. Не маючи глибоких навичок, вони можуть викликати збої в роботі, але рідко досягають серйозних зламів системи.

– Особи або угруповання, які проводять кібератаки заради просування своїх ідей та цінностей. Вони можуть атакувати банки та фінансові установи з ідеологічних міркувань або для того, щоб завдати економічної шкоди "ворогам". Хактивісти часто прагнуть максимальної розголосу своїх атак.

– Злочинці або екстремістські угруповання, метою яких є завдання шкоди суспільству шляхом кібератак на критичну інфраструктуру та інформаційні системи. Вони можуть атакувати банки, щоб дестабілізувати фінансову систему країни, посіяти паніку, завдати збитків економіці. Їх атаки носять ідеологічний характер.

Усі ці типи зловмисників можуть застосовувати широкий спектр методів та засобів для атак на системи інтернет-банкінгу. Такі як: соціальна інженерія, фішинг, викрадення cookie-файлів, MITM атаки, встановлення шкідливого ПЗ, аналіз трафіку, DDoS атаки, експлуатація вразливостей ПЗ, атаки на web-додатки, викрадення баз даних, атаки side-channel, інсайдерські атаки, атаки на хмарні сервіси та API, та інші. Детальніше про кожен з методів.

Соціальна інженерія передбачає маніпулювання людьми з метою отримання конфіденційної інформації або доступу до систем. Це один з найпоширеніших методів атак на інтернет-банкінг. Зловмисники можуть вдавати працівників банку по телефону або електронній пошті, стверджуючи про наявність проблем з безпекою і вимагаючи паролі чи OTP коди для їх вирішення. Інший поширений метод - фішинг. Його мета - спрямувати користувача на шахрайський сайт, схожий на справжній сайт банку, і виманити його дані. Також застосовується таргетований фішинг з використанням персональної інформації жертви для підвищення довіри. Соціальна інженерія вимагає від зловмисників психологічних навичок та глибокого розуміння людської природи. Щоб успішно протидіяти їй, користувачі мають бути обізнаними щодо можливих способів маніпуляції та перевіряти достовірність будь-яких несподіваних прохань надати конфіденційну інформацію.

Як зазначено вище, фішинг використовує соціальну інженерію для виманювання у користувачів конфіденційних даних. Зловмисники створюють підроблені сайти, майже ідентичні справжнім, і розсилають посилання на них через електронні листи та SMS, видаючи їх за офіційні повідомлення від банку. Коли користувач заходить на такий сайт і вводить свої дані, вони потрапляють до шахраїв. Різновидом фішингу є вішинг - атака через телефонний дзвінок від імені банку. Щоб уникнути фішингу, слід уважно перевіряти адреси сайтів у посиланнях та ніколи не вводити дані через ненадійні джерела.

Cookie-файли містять дані сесії користувача і можуть використовуватися для авторизації в системі без необхідності вводити пароль. Зловмисники можуть викрасти cookie з браузера жертви різними способами: через шкідливе ПЗ,

перехоплення незашифрованого трафіку, експлуатацію вразливостей сайту тощо. Володіння cookie дозволяє отримати доступ до рахунку користувача. Сучасні браузери блокують доступ сторонніх сайтів до cookie, але користувачам слід бути пильними при роботі з інтернет-банкінгом на публічних пристроях.

При атаці типу «людина посередині» (man-in-the-middle) зловмисники перехоплюють трафік між користувачем і сервером інтернет-банкінгу, дозволяючи їм читати, модифікувати та блокувати дані. Це може відбуватися шляхом компрометації Wi-Fi мережі, отруєння ARP кешу, перехоплення на маршрутизаторах тощо. Для захисту слід використовувати надійне шифрування трафіку за допомогою SSL/TLS.

Шкідливе ПЗ, таке як трояни, keylogger'и, програми-вимагачі, може таємно встановлюватися на пристрій жертви під час відвідування зламаних сайтів, відкриття вкладень електронної пошти тощо. Воно здатне перехоплювати введення користувача, робити скріншоти, викрадати файли cookie та паролі, щоб передати їх зловмисникам. Для захисту потрібно використовувати антивірусне ПЗ, не встановлювати програми з ненадійних джерел, регулярно сканувати на наявність вірусів.

Зловмисники можуть перехоплювати і аналізувати мережевий трафік на предмет наявності цінної інформації, такої як паролі, номери рахунків, персональні дані тощо. Аналіз трафіку можливий в незахищених Wi-Fi мережах, через компрометацію мережевого обладнання, використання сниферів на суміжних вузлах. Для протидії потрібно застосовувати надійне шифрування трафіку, використовувати VPN з'єднання, уникати публічних точок доступу Wi-Fi при роботі зі своїм інтернет-банкінгом.

Розподілені атаки на відмову в обслуговуванні (DDoS) паралізують роботу систем інтернет-банкінгу шляхом перевантаження серверів величезною кількістю запитів з різних джерел. Це призводить до тимчасової недоступності сайту та сервісів банку для клієнтів. DDoS може використовуватися для відволікання уваги безпеки під час іншої атаки чи заподіяння прямих фінансових збитків. Захист передбачає використання спеціальних сервісів захисту від DDoS

на рівні провайдера, налаштування мережевого та апаратного обладнання, масштабування ресурсів серверів.

Уразливості програмного забезпечення, такі як SQL ін'єкції, cross-site scripting (XSS), використання пошкоджених файлів тощо, можуть дозволити зловмисникам виконувати шкідливий код, обходити автентифікацію, отримувати несанкціонований доступ до даних. Своєчасне оновлення ПЗ, тестування на проникнення, аналіз коду на наявність вразливостей допомагає убезпечити систему від подібних атак.

Web-додатки інтернет-банкінгу можуть піддаватися різноманітним атакам, включаючи сканування, SQL-ін'єкції, підбір параметрів, тестування на проникнення тощо. Мета - знайти вразливості в коді, логіці та архітектурі додатку, які дозволять отримати несанкціонований доступ, обійти авторизацію, виконати шкідливі дії. Захист вимагає ретельного тестування безпеки додатків, перевірки вхідних даних, аутентифікації та авторизації користувачів, обмеження доступу.

Зловмисники можуть атакувати сервери баз даних інтернет-банкінгу, щоб отримати конфіденційну інформацію клієнтів - персональні дані, номери рахунків, логіни та паролі тощо. Після крадіжки бази даних вони намагаються розшифрувати та проаналізувати її вміст для подальшого використання або продажу цієї інформації. Для захисту баз даних потрібно використовувати шифрування даних, обмежувати та контролювати доступ до БД, регулярно

Side-channel атаки використовують аналіз побічних сигналів, таких як час виконання операцій, споживання електроенергії процесором, електромагнітне випромінювання, звук, вібрації тощо, для отримання інформації. Це може допомогти зловмисникам визначити вразливості системи, відновити криптографічні ключі для дешифрування даних. Захист передбачає використання спеціального обладнання та алгоритмів із захистом від side-channel атак.

Інсайдери - працівники банку або підрядники, які мають доступ до внутрішніх систем - можуть навмисно або випадково порушити політики

безпеки. Вони здатні красти дані, здійснювати шахрайські операції, надавати стороннім особам доступ до систем, поширювати шкідливе ПЗ. Ключовими заходами протидії є ретельна перевірка персоналу, розмежування прав доступу, моніторинг активності, навчання з питань безпеки.

Якщо банк використовує хмарні сервіси або API для надання функцій інтернет-банкінгу, зловмисники можуть атакувати саме їх, щоб отримати доступ до даних або можливості керування системою. Необхідно ретельно налаштовувати права доступу та автентифікацію для API, шифрувати дані, використовувати міжмережеві екрани, слідкувати за конфігурацією хмарних сервісів.

Якщо зловмисник отримає фізичний доступ до пристрою користувача або працівника банку, він може скомпрометувати його різними способами - встановити на нього шпигунське ПЗ, зламати BIOS, підключитися до мережі тощо. Це відкриває шлях для подальшого проникнення в корпоративну мережу та системи банку. Для захисту критично важливо використовувати надійне шифрування дисків, унеможливити завантаження сторонніх ОС та ПЗ, обмежити фізичний доступ до пристроїв.

Нульовий день - це раніше невідома вразливість в ПЗ, для якої ще немає заплатки безпеки. Зловмисники можуть використовувати нульові дні для атак на системи інтернет-банкінгу, поки вразливість не буде виправлено. Важливо оперативно оновлювати всі компоненти ПЗ після виходу оновлень безпеки, щоб уникнути компрометації через нульові дні.

Зловмисники можуть намагатися "зламати" криптографічні алгоритми, які використовуються в інтернет-банкінгу для шифрування трафіку та даних. Це може включати криптоаналіз, підбір ключів, використання вразливостей реалізації алгоритмів тощо. Для захисту потрібно використовувати сучасні стійкі алгоритми, такі як AES, RSA, згідно рекомендацій НБУ та інших регуляторів.

Зловмисники можуть збирати цінну інформацію про цілі атак з відкритих джерел - сайту банку, тендерів, соцмереж, публічних реєстрів тощо. Це допомагає краще підготуватися до атаки, виявити слабкі місця в інфраструктурі,

скласти профілі працівників. Банкам варто мінімізувати обсяг конфіденційної інформації у відкритому доступі, використовувати приховані сервери та домени.

Зловмисники можуть атакувати постачальників та партнерів банку, щоб отримати доступ до його внутрішніх систем чи даних через ланцюжок взаємодій. Наприклад, зламавши IT компанію, яка обслуговує банк, можна отримати доступ до його мережі. Потрібно ретельно перевіряти надійність партнерів, обмежувати їх доступ, шифрувати дані.

Зловмисники можуть вдавати реальних клієнтів банку, використовуючи викрадені чи підроблені документи для ідентифікації. Це дозволяє їм відкривати рахунки, отримувати кредити, картки для подальших шахрайських операцій. Банкам необхідно ретельно перевіряти особу клієнтів, використовувати біометричні дані, аналізувати ризики [12].

Шахрайство через call-центри. Оскільки call-центри банків мають доступ до персональних даних і можуть ініціювати фінансові операції, вони можуть стати об'єктом шахрайства. Зловмисники можуть підкуповувати операторів, здійснювати соціальну інженерію по телефону, використовувати викрадені дані клієнтів для незаконних операцій через call-центр. Потрібно ретельно перевіряти операторів, обмежувати їх доступ, записувати усі дзвінки, аналізувати транзакції.

Кібертерористи або екстремістські угрупування можуть здійснювати атаки на банки як частину своєї терористичної діяльності, щоб заподіяти шкоду економіці чи посіяти хаос. Це вимагає від банків підвищеної уваги до кібербезпеки як частини протидії фінансуванню тероризму та взаємодії з правоохоронними органами.

