Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: «Вдосконалення захисту електронних банківських послуг за рахунок впровадження сучасних технологій безпеки»

Виконавець: студентка IV курсу, групи КБ-43мс

_____ **Анастасія ПІСЬМЕНЮК**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник роботи	Юрій ЩЕБЛАНІН	

Нормоконтроль	Олена БОГУСЛАВСЬКА	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-43 мс** **Анастасії Романівни Письменюк**
(група) (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи «Вдосконалення захисту електронних банківських послуг за рахунок впровадження сучасних технологій безпеки»

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Сучасні технології захисту електронних банківських послуг

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися із сучасними технологіями захисту електронних банківських послуг, їх типовими ризиками та можливими вразливостями.
Розробити рекомендацій щодо підвищення рівня захищеності електронних банківських послуг.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність роботи полягає у використанні отриманих результатів для підвищення рівня захищеності електронних банківських послуг

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Анастасія ПІСЬМЕНЮК (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 20.01.2023	*виконано*
2	Аналіз літератури	21.01.2023 – 10.02.2023	*виконано*
3	Обґрунтування вибору рішення	11.02.2023 – 15.02.2023	*виконано*
4	Аналіз нормативно-правового регулювання надання електронних банківських послуг	16.02.2023 – 03.03.2023	*виконано*
5	Аналіз переваг використання електронних банківських послу	04.03.2023 – 24.03.2023	*виконано*
6	Дослідження особливостей кібератак на банківську систему	25.03.2023 – 07.04.2023	*виконано*
7	Дослідження історії розвитку та ризиків використання електронних банківських послуг	08.04.2023 – 28.04.2023	*виконано*
8	Розробка рекомендацій щодо підвищення рівня захищеності електронних банківських послуг	29.04.2023 – 10.05.2023	*виконано*
9	Оформлення пояснювальної записки	11.05.2023 – 05.06.2023	*виконано*
10	Підготовка до захисту кваліфікаційної роботи	06.06.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Анастасія ПІСЬМЕНЮК (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 73 сторінки, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки та список джерел. У пояснювальній записці кваліфікаційної роботи міститься 11 рисунків і 1 таблиця.

Метою роботи є розробка рекомендацій для підвищення захищеності безпеки електронних банківських послуг.

Об'єктом дослідження є процес захисту електронних банківських послуг.

Предметом дослідження є сучасні технології захисту електронних банківських послуг.

Під час виконання кваліфікаційної роботи були використані наступні *методи*:

- аналіз відкритих джерел;
- порівняння та протиставлення;
- статистичний, системний, структурний та історичний аналіз.

Практична цінність роботи полягає у використанні отриманих результатів для підвищення рівня захищеності електронних банківських послуг та забезпечує зручність для користувачів. Результати дослідження показують, що використання біометричної аутентифікації з розпізнаванням обличчя значно мінімізує ризики підробки, викрадення даних та шахрайства. При використанні цього методу, очікується зменшення відмов при підтвердженні, що в свою чергу позитивно вплине на показник конверсії.

Ключові слова: кібербезпека, електронний платіж, 3D Secure, вразливості, захист персональних даних, біометрія, біометричні методи аутентифікації.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

3DS	–	3-D Secure
APWG	–	Anti-Phishing Working Group
EMV	–	Europay & MasterCard & VISA
iOS	–	iPhone operating system
NFC	–	Near Field Communication
PCI DSS	–	Payment Card Industry Data Security Standard
RFID	–	Radio frequency identification
SSL	–	Secure Sockets Layer
SWIFT	–	Society for Worldwide Interbank Financial Telecommunications
UPC	–	Universal Product Code
XML	–	Розширювана мова розмітки
ЕПЗ	–	Електронні платіжні засоби
ЗЗІ	–	Засоби захисту інформації
КЗІ	–	Криптографічний захист інформації
НБУ	–	Національний банк України
НСМЕП	–	Національна система масових електронних платежів
ПС	–	Платіжна система
ПТКС	–	Програмно-технічний комплекс самообслуговування
СЕП	–	Система електронних платежів

ВСТУП

Неможливо уявити сучасну людину без телефона, ноутбука або смарт-годинника. Так само не можна уявити ці пристрої без їхнього доступу до мережі Інтернет. Все життя сучасної людини концентрується в смартфоні.

Розвиток технологій та суспільства впливає на зміни в системі розрахунків, які спрямовані на забезпечення ефективності грошових переказів відповідно до потреб суспільства. Однією із значних тенденцій є зростання популярності миттєвих платіжних систем, які поєднують в собі швидкість операцій та потенційно низькі витрати на їх обробку. В Україні миттєві платежі, зокрема платежі з картки на картку, становлять 43% від загальної суми безготівкових операцій з використанням платіжних карток. Останнім часом пандемія ще більше прискорила впровадження безготівкових розрахунків і одночасно підкреслила важливість їх економічної ефективності. Таким чином, миттєві платежі стають необхідністю у сфері платежів. Це ставить перед нами завдання якісної трансформації грошової системи з використанням безготівкових розрахунків, які регулюються законодавством і враховують перспективи подальшого розвитку.

За останні кілька років спостерігається значне збільшення обсягу покупок електронної комерції, що здійснюються онлайн. За даними статистики, близько 18% усіх продажів у світі вже здійснюється через Інтернет. З кожним днем з'являються нові банківські рахунки, термінали та інші електронні засоби платежів, що робить фінансові послуги широко доступними для користувачів. Проте, разом із зростанням цифрових технологій, збільшується і кількість кіберзлочинів. Зловмисники намагаються здійснити атаки на банківські системи, отримати несанкціонований доступ до особистих даних клієнтів або зламати їх рахунки.

Переважні способи оплати споживачів також продовжують змінюватися. Платіжні картки все ще домінують, і ми не бачимо жодних ознак того, що це зміниться найближчим часом.

Однак мобільні платежі продовжують набирати обертів і зараз досягли важливої відмітки: споживачі віддають перевагу їм більше, ніж готівці в усіх скандинавських країнах.

Крім того, все більш широке використання цифрових платежів і посилення міжканальної інтеграції дають можливість зібрати більше даних про клієнтів, що також важливо для вдосконалення системи безпеки.

Актуальність роботи полягає в тому, що розвиток технологій та зростання популярності електронних платежів створюють нові виклики у сфері безпеки банківських операцій. Хоч електронний банкінг надає багато переваг приватним клієнтам, підприємствам і банкам, однак не варто нехтувати ризиками, котрі з ним пов'язані. Тож ця робота спрямована на розробку рекомендацій по впровадженню біометричної аутентифікації з використанням системи розпізнавання обличчя, для забезпечення захисту особистої інформації та коштів, та зручності користувачів, що може покращити бізнес-показники і позитивно вплинути на конверсію.

Метою роботи є розробка рекомендацій для підвищення захищеності безпеки електронних банківських послуг.

Для досягнення зазначеної мети кваліфікаційної роботи необхідно вирішити наступні *завдання*:

- провести аналіз нормативно-правового забезпечення надання електронних банківських послуг;
- дослідити ризики використання електронних банківських послуг;
- дослідити сучасні кібератаки на банківську систему;
- дослідити протокол безпеки для онлайн-транзакцій платіжних карток;
- розробити рекомендації щодо підвищення рівня захищеності електронних банківських послуг.

Об'єктом дослідження є процес захисту електронних банківських послуг.

Предметом дослідження є сучасні технології захисту електронних банківських послуг.

Під час виконання кваліфікаційної роботи були використані наступні *методи*:

- аналіз відкритих джерел;
- порівняння та протиставлення;
- статистичний, системний, структурний та історичний аналіз.

Практична цінність роботи роботи полягає у використанні отриманих результатів для підвищення рівня захищеності електронних банківських послуг та забезпечує зручність для користувачів. Результати дослідження показують, що використання біометричної аутентифікації з розпізнаванням обличчя значно мінімізує ризики підробки, викрадення даних та шахрайства. При використанні цього методу, очікується зменшення відмов при підтвердженні, що в свою чергу позитивно вплине на показник конверсії.

РОЗДІЛ 1
АНАЛІЗ СУЧАСНОГО СТАНУ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ БАНКІВСЬКИХ ПОСЛУГ

1.1 Поняття і характеристики електронних банківських послуг

Безготівкові розрахунки – швидкий, зручний та безпечний спосіб оплати товарів та послуг. Розширення сфери безготівкових розрахунків сприяє прозорості платежів та економічному росту країни. Національний банк встановлює правила для здійснення безготівкових розрахунків та сприяє їх безпеці та надійності. [2]

Швидке та надійне проведення безготівкових розрахунків забезпечують платіжні системи.

