МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра кібербезпеки

«До захисту допущено»
Завідувач кафедри
_____ _____
(підпис) (Ім'я та ПРІЗВИЩЕ)
____ _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 Кібербезпека, освітньо-професійної програми Кібербезпека
на тему: Дослідження шляхів та вироблення рекомендацій щодо підвищення ефективності захисту банківських транзакцій в системах інтернет-банкінгу
Здобувача групи КБ-01 Сергійко Станіслава Ігоровича

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

_____ Станіслав СЕРГІЙКО
(підпис)

Керівник _____ _____
(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Суми – 2024

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра кібербезпеки

«Затверджую»
Завідувач кафедри
_____ Володимир ЛЮБЧАК
(підпис)
«___»_____ 20___ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр
зі спеціальності 125 – Кібербезпека, освітньо-професійної програми «Кібербезпека»
здобувача групи КБ-01 Сергійко Станіслава Ігоровича

1. Тема роботи: «Дослідження шляхів та вироблення рекомендацій щодо підвищення ефективності захисту банківських транзакцій в системах інтернет-банкінгу».

затверджено наказом по СумДУ Наказ №0212-VI від 04.03.2024 р. зі змінами згідно Наказу №0566-VI від 21.05.2024 р.

2. Термін подання студентом роботи: «____» _____ 20 ___ р.

3. Вихідні дані до роботи: _____

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити):
1) Огляд основних ризиків кібербезпеки. 2) Основні методи покращення безпеки. 3)Приклади на основі відомих систем. 4) Надання рекомендацій на основі вивченого матеріалу.
5. Перелік графічного матеріалу (із зазначенням плакатів, презентацій тощо) Презентація

5. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ Керівник _____
(підпис) (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	Визначення мети роботи		
2	Збір і детальне вивчення матеріалу		
3	Робота над теоретичними розділами		
4	Робота над практичним розділом		
5	Оформлення звіту і підготовка до захисту		

Здобувач вищої освіти _____ Керівник _____
(підпис) (підпис)

Анотація

Кваліфікаційна робота виконана на 44 аркушах та містить 1 рисунок і 17 джерел.

Об’єкт дослідження: процес захисту банківських транзакцій у системах інтернет-банкінгу.

Мета роботи: дослідження шляхів та розробка рекомендацій щодо підвищення ефективності захисту банківських транзакцій в інтернет-банкінгу.

Метод дослідження: аналіз кіберінцидентів, вивчення існуючих методів захисту та розробка рекомендацій на основі сучасних технологій та практик.

Результати роботи: у процесі дослідження було визначено основні загрози та вразливості у системах інтернет-банкінгу, а також запропоновано комплекс заходів для підвищення кібербезпеки. Запропоновані заходи включають впровадження стійкої політики безпеки, застосування штучного інтелекту та машинного навчання для моніторингу загроз, реалізацію політики нульової довіри, врахування ризиків з боку третіх сторін, введення точок відновлення та проведення інструктажів серед працівників.

Ключові слова: кібербезпека, інтернет-банкінг, банківські транзакції, кіберзагрози, політика безпеки.

Зміст

Вступ

Банківська система є центральною ланкою сучасної ринкової економіки та виконує низку ключових функцій, найважливішими серед яких є акумуляція та перерозподіл вільних грошових ресурсів, а також забезпечення руху фінансових інструментів між усіма економічними суб'єктами та підтримка процесів відтворення. Це означає, що банки збирають заощадження населення, підприємств та інших організацій, концентруючи ці кошти у вигляді депозитів, і потім розподіляють їх у вигляді кредитів, інвестицій та інших фінансових інструментів. Крім того, банки забезпечують ефективне здійснення платежів, управління ризиками та підтримку ліквідності в економіці.

Онлайн-банкінг став надзвичайно привабливим і зручним інструментом для сучасних користувачів, оскільки він дозволяє здійснювати фінансові операції швидко і безпечно з будь-якої точки світу. За допомогою мобільних додатків та веб-сайтів клієнти можуть перевіряти баланс рахунків, здійснювати перекази коштів, оплачувати рахунки, відкривати депозити та отримувати кредити, не виходячи з дому. Така зручність особливо цінна в умовах стрімкого ритму життя, коли час стає найважливішим ресурсом. Додатково, онлайн-банкінг забезпечує доступ до фінансової інформації в режимі реального часу, що дозволяє користувачам оперативно реагувати на зміни у своїх фінансових справах. Це робить онлайн-банкінг незамінним інструментом для сучасного споживача, який цінує ефективність та гнучкість у керуванні своїми фінансами.

Однак, через значні обсяги фінансових ресурсів, які обертаються в банківській системі, ця сфера стає привабливою для кіберзлочинців. Злочинці намагаються отримати доступ до банківських рахунків, викрасти конфіденційну інформацію або здійснити шахрайські операції. Кіберзлочинність у банківському секторі може мати серйозні наслідки, включаючи фінансові втрати, підрив довіри до фінансових установ та загрозу стабільності економіки.

Фінансова безпека банківських установ в наш час визначається не лише традиційними підходами, але й рівнем насиченості банківської системи засобами обробки інформації, які використовують мережу Інтернет та сучасні алгоритми для проведення операцій. Завдяки впровадженню інноваційних технологій, таких як штучний інтелект, блокчейн та машинне навчання, банки мають можливість автоматизувати багато процесів, підвищувати точність оцінки ризиків, знижувати операційні витрати та покращувати рівень обслуговування клієнтів[1].

Цифрові технології дозволяють значно підвищити простоту, якість та швидкість обміну даними між фінансовими установами та їхніми клієнтами, що, у свою чергу, визначає перспективи подальшого розвитку та інтеграції цих технологій у банківську сферу. Сучасні алгоритми обробки великих обсягів даних забезпечують можливість швидкого аналізу фінансових операцій, виявлення шахрайських дій та надання клієнтам персоналізованих фінансових послуг.

У той же час виникає серйозна проблема захисту інформації від кібератак. З розвитком цифрових технологій кіберзагрози стають все більш складними та різноманітними, що вимагає від банків впровадження ефективних заходів безпеки. Це потребує введення таких понять, як «кібербезпека» та «кіберзлочинність», що відноситься до інформаційно-цифрового забезпечення банківської системи. Банки повинні інвестувати в захисні технології, такі як шифрування даних, багатофакторна автентифікація, системи виявлення та запобігання вторгненням, а також у навчання персоналу з питань кібербезпеки.

Таким чином, інтеграція цифрових технологій у банківську систему є двосічним мечем: з одного боку, вона відкриває нові можливості для розвитку та підвищення ефективності, а з іншого – створює нові виклики у сфері захисту інформації, які вимагають постійного вдосконалення та адаптації до змінних умов кіберпростору.

Також незважаючи на значні успіхи, досягнуті банками у зміцненні своїх засобів захисту від кіберзагроз, питання залишається відкритим: Чи достатньо

цього? Ландшафт кіберзагроз постійно змінюється, а хакери постійно вигадують нові методи обходу захисту. Хоча банки докладають похвальних зусиль для посилення своїх заходів кібербезпеки, динамічний характер кіберзагроз вимагає постійної пильності та адаптації. Це перегони з часом і технологіями, де самовпевненість може призвести до вразливості. Таким чином, шлях до кібербезпеки триває, вимагаючи невпинних зусиль та інновацій[2].

1. Основні ризики кібербезпеки

Основними ризиками кібербезпеки для банківської системи є:

- Соціальна інженерія, наприклад фішинг.
- Зловмисне програмне забезпечення.
- DDoS-атаки.
- Внутрішні загрози або людський фактор.
- Фізичні загрози.
- Кібератаки на онлайн банкінг.

