Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав.кафедрою БІСТ

Сватовський І.І._____

« » червня 2023р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

спеціальність: 125 Кібербезпека

на тему: «Аналіз загроз безпеки та методів захисту від них для сучасних банківських платіжних систем Visa, MasterCard»

оцінка « »

Голова ЕК

Лемешко О.В._____

Керівник Кошман С.О.
(прізвище та ініціали/підпис)

Рецензент проф. Краснобаєв В. А.
(прізвище та ініціали/підпис)

Виконавець студент групи КБ-42

Россомаха М.С
(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Дипломна робота містить: 48 сторінок, 8 рисунків, 1 додаток, 22 джерела.

Метою дослідження є розкриття проблем, що виникають у сфері безпеки банківських платіжних систем, визначення методів їх захисту від зловмисних атак та внесення пропозицій щодо покращення їх безпеки.

Об'єкт дослідження – сучасні банківські платіжні системи.

Предмет дослідження – загрози безпеці, з якими стикаються сучасні банківські платіжні системи, а також методи захисту від цих загроз.

Методи дослідження – аналіз теоретичних аспектів безпеки банківських платіжних систем та дослідження міжнародних стандартів безпеки в цих системах.

У результаті виконання роботи буде отримана можливість здобути більш повну картину про те, як функціонують банківські платіжні системи та які існують загрози для їх безпеки. Також буде проаналізована ефективність методів захисту від зловмисних атак та запропоновані рекомендації щодо їх вдосконалення.

Важливість безпеки в банківських платіжних системах не може бути недооцінена. Вразливості та атаки на такі системи можуть призвести до фінансових втрат для клієнтів і банків, а також пошкодження репутації фінансових установ. Розуміння загроз безпеці та вжиття відповідних заходів є критичним для забезпечення довіри до банківських платіжних систем.

Ключові слова: ПЛАТІЖНІ СИСТЕМИ, ЗАГРОЗИ БЕЗПЕЦІ, МЕТОДИ АВТЕНТИФІКАЦІЇ, PCI DSS, ШАХРАЙСЬКІ ДІЇ, ФІНАНСОВІ ПОСЛУГИ.

ABSTRACT

The thesis contains: 48 pages, 8 figures, 1 appendice, 22 sources.

The aim of the thesis is to reveal problems arising in the field of security of bank payment systems, to determine methods of protecting them from malicious attacks, and to make proposals for improving their security.

The subject matter is modern banking payment systems.

The scope of the study is security threats faced by modern banking payment systems, as well as methods of protection against these threats.

Research methods – analysis of theoretical aspects of security of bank payment systems and research of international security standards in these systems.

As a result of the work, it will be possible to get a more complete picture of how bank payment systems function and what are the threats to their security. The effectiveness of protection methods against malicious attacks will also be analyzed and recommendations for their improvement will be offered.

The importance of security in banking payment systems cannot be underestimated. Vulnerabilities and attacks on such systems can lead to financial losses for customers and banks, as well as damage to the reputation of financial institutions. Understanding security threats and taking appropriate measures is critical to ensuring trust in banking payment systems.

Keywords: PAYMENT SYSTEMS, SECURITY THREATS, AUTHENTICATION METHODS, PCI DSS, FRAUD, FINANCIAL SERVICES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

GDPR	-	Загальний регламент з захисту даних
БПС	-	Банківська платіжна система
CVV/CVC	-	Card Verification Value/Code
PCI DSS	-	Payment Card Industry Data Security Standard
PIN	-	Personal Identification Number
EMV	-	Europay + MasterCard + VISA
RSA	-	(Rivest, Shamir и Adleman), криптоалгоритм
ECC	-	Elliptic Curve Cryptography
OTP	-	One Time Password
DDoS	-	Distributed Denial of Service

ВСТУП

В сучасному цифровому світі банківські платіжні системи займають центральне місце у фінансовій інфраструктурі, надаючи зручність та швидкість проведення фінансових операцій. Однак, разом із зростанням популярності та використання банківських платіжних систем, зростають і загрози безпеці, пов'язані з кіберзлочинністю та шахрайством [1].

Сучасний фінансовий світ робить ставку на розвиток банківських платіжних систем, які надають зручність та ефективність для клієнтів. Застосування сучасних технологій, таких як мобільні платежі, електронні гаманці та онлайн-банкінг, робить можливим проведення фінансових операцій у будь-який час та з будь-якого місця. Проте, цей швидкий розвиток також створює нові виклики та загрози безпеці, які потребують пристосування та захисту з боку банківських платіжних систем.

Актуальність теми полягає в тому, що банківські платіжні системи є невід'ємною частиною сучасного економічного та фінансового життя. Тому аналіз загроз безпеці та розробка ефективних методів їх захисту є важливим завданням для забезпечення стійкості та надійності банківських платіжних систем у сучасному фінансовому середовищі.

Оскільки безпека банківських платіжних систем є складним завданням, яке постійно еволюціонує разом із розвитком технологій та кіберзлочинності, ця дипломна робота має на меті надати уявлення про основні проблеми та виклики, що стоять перед сучасними банківськими платіжними системами, а також запропонувати конкретні рекомендації для покращення їхньої безпеки [1]. Застосування рекомендацій та впровадження вдосконалених методів захисту допоможуть зберегти довіру клієнтів та ефективно опиратися на загрози безпеці, забезпечуючи безпечну та надійну роботу банківських платіжних систем у майбутньому.

1 ТЕОРЕТИЧНІ АСПЕКТИ БЕЗПЕКИ БАНКІВСЬКИХ ПЛАТІЖНИХ СИСТЕМ

1.1 Аналіз літературних джерел щодо безпеки банківських платіжних систем

Вперше електронні платежі з'явилися в 1960-х роках з використанням телекомунікаційних мереж. Ці системи були забезпечені шифруванням, але вони були дуже вразливі до крадіжки даних. У 1970-х роках з'явилися перші банкомати, які також використовували телекомунікаційні мережі. Однак, ці системи також були вразливими до атак [2].

У 1980-х роках з'явилися перші комп'ютерні системи для обробки банківських транзакцій, що зробило платіжні системи більш ефективними та швидкими. Проте, збільшення обсягу електронних транзакцій призвело до зростання кількості кібератак та шахрайства [2].

У 1990-х роках банки почали використовувати віртуальні приватні мережі та спеціальні протоколи для захисту електронних транзакцій. Ці системи були дуже дорогими та складними у використанні [2].

У 2000-х роках було розроблено багато нових технологій, що забезпечували безпеку банківських платіжних систем. Одна з найбільш важливих технологій, що з'явилася в цей час, - це 3-D Secure, що забезпечує безпеку платежів в Інтернеті. Крім того, банки стали використовувати системи біометричної ідентифікації, які дозволяють підтверджувати ідентифікацію клієнтів за допомогою відбитків пальців, скану обличчя та інших біометричних даних [2].

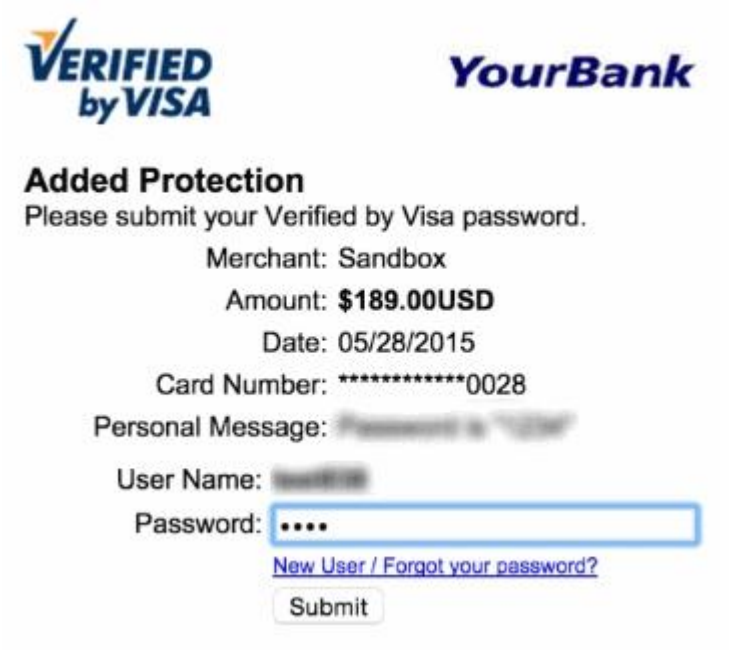


Рисунок 1.1 – Приклад додаткової аутентифікації за допомогою технології 3-D Secure [21].

У 2010-х роках з'явилися нові методи захисту платіжних систем, зокрема, використання штучного інтелекту та машинного навчання для виявлення шахрайства та кібератак. Також було розроблено нові методи шифрування та технології блокчейн, які дозволяють зберігати дані безпечним чином та підтверджувати транзакції без участі посередників [2].

Одним із ключових переломних моментів в історії захисту банківських платіжних систем була кібератака на систему JPMorgan Chase у 2014 році, яка стала найбільшою кібератакою на фінансовий сектор в історії. Ця атака викликала збитки в $300 мільйонів та змусила фінансові установи уважніше стежити за безпекою своїх систем.