Отже, зловмисники мають в своєму арсеналі велику кількість методів для атак на системи інтернет-банкінгу. Побудова ефективного захисту вимагає комплексного підходу, що включає технічні, організаційні та правові заходи для протидії усім можливим векторам атак. Постійний моніторинг загроз та вдосконалення захисту є запорукою безпеки інтернет-банкінгу [11].

## 2.2 Системи виявлення та моніторингу порушень безпеки

Інформаційна безпека є надзвичайно важливою у сфері інтернет-банкінгу, оскільки вона забезпечує захист конфіденційних даних клієнтів та їхніх фінансових активів. Першим кроком має бути надійна аутентифікація користувачів за допомогою сильних паролів, ПІН-кодів, біометричних даних тощо. Це дозволить переконатися, що тільки авторизовані особи отримують доступ до системи. Ще одним важливим елементом є шифрування всіх даних під час їх передачі між користувачем та банком, наприклад, за допомогою протоколу HTTPS.

Крім того, банки повинні приділяти значну увагу захисту від фішингових атак, які є поширеною загрозою в інтернеті. Для цього можна застосовувати поєднання технологічних рішень, таких як моніторинг підозрілої активності, та навчання клієнтів не розголошувати свої дані через ненадійні канали зв'язку. Використання двофакторної аутентифікації також ускладнює реалізацію атак фішингу.

Банкам варто запровадити комплексний моніторинг активності користувачів та аномалій, що можуть вказувати на спроби несанкціонованого доступу. У разі виявлення підозрілої поведінки система має негайно сповіщати відповідні підрозділи безпеки.

Інфраструктура банку, включаючи сервери та мережеве обладнання, також потребує ретельного захисту як від зовнішніх загроз, так і від внутрішніх, зокрема неавторизованих дій персоналу. Для цього доцільно застосовувати комплексні рішення, що включають фізичну охорону, мережеву безпеку, жорсткий контроль доступу, резервне копіювання, оновлення ПЗ тощо.

Загалом, гарантування безпеки в інтернет-банкінгу вимагає постійної уваги та вдосконалення існуючих заходів. Банки мають регулярно оцінювати нові загрози та ризики і модернізувати свої системи безпеки відповідно до них. Лише комплексний та багаторівневий підхід дозволить мінімізувати ризики та забезпечити надійний захист інформації в інтернет-банкінгу. Розроблено проект

політики інформаційної безпеки з урахуванням виявлених загроз та пріоритетів захисту.

Спочатку проведено інвентаризацію інформаційних активів та їх пріоритезацію за критичністю для бізнесу. Далі на основі розробленої раніше моделі порушника ідентифіковано можливі сценарії атак та оцінено відповідні ризики. З урахуванням цього сформовано вимоги та контрзаходи у сферах управління доступом, фізичної та мережевої безпеки, захисту даних, інцидент-менеджменту тощо.

## 2.3 Криптографічні методи захисту конфіденційних даних

Криптографія - це наука про математичні методи захисту інформації, що забезпечують конфіденційність, цілість та автентичність даних. Вона включає:

– Конфіденційність це забезпечення доступності лише конкретної інформації групі людей, на яку він спрямований. Порушення цієї категорії називається крадіжкою або розголошенням інформації.

– Цілісність це впевненість у тому, що інформація на даний момент знаходиться у своїй оригінальній формі, тобто не було несанкціонованого доступу під час зберігання чи передачі. Дії, що порушують цю категорію, називаються вигадками в пресі.

– Надійність (автентичність) це впевненість у тому, що джерело інформації є правильною особою, яка використовує інформацію. Порушення в цій категорії, також відомі як підробка, пов’язані з автором повідомлення.

Шифрування - процес перетворення звичайного тексту або інформації у незрозумілий формат (зашифрований текст), що може бути розшифрований лише з допомогою правильного ключа або паролю. У контексті інтернет-банкінгу шифрування є важливою складовою інформаційної безпеки, оскільки воно захищає дані, які передаються між користувачем і банком під час онлайн-транзакцій та взаємодії з банківськими системами.

У сучасному світі криптографія набуває все більшого значення через широке використання комп’ютерних мереж та Інтернету для обміну конфіденційною інформацією – онлайн-банкінг, електронна комерція, урядові дані тощо.

Основним методом криптографії є шифрування - перетворення вихідних даних (відкритого тексту) у зашифрований текст за допомогою спеціального алгоритму та ключа. Розшифровка відбувається за допомогою наявного ключа.

Існують симетричні алгоритми шифрування, що вибирають один ключ (AES), та асиметричні, що застосовують пару ключів (RSA). Розширений стандарт шифрування (AES) — це симетричний блоковий алгоритм шифрування, прийняте як стандарт урядом США в результаті конкуренції, здійснюється між технічними закладами. замінити старі дані. Стандарт шифрування (DES) більше не відповідає потребам мережі .Алгоритм AES представляє блоки даних як двовимірні байти. Усі операції виконуються над окремими байтами масиву.

RSA (Rivest, Shamir і Adleman) – це метод шифрування, який використовує відкритий ключ і базується на складності обчислень, пов'язаній з розкладанням великих цілих чисел на прості множники [20].

Алгоритм RSA складається із чотирьох етапів: генерації ключів, передачі ключів, шифрування та дешифрування. Криптографічні системи із відкритим ключем оперують за допомогою односторонніх функцій.

Також для незалежних стовпців і рядків схематично види шифрування вказано на рисунку 2.1.

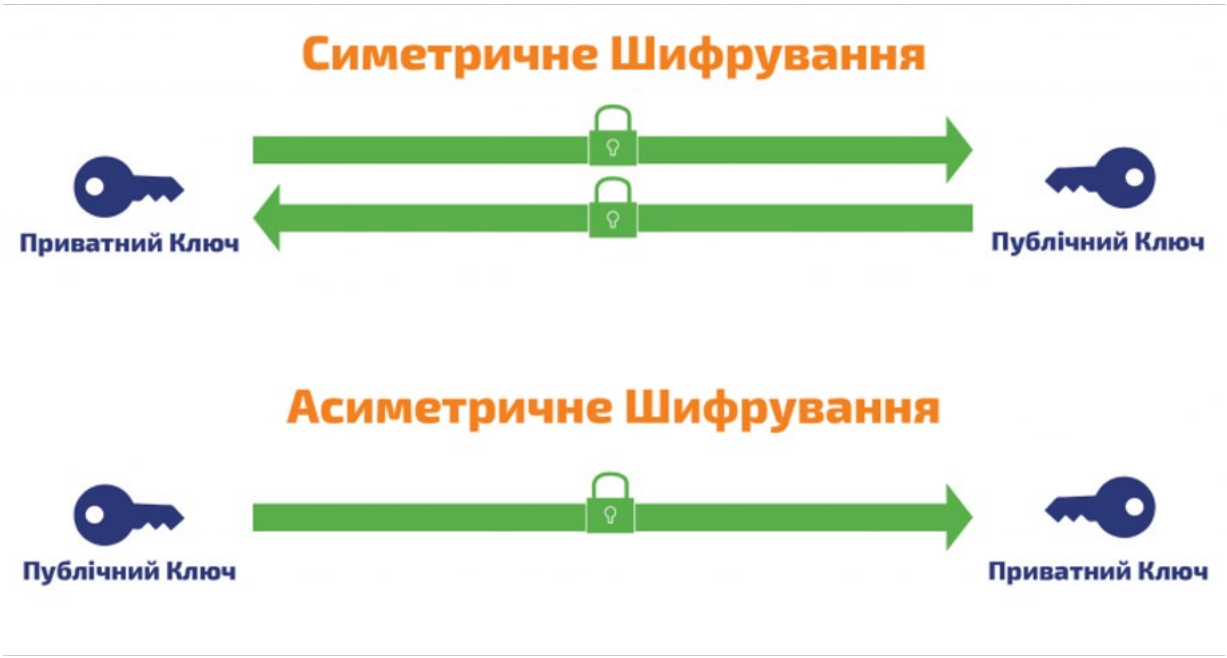


Рисунок 2.1 – Види шифрування

Останнім часом криптографія стикається з новими викликами через розвиток технологій. Поява квантових комп'ютерів може зламати існуючі алгоритми. Також з'являються нові кібератаки на криптосистеми.

Тому постійний розвиток криптографії є вкрай важливим для забезпечення безпеки даних у цифровому світі. Подальші дослідження дозволять створити надійніші алгоритми шифрування в майбутньому [7,9].

## 2.4 Організаційні заходи збереження інформаційної безпеки

Розробка політики інформаційної безпеки.

Політика інформаційної безпеки є базовим документом, який визначає загальну стратегію та підходи банку в цій сфері. Вона має чітко встановлювати цілі, принципи, структуру управління ІБ, розподіл ролей та відповідальності, а також конкретні вимоги щодо захисту інформації.

Створення відділу інформаційної безпеки.

Ефективна організація інформаційної безпеки в банку вимагає створення спеціального структурного підрозділу та посади відповідального за ІБ на рівні топ-менеджменту:

Відділ ІБ відповідає за поточне адміністрування заходів безпеки, моніторинг, реагування на інциденти, тестування тощо.

CISO (Chief Information Security Officer) очолює відділ ІБ та координує зусилля з інформаційної безпеки на рівні всього банку.

CISO підпорядковується безпосередньо керівництву банку та має вплив на прийняття стратегічних рішень в сфері ІБ.

Важливо забезпечити належне фінансування, кадрове забезпечення та повноваження відділу ІБ для ефективного виконання функцій.

Управління інцидентами ІБ та моніторинг.

Потрібно розробити чіткі плани реагування на можливі інциденти ІБ, такі як витік даних, DDoS атаки, цільові атаки тощо.

Для виявлення інцидентів в режимі реального часу створюється Центр моніторингу ІБ, який аналізує попередження систем захисту, журнали подій, звіти про порушення та ін.

Підвищення обізнаності персоналу в сфері ІБ.

Усі співробітники банку мають регулярно проходити навчання та тренінги з питань інформаційної безпеки. Необхідно інформувати персонал про поточні загрози та тренди в сфері кібербезпеки. Деякі теми для навчання:

– Політики та процедури інформаційної безпеки в банку.
– Загрози соціальної інженерії та фішингу. Як розпізнавати шахрайство.
– Безпечне використання електронної пошти та Інтернету.
– Правила роботи з конфіденційними даними та персональними даними клієнтів.
– Класифікація та позначення інформації.
– Вимоги щодо паролів та безпечного доступу в системи.
– Застереження при роботі з мобільними пристроями та віддаленим доступом.

Навчання має бути регулярним та оновлюваним. Періодично треба проводити перевірки знань персоналу з питань ІБ.