Для клієнта процес покупки в електронній комерції починається зі взаємодії з платіжним провайдером. Саме завдяки чіткій та злагодженій роботі платіжних провайдерів, банків, процесингових систем та інших учасників екосистеми користувач може здійснити оплату буквально за кілька кліків, а час виконання транзакції становить від кількох секунд до кількох днів (в особливих випадках). Частка ж шахрайських операцій, за даними НБУ, порівняно із загальним обсягом безготівкових операцій є дуже невеликою – у 2020 році ця цифра становила близько 0,005%.

Переважні способи оплати споживачів також продовжують змінюватися. Платіжні картки все ще домінують, і ми не бачимо жодних ознак того, що це зміниться найближчим часом. Оскільки електронні платежі з кожним роком виконуються дедалі швидше, а рівень їхньої безпеки зростає, збільшується і частка cashless-операцій. Подібні тенденції стимулюватимуть стабільне зростання частки безготівкових розрахунків у світі у різних сферах бізнесу. І якщо використання готівки досить втрачає популярність, то мобільна оплата тільки набирає обертів, статистичні дані відображено на рисунку 1.1.

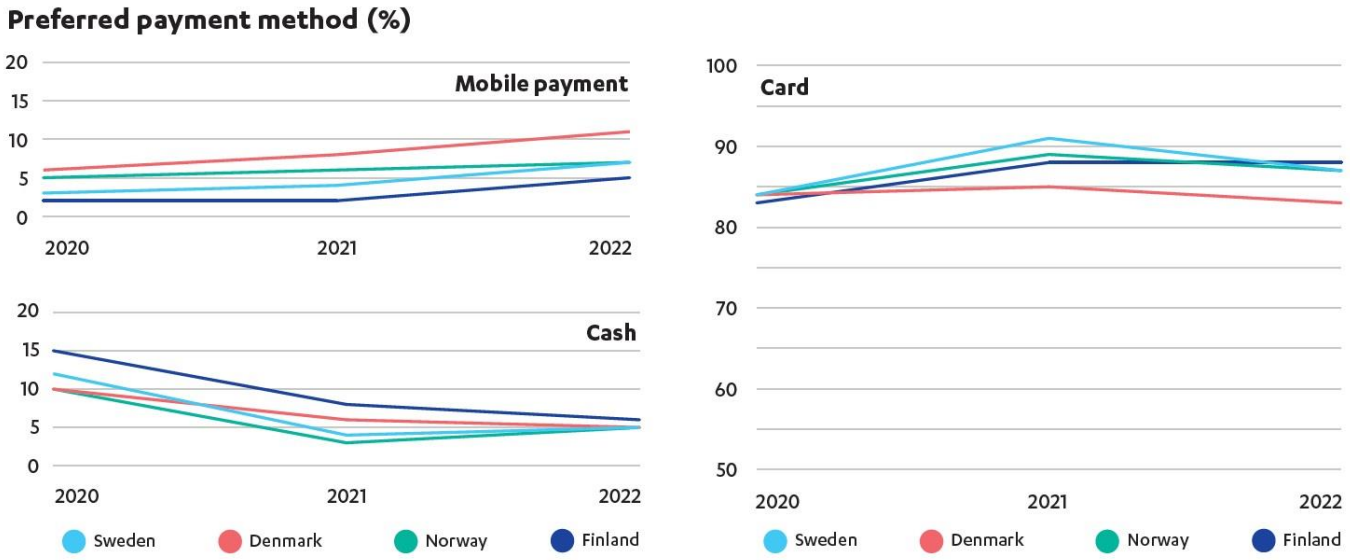

Рисунок 1.1 – Використовувані методи оплати

До складу платіжної системи як екосистеми в цілому входить ціла низка учасників: платіжні провайдери, банки, центральний координуючий орган (як правило, центробанк країни), процесингові центри та провайдери технічної інфраструктури, що забезпечують обчислювально-комунікаційну базу для проведення платежів. Усі учасники системи взаємодіють між собою за певними правилами та домовленостями, спираючись на чітко виписану законодавчу основу.

Загалом у проведенні електронних платежів задіяна ціла екосистема, до якої, як згадувалося вище, входить безліч учасників. Однак є в цій екосистемі особливий учасник, який відповідає за координацію всіх інших ланок, – платіжна система. ПС не емітує картки, не видає кредитів, не визначає тарифи для еквайрингу. Основне завдання ПС – забезпечувати ефективні та надійні фінансові послуги.

У цілому нині ПС можна розділити на першого і другого покоління, а також на національні та міжнародні.

Найбільшими міжнародними платіжними системами першого покоління є американські Mastercard, Visa, American Express, Diners Club International, китайська UnionPay та японська JCB. Усі ці ПС починали з діяльності всередині однієї країни, проте сьогодні оперують практично у всіх країнах світу.

Міжнародні платіжні системи працюють із банками та платіжними провайдерами багатьох країн, їхні картки можна прив'язувати до різних рахунків, переказувати гроші з однієї країни до іншої та оперувати різною валютою.

Картки національних ПС працюють виключно у межах однієї країни. Національна платіжна система України, створена Національним банком України, має назву ПРОСТІР (повна назва – «Український платіжний простір»). До 2016 року вона мала назву Національна система масових електронних платежів (скорочено НСМЕП). На сьогодні до НПС «ПРОСТІР» входять 53 учасники, всього випущено 625 тисяч карток. [3]

До другого покоління належать небанківські платіжні системи, такі як PayPal. Нові ПС як транспортну інфраструктуру використовують інтернет і працюють із так званими електронними грошима. Це можуть бути або традиційні валюти, які переведені з розрахункового або карткового рахунку на обліковий запис у такій платіжній системі, або недержавні грошові одиниці, наприклад, криптовалюта.

Грошовий переказ тут виконується онлайн і тільки між акаунтами користувача в цій системі. Тобто і покупець, і продавець повинні мати облікові записи у відповідній електронній ПС. Отримані продавцем гроші надходять до електронного гаманця, далі їх можна використовувати для покупок усередині системи або вивести на його розрахунковий рахунок.

Окремо варто виділити службові ПС для міжбанківських розрахунків, до яких у пересічних споживачів відсутній безпосередній доступ. Наприклад, 1973 року було створено платіжну систему для міжнародних платежів SWIFT – Society for Worldwide Interbank Financial Telecommunications. Система забезпечує обмін фінансовою інформацією у цілодобовому режимі з високим рівнем безпеки.

Також до закритих платіжних систем належать внутрішньонаціональні мережі, за допомогою яких відбувається обмін інформацією між центробанком та іншими банками. В Україні це Система електронних платежів (СЕП) Національного банку України. Участь у СЕП є обов'язковою для всіх комерційних банків країни.

Громадяни та організації можуть здійснювати безготівкові розрахунки в Україні, використовуючи емісійні платіжні інструменти.

Випуск платіжних інструментів - це платіжна послуга, яку надає провайдер платіжних послуг на основі договору з платником, і яка включає випуск (предоставлення) платіжного інструменту платнику для ініціювання та обробки платіжних транзакцій. Емісійні платіжні інструменти включають такі засоби, як електронні платіжні засоби, платіжні картки та попередньо оплачені платіжні інструменти.

Електронний платіжний засіб (ЕПЗ) - це платіжний інструмент, який використовує будь-який носій, що містить в електронній формі дані, які необхідні для ініціювання платіжної операції або проведення інших операцій, визначених у договорі з емітентом.

Платіжна картка - це вид електронного платіжного засобу, який зазвичай реалізується у формі пластикової або іншої картки.

Електронні банківські послуги - це фінансові послуги, які надаються клієнтам через електронні канали зв'язку, такі як Інтернет, мобільні додатки або телефон та з використанням електронних платіжних засобів. Ці послуги дозволяють клієнтам здійснювати банківські операції та управляти своїми фінансами онлайн, зручно та безпечно.

До електронних банківських систем відносять:

Інтернет-банкінг. Це можливість здійснювати банківські операції через веб-портал банку. Клієнти можуть перевіряти баланс рахунків, здійснювати перекази між рахунками, платити рахунки, замовляти чеки та інше.

Телефонний банкінг. Це можливість використовувати банківські послуги через мобільні додатки на смартфонах або планшетах. Цей тип послуг дозволяє клієнтам здійснювати різні банківські операції, такі як перекази коштів, оплата рахунків, керування картками та перегляд історії транзакцій, зручно та в будь-який час.