Іншим важливим моментом було введення в дію Загального регламенту з захисту даних (GDPR) в Європейському Союзі у 2018 році. Цей регламент вимагає від організацій захищати персональні дані своїх клієнтів та забезпечувати їх безпеку від кібератак.

Одним з найбільш відомих прикладів кібератак на банківські платіжні системи є кібератака на компанію SWIFT у 2016 році, яка призвела до крадіжки $81 мільйонів з рахунку Банку Бангладеш.

У сучасних банківських платіжних системах зазвичай використовуються декілька методів захисту, такі як багаторівнева автентифікація, моніторинг транзакцій та виявлення кібератак, шифрування даних, захист від фішингу та шахрайства, біометрична ідентифікація та використання технологій блокчейн. Наприклад, багаторівнева автентифікація дозволяє вимагати від користувача декілька різних видів ідентифікації, таких як пароль, підтвердження через смартфон або пальцевий сканер, що зменшує ризик крадіжки даних. Моніторинг транзакцій допомагає виявляти нестандартні транзакції, які можуть свідчити про шахрайство або кібератаку. Шифрування даних дозволяє зберігати дані в зашифрованому вигляді, що ускладнює доступ до них з боку зловмисників. Технології блокчейн дозволяють зберігати дані безпечним чином та підтверджувати транзакції без участі посередників [2].

Ще одним переломним моментом в історії захисту банківських платіжних систем була поява у 2020 році пандемії COVID-19. Ця пандемія призвела до збільшення кількості онлайн-транзакцій та зростання ризику кібератак.

1.2 Огляд банківських платіжних систем

Банківська платіжна система (БПС) - це комплекс програмних, технічних та організаційних засобів, які забезпечують обслуговування банківських розрахунків між банками та їх клієнтами. БПС є ключовим елементом фінансової інфраструктури кожної країни, оскільки вона забезпечує переказ коштів між різними банками та фінансовими установами.

Зважаючи на те, що основна мета банківських платіжних систем полягає в забезпеченні безпечного та швидкого здійснення операцій з грошима, важливо мати чітке розуміння того, як вони працюють та які фактори впливають на їх ефективність та безпеку.

Для початку, слід зазначити, що банківські платіжні системи можуть бути класифіковані за декількома критеріями, включаючи обсяг операцій,

рівень доступності для користувачів, рівень безпеки, інтерфейс користувача та багато іншого.

Visa є однією з найбільших банківських платіжних систем в світі, яка відкриває доступ до безлічі електронних транзакцій. Ця система дозволяє користувачам здійснювати онлайн-платежі через мобільні додатки, платіжні термінали та інтернет-магазини.

Рисунок 1.2 – Логотип платіжної системи Visa [3].

Однією з головних переваг Visa є її міжнародна популярність та широке поширення. Багато компаній та інтернет-магазинів приймають платежі через Visa, що робить її відмінним вибором для онлайн-покупок. Також, Visa забезпечує високий рівень безпеки для своїх користувачів. Для забезпечення безпеки та запобігання шахрайства Visa використовує різноманітні заходи, такі як перевірка платіжної інформації, двофакторна автентифікація та шифрування даних.

MasterCard - це одна з найпоширеніших світових платіжних систем, що забезпечує обробку транзакцій з використанням кредитних і дебетових карт. Компанія MasterCard Worldwide, заснована у 1966 році, має штаб-квартиру в Нью-Йорку, США.

Рисунок 1.3 – Логотип платіжної системи MasterCard [22].

Основними принципами роботи MasterCard є забезпечення швидкої, безпечної і зручної оплати товарів і послуг у всьому світі. Картки MasterCard використовуються мільйонами людей і багатьма підприємствами в усьому світі.

Основні складові системи MasterCard включають:

1) Картки MasterCard: MasterCard видавати фінансові установи, такі як банки, і вони можуть бути використані для здійснення покупок в роздрібних магазинах, онлайн-магазинах, а також для зняття готівки з банкоматів.

2) Електронні платіжні системи: MasterCard розробив кілька електронних платіжних систем, таких як MasterPass і MoneySend, які дозволяють здійснювати безконтактні платежі та переказувати гроші з використанням мобільних пристроїв.

3) Безпека: MasterCard активно працює над забезпеченням безпеки транзакцій. Для цього використовуються різні технології, включаючи чіпи на картках (EMV-стандарт), тривалу аутентифікацію, двофакторну автентифікацію та інші методи.

4) Глобальна мережа: MasterCard має широку мережу партнерів і приймаючих установ, що дозволяє користувачам карток MasterCard здійснювати платежі практично у будь-якій країні світу.

5) Програми лояльності: MasterCard пропонує різні програми лояльності для користувачів своїх карток, які дозволяють збирати бонусні бали, знижки або спеціальні пропозиції від партнерів системи.

Мережа MasterCard використовується в більш ніж 210 країнах і територіях. Картки MasterCard приймаються в мільйонах місць по всьому світу, що робить їх одними з найпоширеніших платіжних засобів.

Важливо відзначити, що MasterCard не видаватиме картки напряму кінцевим користувачам. Картки видаватимуться банками та іншими фінансовими установами, які мають ліцензію на використання бренду MasterCard і забезпечують обслуговування клієнтів.

MasterCard продовжує розвиватися, впроваджує нові технології і спрощує оплату, щоб зробити її ще більш зручною для користувачів у всьому світі.

Іншою поширеною банківською платіжною системою є SWIFT (Society for Worldwide Interbank Financial Telecommunication). Ця система була створена в 1973 році, і вона забезпечує міжнародний грошовий переказ між банками. SWIFT дозволяє банкам взаємодіяти між собою та передавати фінансову інформацію захищеним шляхом.

Рисунок 1.4 – Логотип платіжної системи SWIFT [4].

Ще однією популярною банківською платіжною системою є CHIPS (Clearing House Interbank Payments System). Ця система забезпечує обробку більш ніж 95% всіх міжнародних платежів у доларах США. CHIPS працює за допомогою мережі банків-учасників, які надсилають платежі до центрального процесора, який здійснює обробку платежів.

Іншою важливою банківською платіжною системою є Fedwire, яка є найбільшою платіжною системою у США. Fedwire дозволяє банкам здійснювати безготівкові перекази коштів між собою та з клієнтами, що

знаходяться в різних частинах світу. Fedwire працює на основі мережі банків-учасників, які обмінюються платежами через центральний процесор.

Також популярною банківською платіжною системою є SEPA (Single Euro Payments Area), яка забезпечує безготівкові перекази в євро між банками, які знаходяться в європейському економічному просторі. SEPA дозволяє банкам та їх клієнтам здійснювати платежі з одного банку в інший без зайвих комісій та обмежень.

Також існують регіональні банківські платіжні системи, які призначені для здійснення безготівкових переказів у межах конкретної країни чи регіону. Наприклад, у Японії існує платіжна система Zengin, яка забезпечує безпечні та швидкі грошові перекази між банками усередині країни. У Індії існує система National Electronic Funds Transfer (NEFT), яка дозволяє банкам та їх клієнтам здійснювати безготівкові перекази в індійських рупіях.

Усі банківські платіжні системи мають власні технічні та організаційні особливості, але вони мають спільну мету - забезпечення безпечних та ефективних грошових переказів між банками та їх клієнтами. Крім того, банки можуть використовувати декілька платіжних систем одночасно, щоб забезпечити різноманітність та надійність своїх фінансових операцій.

У сучасному світі зростає популярність електронних платіжних систем, таких як PayPal, Stripe, Skrill та інші. Вони дозволяють здійснювати онлайн-платежі між клієнтами та магазинами без прив'язки до банківської системи. Однак, банківські платіжні системи є основою фінансової системи країни та мають значний вплив на економіку в цілому. Ці системи дозволяють здійснювати швидкі та безпечні фінансові транзакції, що стає надзвичайно важливим у світі, де міжнародна торгівля та бізнес є все більш глобальними [5].

Однак, банківські платіжні системи також мають свої недоліки. Наприклад, деякі системи можуть бути дорожчими для використання, особливо якщо вони залежать від інтернаціональних платіжних мереж, таких як SWIFT. Також вони можуть бути вразливі до кібератак та шахрайства.

У зв'язку з цим, багато банків та регулюючих органів вкладають значні зусилля у поліпшення безпеки та ефективності банківських платіжних систем. Наприклад, використання біометричних технологій, таких як відбитки пальців та розпізнавання обличчя, може допомогти запобігти шахрайству та зловживанню. Також розробка блокчейн технологій може допомогти забезпечити більш безпечні та швидкі грошові перекази.

1.3 Поняття безпеки банківських платіжних систем

Важливою складовою банківської діяльності є забезпечення безпеки платіжних систем. Захист від можливих загроз і шахрайства є основною метою всіх банківських платіжних систем.

Перш за все, необхідно визначити поняття безпеки. У банківських платіжних системах це означає забезпечення надійності, конфіденційності, цілісності та доступності даних та фінансових ресурсів клієнтів:

1) Надійність означає, що система завжди працює правильно і безперебійно, навіть за умови виникнення непередбачуваних обставин, таких як відмова обладнання або введення неправильних даних.