Аудит інформаційної безпеки

Регулярний аудит інформаційної безпеки дозволяє оцінити реальний стан справ та виявити недоліки в існуючих заходах захисту. Рекомендовані види аудиту:

Аудит відповідності політикам та стандартам ІБ - перевірка дотримання існуючих вимог і процедур безпеки. Технічний аудит ІТ-інфраструктури та інформаційних систем - пошук вразливостей, перевірка конфігурації. Тестування на проникнення - спроба зламати системи захисту, щоб оцінити їх стійкість. Аудит кібер-гігієни - аналіз безпечної поведінки персоналу, дотримання правил ІБ в роботі. Аудит третіх сторін - оцінка безпеки підрядників, постачальників та бізнес-партнерів.

За результатами аудиту складається звіт з рекомендаціями, на основі якого приймаються рішення щодо вдосконалення системи захисту інформації.

Контроль фізичного доступу

Потрібно обмежити та жорстко контролювати фізичний доступ до критично важливих об'єктів інфраструктури: серверних, комірок зберігання резервних копій, приміщень банкоматів тощо. Заходи контролю включають:

Електронні системи контролю та управління доступом з використанням карток, біометрії. Відеоспостереження, охорона периметру та внутрішніх зон. Обмеження доступу за принципом мінімальних привілеїв - тільки для авторизованих осіб з повноваженнями. Ведення журналів відвідувань. Використання сигналізації та датчиків руху.

Регулярний аудит прав доступу та перевірка ідентифікації відвідувачів.

Розробка планів забезпечення безперервності бізнесу та відновлення після аварій

Банки повинні бути готові ефективно реагувати на надзвичайні ситуації, такі як стихійні лиха, тривалі збої в роботі систем, пожежі тощо.

Регулярне тестування та оновлення планів дозволяє підтримувати готовність до можливих аварійних ситуацій.

Створення захищеної ІТ-архітектури

При проектуванні IT-інфраструктури банку потрібно реалізовувати принципи безпечної архітектури: Сегментація мережі на зони (демілітаризована зона, зона баз даних, внутрішня локальна мережа тощо). Обмеження з'єднань та контроль доступу між сегментами на основі правил міжмережевого екрану. Розгортання систем захисту на межах мережевих сегментів (IDS/IPS, антивірус, шлюзи безпеки). Шифрування внутрішнього трафіку між вузлами інфраструктури. Використання віртуалізації та сегментації для ізоляції процесів. Реалізація концепції нульового довіри до внутрішніх ресурсів (zero trust architecture).

Така архітектура ускладнює рух загроз всередині мережі та пом'якшує наслідки атак.

Отже, організаційні заходи є критично важливою складовою забезпечення інформаційної безпеки в банках. Вони мають поєднуватися з технічними засобами захисту для створення надійної багаторівневої системи.

### 2.5 Навчання персоналу з питань кібербезпеки

Навчання має бути регулярним та оновлюватися відповідно до нових загроз. Рекомендується проводити тренінги та освітні заходи щонайменше раз на квартал. Особливу увагу слід приділити навчанню щодо фішингових атак, оскільки вони є однією з найпоширеніших загроз для користувачів інтернет-банкінгу. Співробітники мають навчитися розпізнавати фішингові листи та повідомлення.

Персонал повинен знати основні правила кібергігієни - сильні паролі, двофакторна автентифікація, оновлення програмного забезпечення, обережність при завантаженні файлів та відвідуванні сайтів. Слід пояснити співробітникам, як безпечно користуватися Wi-Fi мережами, щоб уникнути перехоплення даних. Регулярно нагадувати персоналу про ризики клікання на підозрілі посилання, відкриття файлів від невідомих відправників тощо. Проводити тестування та симуляції фішингових атак, щоб перевірити готовність співробітників.

Організовувати навчання щодо новітніх методів соціальної інженерії та кіберзлочинів. Забезпечити персонал чіткими інструкціями, як реагувати у разі підозри на компрометацію облікових даних або шахрайство. Проводити внутрішні тренінги щодо політик та процедур кібербезпеки банку. Запрошувати зовнішніх експертів для проведення спеціалізованих тренінгів з актуальних тем.

Стимулювати співробітників повідомляти про підозрілу активність та винагороджувати за виявлені вразливості. Поширювати інформаційні бюлетені та пам'ятки з основ кібергігієни серед персоналу. Залучати керівництво до просування культури кібербезпеки в організації.

# 3 КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ БАНКІВСЬКОЇ МЕРЕЖІ

## 3.1 Розробка та впровадження системи захисту інформації

Системи захисту інформації в інтернет-банкінгу є надзвичайно важливими для забезпечення безпеки фінансових транзакцій та конфіденційності клієнтських даних в онлайн-середовищі. Ось деякі основні складові інформаційної безпеки в інтернет-банкінгу:

Перший рівень захисту це аутентифікація користувача. Користувачі повинні підтверджувати свою ідентичність за допомогою паролів, PIN-кодів, біометричних даних (відбитків пальців, розпізнавання обличчя і т. д.) та інших методів аутентифікації. Аутентифікація користувача - це процес перевірки і підтвердження ідентичності особи, яка намагається отримати доступ до певних ресурсів, системи або послуги. У контексті інтернет-банкінгу аутентифікація користувача виконується для того, щоб забезпечити безпеку фінансових транзакцій та конфіденційність клієнтських даних. Ось деякі способи аутентифікації користувачів у інтернет-банкінгу:

Користувачі вводять унікальні паролі, які повинні бути складними і важкими для вгадування. Добре практикувати регулярну зміну паролів і не використовувати один пароль для різних сервісів. Користувачі вводять персональний ідентифікаційний номер (PIN) для доступу до свого банківського облікового запису чи карти. Деякі системи інтернет-банкінгу використовують біометричну аутентифікацію, таку як відбитки пальців, розпізнавання обличчя, сканування очей і т. д.

Користувачі отримують одноразові паролі (OTP) через SMS, мобільний додаток або апаратний пристрій, які вони використовують для підтвердження своєї ідентичності під час входу в систему або здійснення транзакцій. Для додаткового рівня безпеки користувачі можуть використовувати , PINA, де вони мають поєднувати, наприклад, пароль і одноразовий код для входу. Користувачі можуть використовувати смарт-карти з чіпами для отримання доступу до

банківських послуг. Деякі банки використовують технології розпізнавання голосу для аутентифікації користувачів. Важливо зауважити, що безпека інтернет-банкінгу вимагає комбінації цих методів та постійної актуалізації інструментів аутентифікації, оскільки кіберзлочинці постійно шукають нові способи атаки. Всі дані, що передаються між користувачем і банком через інтернет, мають бути зашифровані. Зазвичай для цього використовується протокол HTTPS, який використовує SSL або TLS для захисту інформації.

Основні аспекти шифрування в інтернет-банкінгу включають наступне: Захист від фішингу - це важливий аспект безпеки в інтернет-банкінгу, оскільки атаки фішингу можуть призвести до втрати особистої інформації та фінансових засобів клієнтів. Фішинг - це вид атаки, при якому злочинці намагаються видати себе за довірене джерело, таке як банк чи інший сервіс, для того, щоб вивести користувачів із запитом на надання конфіденційної інформації, такої як паролі, номери карток, пін-коди і т. д.

Банки повинні надавати освіту своїм клієнтам і наголошувати на важливості неприйняття запитів на конфіденційну інформацію через недовірені канали, такі як електронні листи чи SMS. Користувачам слід перевіряти джерело будь-яких повідомлень, що надходять від банку. Це може бути зроблено шляхом телефонних дзвінків на вказані контакти на веб-сайті банку, але не через номери, вказані в сумнівних повідомленнях. Користувачам слід завжди перевіряти URL веб-сайту банку та впевнитися, що вони перебувають на офіційному і безпечному сайті. Важливо використовувати антивірусне програмне забезпечення та антиспам для фільтрації сумнівних повідомлень та веб-сторінок.

Використання 2FA може зробити атаки фішингу менш успішними, оскільки навіть якщо злочинець отримає пароль, він не зможе отримати доступ без додаткового аутентифікаційного фактора. Банки можуть використовувати інструменти моніторингу доменів, щоб виявити схожі або фішингові домени, які намагаються імітувати їхній офіційний веб-сайт. Рекомендується розробити та дотримуватися строгих політик використання електронної пошти для захисту від спаму та фішингу [13].

Захист від фішингу вимагає поєднання технологічних рішень і освіти користувачів. Банки повинні постійно бути бджолами щодо нових методів атак і намагатися попередити їх, а також надавати клієнтам інструменти та рекомендації для захисту своєї інформації. Банк моніторить активність користувачів, таку як вхід в систему, проведення фінансових транзакцій, зміна налаштувань облікового запису тощо. Система моніторингу повинна мати можливість виявити аномальні патерни або поведінку користувачів, які можуть свідчити про потенційні загрози безпеці. Наприклад, якщо користувач здійснює велику суму транзакцій, які різко відрізняються від його звичайної активності. Встановлення правил та спостережень для автоматичного виявлення підозрілої активності, такі як спроби введення невірних паролів, незвичайні IP-адреси, часті спроби доступу тощо.

Якщо система моніторингу виявляє підозрілу активність, вона може сповістити відповідний відділ безпеки банку або сповістити самого користувача через електронну пошту, SMS або інші канали зв'язку. Ведення журналів подій і активностей, що дозволяє зберігати записи про всі події в системі для подальшого аналізу та розслідування. Важливо мати процедури та плани реагування на виявлення підозрілих активностей, включаючи блокування акаунтів, зупинку транзакцій, зміну паролів та інші заходи для захисту інформації користувачів. Банки повинні мати міцну інфраструктуру та системи обмеження доступу, щоб утруднити спроби несанкціонованого доступу до їхніх серверів та даних.

Захист інфраструктури в інтернет-банкінгу є важливим завданням, оскільки інфраструктура банку містить критичну інформацію та операційні системи, які повинні бути надійними та захищеними від несанкціонованого доступу. Ось кілька ключових аспектів захисту інфраструктури в інтернет-банкінгу. Забезпечення фізичної безпеки серверних приміщень та дата-центрів, де розміщені банківські сервери і обладнання. Це включає в себе контроль доступу, моніторинг, системи відеоспостереження та інші заходи безпеки для запобігання фізичному вторгненню.

Використання мережевих заходів безпеки, таких як брандмауери, системи виявлення вторгнень (IDS) та системи запобігання вторгнення (IPS), для захисту від мережевих атак і злому. Захист даних під час передачі через мережу, а також зберігання даних на серверах з використанням сильного шифрування. Введення механізмів автентифікації та авторизації для обмеження доступу до інфраструктури тільки для вповноважених користувачів та адміністраторів. Розробка планів відновлення після аварій та регулярне проведення резервних копій даних для забезпечення можливості відновлення інфраструктури в разі виникнення проблем.