Електронні платіжні системи. Призначені для здійснення електронні перекази грошей між різними особами або організаціями. Прикладами є PayPal, Stripe, Skrill, Google Pay та інші.

Електронні кредити та позики. Банки також надають можливість оформлення кредитів та позик через електронні канали. Клієнти можуть подавати заявки на кредити, переглядати умови позик та отримувати гроші на свої банківські рахунки.

Передплачений платіжний інструмент - платіжний інструмент для здійснення операцій з електронними грошима. Передплачений платіжний інструмент використовується відповідно до схеми виконання платіжних операцій відповідного емітента електронних грошей та/або правил платіжної системи, згідно з якими випускаються платіжні інструменти, та з дотриманням вимог законодавства України [4].

Емісію платіжних інструментів у межах України має право здійснювати емітент – надавач платіжних послуг, який надає послугу еквайрингу платіжних інструментів та має ліцензію на надання такої послуги відповідно до Закону України "Про платіжні послуги" [4].

Для здійснення емісії платіжних інструментів для використання в платіжній системі емітент (крім отримання ліцензії у Національному банку) має укласти договір з оператором відповідної платіжної системи.

Платіжний інструмент може бути:

– особистим – для власних потреб фізичних осіб;

– корпоративним (бізнесовим) – для потреб господарської/ підприємницької/ незалежної професійної діяльності.

– Платіжний інструмент дозволяє:

– розрахуватися за товари і послуги;

– переказати кошти іншій особі;

– отримати готівку;

– отримати інформацію про належні держателю кошти.

При цьому порядок та умови використання платіжного інструменту визначаються у договорі з емітентом.

1.1.1 Обмін даними між платіжним провайдером, ПС, мерчантом та банком.

Припустимо, що клієнт вирішив купити певний товар в онлайн-магазині. Він вводить дані своєї кредитної картки на веб-сайті або в мобільному додатку торговельного підприємства. Ці дані, в зашифрованому форматі, надсилаються через платіжний шлюз провайдера до банку-еквайрера, який обслуговує платежі безготівкового розрахунку для даного магазину. Потім ці дані передаються до процесингового центру платіжної системи (наприклад, Mastercard, Visa, ПРОСТІР тощо).

Платіжна система запитує в банку-емітента (банку, що випустив картку клієнта), чи може бути проведено транзакцію. Якщо коштів на рахунку достатньо, і рахунок не заблоковано, банк-емітент надає дозвіл банку-еквайру. Еквайрер переказує відповідні кошти на рахунок продавця. Це приблизне уявлення про те, як відбуваються онлайн-платежі.

Для того, щоб онлайн-покупка була максимально зручною для клієнта, продавці використовують платіжні шлюзи. Це захищені канали, надані платіжним провайдером, через які передаються зашифровані дані кредитної картки клієнта.

Платіжний шлюз забезпечує шифрування даних та передачу їх до банку для затвердження, а також пропонує додатковий захист від шахрайства. Постачальник послуг продавця пакує повідомлення з даними транзакції та доставляє його емітенту за допомогою запиту автентифікації. Постачальник послуг емітента визначає ризик транзакції та може запропонувати власнику картки для підтвердження своєї особи за допомогою, наприклад, одноразового пароля. Якщо на балансі є достатньо коштів для здійснення покупки, емітент надсилає підтвердження назад через платіжний шлюз. Потім продавець отримує це підтвердження та завершує транзакцію. Процес проведення онлайн-оплати детально зображений на рисунку 1.2.

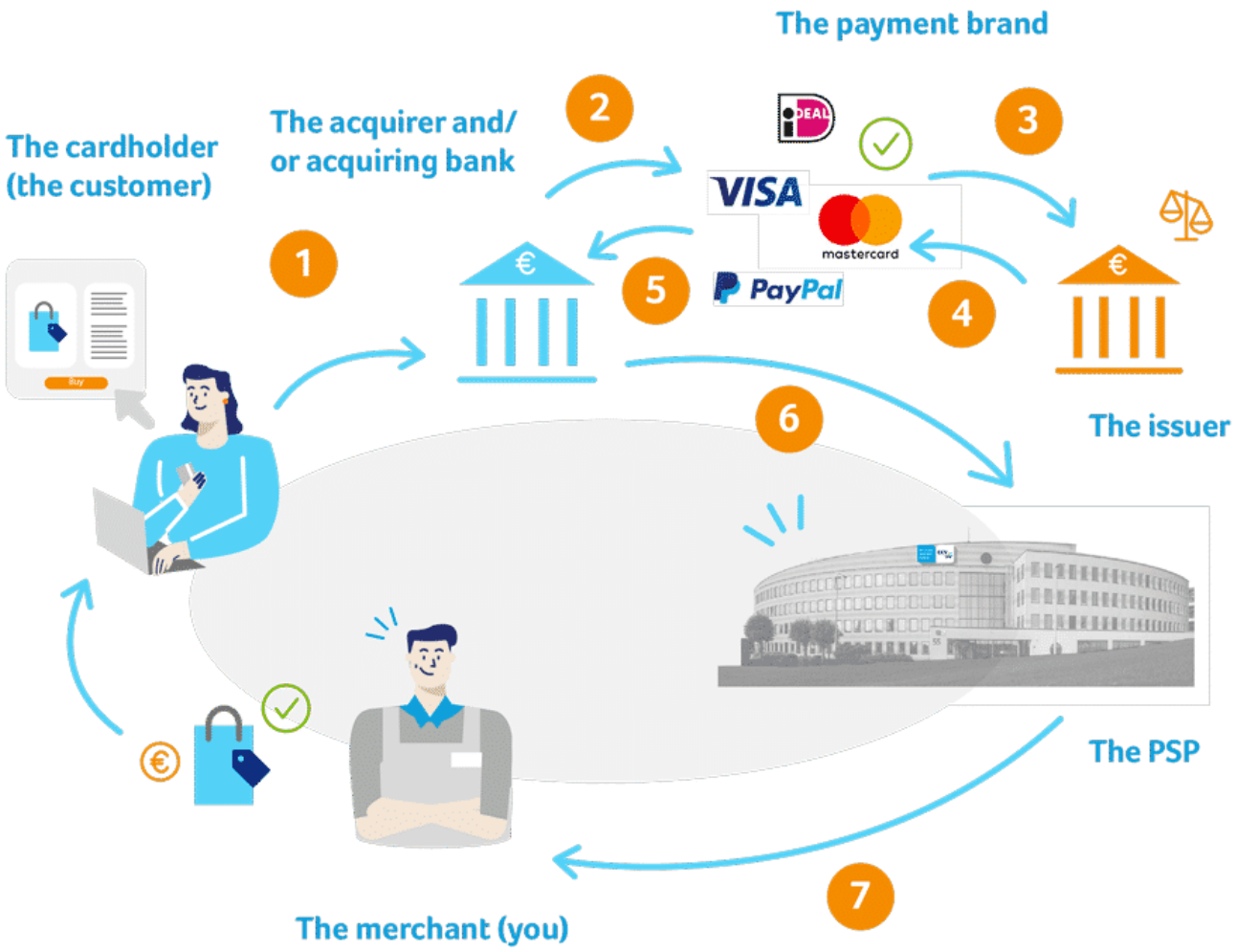

Рисунок 1.2 – Процес проведення онлайн-оплати

Один з найвідоміших прикладів платіжного шлюзу - це PayPal. Коли користувач виконує покупку на веб-сайті та вибирає PayPal як спосіб оплати, дані про транзакцію передаються через PayPal, який виступає як посередник між продавцем і банком користувача. Це забезпечує безпеку транзакції і зменшує ймовірність шахрайства або крадіжки даних.

Якщо не використовувати платіжний шлюз, клієнту доведеться перейти з веб-сайту продавця на веб-сайт банка емітента для здійснення платежу. Це збільшує час на проведення транзакції, що негативно впливає на конверсію і загалом може погіршити бізнес-показники.