2) Конфіденційність означає, що інформація, яку надає клієнт, залишається приватною і не може бути доступна третім особам без згоди власника.

3) Цілісність означає, що дані та фінансові ресурси клієнтів захищені від незаконних змін або втручання в систему з боку зловмисників.

4) Доступність означає, що система завжди доступна для клієнтів і не допускається ніяких перешкод, які можуть унеможливити проведення платежів.

Принципи безпеки банківських платіжних систем полягають у забезпеченні цих чотирьох складових [6]. Ці принципи включають захист від шахрайства, фішингу, вірусів та хакерських атак:

1) Шахрайство - це одна з найпоширеніших загроз безпеці банківських платіжних систем. Шахраї можуть спробувати шляхом шахрайства здійснити незаконні операції з використанням чужих банківських

рахунків або вкрасти особисту інформацію користувача, що дає можливість отримати доступ до його коштів.

2) Фішинг - це тип атаки, при якому зловмисники намагаються отримати доступ до особистої інформації користувача, шляхом відправки електронного листа, що містить посилання на підроблену сторінку веб-сайту, що схожа на банківський портал. Користувач, не підозрюючи нічого поганого, вводить свої дані на підробленому сайті, що дозволяє зловмисникам отримати доступ до його банківського рахунку.

3) Віруси - це програми, які призначені для виконання певних дій на комп'ютері, без дозволу власника комп'ютера. Віруси можуть бути використані для злому банківських систем та отримання доступу до особистої інформації користувачів.

4) Хакерські атаки - це атаки на банківські системи з метою отримання несанкціонованого доступу до них. Хакери можуть використовувати різні методи для злому банківських систем, такі як використання підроблених авторизаційних даних, використання вразливостей систем безпеки, або використання соціальної інженерії.

Одним із ключових аспектів безпеки банківських платіжних систем є забезпечення конфіденційності та захисту персональних даних клієнтів. Банки повинні дотримуватись строгих правил та стандартів щодо обробки та зберігання інформації про клієнтів, щоб забезпечити надійний захист персональних даних та уникнути можливих витоків інформації. Окрім цього, безпека банківських платіжних систем повинна бути забезпечена на різних рівнях, включаючи апаратну, програмну та мережеву безпеку. Для забезпечення максимальної безпеки, банки використовують різні методи та технології, такі як двофакторна автентифікація, шифрування даних, системи виявлення вторгнень тощо[6].

Зокрема, система безпеки банківських платіжних карт може включати наступні елементи:

1) Захист персональних даних клієнта та карткової інформації (зокрема, коду CVV/CVC, дати закінчення терміну дії карти тощо).

2) Використання технологій шифрування, які захищають дані в процесі їх передачі по мережі.

3) Встановлення механізмів виявлення та усунення можливих вторгнень та інших загроз безпеці.

4) Використання системи двофакторної автентифікації для підтвердження операцій, що вимагають підвищеного рівня безпеки.

1.4 Висновки до першого розділу

У даному розділі були розглянуті теоретичні аспекти безпеки банківських платіжних систем, що є основою для розуміння загроз та методів захисту. Проаналізовано поняття безпеки та її значення для функціонування банківських платіжних систем.

Основними цілями безпеки банківських платіжних систем є забезпечення конфіденційності, цілісності та доступності даних, а також запобігання шахрайству та зловживанням. Для досягнення цих цілей необхідно впроваджувати комплексний підхід до безпеки, який включає технічні, організаційні та правові аспекти.

Таким чином, забезпечення безпеки банківських платіжних систем є одним з головних пріоритетів для банків та організацій, які працюють у сфері фінансових послуг [7].

2 ДОСЛІДЖЕННЯ МІЖНАРОДНИХ СТАНДАРТІВ БЕЗПЕКИ В БАНКІВСЬКИХ ПЛАТІЖНИХ СИСТЕМАХ

2.1 Дослідження міжнародного стандарту безпеки PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) - це міжнародний стандарт безпеки, розроблений з метою захисту інформації про платіжні картки. Він був створений спільно кількома провідними міжнародними платіжними системами, включаючи American Express, Visa, MasterCard, Discover і JCB.

Рисунок 2.1 – Логотип стандарту безпеки PCI DSS [19].

PCI DSS встановлює мінімальні вимоги до безпеки обробки, зберігання і передачі інформації про платіжні картки. Він також регулює процеси аудиту та сертифікації компаній, які обробляють, зберігають або передають інформацію про платіжні картки [13].

Для дослідження міжнародного стандарту безпеки PCI DSS необхідно розглянути його основні вимоги. Загалом стандарт включає 12 вимог, які поділяються на 6 груп:

1) Захист мережі. Ця група вимог включає захист мережевих пристроїв і забезпечення безпеки передачі даних через мережу. Захист мережі включає в себе вимоги до захисту мережевого периметру, забезпечення безпеки Wi-Fi мережі, захисту пристроїв мережі та мережевих ресурсів.

2) Захист даних. Ця група вимог включає захист даних про платіжні картки, які зберігаються на серверах або пересилаються по мережі. Вимоги до захисту даних включають в себе вимоги до зберігання та захисту даних, передачі даних та захисту даних від вторгнень.

3) Захист програмного забезпечення. Ця група вимог включає захист програмного забезпечення, яке використовується для обробки даних про платіжні картки. Вимоги до захисту програмного забезпечення включають в себе вимоги до розробки безпечного програмного забезпечення, захисту програмного забезпечення від вторгнень, регулярної оновлення програмного забезпечення та контролю за доступом до програмного забезпечення.

4) Захист системи. Ця група вимог включає захист системи, яка використовується для обробки даних про платіжні картки. Вимоги до захисту системи включають в себе вимоги до захисту серверів, контролю за доступом до системи, моніторингу системи та аудиту системи.

5) Захист процесів. Ця група вимог включає захист процесів, які використовуються для обробки даних про платіжні картки. Вимоги до захисту процесів включають в себе вимоги до контролю доступу до процесів, забезпечення безпеки процесів та моніторингу процесів.

6) Управління безпекою. Ця група вимог включає управління безпекою, яке забезпечує ефективне управління ризиками безпеки даних про платіжні картки. Вимоги до управління безпекою включають в себе вимоги до політик та процедур безпеки, навчання персоналу, ведення журналів подій та проведення аудитів безпеки.

Для дотримання міжнародного стандарту безпеки PCI DSS компанії повинні розробляти та впроваджувати політики та процедури безпеки, а також проводити аудити та сертифікацію відповідно до вимог стандарту. Дотримання стандарту забезпечує безпеку даних про платіжні картки та сприяє підвищенню довіри клієнтів до компанії.

Дослідження міжнародного стандарту безпеки PCI DSS є важливим, оскільки стандарт має значний вплив на безпеку платіжних транзакцій та захист інформації про платіжні картки в усьому світі. Він є важливим інструментом для забезпечення безпеки даних про платіжні картки, зокрема для підприємств, які обробляють ці дані. Дослідження стандарту дозволяє краще зрозуміти вимоги до безпеки даних про платіжні картки та допомагає забезпечити відповідність цим вимогам. Відповідність стандарту PCI DSS є обов'язковою для багатьох компаній, які обробляють платіжні картки. Відсутність відповідності стандарту може призвести до витоку даних, крадіжки грошей та негативно позначитися на репутації компанії. Також, компанії, які не відповідають стандарту, можуть бути позбавлені можливості обробляти платіжні картки [13].

Загалом, дослідження міжнародного стандарту безпеки PCI DSS є важливим кроком для підприємств, які обробляють дані про платіжні картки. Дотримання стандарту допомагає забезпечити безпеку даних та підвищити довіру клієнтів до компанії. Крім того, відповідність стандарту є обов'язковою для багатьох компаній та може вплинути на їхню репутацію та можливість обробляти платіжні картки.

2.2 Порівняльний аналіз міжнародних стандартів безпеки

Порівняльний аналіз таких стандартів може допомогти обрати найбільш підходящий варіант для конкретної організації.

Ось декілька міжнародних стандартів безпеки банківських платіжних систем:

1) PCI DSS - Payment Card Industry Data Security Standard. Цей стандарт розроблений консорціумом PCI Security Standards Council та встановлює вимоги до захисту персональних даних клієнтів, які зберігаються в банківських системах. PCI DSS включає такі елементи, як захист мережі, захист даних та управління доступом.

2) ISO 27001 - стандарт, розроблений Міжнародною організацією по стандартизації, який встановлює вимоги до систем управління інформаційною безпекою. Цей стандарт охоплює широкий спектр вимог, включаючи фізичну та логічну безпеку, управління ризиками та організаційні заходи.

3) SWIFT Customer Security Programme - програма безпеки клієнтів SWIFT. SWIFT - це світова система передачі фінансових повідомлень між банками. Ця програма встановлює вимоги до захисту клієнтських терміналів, управління ризиками та інші заходи безпеки [10].

4) EMV - це стандарт безпеки для кредитних та дебетових карток, що використовуються в банківських системах. Цей стандарт встановлює вимоги до захисту даних на картці та в процесі здійснення транзакції.