Постійний моніторинг активності в мережі та на серверах, а також ведення журналів подій для відстеження незвичайної активності та аналізу інцидентів безпеки. Регулярне оновлення і патчінг операційних систем, програмного забезпечення та обладнання для запобігання використанню вразливостей. Аудит та журналювання - це важливі процедури в галузі інформаційної безпеки, які дозволяють відстежувати активність користувачів та події в інформаційній системі, забезпечуючи контроль, виявлення помилок, розслідування інцидентів та відповідність правилам і політикам безпеки. Журнали подій (логи): Системи та додатки в інформаційній інфраструктурі банку реєструють події та активності в журналах. Це включає в себе вхід у систему, вихід, виконання команд, доступ до файлів, мережеву активність і т. д. Використання суворої системи аутентифікації та авторизації для контролю доступу до банківських систем.

Кожний користувач повинен мати лише той рівень доступу, який необхідний для виконання його обов'язків. Захист від внутрішніх загроз вимагає комплексного підходу, який включає в себе технічні, організаторські та психологічні заходи безпеки. Банки повинні ретельно контролювати та аудитувати діяльність співробітників та інших осіб, які мають доступ до систем та даних, і вживати необхідних заходів для мінімізації внутрішніх загроз.

Також важливо враховувати, що загрози внутрішнього походження можуть виникнути не тільки внаслідок злочинної діяльності, але і в результаті помилок, неуважності та несанкціонованих дій користувачів. Тому освіта та

контроль є важливими складовими виявлення та запобігання внутрішнім загрозам. CDN (мережа доставки контенту): Використання CDN для розподілення трафіку та фільтрації DDoS-атак на обласному рівні перед тим, як трафік досягає інфраструктури банку. Ці елементи допомагають забезпечити високий рівень безпеки інформації в інтернет-банкінгу, але безпека завжди є постійною роботою, і банки постійно вдосконалюють свої заходи безпеки, оцінюючи нові загрози та ризики [27].

Впровадження системи захисту інформації для інтернет-банкінгу на мові програмування Python може бути важливим завданням для забезпечення безпеки клієнтських даних та транзакцій. Ось кілька кроків, які можна виконати для створення такої системи: Вибір імплементації: Визначте, які конкретні заходи забезпечення ви хочете впровадити у вашому інтернет-банкінгу. Це може включати аутентифікацію, авторизацію, шифрування даних, моніторинг активності користувачів тощо.

Використання відповідних бібліотек: Python має багато бібліотек і фреймворків для розробки системи захисту. Наприклад, можна використовувати бібліотеки, такі як cryptography, PyCryptodome для шифрування даних, або Flask або Django для розробки веб-інтерфейсу. Реалізація сильної аутентифікації для користувачів, можливо, використовуючи двофакторну аутентифікацію. Забезпечення, що доступ до фінансових операцій обмежений тільки для авторизованих користувачів. Шифрування конфіденційних даних, які передаються через мережу та зберігаються на серверах.

Використання сучасних алгоритмів шифрування. Розробка заходів захисту від таких атак, як SQL-ін'єкція, кросс-сайтовий скриптінг (XSS), кросс-сайтовий запрос форжінг (CSRF) та інші. Ведення журналу подій, щоб відслідковувати активність користувачів та виявляти можливі вторгнення. Використання моніторингу систем для негайного реагування на підозрілі активності. Регулярне тестування системи на вразливості та оновлення її, щоб виправити знайдені помилки та вразливості.

Дотримання стандартів безпеки, таких як OWASP Top Ten, для забезпечення найвищого рівня безпеки. Забезпечення навчання користувачів: навчання користувачів правильним практикам безпеки, наприклад, як створювати сильні паролі і уникають підозрілих дій. Перевірка безпеки коду: використання інструментів для автоматичної перевірки безпеки коду, такі як статичні аналізатори. Захист інформації в інтернет-банкінгу - це складне завдання, і воно вимагає систематичного підходу та постійного оновлення для забезпечення найвищого рівня безпеки.

Зважаючи на те, що розробка повноцінної програми для інтернет-банкінгу - це дуже складний і обсяжний проект, нижче наведений приклад простої програми на Python, яка може ілюструвати деякі засоби забезпечення безпеки, такі як хешування паролів і валідація користувачів та інші.

Ця програма використовує бібліотеку Flask для створення веб-інтерфейсу, а також бібліотеку hashlib для хешування паролів (лістинг 3.1).

Лістинг 3.1 – Хешування даних

```
from flask import Flask, request, jsonify
import hashlib
app = Flask(__name)
# Мокап бази даних користувачів (в реальній роботі використовуйте
реляційну БД або NoSQL)
users = {'user1': 'password1', 'user2': 'password2'}
@app.route('/login', methods=['POST'])
def login():
    data = request.get_json()
    username = data.get('username')
    password = data.get('password')
    if username in users:
        stored_password = users[username]
        password_hash =
hashlib.sha256(password.encode()).hexdigest()
        if password_hash == stored_password:
            return jsonify({'message': 'Ви увійшли в систему’})
        else:
            return jsonify({'message': 'Неправильний пароль'}),
401
    else:
        return jsonify({'message': 'Користувача з таким ім'ям не
існує'}), 401
if __name__ == '__main__':
    app.run(debug=True)
```

Цей код створює простий веб-сервер, який має один ендпоінт /login для аутентифікації користувачів. Паролі зберігаються у вигляді хешів, і програма порівнює хеш введеного пароля зі збереженим хешем для користувача. Цей код використовує SHA-256 для хешування паролів, але в реальному проекті слід розглядати більш потужні алгоритми та більш складні системи забезпечення безпеки.

На мою думку важливим заходом безпеки з ходом розвитку інформаційної галузі в більшості смартфонів та навіть ноутбуків є відбиток пальців, тож розробимо код з прив’язкою до відбитків пальців.

Прив'язка до відбитків пальців - це високо вищий рівень безпеки, і для цього зазвичай використовуються спеціалізовані бібліотеки та обладнання для читання відбитків пальців. Однак я можу надати вам приклад використання бібліотеки PyFingerprint, яка дозволяє працювати з датчиками відбитків пальців (лістинг 3.2).

Лістинг 3.2 – Аутентифікація за відбитком пальця

```
from pyfingerprint.pyfingerprint import PyFingerprint
# Ініціалізація об'єкту відбитка пальця
f = PyFingerprint('/dev/ttyUSB0', 57600, 0xFFFFFFFF, 0x00000000)
# Перевірка підключення датчика
if not f.verifyPassword():
    raise ValueError('Помилка аутентифікації датчика')
# Зчитування шаблону відбитка пальця
try:
    print('Будь ласка, прикладіть палець до датчика...')
    if f.readImage() == True:
        f.convertImage(0x01)
        result = f.searchTemplate()
        position = result[0]
        if position >= 0:
            print('Відбиток пальця знайдено, позиція: ' +
str(position))
        else:
            print('Відбиток пальця не знайдено')
except Exception as e:
    print('Помилка: ' + str(e))
```

Цей код демонструє простий приклад використання бібліотеки PyFingerprint для реєстрації та перевірки відбитків пальців. Зверніть увагу, що вам потрібно буде мати фізичний датчик відбитків пальців, який підключений до вашого комп'ютера через COM-порт (у цьому прикладі '/dev/ttyUSB0').

Обов'язково слід вивчити документацію до свого конкретного датчика відбитків пальців та налаштувати код відповідно до вашого обладнання і потреб.

Що ж робити з девайсами в яких відсутній відбиток , розглянемо інший приклад розблокування сервісів інтернет банкінгу а саме FaseID:

Для розпізнавання обличчя (Face ID) вам зазвичай потрібно використовувати спеціалізовані бібліотеки та сервіси, оскільки це вимагає обробки зображень обличчя та моделей машинного навчання. Однак я можу надати вам простий приклад використання бібліотеки OpenCV для захоплення зображення з веб-камери та розпізнавання обличчя за допомогою бібліотеки Dlib (лістинг 3.3).

Лістинг 3.3 – Аутентифікація за обличчям

```
import cv2
import dlib
# Ініціалізація детектора обличчя
detector = dlib.get_frontal_face_detector()
# Завантаження натренованої моделі для розпізнавання ключових
точок обличчя
predictor =
dlib.shape_predictor('shape_predictor_68_face_landmarks.dat')
# Ініціалізація відео захоплення
cap = cv2.VideoCapture(0)
while True:
    ret, frame = cap.read()
    if not ret:
        break
    # Перетворення кольорового зображення на відтінки сірого
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    # Детектор обличчя
    faces = detector(gray)
    for face in faces:
        x, y, w, h = face.left(), face.top(), face.width(),
face.height()
        # Розпізнавання ключових точок обличчя
        landmarks = predictor(gray, face)
        for n in range(68):
            x_point = landmarks.part(n).x
```

Продовження лістингу 3.3

```
            y_point = landmarks.part(n).y
            # Малюємо точки ключових точок обличчя на кадрі
            cv2.circle(frame, (x_point, y_point), 2, (0, 255, 0),
-1)
        # Малюємо прямокутник навколо обличчя
        cv2.rectangle(frame, (x, y), (x + w, y + h), (0, 255, 0),
2)
    # Відображення кадру з обличчями
    cv2.imshow('Face Recognition', frame)
    if cv2.waitKey(1) & 0xFF == ord('q'):
        break
cap.release()
cv2.destroyAllWindows()
```

Цей код використовує OpenCV та Dlib для захоплення зображення з веб-камери та розпізнавання обличчя. Важливо вказати шлях до файлу shape_predictor_68_face_landmarks.dat, який містить натреновану модель для розпізнавання ключових точок обличчя. Ви можете встановити цей файл, завантаживши його з репозиторію Dlib.

Обов'язково слід пам'ятати, що цей код - це лише початковий приклад і має обмежену функціональність для розпізнавання обличчя. Для повноцінного використання Face ID слід використовувати більш потужні моделі машинного навчання та сервіси розпізнавання обличчя.

Для підвищення рівня захисту від шахрайських операцій пропонується використання моделей машинного навчання, що дозволяють виявляти аномальну активність користувачів інтернет-банкінгу. Система буде збирати історичні дані про стандартну поведінку клієнтів та на їх основі за допомогою кластеризації та класифікації будувати індивідуальні профілі. Потім в режимі реального часу аналізує сесії користувачів, виявляє відхилення та формує сповіщення про підозри [28,30].

### 3.2 Технічні засоби захисту від загроз

Міжмережеві екрани або фаєрволи - це програмно-апаратні комплекси, які виконують фільтрацію мережевого трафіку на основі заданих правил. Вони

встановлюються на межі між внутрішньою мережею банку та зовнішнім незахищеним середовищем (наприклад, Інтернет) (рисунок 3.1).