1.2 Нормативно-правове регулювання надання електронних банківських послуг

Розвиток інформаційних технологій у банківському секторі призводить до виникнення різноманітних ризиків як для банків, так і для їхніх клієнтів під час здійснення банківських операцій. Відповідно до п. 7 ч. 1 ст. 7 Закону України "Про Національний банк України" від 20.05.1999 № 679-XIV на Національний банк України (далі - НБУ) покладається відповідальність за виявлення та мінімізацію негативного впливу таких ризиків і забезпечення безпеки банківських операцій. Тому НБУ визначає напрями розвитку сучасних електронних банківських технологій, створює та забезпечує безперервне, надійне та ефективне функціонування, розвиток створених ним платіжних та облікових систем, контролює створення платіжних інструментів, систем автоматизації банківської діяльності та засобів захисту банківської інформації. Крім того, стаття 5 Закону України "Про основні засади забезпечення кібербезпеки України" № 2163-VIII від 05.10.2017 відносить НБУ до суб'єктів, які безпосередньо здійснюють заходи з кібербезпеки в межах своєї компетенції. [8]

З метою виконання цих функцій Правління НБУ постановою від 14.04.2023 № 49 затвердило Положення про використання засобів криптографічного захисту інформації Національного банку України. Зокрема, цим Положенням передбачено, що засіб криптографічного захисту інформації Національного банку (далі - засіб КЗІ) - програмний, апаратно-програмний або апаратний засіб, призначений для криптографічного захисту інформації, розробником якого є Національний банк або розроблений на замовлення Національного банку [9].

Окрім того, відповідно до п. 15 зазначеного Положення однією з умов для отримання в користування засобів КЗІ та АРМ-ІНФ є приєднання організації-замовника до ЄДБО для отримання послуг Національного банку, як: розрахунково-касове та інформаційне обслуговування в системі електронних платежів НБУ (для учасників СЕП); система електронної пошти НБУ (далі - "СЕП"); надання в користування засобів захисту інформації НБУ. Водночас для організацій-клієнтів, які

є державними установами (Державна казначейська служба України, Державна служба фінансового моніторингу України, Державна фіскальна служба України, Національне антикорупційне бюро України, Державна установа "Управління з адміністрування проектів міжнародного фінансового співробітництва", Державна іпотечна установа, Фонд гарантування вкладів фізичних осіб, Центральна виборча комісія), такою умовою є укладення договору про використання засобів криптографічного захисту інформації Національного банку між організацією-клієнтом та Національним банком та підключення до СЕП НБУ [10].

Варто зазначити, що інформаційна безпека банку забезпечується, зокрема, засобами технологічного контролю, вбудованими в програмно-технічні комплекси СЕП, а також внутрішнім контролем за функціонуванням системи безпеки розрахунків.

Варто зазначити, що в Національному банку функціонує окремий структурний підрозділ - Департамент безпеки, однією з основних функцій якого є розроблення та реалізація стратегії та політики інформаційної безпеки Національного банку, а також впровадження новітніх технологій для забезпечення ефективного та цілеспрямованого захисту інформації в інформаційній інфраструктурі Національного банку та банківської системи України. Так, Департамент безпеки НБУ відповідно до Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України та Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України затверджених постановою Правління НБУ «Про затвердження нормативно-правових актів з питань інформаційної безпеки» від 26.11.2015 р. № 829, здійснює перевірку дотримання вимог, сертифікацію ВК та надсилає засобами системи електронної пошти Національного банку на адресу організації відповідні сертифікати ВК [9].

Іншим важливим нормативним актом, прийнятим для забезпечення ефективного захисту від кібератак на банківські установи, є Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене Постановою Правління НБУ № 95 від 28.09.2017. Відповідно

до цього Положення банківська установа зобов'язана створити власну систему управління інформаційною безпекою та створити підрозділ інформаційної безпеки у складі не менше двох працівників з числа штатних працівників банку, а також призначити особу, відповідальну за інформаційну безпеку банку, яка має здійснювати стратегічне керівництво з питань інформаційної безпеки банку та контроль за реалізацією заходів з інформаційної безпеки в банку [9].

З огляду на вищезазначене, можна зробити висновок, що правове підґрунтя для системи кіберзахисту банківської системи в Україні створено. На мою думку, пріоритетними напрямами забезпечення кібербезпеки банківської системи України є: моніторинг кіберпростору з метою своєчасного виявлення, запобігання та нейтралізації кіберзагроз; забезпечення захисту банків від кібератак; захист інформаційних ресурсів банку з урахуванням практики країн-членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб сектору безпеки та оборони; розвиток міжнародного співробітництва у сфері кібербезпеки [9].

Статтею 47 Закону України «Про банки і банківську діяльність» визначено перелік банківських послуг, які здійснюються банками для надання фінансових послуг юридичним та фізичним особам. Ці послуги включають залучення вкладів, відкриття та ведення рахунків, розміщення коштів від свого імені, переказ коштів тощо.

Цивільний кодексу України допускає наступні види безготівкових розрахунків: платіжні доручення; акредитиви; чеки; розрахунки по інкасо; інші форми, передбачені законом, встановленими відповідно до нього банківськими правилами й уживаних в банківській практиці звичаях ділових розрахунків.

Платіжна операція, ініційована з використанням платіжного інструменту з метою зарахування коштів на рахунок отримувача, є безготівковим розрахунком для одержувача та платника [3].

Безготівкові розрахунки здійснюються через банки, інші фінансові установи, в яких відкрито відповідні рахунки, якщо інше не випливає із закону та не обумовлено видом безготівкових розрахунків.

Електронні банківські послуги є однією з форм банківських послуг, які надаються банками за допомогою систем "клієнт - банк", "клієнт - Інтернет - банк", "телефонний банкінг", "платіжний застосунок" та інших систем дистанційного обслуговування. Ці послуги дозволяють клієнтам здійснювати різноманітні банківські операції та управляти своїми фінансовими ресурсами в зручний та безпечний спосіб, не відходячи від комп'ютера або мобільного пристрою.

Для виконання різних операцій з рахунком клієнта, як-от оплата комунальних послуг чи телефонних розмов, за допомогою телефонного банкінгу (дистанційне обслуговування клієнтів через телефонні комунікації), клієнт надає банку необхідну інформацію в рамках договору про надання банківських послуг або договору банківського рахунку. В деяких випадках, відповідно до умов договору, клієнт може подавати документи на паперових носіях для обробки банком.

Згідно зі статтею 66 Закону України «Про платіжні послуги», для забезпечення безпеки банківських операцій, банки зобов'язані розробляти та виконувати внутрішні правила, які спрямовані на ефективне зниження та контроль за оперативними ризиками, кіберризиками та ризиками безпеки, пов'язаними з наданням платіжних послуг. Під кіберризиком мається на увазі ризик виникнення внаслідок реалізації кіберзагроз збитків та/або додаткових втрат банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг [4].

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України", термін "кіберзагроза" визначається як поточні та можливі фактори і ситуації, які становлять ризик для життєво важливих національних інтересів України в кіберпросторі та негативно впливають на стан кібербезпеки країни, а також захист її кібернетичних об'єктів [8].

З іншого боку, кіберінцидент описується як подія або послідовність небажаних подій, що можуть бути ненавмисними (природні, технічні, технологічні, помилкові, включаючи ті, що викликані людським фактором) або такими, які мають ознаки можливого (потенційного) кібернападу. Такі події становлять загрозу для безпеки систем електронних комунікацій та систем управління технологічними процесами, можуть призвести до порушення нормального функціонування таких систем

(включаючи переривання та/або блокування системи, або несанкціоноване керування її ресурсами), а також загрожують безпекі (захисту) електронних інформаційних ресурсів [8].

Правила мають включати процедури, які гарантують безпеку платіжних операцій, ідентифікацію помилкових та неправомірних платіжних операцій, а також заходи для запобігання чи припинення таких операцій. Крім того, вони мають включати заходи реагування на інциденти безпеки, моніторинг та ведення реєстру оперативних інцидентів, кіберінцидентів та інцидентів безпеки.

Також важливо відзначити, що технології в сфері платіжних послуг продовжують розвиватися. Дедалі більше банків і фінансових установ впроваджують нові методи аутентифікації клієнтів, такі як біометричні дані та двофакторну аутентифікацію, щоб забезпечити безпеку та ефективність транзакцій.

Враховуючи розвиток технологій та зростання кіберзлочинності, банки також активізували свої зусилля щодо освіти клієнтів у сфері цифрової грамотності та безпеки. Це включає інформування клієнтів про потенційні онлайн-загрози, надання рекомендацій щодо безпечного використання фінансових послуг, а також навчання клієнтів основам захисту власних персональних та фінансових даних.

Важливо зазначити, що відповідальність за безпеку фінансових операцій не лежить лише на банку, але й на клієнті. Банк може надати всі необхідні засоби захисту та інструменти, але клієнт повинен також бути уважним та обережним при використанні цифрових банківських послуг.