5) NIST Cybersecurity Framework - цей стандарт розроблений Національним інститутом стандартів та технологій США та встановлює вимоги до управління кібербезпекою організацій. Цей стандарт складається з п'яти складових: ідентифікації, захисту, виявлення, відгуку та відновлення.

Кожен з цих стандартів має свої особливості та вимоги, проте всі вони мають за мету забезпечення безпеки банківських платіжних систем та захисту фінансових даних клієнтів. PCI DSS та EMV зосереджені на захисті платіжних карток, тоді як ISO 27001 та NIST Cybersecurity Framework ставлять своїми цілями більш загальну безпеку інформаційних систем та кібербезпеку організацій. SWIFT Customer Security Programme відповідає за безпеку системи передачі фінансових повідомлень між банками.

Всі ці стандарти мають деякі спільні елементи, такі як захист мережі та даних, управління доступом та управління ризиками. Однак, кожен стандарт має свої особливі вимоги та підходи до забезпечення безпеки. Наприклад, PCI DSS вимагає використання шифрування для захисту даних, тоді як SWIFT Customer Security Programme ставить акцент на управління правами доступу та захист клієнтських терміналів [18].

Вибір стандарту безпеки для конкретної організації залежить від її потреб та характеристик. Важливо визначити, які вимоги до безпеки має організація та який стандарт забезпечить їх виконання. Крім того, необхідно врахувати витрати на впровадження та використання стандарту, а також можливі наслідки.

2.3. Висновки до другого розділу

У цьому розділі було проведено дослідження міжнародних стандартів безпеки в банківських платіжних системах. Результати аналізу показують, що стандарти безпеки є ключовим елементом у забезпеченні надійності та захищеності платіжних операцій.

Міжнародні стандарти безпеки, зокрема Payment Card Industry Data Security Standard (PCI DSS), визначають вимоги щодо захисту кардхолдерських даних, мереж та систем обробки платежів. Вони встановлюють основні принципи та заходи безпеки, які повинні бути впроваджені банками та іншими учасниками платіжних систем.

Недотримання міжнародних стандартів безпеки може мати серйозні наслідки для банків та їх клієнтів. Вразливості в системі безпеки можуть призвести до витоку конфіденційної інформації, крадіжки грошей або шахрайства. Тому важливо, щоб банки ретельно вивчали та впроваджували міжнародні стандарти безпеки для забезпечення високого рівня захисту.

3 АНАЛІЗ ПРОТОКОЛІВ БЕЗПЕКИ ТА ЗОВНІШНІХ ЗАХИСНИХ ЕЛЕМЕНТІВ ПЛАТІЖНИХ КАРТОК VISA ТА MASTERCARD

3.1 Архітектура протоколу безпеки платіжних карток Visa

Архітектура протоколу безпеки платіжних карток Visa включає різні компоненти та процеси, які співпрацюють для забезпечення безпеки платіжних транзакцій [18]. Основні компоненти архітектури включають наступні елементи:

1) Картка Visa: Це фізична платіжна картка, яка містить елементи фізичного захисту, такі як чип, ембосінг, голограми та інші захисні маркування. Карта також містить інформацію, необхідну для виконання безпечних транзакцій, включаючи номер рахунку та дані власника карти.

2) Термінал: Це пристрій, який використовується для здійснення платіжних транзакцій з використанням карток Visa. Термінал забезпечує взаємодію з карткою та передачу даних про транзакцію до системи обробки платежів.

3) Платіжний шлюз: Це система, яка обробляє платіжні транзакції між терміналом та банком-емітентом, який видав картку Visa. Платіжний шлюз забезпечує шифрування та безпечну передачу даних про транзакцію, а також перевірку достовірності картки та авторизацію операцій.

4) Банк-емітент: Це банк, який видав картку Visa власнику. Банк-емітент забезпечує автентифікацію власника картки, контроль за доступом до рахунку та авторизацію платіжних транзакцій. Він також відповідає за встановлення лімітів та правил використання картки.

5) Банк-аквайер: Це банк, який обслуговує торговців та термінали, приймаючи платежі з використанням карток Visa. Банк-аквайер передає дані

про транзакції до платіжного шлюзу та отримує відповіді про авторизацію та стан транзакцій.

6) Центральна система Visa: Це центральна система, що координує обробку платіжних транзакцій між всіма учасниками. Вона забезпечує безпеку мережі Visa, включаючи моніторинг транзакцій, виявлення шахрайства та заходи безпеки.

Усі ці компоненти взаємодіють між собою для забезпечення безпеки та безпечного здійснення платіжних транзакцій. Наприклад, при здійсненні покупки картка Visa передає дані терміналу через захищену комунікаційну лінію. Термінал передає дані до платіжного шлюзу, який шифрує інформацію та пересилає її до банку-емітента для авторизації. Банк-емітент перевіряє дані, виконує автентифікацію власника карти та вирішує, чи авторизувати операцію. Після цього відповідь про авторизацію передається від банку-емітента до терміналу через платіжний шлюз, і транзакція завершується [14].

3.2 Методи автентифікації та авторизації в протоколі безпеки платіжних карток Visa

Методи автентифікації та авторизації в протоколі безпеки платіжних карток Visa використовуються для підтвердження ідентичності власника карти та забезпечення авторизації платіжних транзакцій. Для забезпечення високого рівня безпеки використовуються наступні методи:

1) Пін-код: PIN (Personal Identification Number) є одним з найпоширеніших методів автентифікації. Власник картки встановлює унікальний числовий код, який потрібно ввести при використанні картки для підтвердження своєї ідентичності [8]. Цей пін-код зберігається в зашифрованому вигляді на чипі картки або в базі даних банку-емітента.

2) Біометричні дані: Сучасні картки Visa також можуть використовувати біометричні дані для автентифікації власника. Наприклад, це може бути сканування відбитка пальця або розпізнавання обличчя.

Біометричні дані зберігаються на картці або в централізованій базі даних і використовуються для порівняння зі зразком біометричних даних, які надає власник картки.

3) Додаткові методи автентифікації: Крім основних методів, Visa також впроваджує додаткові методи автентифікації для забезпечення вищого рівня безпеки. Наприклад, це можуть бути одноразові паролі, смс-підтвердження або використання додаткових безпечних пристроїв, таких як токени або картки з одноразовими кодами.

Усі ці методи автентифікації поєднуються з процесом авторизації, який включає перевірку доступу до рахунку та вирішення, чи авторизувати платіжну транзакцію. Авторизація зазвичай виконується банком-емітентом на основі різних параметрів, таких як наявність коштів на рахунку, ліміти, правила використання картки та аналіз ризиків. Критичність безпеки цих методів полягає у запобіганні несанкціонованому доступу до рахунку та уникненні шахрайства в платіжних транзакціях.

3.3 Захист від шахрайських дій в протоколі безпеки платіжних карток Visa

Захист від шахрайських дій є одним з найважливіших аспектів протоколу безпеки платіжних карток Visa. Для забезпечення безпеки та запобігання шахрайству використовуються різні заходи та технології:

1) Виявлення шахрайства: Центральна система Visa та банки-емітенти постійно моніторять платіжні транзакції з метою виявлення підозрілих або несподіваних змін. Вони аналізують різні параметри, такі як сума транзакції, місцезнаходження, тип торговця та звички власника карти, щоб ідентифікувати потенційно шахрайські операції.

2) Аналіз ризиків: При обробці платіжних транзакцій застосовується аналіз ризиків з використанням різних алгоритмів та моделей. Це дозволяє оцінити рівень ризику кожної транзакції на основі історичних даних та

патернів. Якщо транзакція має високий рівень ризику, можуть бути застосовані додаткові перевірки або блокування картки для запобігання шахрайству.

3) 3D-Secure: 3D-Secure є протоколом, який використовується для авторизації онлайн-транзакцій. Він включає додатковий шар безпеки, де власник картки підтверджує свою ідентичність, виконуючи додаткові кроки автентифікації, наприклад, введення одноразового пароля або відповідей на персональні запитання.

4) Захист від крадіжки даних: Visa встановлює обов'язкові вимоги щодо захисту даних для всіх учасників платіжної системи. Це включає шифрування передачі даних, захист збереження даних, використання захищених протоколів та інші технічні заходи [9]. Мета полягає в тому, щоб запобігти несанкціонованому доступу до особистої інформації власника картки та уникнути крадіжки конфіденційних даних.

5) Системи виявлення шахрайства: Visa використовує спеціалізовані системи виявлення шахрайства, які використовують аналітичні алгоритми та шаблони для виявлення незвичайних або підозрілих патернів у поведінці користувачів та транзакціях. Ці системи аналізують великі обсяги даних та роблять оцінку ризику для швидкого виявлення та блокування шахрайських дій.

3.4 Архітектура протоколу безпеки платіжних карток MasterCard

Архітектура протоколу безпеки платіжних карток MasterCard включає різні компоненти та процеси, які спільно працюють для забезпечення безпеки та захисту платіжних транзакцій. Основні складові архітектури протоколу безпеки MasterCard включають наступне:

1) Банк-емітент: Банк-емітент є установою, яка виділяє платіжні картки MasterCard своїм клієнтам. Він відповідає за автентифікацію власника картки, авторизацію платіжних транзакцій та встановлення правил та

обмежень для використання картки. Банк-емітент зберігає інформацію про власника картки та здійснює моніторинг транзакцій з метою виявлення шахрайських дій.