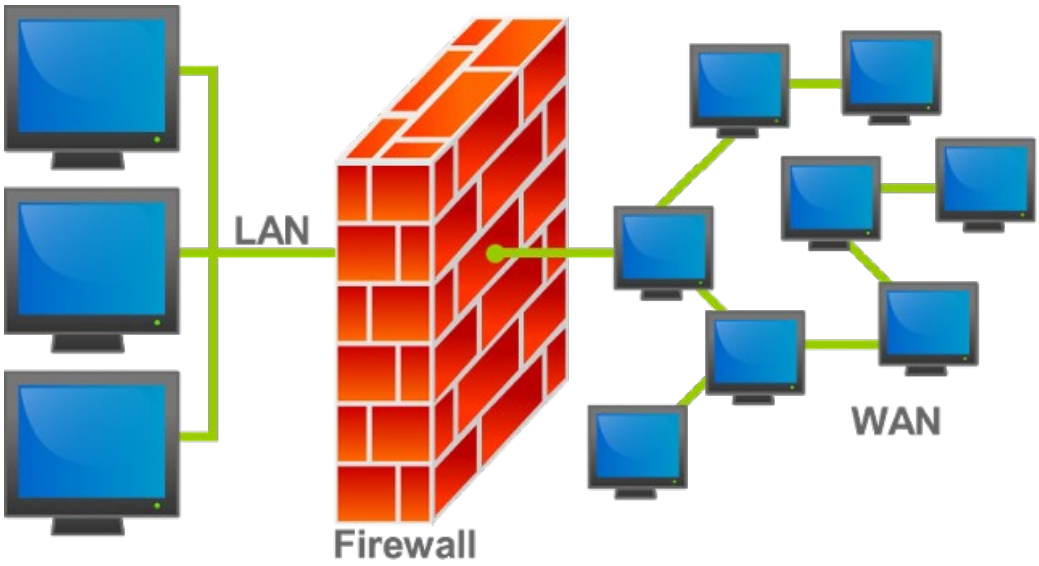


Рисунок 3.1 – Міжмережевий екран

Основне призначення міжмережевих екранів - це запобігання несанкціонованого доступу до внутрішніх ресурсів мережі та поширення шкідливого вмісту всередину мережі. Фаєрволи аналізують весь вхідний і вихідний трафік та приймають рішення про фільтрацію пакетів на основі конфігурації правил.

Термін "брандмауер" є походить з німецької мови і є аналогом англійського терміну "firewall" у його оригінальному сенсі (стіна, що відокремлює суміжні будівлі для захисту від поширення пожежі).

Слова "файрволл", "файрвол", "файервол", "фаєрвол" утворено транслітерацією англійського терміна "firewall", що є еквівалентом терміну "міжмережевий екран".

Фільтрація пакетів. Це одна з трьох відомих характеристик мережевого екрану. У цьому випадку забезпечується дуже проста задача, подібна до тих, яка забезпечує спеціалізовані маршрутизатори; це включає перевірку правильності IP-адреси та порту та заголовка перегляду кожного пакету. Наприклад, пакет, який надсилається через локальний Інтернет, але має адресу призначення, буде

заблокований. Ця функція на всіх сучасних мережевих екранах, і вона відрізняється високою швидкістю доступу та відсутністю потреб у спілкуванні з користувачем.

Система виявлення вторгнень (intrusion detection system, IDS) призначена для моніторингу мережі або інформаційної системи з метою виявлення ознак кібератак та шкідливої активності.

Системи IDS аналізують трафік, події та поведінку в системі за допомогою сигнатур атак, аномальної активності та інших атрибутів. У разі виявлення шкідливої діяльності IDS формують попередження та сповіщають відповідні служби безпеки. Схематично на рисунку 3.2.

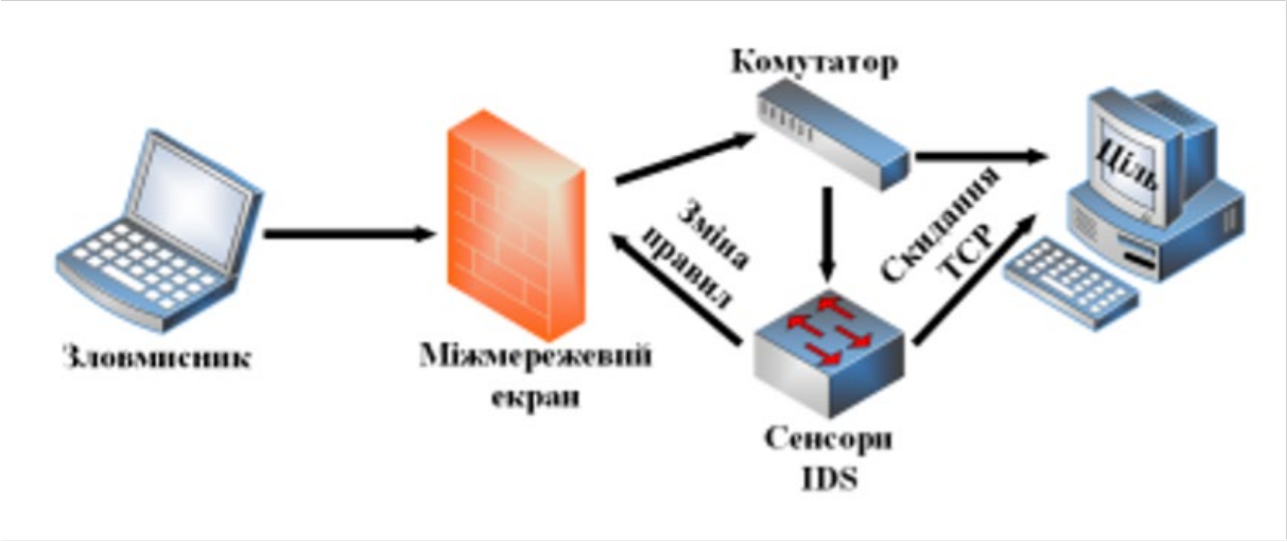


Рисунок 3.2 – Системи виявлення вторгнень (IDS)

Системи запобігання вторгнень (intrusion prevention system, IPS) мають ті ж функції виявлення шкідливої активності, що і IDS, але на відміну від них можуть у режимі реального часу блокувати атаки.

IPS аналізує трафік та поведінку в системі, і у разі виявлення ознак загрози вживає активних заходів, щоб заблокувати її. Це може бути переривання мережевого з'єднання, блокування IP-адреси джерела атаки, блокування доступу користувача, карантин файлу тощо.

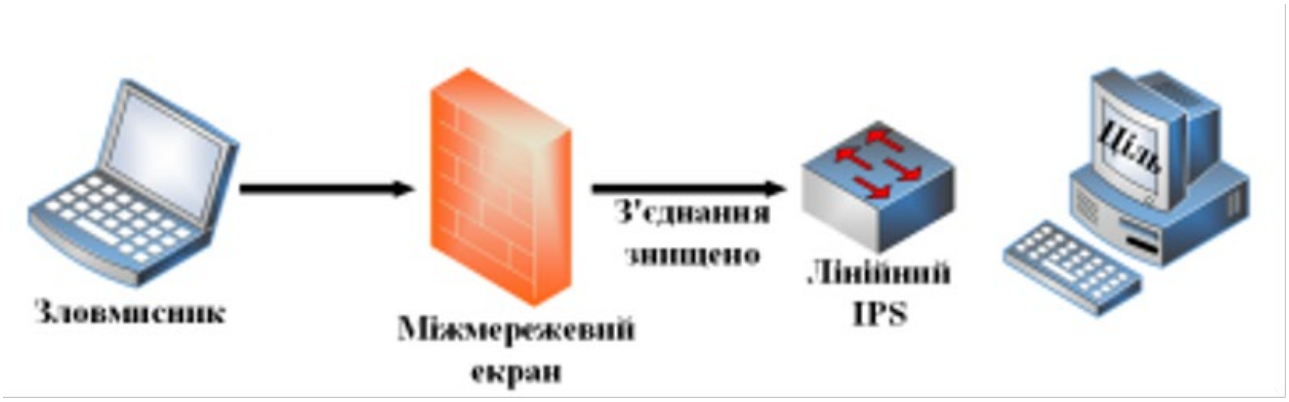


Рисунок 3.3 – Системи запобігання вторгнень (IPS)

VPN

VPN (віртуальна приватна мережа) - це технологія, яка дозволяє створити логічне захищене з'єднання між мережами чи окремими хостами через публічні канали зв'язку, такі як Інтернет. VPN шифрує трафік та "тунелює" його між вузлами, що унеможливлює перехоплення та аналіз даних сторонніми особами.

Основна мета використання VPN в інтернет-банкінгу - забезпечити безпечний віддалений доступ для користувачів. VPN створює логічне приватне з'єднання між пристроєм користувача (комп'ютер, смартфон) та серверами інтернет-банкінгу банку крізь незахищений Інтернет [14,19,25].

Основні типи VPN, які використовуються в інтернет-банкінгу:

– Site-to-site VPN - з'єднання між офісами банку через незахищену мережу.

– Remote access VPN - підключення окремих користувачів до корпоративної мережі.

– SSL VPN - використання протоколу SSL для створення захищеного каналу.

Для максимальної безпеки VPN має використовуватися разом з іншими заходами, такими як аутентифікація, авторизація користувачів, антивірусний захист, моніторинг трафіку тощо.

Криптографія є важливим компонентом захисту конфіденційності та цілісності даних в системах інтернет-банкінгу. Криптографічні методи, що застосовуються:

Поширені алгоритми і протоколи шифрування:

- Симетричні: AES, Triple DES, Blowfish, RC4, RC5, RC6.
- Асиметричні: RSA, ECC (Elliptic curve cryptography), Diffie-Hellman.
- Гешування: SHA-2, SHA-3, MD5, Whirlpool, GOST R 34.11-94.
- Протоколи: TLS, SSL, IPsec, HTTPS, SFTP, PGP, S/MIME.

Важливими аспектами є вибір надійних алгоритмів і протоколів, генерація та розподіл ключів, захист секретних ключів від компрометації.

Криптографія є одним з ключових елементів системи захисту інтернет-банкінгу, що дозволяє запобігти витоку та модифікації конфіденційних даних при передачі та зберіганні.

Антивірусне програмне забезпечення (ПЗ) використовується для виявлення, блокування та лікування шкідливих програм на робочих станціях, серверах, мережевому обладнанні. Сучасні загрози поширення шкідливого ПЗ вимагають комплексного підходу, що поєднує різні технології захисту

Критично важливим є своєчасне оновлення баз даних сигнатур шкідливих програм, налаштування політик і регулярне сканування. Захист від вірусів є важливою ланкою в системі інформаційної безпеки інтернет-банкінгу.

WAF (міжмережевий захист додатків) - це рішення, яке фільтрує, моніторить та блокує трафік між користувачами та веб-додатками: сайтами, сервісами, API.