Сучасний світ пропонує нам багато переваг та можливостей завдяки цифровим технологіям, але він також приносить нові виклики та ризики. Щоб забезпечити максимальну безпеку платежів та інших фінансових операцій, необхідно постійно розширювати свої знання та навички в області кібербезпеки. Захист персональних та фінансових даних — це не лише обов'язок фінансових установ, але й особиста відповідальність кожного клієнта.

Національний банк сприяє переходу економіки України до безготівкових розрахунків та активно підтримує розвиток платіжної інфраструктури. Збільшення

обсягу безготівкових розрахунків сприяє більшій прозорості платежів та стимулює економічний розвиток країни.

1.3 Переваги використання електронних банківських послуг

Безготівкові розрахунки є фінансовими операціями, які здійснюються без використання готівки. Вони передбачають переказ коштів між рахунками клієнтів без використання готівки. Замість цього, оплата здійснюється за допомогою різних електронних засобів передачі грошей, таких як банківські перекази, платіжні картки, мобільні платежі та інші електронні платіжні системи.

Популярність безготівкових розрахунків зростає з кожним роком, і це пов'язано з кількома факторами. Одним з них є широке використання електронних пристроїв, таких як комп'ютери, смартфони та планшети, які дозволяють зручно та швидко здійснювати безготівкові платежі. Крім того, безпека безготівкових транзакцій стала значно вищою завдяки застосуванню шифрування, біометричних технологій та двофакторної аутентифікації.

Переваги безготівкових транзакцій очевидні. Вони забезпечують зручність і ефективність для користувачів, оскільки не потребують постійного носіння готівки або чеків. Завдяки електронній оплаті можна також автоматизувати деякі рутинні справи. Це, скажімо, поповнення мобільного телефону, або регулярна оплата за навчання. Всього одна хвилина вашого часу для налаштування регулярного платежу і ви більше ніколи не зіштовхнетесь з проблемою відсутності інтернету через невчасну оплату рахунку.

Також вони зменшують ймовірність втрати або крадіжки грошей, оскільки всі операції зареєстровано і може бути відстежено. Безготівкові розрахунки сприяють прозорості та зменшенню обороту нелегальних грошей, а також сприяють розвитку економіки шляхом полегшення обігу грошей та збільшення доступності фінансових послуг.

В багатьох країнах зараз практично неможливо зробити велику покупку, скажімо купити автомобіль чи будинок, за готівку. Це пов’язано з тим, що виникне

дуже багато запитань, звідки ці гроші, чи можуть вони бути підроблені та чому людина не хоче використати безпечний і відстежуваний електронний платіж.Крім того, електронні перекази унеможливлюють випадкове чи навмисне недоврахування коштів, під час здійснення оплати.

Зростання популярності безготівкових транзакцій в світі призводить до швидкого розвитку електронних платіжних систем, розширення мережі платіжних терміналів та використання таких систем у різних галузях, включаючи торгівлю, туризм, онлайн-покупки та багато інших.

Безготівкові транзакції роблять дистанційну торгівлю значно зручнішою і забезпечують можливість чіткого контролю за переказом коштів. Використання цифрових форм платежів також може стати основою для розширення фінансових послуг, що особливо важливо у країнах з менш розвиненою фінансовою системою.

Технологічний прогрес радикально змінює світ банківського обслуговування, впроваджуючи нові засоби та інструменти, які спрощують та оптимізують процеси для клієнтів. Це означає, що ми стаємо свідками постійного зростання використання мобільних додатків для банкінгу, безконтактних платежів, біометричної аутентифікації та чат-ботів.

Мобільні додатки відкривають користувачам нові можливості, що надають більшу свободу в управлінні своїми фінансами. Безконтактні платежі надають зручність та швидкість, що вже стали нормою в сучасному світі. Біометрична аутентифікація забезпечує додатковий рівень безпеки, що є важливим в епоху кіберзлочинності. Тим часом чат-боти автоматизують процес обслуговування клієнтів, що дозволяє банкам ефективніше задовольняти потреби своїх клієнтів.

Ці чотири технології вже грають важливу роль в електронному банкінгу і, як очікується, будуть продовжувати впливати на тенденції банківського обслуговування в майбутньому.

Однією з найпопулярніших технологій в електронному банкінгу є мобільні додатки. На початку 2023 року в світі було більше 3 мільярдів смартфонів, і більшість їх власників використовують мобільні додатки для банкінгу. Ці додатки зазвичай пропонують широкий спектр функцій, включаючи перевірку балансу, перекази

коштів, оплату рахунків, мобільну чекову книжку, а також інноваційні функції, такі як функція розбиття рахунків, автоматичне заощадження, інвестиційні сервіси та багато іншого.

За даними eMarketer, в 2022 році 73,9% користувачів смартфонів в США скористалися мобільними платежами, і цей показник продовжує зростати. Безконтактні платежі використовують технологію NFC, що дозволяє користувачам робити покупки, просто притуливши свій смартфон до POS-терміналу.

Деякі банки використовують чат-боти для обслуговування своїх клієнтів. За даними Gartner, до 2022 року 70% клієнтських взаємодій буде автоматизовано. Чат-боти можуть допомогти клієнтам з поширеними питаннями, що забезпечує клієнтам швидкі відповіді і зменшує навантаження на відділ обслуговування клієнтів.

За даними The Economist використання готівки в транзакціях стрімко зменшується і в середньому скоротилося на 25 відсотків на основних світових ринках з 2011 по 2021 рік. Найбільш відчутне зменшення використання готівки спостерігається в країнах з економікою що розвивається. На рисунку 1.3 відображено зміни які відбулися в безготівкових розрахунках від 2011 до 2021 року.

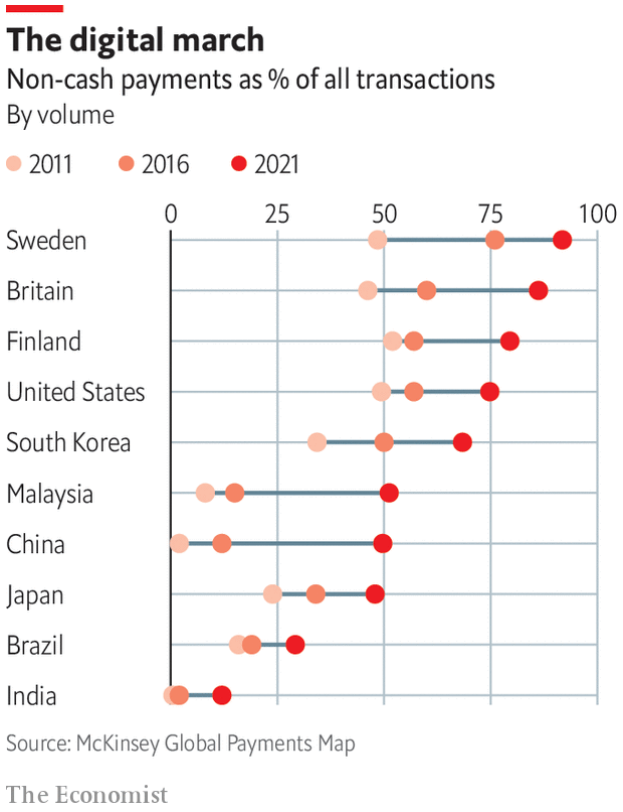

Рисунок 1.3 – Збільшення кількості безготівкових розрахунків у світі

Для забезпечення безпеки багато банківських додатків використовують біометричні дані для аутентифікації користувачів. За даними Juniper Research, кількість мобільних платежів, що використовують біометрію, зросте до 2,5 мільярдів в 2023 році, у порівнянні з 429 мільйонами в 2018 році.

1.3.1 Статистика використання безготівкових розрахунків в Україні

У 2021 році було здійснено 7, 817 млрд транзакцій із використанням платіжних карток, на суму 5 091,7 млрд грн. Для порівняння у 2017 році в Україні було проведено понад 3 мільярди операцій із використанням платіжних карток, котрі було емітовано українськими банками, на суму 2 125 мільярди гривень. Тобто за чотири роки ці показники зросли більше ніж вдвічі [12].

За даними від Національного Банку України від 12 груд. 2022 в Україні упродовж ІІІ кварталу 2022 року з використанням платіжних карток здійснено майже 2 млрд безготівкових операцій на суму близько 1 180 млрд грн. Це більше на 4% за кількістю та на 57% за сумою порівняно з ІІІ кварталом 2021 року [12].