2) Банк-аквайер: Банк-аквайер є установою, яка приймає платежі від торговців, які приймають платіжні картки MasterCard. Він забезпечує зв'язок між торговцем та банком-емітентом для обробки платіжних транзакцій. Банк-аквайер здійснює перевірку транзакцій та передає їх до банку-емітента для авторизації.

3) Централізована система MasterCard: Централізована система MasterCard є центральним хабом для обробки та маршрутизації платіжних транзакцій. Вона включає сервери та програмне забезпечення, що обробляють дані транзакцій та забезпечують безпеку платіжної системи. Ця система виконує функції, такі як автентифікація карток, авторизація транзакцій, виявлення шахрайства та моніторинг безпеки.

4) Протоколи безпеки: Протоколи безпеки включаються в архітектуру протоколу MasterCard для забезпечення захисту даних під час передачі і обробки платіжних транзакцій. Один з найвідоміших протоколів безпеки, який використовується MasterCard, - це EMV (Europay, MasterCard та Visa), який використовує технологію мікросхем для шифрування та автентифікації карток під час платежів.

5) Системи виявлення шахрайства: MasterCard також використовує системи виявлення шахрайства для моніторингу та виявлення підозрілих або несподіваних змін у поведінці користувачів та транзакціях. Ці системи аналізують дані транзакцій, використовують алгоритми та моделі, щоб ідентифікувати потенційно шахрайські операції та запобігти шахрайству.

Архітектура протоколу безпеки платіжних карток MasterCard має на меті забезпечити безпеку та захист платіжних транзакцій, автентифікацію власників карток, виявлення шахрайства та моніторинг безпеки. Компоненти

та процеси працюють спільно для забезпечення надійності та безпеки платіжної системи MasterCard [10].

3.5 Методи автентифікації та авторизації в протоколі безпеки платіжних карток MasterCard

Протокол безпеки платіжних карток MasterCard використовує різні методи автентифікації та авторизації для забезпечення безпеки платіжних транзакцій. Основні методи включають наступне:

1) Пін-код: Пін-код (Personal Identification Number) є одним з основних методів автентифікації в протоколі безпеки MasterCard. При здійсненні платежу в точці продажу або в банкоматі власник картки вводить свій персональний пін-код, який є секретним кодом доступу. Перевірка пін-коду дозволяє підтвердити, що особа, яка здійснює транзакцію, є законним власником картки [11].

2) Відбиток пальця та інші біометричні дані: Деякі нові моделі карток MasterCard можуть містити біометричні дані, такі як відбиток пальця або сканування обличчя, для автентифікації власника картки. Ці дані використовуються для перевірки ідентичності власника картки та забезпечення безпеки транзакцій.

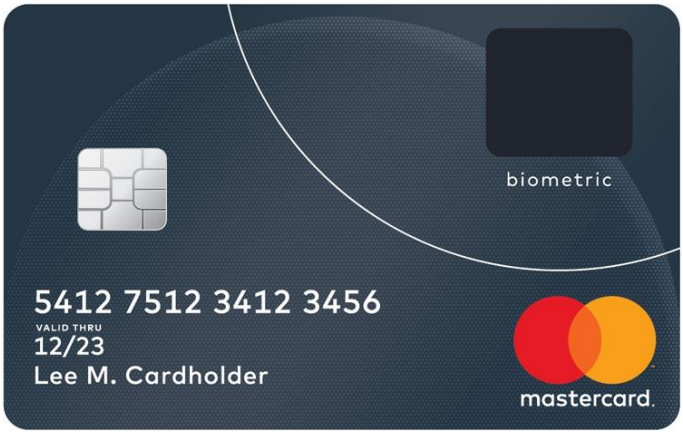


Рисунок 3.1 – Приклад зовнішнього вигляду картки Mastecard із застосування біометричного захисту [20].

3) Tokenization: Токенізація є методом, що застосовується в MasterCard для заміни реального номера картки на унікальний токен під час безконтактних платежів. Токен є випадковим числом або символом, який не містить конфіденційної інформації. Використовуючи токени, здійснення платежів стає безпечніше, оскільки реальний номер картки не розголошується при безконтактних транзакціях.

Ці методи автентифікації та авторизації, які використовуються в протоколі безпеки платіжних карток MasterCard, допомагають забезпечити ідентифікацію та авторизацію власників карток, підтвердження легітимності транзакцій та зменшення ризику шахрайства. Комбінація цих методів сприяє покращенню безпеки платіжних систем MasterCard та захисту конфіденційної інформації власників карток.

3.6 Захист від шахрайських дій в протоколі безпеки платіжних карток MasterCard

Забезпечення захисту від шахрайських дій є одним з найважливіших аспектів протоколу безпеки платіжних карток MasterCard. Щоб забезпечити цей захист, використовуються різні методи та технології:

1) Виявлення шахрайства: Протокол безпеки MasterCard включає системи виявлення шахрайства, які аналізують транзакційні дані та виявляють незвичайні, підозрілі або несподівані зміни у поведінці користувачів та транзакціях. Ці системи використовують алгоритми та моделі для ідентифікації потенційно шахрайських операцій та запобігають шахрайству.

2) Моніторинг транзакцій: Протокол безпеки MasterCard включає системи моніторингу транзакцій, які слідкують за активністю та патернами використання карток. Ці системи аналізують транзакційні дані, враховуючи фактори, такі як час, місцезнаходження, сума платежу та звички власника картки. Якщо система помічає підозрілу активність, вона може спрацювати та

вимагати додаткову автентифікацію або навіть заблокувати транзакцію для запобігання шахрайству.

3) Захист від крадіжки даних: MasterCard приділяє велику увагу захисту конфіденційної інформації, такої як номери карток і особисті дані власників карток. Для цього використовуються різні технології, включаючи шифрування даних, токенізацію та захищені протоколи передачі даних. Ці заходи допомагають уникнути незаконного доступу до конфіденційної інформації та запобігають можливості використання викрадених даних для шахрайських цілей.

4) 3D-Secure: Протокол MasterCard включає 3D-Secure технологію, яка забезпечує додатковий рівень захисту при онлайн-транзакціях. Ця технологія вимагає введення одноразового пароля або підтвердження на мобільний пристрій власника картки, щоб підтвердити його ідентичність та запобігти несанкціонованим транзакціям [11].

Дані заходи та технології в протоколі безпеки MasterCard спрямовані на захист власників карток від шахрайських дій та недозволених транзакцій. Широкий спектр захисних механізмів та систем виявлення допомагають забезпечити високий рівень безпеки та довіру до платіжних карток MasterCard.

3.7 Елементи фізичного захисту на платіжних картках Visa та MasterCard

Фізичний захист є важливим аспектом безпеки платіжних карток Visa та MasterCard і включає різні елементи, які забезпечують захист картки в реальному світі. Основні елементи фізичного захисту на платіжних картках включають наступне:

1) Ембосінг: Ембосінг - це процес створення вигнутих символів або цифр на поверхні картки. Це дозволяє створити текстурну ідентифікаційну марку, яка може бути використана для визначення легітимності картки. Ембосінг може містити інформацію, таку як ім'я власника картки, номер

картки та дату дії. Цей елемент фізичного захисту допомагає ускладнити підробку картки та захищає власника від можливого шахрайства.

2) Магнітна смуга: Більшість платіжних карток Visa та MasterCard мають магнітну смугу на зворотному боці. Ця смуга містить інформацію про власника картки, таку як номер картки, ім'я та інші деталі. Дані на магнітній смузі можуть бути зчитані за допомогою спеціальних пристроїв, що дозволяє проводити платежі та авторизацію. Однак, з огляду на потенційну вразливість магнітної смуги до копіювання та підробки, нові картки все більше переходять на безконтактні технології.

3) Чіп-карта: Чіп-карта (також відома як EMV-карта) є новітнім елементом фізичного захисту на платіжних картках Visa та MasterCard. Чіп, розташований на картці, містить зашифровану інформацію про власника картки та додаткові захищені дані. При використанні чіп-карти, власник картки повинен ввести ПІН-код для підтвердження транзакції. Це забезпечує більш високий рівень безпеки порівняно з магнітною смугою, оскільки дані на чіпі важко скопіювати або змінити.

4) Сигнатура власника: Деякі платіжні картки Visa та MasterCard можуть мати місце для підпису власника на зворотному боці картки. Це дозволяє порівняти підпис з тим, що виконується під час транзакції, для підтвердження ідентичності власника картки. Хоча цей метод не є надзвичайно надійним через можливість підробки підпису, він все ще може служити як один з елементів фізичного захисту.

Ці елементи фізичного захисту на платіжних картках Visa та MasterCard спільно сприяють ускладненню підробки та недозволених використань карток. Комбінація цих елементів допомагає забезпечити безпеку та довіру власників платіжних карток при фізичних транзакціях.