1.1 Детальний розбір загроз

- Фішинг та соціальна інженерія:
  Злочинці використовують підроблені повідомлення електронної пошти, текстові повідомлення або веб-сайти, щоб обманом змусити клієнтів або співробітників банків надати конфіденційну інформацію, таку як паролі або дані кредитних карток[3].
- Шкідливе програмне забезпечення:
  Зловмисники можуть використовувати шкідливі програми для викрадення інформації, пошкодження систем або вимагання викупу за розблокування даних. Рансомвар може паралізувати діяльність банку, що призведе до значних фінансових втрат і втрати довіри клієнтів[4].
- DDoS-атаки (розподілені атаки на відмову в обслуговуванні):
  Зловмисник «завалює» сервер інтернет-трафіком, щоб перешкодити користувачам отримати доступ до підключених онлайн-сервісів і сайтів. Такі атаки можуть зупинити роботу банківських веб-сайтів та онлайн-сервісів, що перешкоджає клієнтам здійснювати фінансові операції. Це може призвести до значних втрат для банків і незадоволення клієнтів[5].
- Внутрішні загрози:

Співробітники банків, як навмисно, так і випадково, можуть спричинити значну шкоду, надаючи доступ до конфіденційної інформації або здійснюючи шахрайські операції. Внутрішні загрози можуть бути важко виявити, оскільки співробітники мають легітимний доступ до систем[6].

- Злам банкоматів та POS-терміналів:
  Кіберзлочинці можуть використовувати спеціалізоване обладнання або програмне забезпечення для отримання доступу до банкоматів та POS-терміналів, що дозволяє їм викрадати готівку або дані платіжних карток. Ці атаки можуть включати різноманітні методи, такі як встановлення скіммерів на банкоматах, що зчитують дані з магнітних стрічок карток, та використання камер або накладок на клавіатуру для отримання PIN-кодів[7].
- Злам систем онлайн-банкінгу:
  Атаки на системи онлайн-банкінгу можуть дати злочинцям доступ до банківських рахунків клієнтів, що дозволить їм здійснювати несанкціоновані перекази або викрадати фінансові ресурси. Такі атаки можуть включати використання фішингових схем для отримання логінів та паролів користувачів, встановлення шкідливого програмного забезпечення на пристрої клієнтів або злам серверів банку. Зловмисники можуть використовувати викрадені дані для переведення коштів на підконтрольні їм рахунки, оплачувати товари та послуги, або навіть здійснювати складні фінансові махінації, включаючи відмивання грошей. Крім безпосередніх фінансових втрат для клієнтів, злам систем онлайн-банкінгу може мати серйозні наслідки для самих банків. Це може призвести до втрати репутації, зниження довіри клієнтів та регуляторних санкцій. Витрати на розслідування інциденту, компенсацію постраждалим клієнтам та впровадження додаткових заходів безпеки можуть бути значними[8].

2. Способи покращення кібербезпеки

Щоб захистити свої системи від кіберзагроз, банки повинні впроваджувати передові технології безпеки. Це включає в себе:

- Шифрування даних:
  Захист даних, як у стані спокою, так і під час передачі, за допомогою різних методів шифрування.
- Багатофакторна автентифікація (MFA):
  Використання кількох рівнів перевірки особи для доступу до банківських систем та облікових записів клієнтів. Це може бути як підтвердження біометрії, або одноразові згенеровані коди.
- Моніторинг транзакцій у реальному часі:
  Використання систем виявлення аномалій, щоб ідентифікувати та блокувати підозрілі транзакції.
- Навчання персоналу:
  Постійні лекції для співробітників щодо кібербезпеки, включаючи розпізнавання фішингових атак та інших видів соціальної інженерії.
- Оновлення та патчинг програмного забезпечення:
  Регулярне оновлення програмного забезпечення для усунення відомих вразливостей.
- Проведення аудиту безпеки:
  Регулярні перевірки та тестування систем безпеки для виявлення та усунення потенційних загроз.

Підсумовуючі, для захисту від зламу систем онлайн банкінгу банки повинні: впроваджувати багаторівневі системи безпеки, що включають використання шифрування, багатофакторної автентифікації, моніторингу аномалій у транзакціях та регулярних тестів на проникнення. Навчання клієнтів основам кібербезпеки та обізнаності про можливі загрози також є важливим компонентом захисту. Крім того, банки повинні мати плани реагування на

інциденти, які включають швидке виявлення загрози, її нейтралізацію та мінімізацію можливих збитків.

Тільки за умови ефективного управління ризиками та впровадження надійних заходів безпеки банківська система зможе виконувати свої ключові функції безпечно та ефективно. Це сприятиме підтриманню довіри з боку клієнтів і стабільності фінансової системи в цілому.

3. Реальна загроза та цифри

Згідно з звітом [9] більша частина атак на онлайн банкінг відбувається завдяки шкідливому програмному забезпеченню, а саме рансомвар.

За даними Центру стратегічних і міжнародних досліджень, причина, чому кіберзлочинці обирають банки, проста - якщо є банки, то є гроші. Атаки на банки надають кіберзлочинцям численні можливості для отримання прибутку через вимагання, крадіжки та шахрайство. Крім того, держави та хактивісти також розглядають фінансовий сектор як головну мішень для здійснення політичного впливу та просування своїх ідеологічних програм.

Згідно з звіту Державної казначейской служби США за 2021 рік банки втратили більше 1.2 мільярдів долларів у вигляді плати за розблокування їх систем внаслідок атаки рансомварами, це не включаючи витрати на відновлення систем. Також банки посідають друге місце у світі за кількістю цих атак.

Тим не менш, це не єдина загроза для них, оскільки хакери розцінюють банки як простий спосіб заробити через крадіжку і продаж баз даних, або способів несанкціонованого доступу.

Навіть у випадку таких серйозних атак потрібно бути підготовленим і зробити все можливе задля пом’якшення ризику і наслідків, наприклад:

- Ввести систему бекапів, або точок відновлення. Завдяки цьому, у випадку блокування даних програмою вимагачем буде можливість їх відновити.
- Проводити регулярну класифікацію даних задля визначення пріоритетності захисту конфіденційних даних, це дозволить вживати більш спрямовані заходи захисту.
- Введення політики нульової довіри, детальний план розподілу обов’язків і контролю доступу. Такими діями можна обмежити, або звести до нуля можливості зловмисників всередині системи, навіть якщо вони отримали доступ до неї.

- Ввести шифрування даних, особливо для найбільш важливої інформації. Таким чином, у випадку витоку інформації вона буде непотрібною і не матиме ніякої цінності.

4. Відомі практики покращення кібербезпеки

4.1 Основні цілі кібербезпеки

Основними цілями є перешкоджання або запобігання таким загрозам як:

- Розкриття інформації з обмеженим доступом.
- Порушення цілісності, модифікація, знищення або нав’язування помилкової інформації.
- Несанкціоноване використання ресурсів або блокування доступу до них.

4.2 Захист інформації з правової сторони

В основу організації режиму захисту банківської інформації покладено положення таких законодавчих актів:

- Закону України "Про банки і банківську діяльність" (ст.52 "Банківська таємниця").
- Закону України "Про підприємства в Україні" (ст. 30 "Комерційна таємниця підприємства").
- Закону України "Про інформацію" (ст. 30 "Інформація з обмеженим доступом").

Відповідно до положеннь статей цих законів склад банківської інформації можна розглядати так, як це вказано на Рис. 4.2.1

Рисунок 4.2.1 – Класифікація інформації в банківській сфері

Класифікуючи різні види інформації банки визначають ступінь захисту по відношенню до них.