Згідно інформації від компанії Українського Процесингового Центру, котрий обслуговує платіжн картки для 36 українських банків, у першому кварталі 2023 року було зафіксовано зниження загальної кількості транзакцій на 2% в порівнянні з однаковим періодом 2022 року, при цьому грошові обсяги транзакцій в той же час зросли на 6,5%.

Платежі в POS-терміналах продовжують залишатися лідерами серед безготівкових платежів, із середньою сумою чеку, яка зросла на 20% до 564 грн за рік. Загальний обсяг покупок лишився майже незмінним (+2%), але витрати на них зросли на 22,2%.

Операції з виведення готівки в банкоматах знизилися на 36,9%. Громадяни України стали рідше використовувати банкомати для виведення готівки - протягом місяця ця операція відбувалася лише раз, але при цьому суми зняття зросли на 59%.

Зростання платежів в інтернеті становило 1,3%, із збільшенням їх загального обсягу на 12,3%. Середня сума чеку склала 1 681 грн, що на 11,0% більше, ніж в попередньому році.

Сервіс p2p-переказів показав найбільший прогрес у першому кварталі 2023 року, оскільки кількість таких переказів зросла на 24,6%, а грошові обсяги цих переказів збільшилися на 16,4%. Середня сума операції становила 2 275 грн.

Варто зауважити, що значне зростання переказів може бути результатом активної підтримкою благодійних фондів, армії.

На рисунку 1.4 показано аналітичні дані по операціях з використанням платіжних карток в Україні та за кордоном за даними НБУ за травень-грудень 2022 року. Там також є відсоткове співвідношення, яке показує зростання безготівкових операцій за сумою та кількістю в Україні.

Рисунок 1.4 – Аналітичні дані по операціях з використанням платіжних карток

З графіків можна зробити висновок, що в Україні частка безготівкових операцій за сумою збільшується щорічно орієнтовно на 5%, а використання платіжної картки для отримання готівки відповідно знижується. Якщо казати про кількість безготівкових операцій, цей показник також щорічно стрімко зростає, і станом на травень-грудень 2022 безготівкові операції складають 92,8% від всіх операцій з платіжною карткою. Відповідно для зняття готівки платіжну картку використовують лише в 7,2% випадків.

Висновки за розділом 1

У першому розділі було проведено аналіз нормативно-правової бази, що стосується безготівкових розрахунків. Було визначено що українське законодавство передбачає різні види безготівкових розрахунків, які проводяться через банки та інші фінансові установи. Електронні банківські послуги надають зручний та безпечний спосіб здійснення банківських операцій через електронні канали зв'язку.

Дослідження ризиків безпеки електронного банкінгу та шляхів їх уникнення показало, що з урахуванням зростаючих кіберризиків та ризиків безпеки, банки зобов'язані розробляти та дотримуватися внутрішніх правил, спрямованих на забезпечення безпеки операцій та захисту від кіберзагроз. Це включає процедури ідентифікації, запобігання та реагування на неналежні платіжні операції, а також моніторинг та облік операційних інцидентів.

На основі викладеного матеріалу, варто зробити висновки про важливість формування законодавчої бази для вдосконалення кіберзахисту банківської системи України. Першочерговими напрямами для поліпшення кібербезпеки банківської системи України є: моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації та забезпечення захищеності банків від кібератак.

РОЗДІЛ 2
СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ ЕЛЕКТРОННИХ БАНКІВСЬКИХ ПОСЛУГ

2.1 Ризики використання електронних банківських послуг

Разом із зростанням безготівкових операцій, важливо покращувати безпеку банківських послуг. Забезпечення безпеки фінансових транзакцій є пріоритетним завданням для банків та фінансових установ. Для цього вони впроваджують різноманітні заходи та технології.

Одним з головних напрямків покращення безпеки є використання сучасних технологій шифрування та захисту даних. Банки встановлюють надійні системи шифрування, які захищають особисту і фінансову інформацію клієнтів від несанкціонованого доступу.

Також важливим аспектом безпеки є багаторівнева аутентифікація. Банки впроваджують системи, що вимагають не лише введення пароля, але й додаткових факторів перевірки, таких як відбиток пальця, сканування обличчя або використання одноразових кодів.

Для мінімізації ризиків шахрайства та шахрайських дій, банки постійно вдосконалюють системи виявлення та попередження фінансових злочинів. Вони аналізують поведінкові шаблони клієнтів, виявляють незвичайні або підозрілі транзакції, що допомагає запобігти шахрайським діям.

Помітним трендом є також використання біометричних технологій для аутентифікації клієнтів. Відбитки пальців, розпізнавання обличчя або сканування раковини ока можуть використовуватись для підтвердження особи клієнта та запобігання несанкціонованому доступу до його фінансових ресурсів.

Крім того, банки активно співпрацюють з регуляторними органами та міжнародними організаціями для обміну інформацією про нові методи шахрайства та

способи їх запобігання. Це дозволяє вчасно впроваджувати необхідні заходи та покращувати системи безпеки.

Загалом, покращення безпеки банківських послуг - постійний процес, що вимагає впровадження сучасних технологій, надійних систем шифрування та аутентифікації, а також активної співпраці зі спеціалістами та регуляторами. Це необхідно для забезпечення надійності та довіри клієнтів до безготівкових банківських операцій.

Більшість витоків банківських даних є результатом внутрішніх помилок співробітників. Відповідно до цього дослідження, проведеного Ponemon Institute, 54% витоків даних викликані недбалістю співробітників. Одним із прикладів є тепер сумно відомий злом Equifax у 2017 році, під час якого було розкрито особисту інформацію майже 146 мільйонів американців. Причиною цьому стало те, що один працівник технологічного відділу компанії не встановив рекомендоване оновлення програмного забезпечення.

Для уникнення подібних ситуацій необхідно підвищувати рівень знань, розуміння і усвідомлення людьми щодо кібербезпеки, кіберзагроз та безпечного користування цифровими технологіями. Це включає у себе знання про потенційні кіберризики, методи захисту від кібератак, свідоме використання паролів, розпізнавання підозрілих електронних листів та небезпечних посиланнь.

Ще одним з дуже вагомих ризиків є застаріле системне програмне забезпечення. Опитування 35 000 компаній у 2017 році показало, що майже 25% із них використовують застарілі браузери. Ці компанії мали вдвічі більше шансів зіткнутися з витоком даних. Тому необхідно вчасно оновлювати систему. Існують навіть програми для моніторингу вашої системи на наявність оновлень.

Одним з основних принципів управління операційними ризиками та ризиками інформаційної безпеки є підхід, що ґрунтується на переконанні, що краще попередити негативні наслідки, ніж потім вирішувати їх.

У вимогах, викладених у Положенні про порядок емісії та еквайрингу платіжних інструментів, відзначено, що пріоритетним підходом є передбачення можливих ризиків та прийняття заходів для їх запобігання. Ключовим принципом

управління операційними ризиками та ризиками інформаційної безпеки є націленість на попередження подій, а не вирішення їх наслідків. Таким чином, відповідальність емітента/еквайра полягає в постійному моніторингу платіжних операцій, що здійснюються з використанням платіжних інструментів [3].

Це дозволяє вчасно виявляти та ідентифікувати помилкові та неналежні платіжні операції, а також суб'єктів, які здійснюють такі операції. Крім того, емітент/еквайр зобов'язані приймати необхідні заходи для запобігання або припинення виникнення таких операцій. Такий підхід дозволяє ефективно знизити ризики та забезпечити безпеку платіжних операцій, що здійснюються з використанням платіжних інструментів, у відповідності до внутрішніх правил та вимог законодавства України.

Ще одним вагомим ризиком є збереження даних банківських карток неналежним чином. Зберігати цю інформацію необхідно відповідно до стандартів PCI DSS.

2.2 Вимоги сандарту PCI DSS щодо захисту електронних банківських послуг

Стандарт безпеки даних індустрії платіжних карток (PCI DSS) — це стандарт безпеки, розроблений для захисту транзакцій із платіжними картками, яким керує Рада стандартів безпеки PCI (PCI SSC). Заснована в 2006 році п’ятьма найбільшими постачальниками кредитних карток: MasterCard, Visa, Discover, Amex і JCB International. Рада гарантує, що постачальники послуг і продавці захищають інформацію про кредитну картку своїх клієнтів під час транзакцій і під час її зберігання [20].

Закон не вимагає відповідності PCI. Проте вкрай бажано, щоб продавці, які приймають платежі картками, дотримувалися правил, встановлених PCI SSC, щоб уникнути будь-якого потенційного порушення прав на дані та великих штрафів за недотримання вимог. Це стосується як торгових точок (магазинів, ресторанів та інших підприємств), які приймають платежі з використанням платіжних карток, так і

організацій, які здійснюють операції з платіжними картками в інший спосіб (наприклад, онлайн-торгівля або телефонні платежі). Вимоги для досягнення PCI-сумісності залежать від того, як працює ваша компанія.