WAF діє за допомогою набору правил, які часто називають політиками. Ці політики спрямовані на захист від вразливостей у програмі шляхом фільтрації шкідливого трафіку. Цінність WAF частково полягає у швидкості та легкості, з якою може бути реалізована модифікація політики, що дозволяє швидше реагувати на різні вектори атак; під час DDoS-атаки обмеження швидкості можна швидко реалізувати, змінивши політики WAF.Схематично на рисунку 3.4.

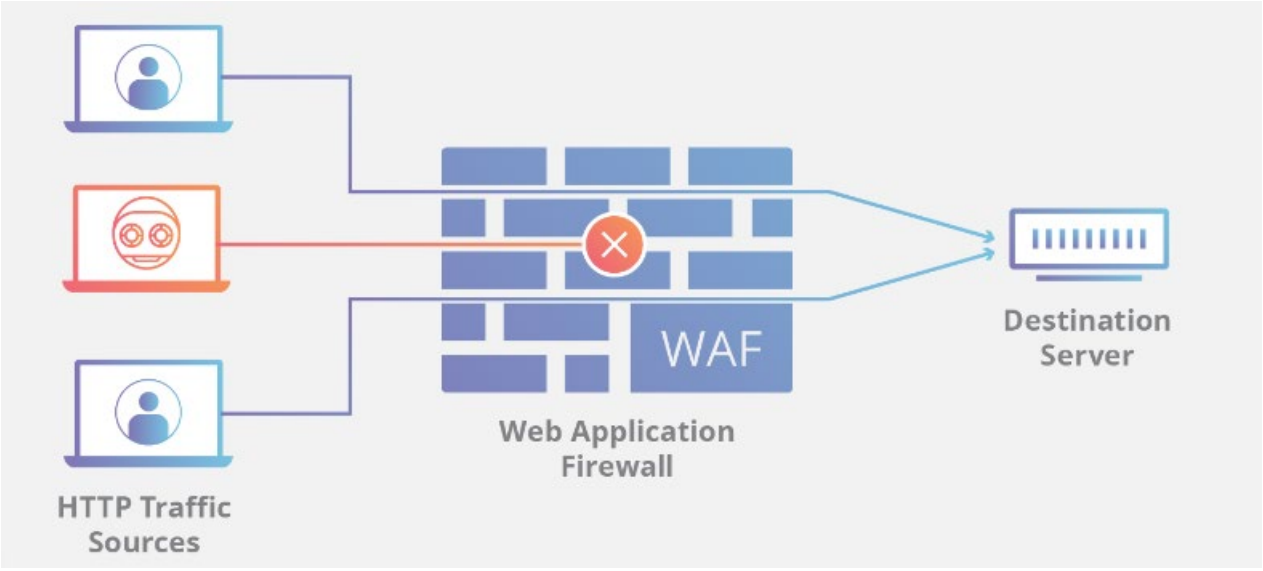


Рисунок 3.4 – Брандмауер веб-додатків

Захист від DDoS атак є важливою складовою інформаційної безпеки інтернет-банкінгу, оскільки такі атаки націлені на блокування доступності сервісів.

Основні методи захисту від DDoS це використання хмарних сервісів DDoS-протидії, які фільтрують атаки до досягнення інфраструктури банку. Ці сервіси мають велику пропускну здатність каналів та обробки запитів [1,10].

### 3.3 Організація захищеного зберігання та обробки даних

Компанії найбільше турбуються про обробку та захист персональних даних. Необхідність отримувати більше та більше інформації про людей пояснює такий порядок речей. Крім того, законодавство про захист персональних даних покращується. Ухвалення Європейським Союзом Загального регламенту про захист даних спричинило новий підйом занепокоєння щодо правильної роботи з персональними даними.

Будь-яка компанія, установа або організація, яка працює з персональними даними, вважається оператором і повинна дотримуватися правил, встановлених законодавством.

Деякі рекомендації по організація захищеного зберігання та обробки даних

Шифрування даних є одним з ключових заходів захисту конфіденційної інформації в інтернет-банкінгу. Воно перешкоджає несанкціонованому ознайомленню з даними в разі їх витоку. Шифрування має застосовуватися як для даних в стані спокою (на серверах, в базах даних), так і під час передачі по мережі.

Для шифрування трафіку між клієнтом і сервером використовуються протоколи TLS, SSL, IPsec, що забезпечують конфіденційність і цілісність даних.

Фінансові документи та особисті дані користувачів мають шифруватися на серверах і в базах даних з використанням сучасних алгоритмів, таких як AES-256, що вважається криптографічно стійким.

Резервні копії та архіви, що містять конфіденційні дані, повинні зберігатися виключно в зашифрованому вигляді. Шифрування дисків серверів баз даних та backup-сховищ ускладнює несанкціонований доступ до даних у разі фізичної крадіжки носіїв або компрометації внаслідок кібератаки.

Важливо правильно організувати процеси генерації, зберігання та розподілу криптографічних ключів для шифрування. Необхідно унеможливити втрату ключів та їх розкриття стороннім особам [5,8].

Важливим принципом є надання користувачам та адміністраторам мінімально необхідних прав доступу до даних відповідно до їх посадових обов'язків. Це ускладнює несанкціонований перегляд та копіювання конфіденційної інформації.

Рекомендується впроваджувати рольову модель доступу. Користувачі та процеси отримують права на виконання певних операцій з даними на основі призначених їм ролей. Наприклад, оператор call-центру має доступ лише до персональних даних клієнта, необхідних для верифікації.

Адміністратор бази даних не повинен мати доступу до читання особистих даних клієнтів, а лише до управління самою БД.

Потрібно обмежити та жорстко контролювати надання привілейованого доступу до даних, такого як доступ root/administrator до серверів БД.

Також важливо регулярно переглядати надані права доступу і вносити своєчасні зміни, наприклад при звільненні співробітників.

Системи запобігання витоку даних (Data Loss Prevention, DLP) допомагають виявляти та блокувати спроби несанкціонованого копіювання чи передачі конфіденційних даних за межі корпоративної мережі.

DLP працює шляхом глибокого аналізу змісту трафіку та дій користувачів із даними - електронною поштою, файлами, доступом до БД тощо.

За допомогою DLP можна, наприклад:

– Виявляти пересилання клієнтських даних на особисту пошту співробітниками.

– Блокувати спроби запису великих масивів даних на зовнішні накопичувачі.

– Попереджати про спроби відкриття баз даних через нетипові додатки.

– Виявляти передачу конфіденційних документів через хмарні сервіси.

Таким чином DLP допомагає запобігти як навмисним, так і випадковим витокам даних внаслідок дій персоналу.

Дії з боку інсайдерів є однією з найнебезпечніших загроз для безпеки даних в інтернет-банкінгу. Спеціальні системи дозволяють виявляти ознаки шкідливої внутрішньої активності, такі як:

– Аномальна інтенсивність запитів до БД з боку визначених користувачів.

– Нетипові для користувача операції з даними.

– Несанкціоновані зміни в критичних даних чи системних файлах.

– Спроби передачі великих масивів даних через канали, не призначені для цього.

– Невиправдано тривалий сеанс роботи з системою.

– Активність з нестандартних пристроїв або географічних регіонів.

Ці та інші аномалії можуть бути ознакою шкідливих інсайдерських дій і мають негайно розслідуватися службою безпеки.

Регулярне тестування на проникнення дає змогу виявити недоліки в системі захисту даних до того, як їх зможуть використати зловмисники.

Етичні хакери будуть намагатися знайти способи обійти наявні засоби захисту, отримати несанкціонований доступ до даних, викрасти чутливу інформацію тощо.

За результатами тестування складається звіт з рекомендаціями щодо усунення знайдених вразливостей, який дозволить посилити захист даних від можливих атак.

Перенесення частини інфраструктури інтернет-банкінгу в хмару, що дозволить оптимізувати захищеність та масштабованість. Рекомендовано використання хмарних баз даних, веб та аплікаційних серверів з автоматичним балансуванням навантаження, що спростить протидію DDoS. Також запропоновано контейнеризацію окремих мікросервісів (WAF, IPS/IDS тощо), що полегшить оновлення та розгортання захисних компонентів.

# 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

## 4.1 Охорона праці

Галузь інтернет-банкінгових систем, як і будь яка інша, вимагає дотримання норм охорони праці в першу чергу визначених частиною 1 статті 13 Закону про охорону праці [44]. Забезпечення на робочому місці умови праці відповідно до нормативно-правових актів та додержання вимог законодавства щодо прав працівників у галузі охорони праці мінімізує ризики діяльності підприємства та їх учасників. Саме тому на основі таких документів було сформовано перелік вимог, яких варто дотримуватися і у підприємствах, робота яких пов’язана з інтернет-банківською справою.

Зокрема, пункт 2 ДСанПІН 3.3.2.007-98 [46] врегульовує вимоги до виробничих приміщень для експлуатації візуальних дисплейних терміналів, де зазначено, що розміщення робочих місць у підвальних приміщеннях, на цокольних поверхах заборонено, а площа на одне робоче місце має становити не менше ніж 6 м$^2$. Ці приміщення повинні мати природне та штучне освітлення. Визначено також і норми шуму та вібрації, згідно з якими робочі приміщення не повинні межувати з приміщеннями, в яких рівні шуму і вібрації перевищують допустимі значення. Окрім того приміщення для роботи мають бути обладнані системами опалення, кондиціонування повітря, або припливно-витяжною вентиляцією відповідно до ч. Для систем інтернт-бакінгу важливим є збереження та оборка інформації, тому відповідно до підпункту 2.14. приміщення можуть обладнуватись шафами для зберігання документів, магнітних дисків, полицями, стелажами, тумбами тощо з урахуванням вимог до площі приміщень.

Специфіка роботи фахівців у сфері інтернет-банкінгу полягає у великому об’ємі часу проведення в закритих приміщення перед моніторами комп’ютера, тому важливо подбати про забезпечення дотримання вимог пункту 3 ДСанПІН 3.3.2.007-98 [46], який регулює гігієнічні вимоги до параметрів виробничого

середовища приміщень, зокрема освітлення. Згідно цих вимог освітлення на поверхні робочого столу в зоні розміщення документів має становити 300-500 лк. Якщо ці значення освітленості неможливо забезпечити системою загального освітлення, допускається використовувати місцеве освітлення. Необхідно обмежувати відбиту блискість на робочих поверхнях відносно джерел природного і штучного освітлення. Показник осліпленості у разі використання джерел загального штучного освітлення у виробничих приміщеннях має не перевищувати 20.