4.3 Практичні методи покращення кібербезпеки

4.3.1 Віртуальні приватні мережі

Щодо практичної частини, доволі відома практика використання віртуальних приватних мереж або так званих VPN.

В основі концепції захищених віртуальних мереж лежить така ідея: Якщо в глобальній мережі потрібно передати інформацію з одного місця в інше, то для забезпечення конфіденційності між цими точками створюється віртуальний тунель, доступ до якого буде неможливий тим особам, котрі не мають легального доступу до нього.

Стосовно задач VPN критерії безпеки можуть бути визначені в такий спосіб:

- Конфіденційність – гарантія того, що в процесі передачі інформації по захищеним каналам, дані будуть відомі тільки відправнику і одержувачу.

- Цілісність – гарантія того, що дані не будуть перехоплені та змінені на шляху до точки призначення, у теоретично можливій атаці Man-in-the-Middle.
- Доступність – гарантія того, що засоби які забезпечують безпеку будуть доступні і не будуть обмежувати доступ простому користувачу.

4.3.2 Протокол захищених електронних транзакцій

Одним із перших протоколів захисту платежів в онлайн просторі був протокол «Secure Electronic Transaction» (SET), або протокол захищених електронних транзакцій. Цей протокол являв собою відкриті специфікації шифрування і захисту, розроблені виключно для забезпечення надійності фінансових операцій. Протокол SET був створений у середині 1990-х років провідними компаніями у сфері фінансових технологій, такими як Visa і MasterCard, за участі інших ключових виконавців, включаючи Microsoft, IBM і Netscape. Метою було розробити стандартизовану платформу, яка б дозволила здійснювати безпечні електронні транзакції між покупцями, продавцями та фінансовими установами.

SET використовував складні методи шифрування для забезпечення конфіденційності, цілісності та автентичності транзакцій.

SET був доволі перспективною системою завдяки своїм високим стандартам безпеки та здатності забезпечувати захист даних під час електронних транзакцій. Однак, попри технологічну досконаліть, протокол не здобув широкого поширення і згодом був відкинутий. Причини цього включали складність впровадження та використання, а також високу вартість інтеграції з існуючими системами. Багато потенціальних користувачів і споживачів вважали його занадто складним та непрактичним для повсякденного використання.

У підсумку, протокол SET став важливим етапом в еволюції технологій захисту електронних платежів, але його складність і висока вартість впровадження призвели до того, що він не зміг закріпитися на ринку. Проте

його концепції та інновації продовжують впливати на розвиток сучасних систем безпеки електронних платежів, забезпечуючи основу для нових, більш ефективних і зручних рішень. [10].

4.3.3 3-D Secure

На заміну вищезгаданому SET прийшов так званий «3-D Secure». Цей протокол був також розроблений компаніями, які працювали над SET, включаючи Visa та MasterCard, але він був набагато простішим в інтеграції та зручнішим для повсякденного використання типовим користувачем.

Назва протоколу може відрізнятися залежно від платіжної системи, яка його використовує. Для Visa це 3-D Secure, а для MasterCard — SecureCode. Інші платіжні системи також впровадили аналогічні протоколи, такі як American Express — SafeKey та JCB — J/Secure, що забезпечують додатковий рівень захисту для онлайн-транзакцій.

Принцип роботи 3-D Secure полягає у додатковій автентифікації користувача під час здійснення онлайн-платежів. Тобто, під час проведення операції оплати в мережі додається додатковий етап, який вимагає від користувача введення одноразового згенерованого коду-паролю. Цей код надсилається користувачеві через SMS, електронну пошту або генерується у мобільному додатку банку. Такий підхід підтверджує, що транзакцію проводить саме власник картки, а не шахрай, який випадково отримав доступ до даних картки.

Цей спосіб є більш дієвим, оскільки до його впровадження більшість банків використовували для підтвердження особи фіксований пароль. Фіксовані паролі мають значні вразливості, оскільки можуть бути перехоплені або викрадені під час фішингових атак, що дозволяє зловмисникам здійснювати несанкціоновані транзакції. Одноразові паролі значно знижують ризик таких атак, оскільки кожен код може бути використаний лише один раз і діє лише протягом обмеженого часу.

Крім підвищення рівня безпеки, 3-D Secure також зручний для користувачів. Він не вимагає встановлення додаткового програмного забезпечення або

складних процедур налаштування. Більшість користувачів вже мають доступ до засобів отримання одноразових паролів, таких як мобільні телефони. Це робить процес автентифікації простим і швидким, мінімізуючи незручності під час здійснення онлайн-платежів.

Впровадження 3-D Secure значно підвищило рівень довіри до онлайн-транзакцій, як з боку споживачів, так і з боку продавців. Банки та платіжні системи також отримали додаткові переваги у вигляді зниження кількості шахрайських транзакцій та зменшення фінансових втрат, пов'язаних з шахрайством. Завдяки цьому, 3-D Secure став стандартом безпеки для більшості міжнародних платіжних систем і продовжує розвиватися, включаючи нові функції та покращення для ще більшої ефективності захисту електронних платежів[11].

У звичайних транзакціях, здійснених без використання протоколу 3-D Secure, відповідальність за шахрайські операції, такі як оплата краденими картками, несе торговець — підприємство, на сайті якого було куплено товар чи послугу. Це означає, що у разі виявлення шахрайства, саме торговець змушений покривати збитки та вирішувати питання з компенсаціями для постраждалих клієнтів. Такий підхід створює значні фінансові ризики для підприємств і може вплинути на їхню репутацію.

Однак, у разі застосування протоколу 3-D Secure, відповідальність за шахрайські операції переходить до емітента картки, тобто банку, що відоме як "liability shift". Це означає, що у випадку, якщо транзакція виконана з використанням 3-D Secure виявиться шахрайською, збитки покриватиме не торговець, а банк-емітент картки. Такий перерозподіл відповідальності значно знижує ризики для торговців і робить впровадження протоколу 3-D Secure вигідним для них.

Цей механізм працює наступним чином: коли покупець здійснює платіж на сайті торговця, який підтримує 3-D Secure, він проходить додаткову автентифікацію через одноразовий код-пароль, надісланий банком-емітентом. Якщо транзакція авторизується через цей процес банк-емітент підтверджує, що

покупець є справжнім власником картки і бере на себе відповідальність за будь-які можливі шахрайські дії, пов'язані з цією транзакцією.

У жовтні 2016 року EMVCo опублікувала специфікацію протоколу 3-D Secure 2.0. Ця нова версія протоколу була розроблена для того, щоб бути менш нав'язливою, ніж перша версія, дозволяючи надсилати до банку клієнта більше контекстних даних для перевірки та оцінки ризику транзакції. Ці дані можуть включати: поштові адреси, історію транзакцій, інформацію про пристрій та багато іншого. Завдяки цьому банки можуть краще оцінювати ризик кожної транзакції в режимі реального часу, мінімізуючи необхідність у додаткових перевірках для більшості операцій.

Однією з ключових особливостей 3-D Secure 2.0 є те, що клієнт повинен проходити автентифікацію лише в тому випадку, якщо його транзакція визначена як операція з високим ризиком. Це значно покращує досвід використання, знижуючи кількість переривань під час процесу покупки. Крім того, робочий процес для автентифікації був оптимізований таким чином, що він не вимагає переадресації на окрему сторінку. Замість цього автентифікація може бути інтегрована безпосередньо в інтерфейс торгового майданчика, що робить процес більш плавним і непомітним для користувача.