Основна мета стандарту PCI DSS полягає в забезпеченні безпеки мережевої інфраструктури і захисту даних власників платіжних карток, оскільки саме ці дані є найбільш вразливими і загрожують конфіденційності та втраті коштів. Вимоги стандарту PCI DSS ставляться перед торговими підприємствами та постачальниками послуг, що обробляють платежі від покупців через платіжні системи, такими, як VISA і MasterCard, з метою забезпечення безпеки збереження коштів клієнтів.

Стандарт PCI DSS також регламентує правила експлуатації платіжних систем і встановлює процедури їх розробки і моніторингу. Це допомагає забезпечити виконання вимог безпеки та зменшити ризик порушення безпекових заходів у платіжних системах. Враховуючи швидкий розвиток технологій та постійні загрози кібербезпеці, дотримання стандарту PCI DSS є важливою складовою для забезпечення довіри клієнтів та збереження надійності платіжних систем.

Його мета полягає в захисті конфіденційної інформації про платіжні картки та забезпеченні безпеки платіжних транзакцій.

Існують різні рівні відповідності стандарту PCI, які залежать від кількості платежів, що здійснюються у ваших бізнес-процесах щороку (за 12 місяців). Існує один компонент, який залишається необхідним у всіх випадках, а саме: бізнес повинен дійсно досягти 100% відповідності стандарту PCI та підтримувати його, щоб забезпечити безпеку даних своїх клієнтів. Вимоги стандарту PCI DSS стосуються торгових підприємств, банків, постачальників різноманітних послуг і сервісів, роздрібних магазинів, call-центрів, платіжних шлюзів та інших підприємств і організацій, діяльність яких тісно пов’язана з обробкою, передачею і зберіганням даних власників платіжних карток [20].

Тобто якщо інформація про власника картки зберігається в компанії, вони зазвичай не матимуть доступу до повного номера картки. Це тому, що інформація зашифрована та зберігається безпечно третьою стороною. Коли працівник переглядає файл власника картки, він має бачити лише останні 4 символи номера картки. Це

захищає від хакерів, а також від незадоволених співробітників, які можуть викрасти цю інформацію.

Стандарт PCI включає 6 основних напрямків, які поділяються на 12 вимог, що описані нижче: [21]

Побудова та підтримка безпечної мережі та системи.

1) Встановіть і підтримуйте конфігурацію брандмауера для захисту даних держателів карток.

2) Не використовуйте надані постачальником значення за замовчуванням для системних паролів та інших параметрів безпеки.

Захист даних держателів карток.

3) Захищайте збережені дані про власника карток.

4) Шифруйте передачу даних держателів карток через відкриті загальнодоступні мережі.

Підтримка програми керування вразливостями.

5) Захищайте всі системи від шкідливого програмного забезпечення та регулярно оновлюйте антивірусне програмне забезпечення або програми.

6) Розробляйте та підтримуйте безпечні системи та додатки.

Впровадження суворих заходів контролю доступу.

7) Обмежуйте доступ до даних держателів карток лише за службовою необхідністю.

8) Ідентифікуйте та аутентифікуйте доступ до компонентів системи.

9) Обмежте фізичний доступ до даних власника картки.

Регулярний контроль та тестування мережі.

10) Відстежуйте та контролюйте весь доступ до мережевих ресурсів та даних про держателів карток.

11) Регулярно тестуйте системи та процеси безпеки.

Підтримка політики інформаційної безпеки.

12) Підтримуйте політику, яка стосується інформаційної безпеки для всього персоналу.

У деяких випадках повний процес аудиту PCI DSS не потрібен, натомість виконується анкета для самооцінки (SAQ). Існує кілька типів SAQ, залежно від того, який рівень підходить для вашого бізнесу.

Компанії повинні заповнити відповідну анкету самооцінки PCI DSS (SAQ) і надати докази того, що компанія виконала та пройшла перевірку вразливостей за допомогою PCI SSC Approved Scanning Vendor (ASV).

Відповідність PCI поширюється на будь-яку організацію чи продавця (включно з міжнародними продавцями/організаціями), які зберігають, обробляють або передають дані власників карток. Стандарт PCI-DSS зазвичай охоплює певні типи підприємств: електронну комерцію, служби онлайн-платежів, банки, супермаркети, туристичні агентства та платіжні системи.

Найбільшим ризиком для компаній через недотримання PCI-DSS буде недовіра з боку їхніх клієнтів і партнерів через те, що вони не приділяють уваги безпеці.

2.3 Найбільш поширені кібератаки на банківську систему

Кібератаки нині стали важливою проблемою для всіх галузей економіки, але деякі індустрії стають особливо заманливими цілями для кіберзлочинців через обсяги конфіденційної інформації, яку вони обробляють, та потенційні прибутки, що можуть бути отримані. Фінансовий сектор є переважаючим у цьому контексті. Він має величезну кількість цінної та конфіденційної інформації, що робить його привабливим для кіберзлочинців, і надає великий спектр можливостей для незаконного отримання прибутку.

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

Переважна більшість випадків шахрайства в системах інтернет-банкінгу припадає на шахрайство з застосуванням шкідливого програмного забезпечення, соціальної інженерії та фішингових атак [27].

2.3.1 Фішинг

Фішинг – це тип атаки соціальної інженерії, який часто використовується для викрадення даних користувачів, зокрема облікових даних і номерів кредитних карток.

Під час атаки зловмисник, видаючи себе за надійну особу, переконує відкрити електронний лист або текстове повідомлення. Потім одержувача обманом змушують натиснути зловмисне посилання. Взаємодія з будь-яким із заражених посилань або вкладень у фішингових електронних листах може ініціювати встановлення зловмисного програмного забезпечення на цільовій комп'ютерній системі або завантажити підроблену веб-сторінку, яка збирає облікові дані для входу.

Повідомлення зазвичай включає посилання на підроблений веб-сайт, який імітує автентичність реального джерела. На цьому сайті користувач розпізнає знайомий інтерфейс і без зайвих підозр вводить свої облікові дані. Зловмисник таким чином отримує доступ до персональних даних і використовує їх для незаконних дій.

Хоча фішингові атаки не вимагають високих технічних навичок, вони є дуже ефективними для шахрайських схем. Статистика останніх років показує тривожну динаміку: кількість та різноманітність фішингових атак зростає з року в рік, а їх жертвами стають як корпорації, так і окремі користувачі. Згідно з Trend Micro, провідною компанією у сфері кібербезпеки, у 2019 році було виявлено 11,3 мільйона спроб фішингових атак [35].

Особливо поширені стали фішингові електронні листи з темами, що стосуються "зміни пароля", "підтвердження облікового запису", "оновлення умов підписки" або "встановлення оновлення для MacOS".

Для одержувача, який нічого не підозрює, ці шахрайські електронні листи здаються дуже переконливими, особливо коли вони подаються з відчуттям терміновості. На рисунку 2.1 наведено приклад фішингового електронного листа. У листі стверджується, що термін дії пароля користувача закінчується. Надано інструкції перейти на myuniversity.edu/renewal, щоб оновити свій пароль протягом 24 годин.

Зазвичай, шахраї надсилають електронні повідомлення з адреси, що виглядає подібно до довіреної адреси компанії чи організації. Наприклад, замість адреси електронної пошти "@google.com" можуть використовувати "@gogel.com" або "@goo.gle.com". Або замість адреси "@company.com" можуть використовувати "@campany.com".

При отриманні підозрілого електронного повідомлення, важливо бути обережним і не відкривати посилання або надавати особисті дані, якщо ви не маєте повної впевненості щодо його походження. Рекомендується завжди перевіряти адресу відправника, добре аналізувати контент повідомлення і уникати надавання конфіденційної інформації через ненадійні канали зв'язку.