У розділі 4 ДСанПІН 3.3.2.007-98 [46] важливим підпунктом також є вимоги щодо матеріального забезпечення робочого місця згідно з якими конструкція робочого столу має відповідати сучасним вимогам ергономіки і забезпечувати оптимальнерозміщення на робочій поверхні використовуваного обладнання (дисплея, клавіатури, принтера). Висота робочої поверхні робочого столу має регулюватися в межах 680...800 мм, а ширина і глибина - забезпечувати можливість виконання операцій у зоні досяжності моторного поля (рекомендовані розміри: 600...1400 мм, глибина - 800..1000 мм). Робочий стіл повинен мати простір для ніг заввишки не менше ніж 600 мм, завширшки не менше ніж 500 мм, завглибшки (на рівні колін) не менше ніж 450 мм, на рівні простягнутої ноги. Робочий стілець має бути підйомно-поворотним, регульованим за висотою, з кутом і нахилу сидіння та спинки і за відстанню від спинки до переднього краю сидіння поверхня сидіння має бути плоскою, передній край -заокругленим. Регулювання за кожним із параметрів має здійснюватися незалежно, легко і надійно фіксуватися. Робоче місце має бути обладнане підставкою для ніг завширшки не менше ніж 300 мм, завглибшки не менше ніж 400 мм, що регулюється за висотою в межах до 150 мм і за кутом нахилу опорної поверхні підставки до 20 градусів.

Для того, щоб забезпечити максимальну продуктивність та ефективність роботи працівників необхідно подбати і про належний рівень відпочинку працівників. Зокрема, у пункті 5 ДСанПІН 3.3.2.007-98 [46] передбачено забезпечення перерви для відпочинку працівників для збереження їх здоров'я,

запобігання професійним захворювання і підтримки працездатності. Серед них визначаються:

– перерви для відпочинку і вживання їжі (обідні перерви);

– перерви для відпочинку і особистих потреб (згідно з трудовими нормами);

– додаткові перерви, що вводяться для окремих професій з урахуванням особливостей трудової діяльності.

Роботи в галузі інтернет-банкінгу несе загрозу для життя та здоров'я її працівників, з огляду на те, що в таких приміщеннях присутня велика кількість електронно-обчислювальних машин, тому згідно Закону України «Про охорону праці» [44] працівники під час прийняття на роботу та протягом роботи мають проходити інструктаж з питань охорони праці. Тих, хто не пройшов інструктаж, не допускають до роботи.

Працівники під час прийняття на роботу та періодично повинні проходити на підприємстві інструктажі з питань охорони праці, надання першої медичної допомоги потерпілим від нещасних випадків, а також з правил поведінки та дій при виникненні аварійних ситуацій, пожеж і стихійних лих.

Під ведення війни, потрібно пам'ятати і про заходи забезпечення безпеки та організацію роботи в таких умовах. Зокрема, у Законі України «Про організацію трудових відносин в умовах воєнного стану» від 15.03.2022 № 2136-IX [45] змінено порядок оформлення працівника на роботу. Допуск відбувається без укладення письмового трудового договору та з випробувальним строком без обмеження кола працівників. Також можна укладати строковий договір з новими працівниками на час відсутності працівника.

Змінено й графік роботи та відпочинку. Під час воєнного стану роботодавець має право збільшити тривалість робочого часу на тиждень до 60 годин. Окрім цього, роботодавець може змінити робочий графік, встановити 6-тижневий робочий тиждень, скоротити відпочинок (тривалість щотижневого відпочинку – не менше ніж 24 години) [45].

## 4.2 Безпека в надзвичайних ситуаціях

Надзвичайна ситуація - це порушення звичайних умов життя та діяльності людей на певній території чи об'єкті, що виникає внаслідок аварії, катастрофи, стихійного лиха чи іншої небезпечної події, такої як епідемія чи пожежа. Ця ситуація може призвести до значних наслідків, таких як загроза життю та здоров'ю людей, їхня загибель, великі матеріальні збитки та неможливість проживання чи господарювання на даній території чи об'єкті.

Надзвичайні ситуації розрізняються за джерелом, будь то техногенні, природні або інші. Техногенні ситуації, зокрема, є основним видом на підприємствах, де здійснюється розробка та впровадження програмних продуктів, якими є й інтернет-банкінгові системи.

Працівники підприємств повинні бути обізнані і виконувати правила техніки безпеки на робочому місці. У випадку надзвичайної ситуації, працівники зобов'язані оперативно повідомити керівництво підприємства та вжити негайних заходів для ліквідації наслідків події. Привертається увага працівників до того, що вони особисто несуть відповідальність за своєчасні заходи щодо запобігання надзвичайним ситуаціям.

Після кожного нещасного випадку або надзвичайної ситуації на виробництві очевидець або учасник події, після надання першої допомоги, повинен негайно повідомити керівника, використовуючи всі доступні засоби зв'язку. Недотримання цієї вимоги може призвести до погіршення стану здоров'я потерпілого та несвоєчасного прийняття оперативних заходів для контролю ситуації та мінімізації її наслідків.

Кожне підприємство повинно мати інструкцію щодо поведінки в надзвичайних ситуаціях, яка розробляється відповідно до законодавства України про захист населення і території від надзвичайних ситуацій техногенного та природного характеру. Привертається увага до того, що працівники зобов'язані знати та дотримуватись даної інструкції, яка повинна бути затверджена керівником підприємства. В інструкції має міститися інформація про потенційно

можливі надзвичайні ситуації на виробництві, методи оповіщення керівництва про надзвичайну ситуацію, заходи щодо збереження матеріальних цінностей підприємства та маршрути евакуації персоналу.

Перед нами також постало важливе завдання забезпечення безпеки працівників в умовах ведення війни та бомбардування, особливо в прифронтових зонах, та зонах підвищеної небезпеки. Можна виділити дві групи заходів в таких ситуаціях: стратегії уникнення та стратегії управління наслідками.

До першої можна віднести:

– розробку та провдення тренувань для персоналу з питань безпеки та евакуації;

– визначення безпечних місць для притулку та організація їхньої доступності у разі потреби;

– встановлення системи раннього попередження для оперативного виявлення та сповіщення про можливі загрози.

До другої:

– розроблення та реалізації заходів для захисту критичних інфраструктурних об'єктів від можливих атак;

– органіація системи медичної допомоги та готовності для надання першої допомоги та лікування поранених;

– надання психологічної підтримки персоналу та мешканцям для зменшення психологічного впливу стресу та травм;

– співпраця із місцевими та міжнародними владними структурами для координації заходів управління наслідками та отримання допомоги;

– розроблення ефективної системи комунікації для інформування персоналу та громадськості про ситуацію та надання інструкцій;

– планування заходів відновлення та реконструкції після закінчення війни для якнайшвидшого відновлення нормального життя та роботи.

Аналізуючи події останніх років, до надзвичайних ситуацій можна віднести і атаки на інформаційну безпеку підприємства, які трапляються все

частіше, особливо після переходу на дистанційну роботу. Тому потрібно забезпечити дії та протидії виникнення таких ситуацій.

– Регулярні резервні копії. Потрібно здійснювати регулярне створення резервних копій важливих даних, визначити частоту резервного копіювання залежно від обсягу та частоти змін в інформації.

– Шифрування даних. Застосування шифрування для захисту конфіденційних інформаційних ресурсів від несанкціонованого доступу. Використання міцних алгоритмів шифрування для забезпечення безпеки даних під час передачі та зберігання.

– Керування доступом. Визначення і керування правами доступу для працівників, обмежуючи їхні можливості отримання доступу до чутливої інформації лише на необхідний мінімум. Застосування принципу найменших привілеїв для зменшення ризику несанкціонованого доступу.

– Фізична безпека. Забезпечення фізичної безпеки серверних приміщень та дата-центрів, де зберігаються сервери та обладнання. Встановлення системи контролю доступу та відеоспостереження для запобігання несанкціонованому доступу.

# ВИСНОВКИ

В кваліфікаційній роботі магістра було досягнуто таких науково-технічних результатів: під час створення технічного захисту інформації в інформаційно-технічних системах необхідно дотримуватися певних методологічних принципів досліджень, проектування, експлуатації та розвитку таких систем відповідно до законодавства України. Кожен суб'єкт інформаційно-технічної системи в Україні, незалежно від організаційно-правової форми та форми власності, повинен дотримуватися порядку створення технічного захисту інформації.

Це особливо стосується інформаційно-технічних систем, в яких обробляється державна інформація. Мета полягає в тому, щоб максимізувати захист за допомогою синхронного застосування усіх потрібних ресурсів та методів й засобів, щоб запобігти несанкціонованому доступу до інформації в приватних секторах, а також створити умови обробки інформації відповідно до відповідних законодавчих актів України щодо захисту інформації.

Таким чином, в роботі розглянуто як об'єкт приватної сфери - інтернет-банкінг. Проаналізовано всі можливі витоки особливої інформації компанії та запропоновано способи їх уникнення та покращення деяких важливих способів ідентифікації особи , що в свою чергу забезпечує більшу безпеку користувачам банкінгу .

В роботі запропоновано новий спосіб побудови комплексу системи забезпечення безпеки інформації в системах інтернет-банкінгу, який поєднує технічні та організаційні заходи безпеки. Розроблено модель потенційного порушника з урахуванням сучасних кіберзагроз. Запропоновано застосування машинного навчання для виявлення аномальної поведінки користувачів. Вперше запропоновано використання приватного блокчейну в інтернет-банкінгу для підвищення прозорості та незмінності транзакцій. Результати, отримані в ході виконання роботи, несуть в собі наукову новизну та практичне застосування для підвищення рівня захищеності систем інтернет-банкінгу.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Бєлай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ : Національна академія Служби безпеки України, 2018. 408 с
2. Брижко В. М. Електронний банкінг у контексті захисту персональних даних / В. М. Брижко, Ю. К. Базанов, М. Я. Швець. – К. : НДЦПІ АПрН України, 2008. – 140 с.
3. Гайдай І. Ю. Зарубіжний досвід упровадження Інтернет-банкінгу та перспективи його використання в Україні [Електронний ресурс] / І. Ю. Гайдай, Р. Ф. Гайдай, Д. В. Меркушева. – Режим доступу : http://archi–ve.nbuv.gov.ua/portal/soc_gum./VDie/2011_1/files/47.pdf.
4. Красовська, І. Підключення до системи "Клієнт-банк" [Текст] / І. Красовська // "ГоловБух". – 2010. – № 62(541). – С. 24–27.
5. Кулініч О. А. Інтернет-банкінг в Україні як складова розвитку мережної інфраструктури / О. А. Кулініч // Економічна стратегія і перспективи розвитку сфери торгівлі та послуг : зб. наук. пр. – Х. : ХДУХТ, 2011. – Вип. 2 (14). – С. 421–429.
6. Нікітін, А. В. Маркетинг у банку [Текст] : навч. посіб. / А. В. Нікітін, Г. П. Борт- ніков, А. В. Федорченко. – К. : КНЕУ, 2009. – 432 с.
7. Рогач, І. Ф. Інформаційні системи у фінансово-кредитних установах [Текст] : навч. посіб. – 2-ге вид., перероб. і доп. / І. Ф. Рогач, М. А. Сендзюк, В. А. Антонюк. – К. : КНЕУ, 2011. – 239 с.
8. Функціонування банківського сектора та кредитної кооперації: теорія і практика [Текст] : монографія / [І. Г. Брітченко, А. О. Пантелеймоненко, С. П. Прасолова та ін.]. – Полтава : РВВ ПУЕТ, 2010. – 152 с.
9. Шалига Т. С. Дистанційне банківське обслуговування роздрібних клієнтів : монографія / Т. С. Шалига. – Ніжин : Аспект-Поліграф, 2013. – 412 с.