Ще однією важливою особливістю 3-D Secure 2.0 є можливість автентифікації через мобільний додаток банку або фінансової установи. Це дозволяє користувачам підтверджувати транзакції за допомогою біометричних даних, таких як відбиток пальця або розпізнавання обличчя, що не тільки підвищує рівень безпеки, але й робить процес автентифікації швидким і зручним.

Цей підхід значно підвищує безпеку онлайн-транзакцій, одночасно покращуючи користувацький досвід. Завдяки використанню додаткових контекстних даних банки можуть більш точно визначати ризикові операції та застосовувати автентифікацію лише тоді, коли це дійсно необхідно. Це знижує

навантаження на користувачів, оскільки більшість транзакцій можуть проходити без перешкод.

Крім того, 3-D Secure 2.0 відповідає вимогам ЄС, щодо надійної автентифікації клієнтів (Strong Customer Authentication, SCA), що є частиною Директиви про платіжні послуги 2 (PSD2). Це забезпечує додатковий рівень захисту для користувачів та підвищує загальний рівень безпеки електронних платежів у Європі[12].

5. Відомі системи і досвід забезпечення інформаційної безпеки в них

5.1 SWIFT

Найбільш відомою з усіх нині існуючих міжнародних платіжних систем є SWIFT (Society for Worldwide Interbank Financial Telecommunication). SWIFT одержала широке поширення в сфері міжнародних банківських розрахунків, завдяки своїй надійності, ефективності та високому рівню безпеки.

SWIFT була заснована в 1973 році в Брюсселі, Бельгія, з метою створення уніфікованої системи для обміну фінансовою інформацією між банками та іншими фінансовими установами по всьому світу. Сьогодні SWIFT об'єднує понад 11,000 фінансових установ у більш ніж 200 країнах, що робить її найбільшою мережею для передачі фінансових повідомлень у світі.

Основною функцією SWIFT є передача стандартних фінансових повідомлень між банками. Це дозволяє банкам: здійснювати міжнародні платежі, валютні операції, торговельне фінансування, виплати дивідендів та інші фінансові операції. Система забезпечує високий рівень безпеки та конфіденційності, завдяки використанню сучасних технологій шифрування та протоколів захисту даних.

Основні переваги системи SWIFT включають:

- Уніфікація стандартів: SWIFT використовує стандартизовані формати повідомлень, що полегшує обмін інформацією між різними фінансовими

установами. Це значно знижує ймовірність помилок і підвищує ефективність операцій.

- Надійність і швидкість: Система забезпечує швидку та надійну передачу фінансових повідомлень, що дозволяє банкам здійснювати транзакції в режимі реального часу.
- Безпека: Використання сучасних методів шифрування та багаторівневих протоколів безпеки гарантує захист фінансової інформації від несанкціонованого доступу та кібератак.
- Глобальне покриття: SWIFT має глобальну мережу, що охоплює більшість банків та фінансових установ по всьому світу. Це робить її незамінним інструментом для здійснення міжнародних платежів та розрахунків.

Еволюція та розвиток SWIFT:

За час свого існування SWIFT постійно вдосконалювала свої технології та розширювала функціональність. Однією з останніх ініціатив SWIFT є впровадження системи SWIFT gpi (Global Payments Innovation), яка спрямована на покращення швидкості, прозорості та простежуваності міжнародних платежів. SWIFT gpi дозволяє банкам та їхнім клієнтам відстежувати статус платежів у режимі реального часу та отримувати інформацію про кінцеві витрати та час зарахування коштів.

Виклики та майбутнє SWIFT:

Попри свої численні переваги, SWIFT стикається з певними викликами, такими як конкуренція з боку нових фінтех-компаній та платіжних платформ, зокрема, блокчейн-рішень. Однак завдяки постійним інноваціям та вдосконаленню технологій, SWIFT залишається лідером у сфері міжнародних фінансових комунікацій і має всі шанси зберегти свої позиції в майбутньому.

З технічної точки зору SWIFT являє собою міжнародну телекомунікаційну мережу, яка забезпечує фінансовим організаціям з різних країн можливість безперешкодно обмінюватися банківською і фінансовою

інформацією. Ця мережа працює за принципом хаби, дозволяючи установам використовувати комп'ютери і термінали різних типів для підключення до неї. Основні технічні аспекти SWIFT включають**:**

- Архітектура мережі: SWIFT використовує багаторівневу архітектуру, яка включає в себе як фізичну інфраструктуру, так і програмні компоненти. Фізична інфраструктура складається з дата-центрів, розташованих у різних частинах світу, які забезпечують безперервність і надійність роботи мережі. Програмні компоненти включають сервіси для маршрутизації, шифрування і обробки фінансових повідомлень.
- Протоколи безпеки: SWIFT використовує передові протоколи безпеки для захисту переданої інформації. Це включає в себе багаторівневе шифрування даних, автентифікацію користувачів, контроль доступу і моніторинг активності в реальному часі. Завдяки цьому забезпечується конфіденційність, цілісність і доступність даних.
- Стандартизація повідомлень: Однією з ключових особливостей SWIFT є стандартизація формату фінансових повідомлень. Використовуючи стандартизовані повідомлення (MT і MX), фінансові установи можуть ефективно і точно обмінюватися інформацією. Це знижує ймовірність помилок і забезпечує сумісність між різними системами.
- Інтеграція з внутрішніми системами: SWIFT надає інструменти і API для інтеграції з внутрішніми системами банків і інших фінансових установ. Це дозволяє автоматизувати процеси обміну даними і знижує потребу в ручному введенні інформації, що підвищує загальну ефективність роботи.
- Моніторинг і управління: SWIFT надає засоби для моніторингу і управління всіма аспектами роботи мережі. Це включає в себе інструменти для відстеження статусу повідомлень, управління користувачами, налаштування параметрів безпеки і генерації звітів. Завдяки цьому фінансові установи можуть забезпечити високу якість обслуговування і швидко реагувати на будь-які інциденти.

- Підтримка різних типів транзакцій: SWIFT підтримує широкий спектр фінансових операцій, включаючи міжнародні платежі, валютні операції, документарні акредитиви, торговельне фінансування та інші. Це дозволяє банкам і фінансовим установам використовувати одну платформу для виконання різноманітних фінансових операцій.
- Висока надійність і доступність: SWIFT забезпечує високу надійність і доступність своєї мережі завдяки використанню резервних центрів обробки даних і систем автоматичного перемикання у разі виникнення збоїв. Це гарантує безперервність роботи мережі навіть у випадку технічних проблем.
- Постійне вдосконалення: SWIFT постійно вдосконалює свої технології і сервіси, адаптуючись до змін у фінансовому середовищі і вимогах клієнтів. Це включає в себе впровадження нових стандартів повідомлень, покращення протоколів безпеки, розширення функціональності і інтеграцію з новими фінансовими технологіями.

Завдяки своїй технічній інфраструктурі і широким можливостям, SWIFT стала невід'ємною частиною глобальної фінансової системи, забезпечуючи швидкий, безпечний і надійний обмін банківською і фінансовою інформацією між установами по всьому світу[13][14].

5.1.1 Методи безпеки які використовуються в SWIFT

Забезпечення безпеки в системі SWIFT є критично важливим, оскільки вона обробляє величезний обсяг конфіденційних фінансових даних. SWIFT використовує багаторівневий підхід до забезпечення безпеки, який включає в себе кілька основних методів і заходів.