3.8 Захист від копіювання та зламу чипів на платіжних картках Visa та MasterCard

Захист від копіювання та зламу чипів на платіжних картках Visa та MasterCard є важливим аспектом фізичного захисту. Цей захист забезпечує безпеку даних, які зберігаються на чипі картки та перешкоджає можливості несанкціонованого доступу до цих даних. Деякі з основних заходів захисту від копіювання та зламу чипів на платіжних картках включають наступне:

1) Криптографічний захист: Чипи на платіжних картках Visa та MasterCard використовують криптографічні алгоритми для захисту конфіденційних даних та перешкоджають можливості їх копіювання або розшифрування [12]. Ці алгоритми шифрують дані, що зберігаються на чипі, і дозволяють тільки авторизованим пристроям і системам отримувати доступ до цих даних.

2) Захист від фізичних атак: Чипи на платіжних картках Visa та MasterCard мають фізичні заходи захисту, які перешкоджають можливості фізичного зламу чипа. Наприклад, чипи можуть мати спеціальні захисні шари, які роблять їх важкими для зламу або знищення. Крім того, можуть бути встановлені механізми виявлення несанкціонованого фізичного доступу до чипу, які спрацьовують при спробі зламу.

3) Захист від електронних атак: Чипи на платіжних картках Visa та MasterCard мають також заходи захисту від електронних атак, які можуть спрямовуватися на незаконне зчитування чипа або злам його захисту. Для цього можуть використовуватись методи, такі як електронне шумове перешкоджання, що ускладнює можливість зчитування чипа або отримання конфіденційних даних з нього.

4) Двофакторна автентифікація: Деякі платіжні картки Visa та MasterCard можуть мати вбудовану двофакторну автентифікацію, яка забезпечує додатковий рівень захисту від копіювання чипа або його

використання без дозволу. Це може включати введення ПІН-коду або використання біометричних даних (наприклад, відбитку пальця) для підтвердження ідентичності власника картки.

3.9 Використання двофакторної автентифікації на платіжних картках Visa та MasterCard

Використання двофакторної автентифікації є важливим аспектом фізичного захисту на платіжних картках Visa та MasterCard. Цей метод забезпечує додатковий рівень безпеки шляхом вимагання двох незалежних факторів для підтвердження ідентичності власника картки. Основні аспекти використання двофакторної автентифікації включають наступне:

1) Чіп-карти та ПІН-код: Одним з найпоширеніших методів двофакторної автентифікації на платіжних картках Visa та MasterCard є поєднання чіп-технології та ПІН-коду. Під час транзакції, власник картки вставляє картку з чіпом в платіжний термінал і одночасно вводить свій унікальний ПІН-код. Чіп на картці перевіряє правильність введеного ПІН-коду, що дає підтвердження ідентичності власника.

2) Біометричні дані: Деякі платіжні картки Visa та MasterCard можуть використовувати біометричні дані, такі як відбитки пальців або сканування обличчя, для двофакторної автентифікації. В цьому випадку, власник картки повинен пройти процедуру реєстрації своїх біометричних даних, які потім будуть використовуватися для підтвердження його ідентичності під час транзакції.

3) Одноразові паролі та токени: Додатковим методом двофакторної автентифікації може бути використання одноразових паролів або токенів. В цьому випадку, окрім фізичної картки, власник отримує одноразовий пароль або токен, який генерується спеціальним пристроєм або мобільним додатком. При транзакції, власник вводить цей одноразовий пароль або використовує токен для підтвердження ідентичності.

4) Додаткові методи автентифікації: Окрім вищезазначених методів, існують інші способи використання двофакторної автентифікації на платіжних картках Visa та MasterCard. Наприклад, це можуть бути спеціальні мобільні додатки, які генерують одноразові паролі або токени, або використання системи розпізнавання голосу або шаблонів підпису для підтвердження ідентичності.

Ці методи двофакторної автентифікації на платіжних картках Visa та MasterCard дозволяють підвищити безпеку та захистити картки від несанкціонованого використання. Вони забезпечують надійне підтвердження ідентичності власника картки та ускладнюють можливість шахрайських дій.

3.10 Висновки до третього розділу

У даному розділі дипломної роботи було проведено аналіз протоколів безпеки та зовнішніх захисних елементів платіжних карток Visa та MasterCard, які є двома з найбільш популярних банківських платіжних систем у світі. Аналіз був спрямований на виявлення загроз безпеці цих систем та оцінку ефективності застосованих методів захисту.

Протоколи безпеки відіграють важливу роль у забезпеченні безпеки платіжних операцій, особливо при онлайн-транзакціях. Результати аналізу показали, що Visa і MasterCard використовують протоколи, такі як 3-D Secure, для автентифікації власника картки та запобігання несанкціонованим транзакціям. Цей протокол вимагає введення додаткового пароля або коду підтвердження під час онлайн-платежів, що підвищує рівень безпеки.

Зовнішні захисні елементи, такі як чіпи на картках EMV (Europay, MasterCard, Visa), є ще одним важливим елементом безпеки платіжних систем. Ці чіпи використовують криптографічні алгоритми для забезпечення безпеки та захисту конфіденційної інформації. Вони генерують унікальні коди для кожної транзакції, що ускладнює завдання кіберзлочинців при спробі підробити або скопіювати картку.

Загальний аналіз протоколів безпеки та зовнішніх захисних елементів показав, що вони виявляються досить ефективними в запобіганні багатьом типам шахрайства та несанкціонованих транзакцій. Однак, варто зауважити, що незважаючи на застосування таких захисних механізмів, існує постійна загроза новим методам атак та шахрайству.

4. ПРОПОЗИЦІЇ ПОКРАЩЕННЯ БЕЗПЕКИ БАНКІВСЬКИХ ПЛАТІЖНИХ СИСТЕМ

У даному розділі будуть розглянуті рекомендації та пропозиції з метою покращення безпеки в сучасних банківських платіжних системах. Ці пропозиції базуються на виявлених загрозах та ризиках і спрямовані на забезпечення високого рівня захисту від них.

4.1. Використання сучасних криптографічних алгоритмів

З метою удосконалення захисту, конфіденційності, цілісності та автентичності даних може бути запропоноване використання наступних криптоалгоритмів:

1) Шифрування даних: Пропонується використання сучасних криптографічних алгоритмів для шифрування конфіденційної інформації, переданої між різними компонентами платіжної системи. Зокрема, можна використовувати асиметричні алгоритми шифрування, такі як RSA або ECC (еліптичні криві), для захисту сесійних ключів, які використовуються для симетричного шифрування [13].

2) Хеш-функції: Рекомендується використання сучасних хеш-функцій, наприклад SHA-256 або SHA-3, для забезпечення цілісності даних. Хеш-функції використовуються для обчислення хеш-кодів, які служать для перевірки цілісності даних та виявлення будь-яких змін у переданих повідомленнях [17].

3) Цифровий підпис: Пропонується використання цифрових підписів для забезпечення автентичності даних та ідентифікації відправника. Для цього можна використовувати асиметричні алгоритми, такі як RSA або ECC, для створення та перевірки цифрових підписів. Цифрові підписи гарантують, що дані не були змінені під час передачі та що вони походять від відповідного відправника.

4) Ключовий обмін: Рекомендується використання безпечних протоколів для обміну ключами між учасниками платіжної системи. Наприклад, можна використовувати протоколи обміну ключами на основі дифі-Хелмана (Diffie-Hellman) або еліптичної кривої для забезпечення безпеки при обміні сесійними ключами.

5) Стійкість до квантових обчислювань: З огляду на швидкий розвиток квантових комп'ютерів, рекомендується використання криптографічних алгоритмів, які стійкі до квантових обчислень. На сьогоднішній день існують алгоритми, такі як RSA та ECC, які можуть бути піддані атакам з використанням квантових комп'ютерів. Тому рекомендується впровадження квантово-стійких криптографічних алгоритмів, які забезпечують безпеку навіть при використанні квантових обчислювальних систем. Наприклад, алгоритми на основі геш-функцій (приклади: хеш-підпис Гровера, хеш-функції на основі суперпозиції алгебро-графових функцій) та латинських квадратів можуть бути використані для забезпечення стійкості до квантових обчислень.

4.2 Розробка механізмів автентифікації та авторизації

Метою розробки є забезпечення високого рівня безпеки та захисту від несанкціонованого доступу до платіжних ресурсів. Нижче наведено деякі пропозиції:

1) Аналіз існуючих механізмів: Проводиться аналіз існуючих механізмів автентифікації та авторизації в банківських платіжних системах, зокрема в системах Visa та MasterCard. Оцінюються їх сильні та слабкі сторони, виявляються можливі уразливості та недоліки, які можуть бути використані зловмисниками для несанкціонованого доступу до системи.

2) Вибір сучасних методів автентифікації: Здійснюється вибір та розробка сучасних методів автентифікації, які забезпечують надійний ідентифікацію користувачів платіжної системи. Наприклад, можуть бути використані методи біометричної автентифікації (відбиток пальця,

розпізнавання обличчя), одноразові паролі (OTP), двофакторна автентифікація та інші сучасні технології.