10. Страхарчук А. Я. Інформаційні системи і технології в банках : навч. посібн. / А. Я. Страхарчук, В. П. Страхарчук. – К. : Знання, 2010. – 516 с.
11. Бурнашов С. В. Проектування та розроблення відкритих wifiмереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С.121-124)
12. Мастяниця Й. І., Соснін О. В., Шиманський Л. Є. Захист інформаційних ресурсів України: проблеми і шляхи їх розв'язання. Київ : Нац. ін-т стратегічних досліджень, 2000. 98 с.
13. Войтович В.С., Гриник Р.О. Необхідність створення комплексної системи захисту інформації. Зб. тез доповідей II Міжвузівської науковопрактичної конференції студентів і курсантів ―Захист інформації в інформаційно-комунікаційних системах‖ (м. Львів, 24 листопада 2017 р.). Львів: ЛДУ БЖД, 2017. С. 10–11.
14. Василюк В. Я., Климчук С. О. Інформаційна безпека держави : курс лекцій. Київ : КНТ, Видавн. дім «Скіф», 2008. 136 с.
15. Галузевий стандарт України: Інформаційні технології. Методи захисту. Система управління інформаційною безпекою (Вимоги Iso/Iec 27001:2005, Mod) [Електронний ресурс] / НБУ – Режим доступу : http://auditagency.com.ua
16. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи. Київ : Видавн. дім «СофтПрес», 2005. 316 с
17. Баранов А. А. Концептуальные вопросы информационной безопасности Украины. Безопасность информации. 1995. № 2. С. 4–10.
18. Міжнародна інформаційна безпека: сучасні виклики та загрози / [Є.А. Макаренко, М. А. Ожеван, М. М. Рижков та ін.]. – К. : Центр Вільної преси, 2006. – 916 с. 72

19. Технічний захист інформації на об’єктах інформаційної діяльності / М. М. Браіловський, С. М. Головень та ін.; за ред. проф. В. О. Хорошка. Київ : ДУІКТ, 2007. 178 с.
20. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
21. Сучасні інформаційні війни в соціальних онлайн-мережах / О. В. Курбан // Інформаційне суспільство. - 2016. - Вип. 23. - С. 85-90. - Режим доступу: http://nbuv.gov.ua/UJRN/is_2016_23_15
22. Полотай О., Мороз Ю., Великий В. Методи технічного захисту інформації у сфері інформаційної безпеки. Інформаційна безпека інформаційні технології: Збірник тез доповідей IV Всеукраїнської науковопрактичної конференції молодих учених, студентів і курсантів. – Львів, 2020. – С. 40-41.
23. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015
24. Янковский А. 5 ключевых проблем в сфере информационной безопасности [Електронний ресурс] / А. Янковский. – Режим доступу : http://cripo.com.ua Информационная безопасность / [под ред. Д. Н. Шакина]. – М. : Оружие и технологии, 2009. – 256 с
25. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374
26. Internal security strategy for The European Union «Towards a European Security Model» [Електронний ресурс]. – Режим доступу : http://www.register.consilium.europa.eu
27. Богуш В. М., Юдін О. К. Інформаційна безпека держави. Київ : «МК-Прес», 2005. 432 с
28. Аволио Ф.М. Защита информации на предприятии / Ф.М. Аволио, Г. Шипли // Сети и системы связи. – 2000. – № 8. – 91-99 с

29. Расторгуев С. П. Информационная война. Москва : Радио и связь, 1999. 416
30. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
31. Про схвалення Методичних рекомендацій щодо організації та функціонування системи ризик-менеджменту в банках України : постанова Правління Національного банку України № 361 від 02.08.2004 р. (у ред. № 255 від 21.06.2012 р.) [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0361500-04
32. Про внесення змін до Положення про здійснення банками фінансового моніторингу : постанова Правління НБУ № 22 від 31.01.2011 р. [Електронний ресурс]. – Режим доступу : http://www.bank.gov.ua/B_zakon/Acts/2011/31012011_22.pdf
33. Лечаченко Т. А. Реалізація інформаційних технологій банкінгу в Україні / Т. А. Лечаченко // Збірник тез доповідей VI Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій», 16-17 листопада 2017 року. — Т. : ТНТУ, 2017. — Том 3. — С. 191–192. — (Економічні та соціальні аспекти нових технологій).
34. Теоретичний аналіз інформаційної безпеки в комп'ютерних мережах / М. П. Карпінський, Я. І. Кінах, О. С. Войтенко, В. Р. Паславський, І. З. Якименко, М. М. Касянчук // Збірник тез доповідей VI Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій», 16-17 листопада 2017 року. — Т. : ТНТУ, 2017. — Том 2. — С. 81–82. — (Комп'ютерно-інформаційні технології та системи зв'язку).
35. Cybersecurity threatscape: Q3 2023 [Електронний ресурс]. – Режим доступу : https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q3/
36. Global Threat Report. Extended enterprise under threat [Електронний ресурс]. – Режим доступу : https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-gtr-extended-enterprise-under-threat-global.pdf

37. Losses from Online Payment Fraud [Електронний ресурс]. – Режим доступу : https://www.juniperresearch.com/press/losses-online-payment-fraud-exceed-362-billion/
38. Ponemon Institute Security [Електронний ресурс]. – Режим доступу : https://www.ponemon.org/research/ponemon-library/security/security.html
39. Cost of a Data Breach Report 2023 [Електронний ресурс]. – Режим доступу : https://www.ibm.com/reports/data-breach
40. LexisNexis Risk Solutions Cybercrime Report [Електронний ресурс]. – Режим доступу : https://risk.lexisnexis.com/insights-resources/cybercrime-report
41. CEOs Lack Confidence in Their Organizations' Ability to Protect Against Cyberattacks Despite Seeing Cybersecurity as Vital to Growth, Accenture Report Finds [Електронний ресурс]. – Режим доступу : https://newsroom.accenture.com/news/2023/ceos-lack-confidence-in-their-organizations-ability-to-protect-against-cyberattacks-despite-seeing-cybersecurity-as-vital-to-growth-accenture-report-finds
42. White Paper: Risk Management Insights from 10 years of Breach Event Monitoring [Електронний ресурс]. – Режим доступу : https://www.riskrecon.com/paper-risk-management-insights-from-10-years-of-data-breach-events
43. Distribution of detected cyberattacks worldwide in 2022 [Електронний ресурс]. – Режим доступу : https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/
44. Закон України про охорону праці [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2694-12#Text
45. Закон України «Про організацію трудових відносин в умовах воєнного стану» [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2136-20#Text
46. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/rada/show/v0007282-98#Text

# ДОДАТКИ

## Додаток А. Тези

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ**

**М А Т Е Р І А Л И**

**XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ**

# «ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

**13-14 грудня 2023 року**

**ТЕРНОПІЛЬ**
**2023**

**УДК 004.056**
**Голда Антон, Стадник Марія, к.т.н., доц.**
Тернопільський національний технічний університет імені Івана Пулюя

## МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ ІНТЕРНЕТ-БАНКІНГУ

**Golda Anton, Stadnyk Mariia, Ph.D., Assoc. Prof.**
## METHODS AND MEANS OF ENSURING INFORMATION SECURITY IN INTERNET BANKING SYSTEMS

Інтернет-банкінг в сучасному світі є не тільки зручним інструментом для фінансових операцій, але і об'єктом зростаючого інтересу для кіберзлочинців. Тому забезпечення інформаційної безпеки у цьому сегменті є надзвичайно важливим завданням для банків та їхніх клієнтів.

Одним з ключових методів є використання криптографічних технологій. Шифрування даних під час їх передачі забезпечує конфіденційність і унеможливлює несанкціонований доступ. Технології SSL/TLS використовуються для захисту від перехоплення чутливої інформації, такої як паролі та особисті дані, під час онлайн-сесій.

Двофакторна аутентифікація є ще однією ефективною мірою безпеки. Окрім звичайного пароля, користувач також підтверджує свою особу, отримуючи, наприклад, одноразовий код на мобільний телефон, також можливе забезпечення додаткової безпеки за допомогою ідентифікації за відбитком пальця, обличчям та інших фізіологічних показників.

Банки активно використовують системи виявлення аномальної активності. Ці системи аналізують звичайну поведінку користувачів та швидко реагують на будь-які незвичайні транзакції чи входи.

Оновлення програмного забезпечення та регулярні патчі важливі для закриття вразливостей. Це означає, що банки повинні постійно вдосконалювати свої системи, щоб утримувати кіберзлочинців на відстані.

Не потрібно забувати і про освіту клієнтів. Банки здійснюють інформаційні кампанії, навчаючи користувачів розпізнавати шахрайство та вживати заходи безпеки в онлайн-середовищі.

Загалом, поєднання технологічних і організаційних заходів дозволяє забезпечити ефективний рівень інформаційної безпеки в інтернет-банкінгу, створюючи надійне середовище для фінансових операцій.

Безпека в інтернет-банкінгу також вимагає постійного моніторингу та реагування на нові загрози. Активна співпраця зі спеціалізованими службами та обмін інформацією про кіберзагрози стає необхідністю. Важливим є розробка стратегій відновлення після інцидентів та регулярне проведення тестів на проникнення для виявлення слабких місць у системах. Ці заходи, поєднані з постійним вдосконаленням технічних і організаційних аспектів, створюють стійкість і надійність в інтернет-банкінгових системах.

Постійне оновлення алгоритмів машинного навчання дозволяє вдосконалювати системи виявлення та запобігання. Застосування технологій блокчейн також може відігравати ключову роль у забезпеченні безпеки та незмінності транзакцій, зменшуючи ризик фінансових маніпуляцій та шахрайства. Такий комплексний підхід забезпечує сталу безпеку в інтернет-банкінгу та зміцнює віру клієнтів у сучасні фінансові технології.

**Література:**

1. Брижко В. М. Електронний банкінг у контексті захисту персональних даних / В. М. Брижко, Ю. К. Базанов, М. Я. Швець. – К. : НДЦПІ АПРН України, 2008. – 140 с.

2. Кулініч О. А. Інтернет-банкінг в Україні як складова розвитку мережної інфраструктури / О. А. Кулініч // Економічна стратегія і перспективи розвитку сфери торгівлі та послуг : зб. наук. пр. – Х. : ХДУХТ, 2011. – Вип. 2 (14). – С. 421–429.