1. Шифрування даних

- Транспортне шифрування**:** Усі дані, які передаються через мережу SWIFT, шифруються за допомогою протоколів шифрування, таких як TLS (Transport Layer Security). Це забезпечує захист даних під час їх передачі від точки відправлення до точки призначення.

- Шифрування на рівні повідомлень: Крім транспортного шифрування, дані у повідомленнях SWIFT можуть бути додатково зашифровані на рівні додатку, що забезпечує ще більший рівень захисту.

2. Аутентифікація та контроль доступу
   - Двофакторна автентифікація (2FA): SWIFT використовує двофакторну автентифікацію для доступу до своїх систем. Це включає в себе поєднання паролю з додатковим фактором, таким як одноразовий пароль (OTP) або апаратний токен.
   - Рольове управління доступом (RBAC): SWIFT впроваджує рольове управління доступом, що означає, що користувачі мають доступ тільки до тих ресурсів і функцій, які необхідні для виконання їхніх службових обов'язків.
3. Моніторинг та управління загрозами
   - Моніторинг у реальному часі: SWIFT постійно моніторить мережу в режимі реального часу, щоб виявляти та реагувати на підозрілу активність або потенційні загрози. Це включає в себе аналіз логів і використання систем виявлення вторгнень (IDS).
   - Аналітика поведінки: Використання аналітики поведінки для виявлення аномалій у поведінці користувачів та систем, що можуть вказувати на можливі загрози або шахрайські дії.
4. Протоколи безпеки та стандарти
   - ISO 20022: SWIFT використовує стандарти ISO 20022 для фінансових повідомлень, що забезпечує високу сумісність та безпеку обміну даними.
   - Криптографічні протоколи: Використання сучасних криптографічних протоколів для забезпечення цілісності та конфіденційності даних.
5. Безпека інфраструктури
   - Фізична безпека дата-центрів: Дата-центри SWIFT захищені фізичними засобами безпеки, такими як контроль доступу, відеоспостереження та охорона.

- Резервування та відновлення: Використання резервних дата-центрів і систем відновлення після збоїв для забезпечення безперервності роботи та мінімізації ризиків простоїв.

6. Процедури та політики безпеки
   - Регулярні аудити та перевірки: Проведення регулярних аудитів безпеки для виявлення вразливостей і забезпечення відповідності стандартам безпеки.
   - Політики безпеки: Впровадження чітких політик безпеки, які регулюють усі аспекти роботи з даними та управління доступом у системі SWIFT.
7. Навчання та підвищення обізнаності
   - Навчальні програми: Проведення навчальних програм для співробітників та користувачів системи SWIFT з метою підвищення обізнаності про безпеку та дотримання кращих практик.
   - Тестування на проникнення: Регулярне проведення тестувань на проникнення для виявлення вразливостей у системі та перевірки ефективності заходів безпеки.
8. Інновації та адаптація
   - Впровадження нових технологій: Постійне впровадження нових технологій та методів захисту для адаптації до змінюваних загроз і викликів у сфері кібербезпеки.
   - Співпраця з партнерами: Співпраця з іншими фінансовими установами, організаціями з кібербезпеки та державними органами для обміну інформацією про загрози та розробки спільних заходів безпеки.

Завдяки цим методам і заходам SWIFT забезпечує високий рівень безпеки для своїх користувачів, знижуючи ризики кіберзагроз та забезпечуючи безперервність і надійність фінансових операцій на глобальному рівні[15].

5.2 SEPA

SEPA (Single Euro Payments Area) - це ініціатива Європейського Союзу, спрямована на гармонізацію та стандартизацію процесу здійснення безготівкових платежів у євро серед країн-учасниць. Метою SEPA є спрощення та прискорення фінансових операцій, зробивши їх такими ж простими та ефективними, як внутрішні платежі в межах окремої країни.

Впровадження SEPA створило умови для формування єдиного ринку платежів у євро, усунувши правові та технічні бар'єри між країнами-учасницями. Це забезпечило можливість здійснювати транзакції у євро за єдиними правилами, незалежно від географічного положення платника та отримувача, що сприяло більшій інтеграції та економічному співробітництву між європейськими державами.

Технічна структура SEPA:

З технічної точки зору SEPA складається з кількох ключових компонентів:

1. SEPA Credit Transfer (SCT):
    - Опис: SCT дозволяє здійснювати кредитні перекази у євро між банківськими рахунками в межах країн-учасниць SEPA.
    - Переваги: Стандартизовані формати платежів, швидка обробка (перекази зазвичай виконуються протягом одного робочого дня).
2. SEPA Direct Debit (SDD):
    - Опис: SDD дозволяє автоматично списувати кошти з рахунку платника на користь отримувача на основі попередньо наданої згоди.
    - Переваги: Зручність для регулярних платежів, таких як комунальні послуги або підписки.
3. SEPA Instant Credit Transfer (SCT Inst):
    - Опис: SCT Inst дозволяє здійснювати миттєві кредитні перекази у євро, доступні 24/7.

- Переваги: Перекази здійснюються за кілька секунд, що робить їх ідеальними для термінових платежів.

SEPA відіграє важливу роль у створенні єдиного європейського ринку платежів у євро, підвищуючи ефективність, зручність і безпеку фінансових операцій. Завдяки впровадженню сучасних стандартів і технологій SEPA забезпечує надійність і швидкість транзакцій, сприяючи економічному зростанню та інтеграції в Європі.

Країни-учасниці SEPA включають усі держави-члени Європейського Союзу, а також деякі інші європейські країни, такі як Норвегія, Ісландія, Ліхтенштейн, Швейцарія, Монако, Сан-Марино і Велика Британія. Завдяки SEPA громадяни та підприємства цих країн можуть здійснювати транзакції у євро так само легко, як і внутрішні платежі, що значно спрощує та прискорює фінансові операції в межах Європи[16].

5.2.1 Безпека SEPA

Безпека в SEPA забезпечується за допомогою таких методів:

1. Шифрування даних:
    - Всі транзакції у системі SEPA шифруються для забезпечення конфіденційності та цілісності даних під час їх передачі через мережу.
2. Аутентифікація та авторизація:
    - Використання багатофакторної автентифікації (MFA) для підтвердження особи користувачів та авторизації транзакцій.
3. Моніторинг транзакцій:
    - Постійний моніторинг транзакцій у режимі реального часу для виявлення та запобігання шахрайству.
4. Європейські стандарти безпеки:
    - Впровадження стандартів безпеки, таких як PSD2 (Revised Payment Services Directive), що вимагає надійної автентифікації клієнтів (SCA) та інших заходів безпеки.

Переваги SEPA

1. Сприяння інтеграції ринку:
    - SEPA сприяє створенню єдиного ринку платежів у євро, що підвищує ефективність і конкуренцію серед банків та фінансових установ.
2. Зручність для споживачів:
    - Споживачі можуть здійснювати транзакції в євро так само легко, як внутрішні платежі, незалежно від країни-учасниці SEPA.
3. Зниження вартості транзакцій:
    - Стандартизація процесів і підвищена ефективність знижують вартість міжнародних переказів у євро.
4. Прозорість та простота:
    - Стандартизовані формати платежів (наприклад, IBAN для номерів рахунків) спрощують обробку та перевірку транзакцій[17].

6. Рекомендації щодо покращення безпеки

Враховуючи стрімкий розвиток систем управління, штучного інтелекту, а також методів обходу захисту з’являється питання: «Якими методами можна покращити безпеку?». Насправді, методів безліч, але потрібно виділити найважливіші і впроваджувати їх, слідкуючи за тенденціями розвитку технологій і кібератак. Рекомендованими методами будуть:

6.1 Введення стійкої політики безпеки

Неформальні політики безпеки без узгодження з персоналом можуть нести в собі численні ризики.