3) Розробка механізмів авторизації: Проводиться розробка механізмів авторизації, які визначають права доступу користувачів до різних функцій та ресурсів платіжної системи. Розробляються правила та політики авторизації, враховуючи різні рівні доступу та види операцій.

4) Впровадження мультифакторної автентифікації: Розглядається можливість впровадження мультифакторної автентифікації, що передбачає використання двох або більше факторів для підтвердження ідентифікації користувача. Наприклад, можуть використовуватися комбінації паролів, фізичних токенів, біометричних даних тощо. Впровадження мультифакторної автентифікації підвищує безпеку системи, ускладнюючи несанкціонований доступ зловмисників.

5) Тестування та оцінка ефективності: Проводиться тестування розроблених механізмів автентифікації та авторизації для оцінки їх ефективності та надійності. Перевіряється відповідність запланованим цілям безпеки, швидкість роботи, масштабованість та інші важливі параметри.

6) Вдосконалення та пропозиції: На основі результатів тестування та оцінки ефективності розроблених механізмів автентифікації та авторизації формулюється вдосконалення та пропозиції з метою подальшого покращення безпеки банківських платіжних систем. Наприклад, можуть бути запропоновані оновлення алгоритмів, використання нових технологій автентифікації, впровадження додаткових заходів безпеки та політик доступу.

4.3 Захист від атак на протоколи

1) Виявлення потенційних загроз: Проводиться аналіз потенційних загроз, які можуть вплинути на протоколи безпеки банківських платіжних систем. Це можуть бути атаки, такі як перехоплення даних, атаки на автентифікацію, атаки на шифрування та інші види атак, які спрямовані на вразливості протоколів.

2) Вдосконалення протоколів безпеки: Здійснюється вдосконалення протоколів безпеки, що використовуються в банківських платіжних системах. Це може включати оновлення алгоритмів шифрування, використання сильних ключів, застосування протоколів забезпечення цілісності даних та інших заходів для запобігання атакам.

3) Впровадження механізмів виявлення вторгнень: Розробляються та впроваджуються механізми виявлення вторгнень, які дозволяють вчасно виявляти та реагувати на підозрілу активність або аномалії в протоколах безпеки. Це можуть бути системи моніторингу, виявлення аномалій, аналізу журналів подій та інші інструменти, які допомагають виявити вторгнення або несправедливу діяльність [14].

4) Застосування шифрування та цифрових підписів: Використовується шифрування та цифрові підписи для забезпечення конфіденційності, цілісності та автентичності даних, які передаються по протоколу безпеки. Застосування шифрування дозволяє захистити дані від перехоплення та несанкціонованого доступу, а цифрові підписи забезпечують автентичність та цілісність даних.

5) Впровадження захисту від DDoS-атак: Розробляються та впроваджуються механізми захисту від DDoS-атак, які спрямовані на перевантаження системи шляхом спаму, великого обсягу запитів або використання ботнетів. Це можуть бути фільтри трафіку, системи розпізнавання та блокування аномального трафіку та інші заходи для забезпечення доступності та безпеки системи під час DDoS-атак [15].

6) Тестування та аудит безпеки: Здійснюється систематичне тестування та аудит безпеки протоколів з метою виявлення вразливостей та потенційних проблем безпеки. Це можуть бути пенетраційні тести, сканування вразливостей, перевірка відповідності стандартам безпеки та інші методи, що допомагають виявити та усунути проблеми безпеки.

4.4 Проведення тестування та аудиту протоколів безпеки

1) Визначення цілей та обсягу тестування: Перед початком тестування визначаються цілі та обсяг тестування. Це включає виявлення потенційних вразливостей, перевірку відповідності протоколів стандартам безпеки, перевірку реалізації протоколів та їхню ефективність.

2) Вибір методів тестування: Вибираються методи тестування, які найбільш ефективно виявлять вразливості протоколів безпеки. Це можуть бути пенетраційні тести, сканування вразливостей, аналіз коду, тестування стійкості до атак та інші методи.

3) Виконання тестування: Здійснюється процес тестування, включаючи запуск тестових сценаріїв, перевірку безпеки комунікаційних протоколів, аналіз вразливостей та експлуатацію можливих проблем безпеки. Під час тестування можуть використовуватись автоматизовані інструменти, а також виконуватись ручні перевірки [16].

4) Аналіз результатів тестування: Після завершення тестування проводиться аналіз отриманих результатів. Виявлені вразливості, проблеми безпеки та недоліки документуються і оцінюються за їхньою серйозністю та впливом на безпеку системи.

5) Розробка рекомендацій та плану вдосконалення: На основі результатів тестування розробляються рекомендації щодо вдосконалення протоколів безпеки. Це можуть бути виправлення вразливостей, впровадження нових захисних механізмів, оновлення стандартів безпеки та інші заходи для підвищення рівня безпеки.

6) Проведення аудиту безпеки: Паралельно з тестуванням може проводитись аудит безпеки для перевірки відповідності протоколів безпеки встановленим стандартам та рекомендаціям. Аудит включає перевірку правильності конфігурації системи, виконання політик безпеки, перевірку застосування криптографічних протоколів та інші аспекти безпеки.

7) Вдосконалення протоколів безпеки: На основі результатів тестування та аудиту розробляються плани вдосконалення протоколів

безпеки. Це може включати внесення змін до архітектури протоколу, реалізацію нових захисних механізмів, оновлення стандартів безпеки та інші кроки для забезпечення найвищого рівня безпеки банківських платіжних систем.

4.5 Висновки до четвертого розділу

У даному розділі були розглянуті пропозиції щодо покращення безпеки сучасних банківських платіжних систем. Зважаючи на постійний розвиток технологій та зростання загроз безпеці, вдосконалення заходів безпеки є надзвичайно важливим завданням для банків та організацій, що працюють у фінансовому секторі.

Загалом, пропозиції щодо покращення безпеки банківських платіжних систем покликані підвищити рівень захисту від сучасних загроз. Важливо впроваджувати інноваційні технології, враховувати найновіші стандарти безпеки та забезпечувати постійне оновлення заходів безпеки. Тільки таким чином можна забезпечити надійність та довіру до банківських платіжних систем у сучасному цифровому світі.

ВИСНОВКИ

У дипломній роботі був проведений детальний аналіз загроз безпеці та методів їх захисту для сучасних банківських платіжних систем. Досліджено теоретичні аспекти безпеки банківських платіжних систем, міжнародні стандарти безпеки, протоколи безпеки та зовнішні захисні елементи платіжних карток Visa та MasterCard. Робота також містить пропозиції щодо покращення безпеки банківських платіжних систем.

Зростання використання банківських платіжних систем та електронних платежів призвело до появи нових загроз безпеці. Кіберзлочинці використовують різноманітні технології та методи для отримання конфіденційної інформації, зламу систем та крадіжки грошей. Тому безпека банківських платіжних систем є надзвичайно важливою проблемою, яку слід постійно вдосконалювати.

Міжнародні стандарти безпеки в банківських платіжних системах є основою для забезпечення безпеки платіжних операцій. Стандарти PCI DSS (Payment Card Industry Data Security Standard) визначають вимоги щодо захисту кардхолдерських даних, захисту мереж та систем обробки платежів. Ці стандарти включають такі елементи, як забезпечення фізичної безпеки, шифрування даних, контроль доступу та моніторинг систем.

Протоколи безпеки та зовнішні захисні елементи платіжних карток Visa та MasterCard також грають важливу роль у забезпеченні безпеки. Протоколи, такі як 3-D Secure, використовуються для автентифікації власника картки під час онлайн-транзакцій. Зовнішні захисні елементи, такі як чіпи на картках EMV, забезпечують більшу безпеку шляхом використання криптографічних алгоритмів та генерації унікальних кодів для кожної транзакції.

Однак, необхідно враховувати той факт, що кіберзлочинці постійно розвивають свої методи атак і шукають слабкі місця у системах. Тому важливо, щоб банківські платіжні системи постійно оновлювали свої заходи безпеки та вдосконалювали їх у відповідності до нових загроз.

З метою покращення безпеки банківських платіжних систем рекомендується впровадження додаткових заходів. Серед таких заходів можуть бути підвищення рівня свідомості клієнтів щодо безпеки та захисту їхніх особистих даних, використання біометричних методів автентифікації, вдосконалення систем виявлення шахрайства та аналізу поведінки користувачів.

У цілому, безпека банківських платіжних систем є складним завданням, що вимагає постійного вдосконалення та оновлення заходів безпеки. Тільки за допомогою комплексного підходу, включаючи використання міжнародних стандартів, протоколів безпеки та зовнішніх захисних елементів, а також впровадження нових заходів, можна забезпечити надійну та безпечну роботу банківських платіжних систем у сучасному світі.

ПЕРЕЛІК ПОСИЛАНЬ

1 Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley. 2008. С. 9-24.

2 Bishop, M. Computer Security: Art and Science. Addison-Wesley. 2003. С. 76-83.

3 Visa Inc. URL: https://uk.wikipedia.org/wiki/Visa_Inc. (дата звернення: 15.05.2023).

4 SWIFT. URL: https://uk.wikipedia.org/wiki/SWIFT (дата звернення: 16.05.2023).

5 Kizza, J. M. Guide to Computer Network Security. 2015. С. 51–62.

6 Stallings, W. Cryptography and Network Security: Principles and Practice. 2017. С. 97-114.

7 Schneier, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. 2015. С. 235-255.

8 Ristic, I. Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications. Feisty Duck. 2018. С. 210-225.

9 Janczewski, L. J., & Colarik, A. M. Managing Information Security Risks: The OCTAVE Approach. 2007. С. 55-60.

10 Whitman, M. E., & Mattord, H. J. Principles of Information Security. Cengage Learning. 2018. С. 112-119.

11 Cherdantseva, Y., Hilton, J., & Florea, A. Cyber Threat Intelligence Sharing: A Perspective on Information Sharing Models. 2019. С. 241-247.

12 Cyber Resilience Oversight Expectations for Financial Market Infrastructures. URL: https://www.ecb.europa.eu/paym/cons/html/cyberresilience.en.html (дата звернення: 29.03.2023).

13 PCI Data Security Standard (PCI DSS). URL: https://www.pcisecuritystandards.org/document_library (дата звернення: 04.04.2023).

14 Framework for Improving Critical Infrastructure Cybersecurity. URL: https://www.nist.gov/cyberframework (дата звернення: 29.04.2023).

15 Cybersecurity: A Governance, Risk, and Compliance Framework. URL: https://openknowledge.worldbank.org (дата звернення: 16.04.2023).

16 Cyber Lexicon. URL: http://www.fsb.org (дата звернення: 21.05.2023).

17 Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. 2023. С. 59. DOI: https://doi.org/10.32620/ICT.23.t1 (дата звернення: 02.04.2023).

18 PCI Security Standards Council. Payment Card Industry (PCI) Data Security Standard. URL: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf (дата звернення: 12.04.2023).

19 PCI-DSS: Payment Card Industry Data Security Standard. URL: https://www.acunetix.com/websitesecurity/pci-dss/ (дата звернення: 02.06.2023).

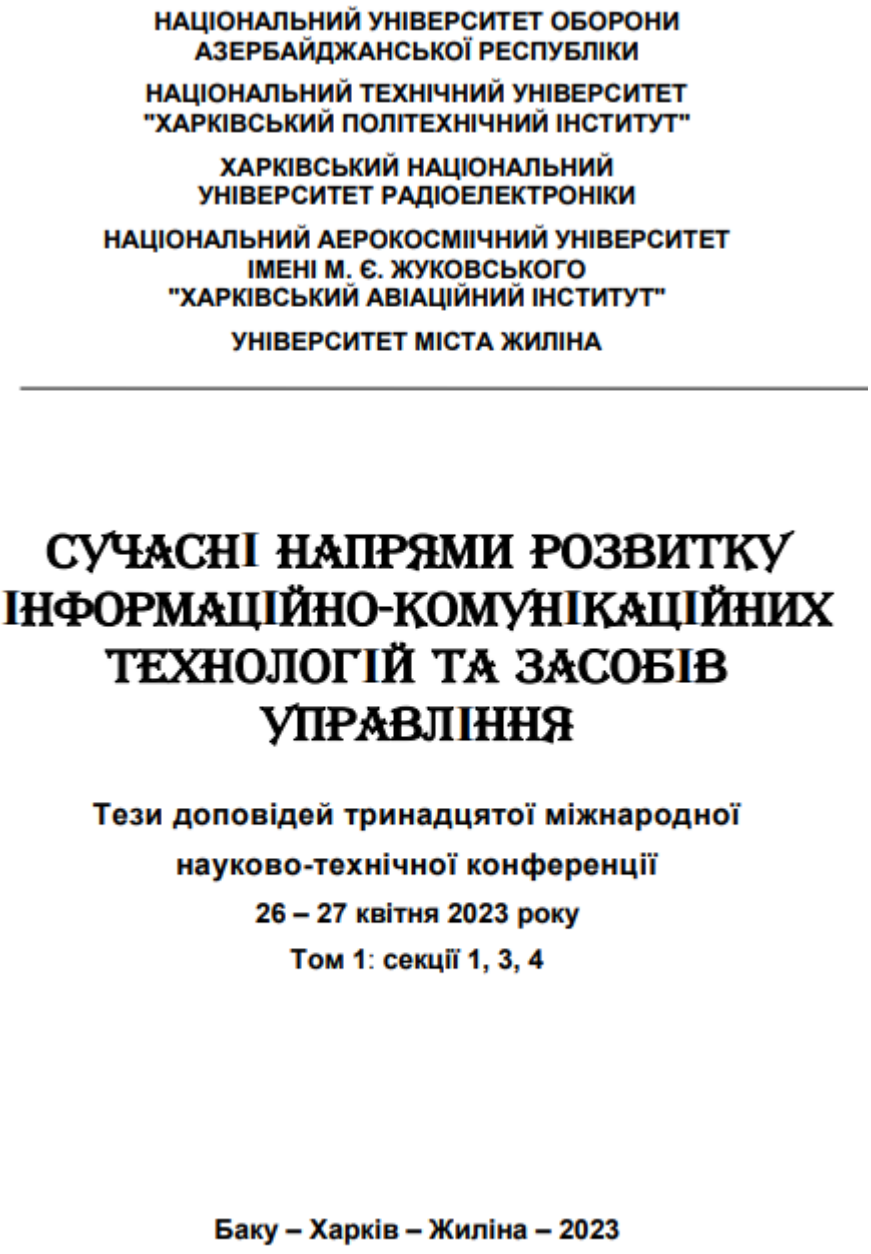
20 MasterCard. URL: https://www.MasterCard.ua/uk-ua.html (дата звернення: 02.06.2023).

21 BigCommerce. URL: https://support.bigcommerce.com/s/article/3D-Secure?language=en_US (дата звернення: 02.06.2023).

22 MasterCard. URL: https://uk.m.wikipedia.org/wiki/MasterCard дата звернення: 02.06.2023).

ДОДАТОК А

Участь у міжнародній конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління».



НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ
АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ М. Є. ЖУКОВСЬКОГО
"ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"

УНІВЕРСИТЕТ МІСТА ЖИЛІНА

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей тринадцятої міжнародної
науково-технічної конференції
26 – 27 квітня 2023 року
Том 1: секції 1, 3, 4

Баку – Харків – Жиліна – 2023

Рисунок А.1 – Титульний лист збірки тез доповідей конференції

СЕКЦІЯ 3
БЕЗПЕКА ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н., проф. О. А. Смірнов, ЦНТУ, Кропивницький
Секретар секції: к.т.н., доц. О. В. Сєвєрінов, ХНУРЕ, Харків

ANALYSIS OF SECURITY THREATS AND PROTECTION METHODS FOR MODERN BANKING PAYMENT SYSTEMS

Koshman S., Krasnobayev V., Rossomakha M.
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine

In today's world, electronic payment systems are an integral part of the financial infrastructure. However, the increasing number of cyberattacks and criminal activity in this sector emphasizes the need to strengthen security measures. One of the most common threats is cyberattacks on Visa and MasterCard systems. Cybercriminals can use various methods to break through the systems' security, such as phishing, viruses, trojans, DDoS attacks, and others [1, 2]. This can result in the loss of data, breaches of confidentiality, theft of money from user accounts, spread of fraud, loss of customer trust and bank reputation, and more. However, Visa and MasterCard are making significant efforts to prevent such security threats [3, 4].

The purpose of the report is to identify vulnerabilities, prevent different types of attacks, eliminate their consequences on banking payment systems, and prevent the possibility of their being hacked.

Research and analysis of literature, information on real cases of attacks on banking payment systems, have shown that to achieve the goal, the most widespread is the use of modern methods of data encryption. Data encryption provides confidentiality and protection against unauthorized access. Modern cryptographic algorithms (such as AES, RSA), the SSL/TLS secure connection protocol, and tokenization methods are used in banking payment systems to protect against hacks and ensure transaction security. Also, Visa and MasterCard use two-factor authentication (2FA), which appears in the form of a request for additional code or other information after entering the main password. This significantly increases the level of security because even if hackers break the user's password, they still cannot access the account without an additional authentication factor. The results of the work can be useful for developing proposals to increase the security of banking payment systems and prevent possible threats. The report emphasizes the need for continuous updating of protection methods and improving security measures in the world of electronic payment systems to ensure protection against potential threats.

References

1. "The security of payment systems: A survey of issues and solutions" by Ross Anderson and Steven Murdoch. (https://www.cl.cam.ac.uk/~rja14/Papers/SE-06.pdf).

2. Security Threats to Electronic Payment Systems - A Review" by S. Chandrakala and N. Kavitha. (https://www.researchgate.net/publication/322890945_Security_...)
3. "Analysis of Security Threats and Vulnerabilities in Payment Systems" by Jong-Hyuk Park, Yunsik Son, and HwaMin Lee.
(https://www.sciencedirect.com/science/article/pii/S2212017313005793)
4. "Card payment frauds in the UK and Europe" by Matteo Crippa and Francesco Saita. (https://www.sciencedirect.com/science/article/pii/S0167923604000876

Рисунок А.2 – Мої тези, підготовлені для конференції