Під неформальними політиками безпеки розуміються правила та заходи, які можуть існувати, але не мають офіційного статусу або не були належним чином доведені до відома співробітників. Такі політики можуть призвести до непорозумінь і невиконання важливих заходів безпеки. Співробітники можуть бути не обізнані про їх існування, що значно підвищує ризик порушення безпеки. Потрібно ввести максимально детальну політику безпеки, яку потрібно буде донести до кожного працівника структури через офіційний спосіб, а також з підтвердженням ознайомлення у вигляді підпису.

Етапи впровадження детальної політики безпеки:

- Аналіз поточних ризиків та вразливостей:

Перед розробкою політики слід провести детальний аналіз існуючих ризиків та вразливостей. Це включає аудит поточних процедур, технологій та інфраструктури безпеки. Визначення найважливіших аспектів, які потребують уваги, допоможе створити ефективні та цілеспрямовані правила безпеки.

- Розробка політики:

Політика безпеки повинна бути максимально деталізованою та включати чіткі інструкції щодо захисту інформації, використання IT-ресурсів, управління доступом та реагування на інциденти. Вона повинна охоплювати всі аспекти

безпеки, включаючи фізичну безпеку, кібербезпеку та заходи протидії внутрішнім загрозам.

- Офіційне впровадження політики:

Політику безпеки слід впроваджувати офіційно через внутрішні канали комунікації, такі як внутрішні наради, електронні листи, корпоративний портал або спеціальні тренінги. Важливо, щоб кожен співробітник отримав копію політики та мав можливість ознайомитися з нею.

Після офіційного впровадження політики необхідно провести навчання для всіх співробітників. Це допоможе їм зрозуміти зміст політики, її важливість та способи дотримання. Регулярні тренінги допоможуть закріпити знання та навички, необхідні для підтримки безпеки.

- Підтвердження ознайомлення:

Кожен співробітник повинен офіційно підтвердити своє ознайомлення з політикою безпеки. Це може бути зроблено шляхом підписання відповідного документа або електронного підтвердження. Така практика дозволяє забезпечити, що всі співробітники знають про вимоги та готові їх дотримуватися.

- Моніторинг та контроль:

Після впровадження політики безпеки необхідно постійно моніторити її дотримання. Регулярні перевірки та аудити допоможуть виявляти порушення та вчасно їх усувати. Використання систем моніторингу безпеки дозволяє автоматизувати цей процес і швидко реагувати на інциденти.

- Відповідальність за порушення:

У політиці безпеки повинні бути чітко визначені санкції за її порушення. Це може включати дисциплінарні заходи, такі як попередження, штрафи або звільнення. Наявність санкцій підвищує відповідальність співробітників за дотримання правил безпеки.

- Актуалізація політики:

Політика безпеки повинна бути динамічною та оновлюватися відповідно до змін у технологіях, законодавстві та нових загрозах. Регулярний перегляд та

актуалізація політики, дозволяють підтримувати її ефективність та відповідність поточним вимогам.

Введення стійкої політики безпеки є важливим кроком для захисту інформаційних ресурсів організації. Чіткі інструкції, офіційне впровадження, навчання співробітників та постійний моніторинг, допоможуть знизити ризики та забезпечити високий рівень безпеки.

6.2 Застосування штучного інтелекту, машинного навчання та аналітиків

Сучасні технології відіграють важливу роль у кіберзахисті, забезпечуючи ефективні засоби для протидії загрозам. Застосування штучного інтелекту (ШІ), машинного навчання (МН) та аналітиків є ключовими компонентами сучасної стратегії кібербезпеки.

Штучний інтелект та машинне навчання здатні обробляти великі обсяги даних з високою швидкістю, що дає змогу швидко виявляти та реагувати на потенційні загрози. Вони використовуються для автоматизації процесів моніторингу, аналізу та реагування на інциденти, що значно підвищує ефективність кіберзахисту. Ось кілька прикладів використання цих технологій:

- Автоматичне виявлення загроз**:**

ШІ та МН можуть аналізувати великий обсяг мережевого трафіку, логів та інших даних, щоб виявляти аномалії та потенційні загрози. Це дозволяє швидко реагувати на нові атаки, які можуть не бути поміченими традиційними методами.

- Проактивне прогнозування загроз**:**

Застосовуючи алгоритми машинного навчання, системи можуть прогнозувати можливі загрози, на основі історичних даних та поведінкових моделей. Це допомагає вживати превентивні заходи для захисту системи до того, як загроза стане реальною проблемою.

- Аналіз вразливостей**:**

ШІ може автоматично перевіряти системи на наявність відомих вразливостей, а також виявляти нові. Це дозволяє забезпечити своєчасне виправлення вразливостей та запобігання можливим атакам.

- Аналіз ризиків**:**

Використовуючи аналітику, ШІ може оцінювати ризики різних кіберзагроз та визначати пріоритетні заходи для їх усунення. Це допомагає організаціям ефективно розподіляти ресурси та зосереджуватися на найбільш критичних аспектах безпеки.

- Виявлення аномалій у реальному часі:

Системи, що базуються на ШІ, здатні виявляти аномалії у поведінці користувачів та мережевому трафіку в режимі реального часу. Це дозволяє швидко реагувати на можливі загрози та мінімізувати їхній вплив.

- Адаптивні системи захисту:

Машинне навчання дозволяє системам постійно навчатися та адаптуватися до нових типів загроз. Це забезпечує більш динамічний та ефективний захист порівняно з традиційними статичними методами.

- Розширена аналітика:

ШІ може виконувати розширену аналітику для глибшого розуміння складних атак та їхніх причин. Це допомагає розробляти більш ефективні стратегії захисту та запобігати подібним інцидентам у майбутньому.

Завдяки застосуванню штучного інтелекту, машинного навчання та аналітиків, організації можуть підвищити свою здатність до виявлення, прогнозування та запобігання кіберзагрозам. Ці технології дозволяють автоматизувати багато аспектів кіберзахисту, що робить його більш ефективним та швидким. Використання таких інструментів стає необхідним для забезпечення надійної кібербезпеки у сучасному цифровому світі.

6.3 Безперервний моніторинг загроз

Безперервний моніторинг загроз є одним з найважливіших аспектів забезпечення кібербезпеки в сучасних умовах. Хакери діють цілодобово, постійно шукаючи вразливості у системах безпеки. Тому організації повинні здійснювати постійний моніторинг своїх систем, щоб своєчасно виявляти та реагувати на потенційні загрози.

Основні компоненти безперервного моніторингу загроз:

- Цілодобовий моніторинг:

Моніторинг систем повинен проводитися 24/7 без перерв. Це забезпечує своєчасне виявлення будь-яких підозрілих дій або аномалій, які можуть свідчити про спробу атаки.

- Система сповіщень у реальному часі:

Використання системи сповіщень у реальному часі дозволяє оперативно інформувати відповідальних осіб про виявлені загрози. Це може включати сповіщення через електронну пошту, SMS, мобільні додатки або спеціалізовані системи управління подіями безпеки.

- Аналіз логів та мережевого трафіку:

Проводиться постійний аналіз логів та мережевого трафіку для виявлення незвичайної активності або аномалій. Використання спеціалізованих інструментів дозволяє автоматизувати цей процес та підвищити його ефективність.

- Використання технологій штучного інтелекту та машинного навчання:

Застосування штучного та машинного навчання для аналізу великих обсягів даних дозволяє швидко виявляти потенційні загрози та реагувати на них. Ці технології можуть автоматично визначати патерни поведінки, характерні для атак, та попереджати про них у режимі реального часу.

- Інтеграція з системами управління подіями безпеки (SIEM):

Інтеграція систем моніторингу з SIEM дозволяє централізовано збирати, аналізувати та корелювати дані з різних джерел. Це допомагає швидко виявляти комплексні атаки та реагувати на них.

- Реагування на інциденти:

Наявність чітко визначених процедур реагування на інциденти є важливою складовою безперервного моніторингу. Це включає визначення відповідальних осіб, протоколи дій у разі виявлення загроз та плани відновлення після інцидентів.

- Регулярне оновлення систем безпеки:

Проводити регулярні оновлення та патчі для всіх програмних та апаратних засобів, щоб зменшити ризик використання відомих вразливостей.

Безперервний моніторинг загроз дозволяє підтримувати високий рівень кібербезпеки, забезпечуючи своєчасне виявлення та реагування на загрози. Це важливий аспект захисту інформаційних систем, який допомагає запобігати потенційним атакам та мінімізувати їхній вплив на організацію.

6.4 Політика нульової довіри:

Політика нульової довіри є сучасним підходом до забезпечення кібербезпеки, що передбачає відсутність довіри до будь-якого користувача або пристрою як всередині, так і за межами мережі організації. Кожен користувач, незалежно від його місця розташування чи ролі, повинен пройти ретельну перевірку перед отриманням доступу до важливих даних або інструментів управління.

Основні принципи політики нульової довіри:

Жоден користувач не може мати доступу до важливих даних або інструментів управління без авторизації та належних прав доступу:

Кожен запит на доступ до ресурсів системи повинен бути перевірений і авторизований відповідно до встановлених правил доступу. Це включає

аутентифікацію користувача, перевірку його прав доступу та оцінку контекстуального ризику.

- Введення політики розмежування доступу:

Доступ до різних ресурсів системи повинен бути суворо розмежований відповідно до принципу найменших привілеїв. Це означає, що користувачі повинні мати доступ тільки до тих ресурсів, які необхідні їм для виконання своїх обов'язків. Наприклад, співробітник відділу фінансів не повинен мати доступ до даних HR, якщо це не входить до його функціональних обов'язків.

- Безперервна перевірка та моніторинг:

Доступ до ресурсів системи повинен постійно моніторитися, а підозрілі дії або спроби доступу повинні негайно блокуватися і розслідуватися. Це може включати аналіз логів, моніторинг мережевого трафіку та використання інструментів для виявлення аномалій.

- Використання багатофакторної аутентифікації (MFA):

Для підвищення рівня безпеки доступу необхідно впровадити багатофакторну аутентифікацію, яка передбачає використання декількох методів підтвердження особи користувача. Це може бути комбінація паролів, одноразових кодів, біометричних даних (відбитки пальців, розпізнавання обличчя) та інших факторів.

- Контроль доступу на основі атрибутів:

Використання моделей контролю доступу на основі атрибутів дозволяє динамічно оцінювати запити на доступ на основі множини атрибутів, таких як роль користувача, його місцезнаходження, тип пристрою та інші фактори. Це дозволяє забезпечити більш гнучкий і точний контроль доступу.

- Регулярне оновлення політик безпеки:

Політики доступу та безпеки повинні регулярно переглядатися та оновлюватися відповідно до змін у бізнес-процесах, технологіях та загрозах безпеці. Це допомагає забезпечити актуальність і ефективність заходів безпеки.

Впровадження політики нульової довіри має великий вплив на безпеку систем, оскільки мінімізує ризик несанкціонованого доступу та підвищує

загальний рівень захисту організації. Це підхід, який дозволяє ефективно протистояти сучасним загрозам та забезпечувати надійну безпеку даних у будь-яких умовах.

6.5 Враховування ризиків з третьої сторони

Використання додаткових систем та сервісів з третьої сторони є звичайною практикою для багатьох банків, оскільки це дозволяє спростити операційні процеси та підвищити ефективність роботи. Проте, такі інтеграції можуть нести значні загрози безпеці, якщо не дотримуватися відповідних заходів захисту.

Основні аспекти врахування ризиків з третьої сторони:

- Використання API:

Банки часто використовують API (інтерфейси програмування додатків) для інтеграції з різними сервісами та системами з третьої сторони. API дозволяють автоматизувати багато процесів та забезпечити зручний обмін даними між системами. Проте, неправильно налаштовані або ненадійні API можуть стати вразливими точками для кібератак.

- Оцінка надійності сторонніх систем:

Перед інтеграцією будь-якої сторонньої системи або сервісу необхідно провести ретельну оцінку їх надійності та безпеки. Це включає перевірку відгуків інших користувачів, аналіз історії безпеки постачальника, проведення аудиту безпеки та тестування систем на наявність вразливостей.

- Аудит безпеки:

Регулярне проведення аудиту безпеки сторонніх систем допомагає виявити потенційні вразливості та слабкі місця. Це може включати перевірку коду, тестування на проникнення (penetration testing) та оцінку відповідності стандартам безпеки.

- Умови договору та рівень обслуговування:

Важливо ретельно опрацювати умови договору та угоди про рівень обслуговування з постачальниками сторонніх систем. В угодах повинні бути чітко визначені обов'язки постачальника щодо забезпечення безпеки даних, реагування на інциденти безпеки та проведення регулярних оновлень.

- Використання протоколів безпеки:

Під час інтеграції сторонніх систем необхідно забезпечити використання надійних протоколів безпеки для передачі даних. Це може включати шифрування даних, використання HTTPS, впровадження багатофакторної аутентифікації та інших заходів безпеки.

- Контроль доступу:

Необхідно суворо контролювати доступ сторонніх систем до внутрішніх ресурсів банку. Використання політики найменших привілеїв дозволяє обмежити доступ тільки до тих ресурсів, які необхідні для виконання конкретних завдань.

- Постійний моніторинг:

Після інтеграції сторонніх систем необхідно здійснювати постійний моніторинг їх роботи та безпеки. Це дозволяє своєчасно виявляти та реагувати на потенційні загрози.

- Оновлення та патчі:

Сторонні системи та API повинні регулярно оновлюватися та патчитися для забезпечення захисту від нових вразливостей та загроз. Важливо стежити за оновленнями від постачальника та своєчасно їх впроваджувати.

Врахування ризиків з третьої сторони є важливим елементом комплексної стратегії кібербезпеки банків. Це дозволяє мінімізувати можливі загрози та забезпечити надійний захист даних і систем банку при використанні сторонніх сервісів.

6.6 Введення точок відновлення

Рансомвар атаки є однією з найпоширеніших загроз для банківських структур, оскільки вони можуть призвести до серйозних фінансових втрат та порушення роботи систем. Найкращим способом уникнути ризику таких атак та забезпечити швидке відновлення систем є впровадження точок відновлення через регулярне створення резервних копій даних (бекапів).

Основні аспекти введення точок відновлення:

- Регулярне створення резервних копій:

Всі важливі дані та системи повинні регулярно зберігатися у вигляді резервних копій. Це може бути щоденне, тижневе або щомісячне копіювання залежно від критичності даних та обсягів змін.

- Дублювання копій:

Резервні копії повинні зберігатися в декількох фізично віддалених місцях, щоб уникнути втрати даних у разі фізичного знищення або пошкодження основного місця зберігання. Це може бути як локальне зберігання, так і хмарні рішення.

- Шифрування бекапів:

Для забезпечення безпеки резервних копій необхідно використовувати шифрування. Це допоможе захистити дані від несанкціонованого доступу у разі втрати або крадіжки носія з бекапами.

- Автоматизація процесу:

Процес створення резервних копій має бути максимально автоматизованим. Це знижує ризик людської помилки та забезпечує своєчасне виконання копіювання.

- Перевірка цілісності та відновлюваності:

Регулярна перевірка цілісності резервних копій та можливість відновлення системи з цих копій. Це допоможе вчасно виявити можливі проблеми та забезпечити, що у разі необхідності відновлення буде успішним.

- Створення точок відновлення системи:

Крім бекапів даних, важливо створювати точки відновлення всієї системи. Це дозволяє відновити не тільки дані, але й налаштування та конфігурації систем у разі атаки або збою.

- Розробка плану відновлення після катастроф:

Розробка і впровадження плану відновлення після катастроф. Він має містити чіткі інструкції щодо відновлення систем і даних у разі раптової атаки або іншої надзвичайної ситуації.

- Навчання персоналу:

Персонал повинен бути навчений діяти відповідно до плану відновлення та знати основні принципи роботи з резервними копіями. Це допоможе швидко і ефективно відновити роботу систем у разі атаки.

Впровадження точок відновлення та регулярне створення резервних копій є критично важливим для забезпечення безперервності роботи банківських структур та захисту від рансомвар атак. Ці заходи дозволяють швидко відновити системи та мінімізувати втрати у разі кібератак або інших загроз.

6.7 Підвищення обізнаності серед працівників

Фішинг є одним з найпопулярніших методів зламу банківських установ, оскільки він використовує людський фактор для отримання доступу до конфіденційної інформації та систем. Для мінімізації ризиків, пов'язаних з фішингом та іншими соціотехнічними атаками, необхідно створити культуру кіберобізнаності серед працівників.

Основні аспекти підвищення обізнаності серед працівників:

- Регулярне навчання та тренінги:

Організовуйте регулярні навчання та тренінги з кібербезпеки для всіх працівників. Це може включати семінари, вебінари, інтерактивні курси та інші форми навчання, які допоможуть співробітникам зрозуміти загрози та методи їх уникнення.

- Симуляції фішингових атак:

Проводьте регулярні симуляції фішингових атак, щоб навчити працівників розпізнавати підозрілі електронні листи та інші форми соціальної інженерії. Це допоможе їм діяти більш обачно та безпечно у своїй повсякденній роботі.

- Інформаційні кампанії:

Розгорніть інформаційні кампанії з кібербезпеки, включаючи розсилку електронних листів, плакати, інформаційні бюлетені та інші матеріали, які нагадуватимуть працівникам про важливість дотримання правил безпеки.

- Чіткі інструкції та політики:

Введіть чіткі інструкції та політики щодо безпечного використання електронної пошти, інтернету та інших комунікаційних засобів. Усі працівники повинні бути ознайомлені з цими політиками та розуміти наслідки їх порушення.

- Звітування про підозрілу активність:

Створіть просту та зрозумілу систему звітування про підозрілу активність. Працівники повинні знати, як і кому повідомляти про підозрілі електронні листи, дзвінки або інші види комунікацій.

- Підтримка відкритої комунікації:

Заохочуйте відкриту комунікацію та обговорення питань кібербезпеки серед працівників. Створіть середовище, в якому співробітники можуть вільно ділитися своїми побоюваннями та пропозиціями щодо покращення безпеки.

- Відповідальність за безпеку:

Розуміння працівників що кібербезпека — це відповідальність кожного. Відповідальність за дотримання політик безпеки повинна бути інтегрована в посадові обов'язки та оцінку ефективності роботи працівників.

- Актуалізація знань:

Оскільки технології та методи атак постійно змінюються, важливо регулярно оновлювати навчальні матеріали та політики безпеки, щоб працівники завжди були в курсі останніх загроз та методів їх протидії.

Підвищення обізнаності серед працівників є ключовим елементом у боротьбі з фішинговими атаками.

Висновки

У процесі виконання цієї роботи було здійснено всебічний аналіз численних звітів з кіберінцидентів у банківській сфері, що дозволило виявити основні загрози та вразливості, з якими стикаються фінансові установи. Всі ці методи мають на меті отримання несанкціонованого доступу до конфіденційної інформації, фінансових ресурсів або блокування діяльності установи з метою вимагання викупу.

Для попередження кіберзагроз було розроблено та запропоновано вичерпний список можливих заходів покращення кібербезпеки у сфері онлайн-банкінгу. Комплексний підхід до кібербезпеки, що включає технічні, організаційні та освітні заходи, є ключовим фактором у забезпеченні надійного захисту банківських установ від сучасних кіберзагроз.

Список літератури

1. Перегляд ФІНАНСОВА БЕЗПЕКА БАНКІВСЬКИХ УСТАНОВ В УМОВАХ ЦИФРОВІЗАЦІЇ. Головна. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3646/3575.
2. Banking on security: navigating the cyber threat landscape in the digital age - the global treasurer. *The Global Treasurer*. URL: https://www.theglobaltreasurer.com/2024/04/04/banking-on-security-navigating-the-cyber-threat-landscape-in-the-digital-age/.
3. Social engineering (phishing and deceptive sites) | google search central | documentation | google for developers. *Google for Developers*. URL: https://developers.google.com/search/docs/monitor-debug/security/social-engineering.
4. What is malware? - definition and examples. *Cisco*. URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html#:~:text=Malware,%20short%20for%20malicious%20software,spyware,%20adware,%20and%20ransomware.
5. What is a ddos attack? Ddos meaning, definition & types | fortinet. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/ddos-attack.
6. Publications I. R. Human factor as insider threat in organizations. *LinkedIn: Log In or Sign Up*. URL: https://www.linkedin.com/pulse/human-factor-insider-threat-organizations-research-publications.
7. Point of sale (POS) | malwarebytes labs. *Malwarebytes*. URL: https://www.malwarebytes.com/blog/threats/point-of-sale-pos.
8. Types of cyberattacks on financial institutions | fortinet. *Fortinet*. URL: https://www.fortinet.com/solutions/industries/financial-services/types-of-cyberattacks-on-financial-

institutions#:~:text=Unauthorized%20Use%20of%20System%20Privileges,create%20backdoors%20into%20compromised%20systems.

9. Ransomware attacks on banking industry - socradar® cyber intelligence inc. *SOCRadar® Cyber Intelligence Inc.* URL: https://socradar.io/ransomware-attacks-on-banking-industry/.
10. Secure electronic transaction (SET) protocol - geeksforgeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/secure-electronic-transaction-set-protocol/.
11. EMV® 3-D Secure | EMVCo. *EMVCo*. URL: https://www.emvco.com/emv-technologies/3-d-secure/.
12. 3D secure 2. *Stripe | Lösungen für die Finanzinfrastruktur des Internets*. URL: https://stripe.com/en-ca/guides/3d-secure-2.
13. Seth S. What is the SWIFT banking system?. *Investopedia*. URL: https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp.
14. SWIFT system: a comprehensive guide - solidgate. *Solidgate*. URL: https://solidgate.com/blog/swift-system/.
15. SWIFT system: a comprehensive guide - solidgate. *Solidgate*. URL: https://solidgate.com/blog/swift-system/#Securing_Your_Transactions.
16. Single euro payments area (SEPA). *European Central Bank*. URL: https://www.ecb.europa.eu/paym/integration/retail/sepa/html/index.en.html.
17. *European Central Bank*. URL: https://www.ecb.europa.eu/pub/pdf/other/ecb.eurosystemretailpaymentsstrategy~5a74eb9ac1.en.pdf?819e76c55e01ed236dac589f980189a2.