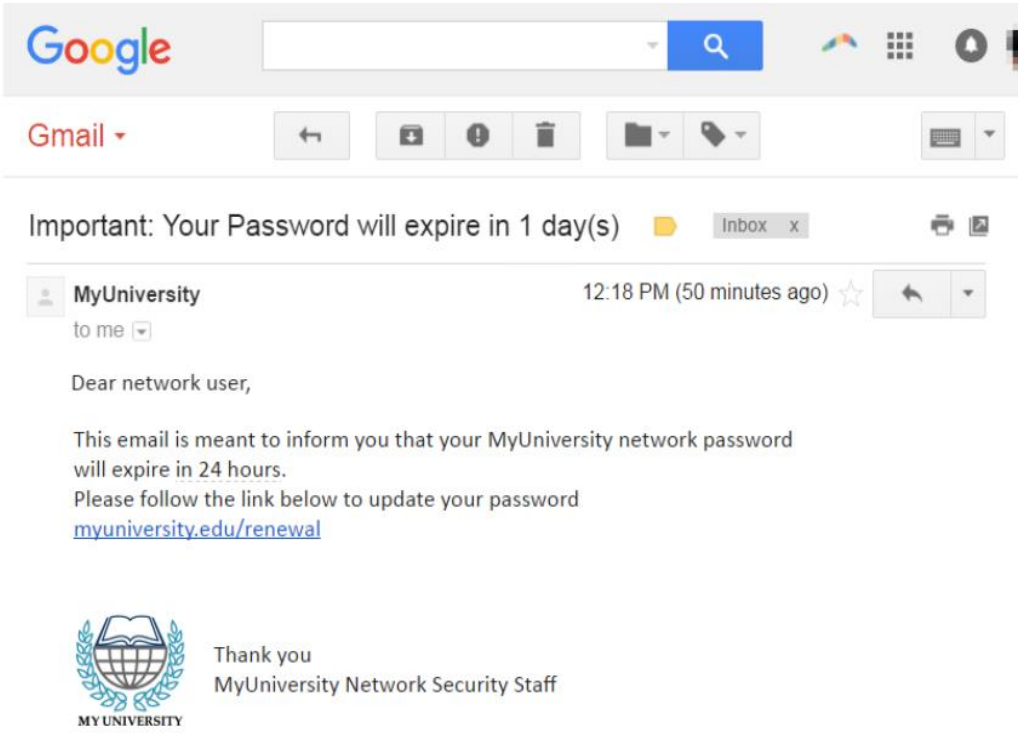

Рисунок 2.1 – Приклад фішингового листа

Фінансовий сектор був найбільш об’єктом фішингових атак у першому кварталі 2021 року. Робоча група з боротьби з фішингом (APWG) виявила, що фішингові атаки були найбільш поширеними серед фінансових установ у першому кварталі 2021 року, статистику зображено на рисунку 2.2. А саме, майже 50% зафіксованих фішингових атак були пов’язані зі сектором фінансових послуг.

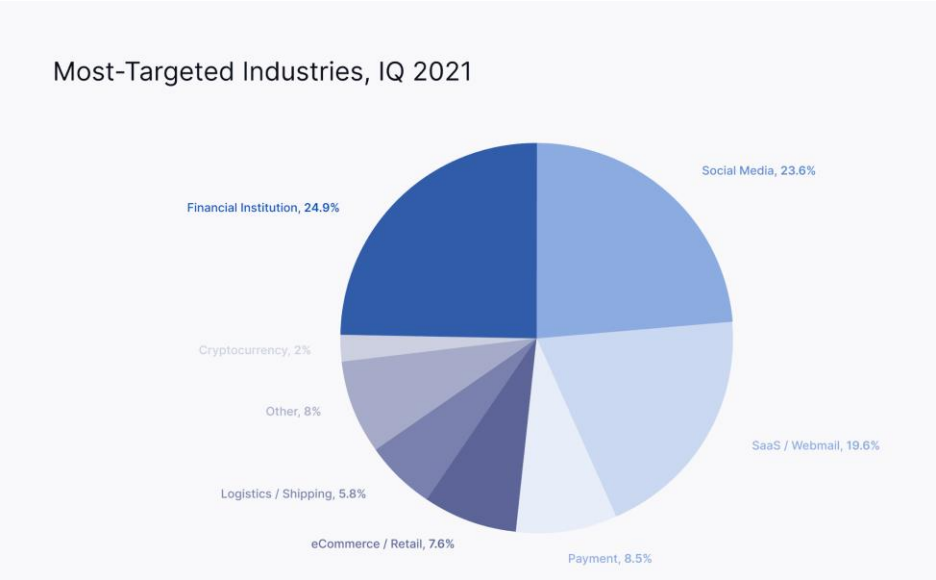

Рисунок 2.2 – Статистика фішингових атак за 2019 рік

2.3.2 DDoS-атаки

Згідно з даними Radware , за перші шість місяців 2022 року кількість DDoS-атак у всьому світі зросла на 203% порівняно з першим півріччям 2021 року. Журнал InfoSecurity повідомив про 2,9 мільйона DDoS-атак у першому кварталі 2021 року, що на 31% більше, ніж за той самий період 2020 року [25].

Атаки розподіленої відмови в обслуговуванні (DDoS) стали повсякденним явищем. Незалежно від того, чи це невелика некомерційна організація, чи величезний багатонаціональний конгломерат, онлайн-сервіси організації – електронна пошта, веб-сайти, будь-що, що має доступ до Інтернету – можуть бути сповільнені або повністю зупинені DDoS- атакою .

DDoS-атака – це атака на комп’ютерні системи органу, організації, установи з метою порушення доступності атакованих вебресурсів. Простими словами, під час атаки одночасно створюється така величезна кількість зовнішніх запитів (рахунок може йти на мільйони), що атакована система не в змозі їх обробити. Як наслідок – виникають збої в її роботі або вона взагалі перестає повноцінно працювати.

Зазвичай DDoS-атаки здійснюють із метою поширення паніки та дестабілізації. Іноді використовують для приховування деструктивних дій, тобто коли DDoS-атака слугує прикриттям атаки іншого виду. Проте самі DDoS-атаки загрози для

персональних даних громадян не становлять. Варто знати, що для проведення DDoS-атак хакери часто використовують зламані пристрої людей. Тому важливо дотримуватися основних правил кібергігієни, користуватися антивірусами, оновлювати вчасно програмне забезпечення тощо.

У листопаді 2021 року Microsoft пом'якшила DDoS-атаку, націлену на клієнта Azure, із пропускною спроможністю 3,45 Тбіт/с і швидкістю пакетів 340 мільйонів PPS, що вважається найбільшою зареєстрованою DDoS-атакою.

Атака на AWS у лютому 2020 року. Amazon Web Services– це сервіс хмарних обчислень, яка обслуговує понад 1 мільйон компаній, урядів і окремих осіб. AWS зазнав атаки в лютому 2020 року, тоді на його сервери надходило навантаження 2,3 терабіта в секунду (Tbps). Хакери зламали каталоги користувачів на серверах CLDAP (CLDAP), щоб наповнити сервери AWS величезними обсягами інформації. Останніми роками більшість DDoS-атак використовують цю саму техніку як спосіб зламати протоколи безпеки AWS. На щастя, Amazon вдалося пом'якшити атаку до того, як вона стала загрозою безпеці користувачів.

DDoS-атаки сьогодні є особливо поширеною формою кібератак на банки. Їх головна мета – зробити банківські веб-сайти чи служби нездатними обробляти зовнішні запити. З цією метою зловмисники організовують масові потоки неавторизованих запитів до ресурсу, обраного жертвою, роблячи його практично недоступним або серйозно знижуючи його продуктивність. Популярність DDoS-атак серед зловмисників полягає в їх доступності та досить високій ефективності.

Найбільший ризик DDoS для банківських клієнтів полягає в тому, що банківські послуги будуть недоступні під час атаки. Клієнти систем ДБО вже звикли в будь-який момент заходити в «особистий кабінет» або мобільний додаток банку і виконувати необхідні операції – платежі, перекази, кредити, відкриття та закриття депозитів тощо. А якщо зловмисники атакували послуги банку, то ці послуги, швидше за все, будуть недоступні для клієнтів, принаймні до завершення атаки. Це означає, що клієнти не зможуть легко і швидко поповнити свій рахунок по телефону в потрібний момент, допомогти грошима комусь із рідних чи друзів, оплатити квитанцію чи хоча б оцінити залишок коштів на рахунку.

Можливий також інший варіант, коли хакери організовують комплексну кібератаку на банк, у якій DDoS-атаки відіграють роль диверсійної тактики. Мета – зосередити зусилля фахівців банку з кібербезпеки на захисті від DDoS-атаки, а поки вони зайняті відновленням атакованих сервісів, спробувати зламати системи банку. Мета злому може бути найрізноманітнішою – від розміщення провокаційних повідомлень на сайтах банків до викрадення особистих даних клієнтів, знищення їхніх рахунків і порушення бізнес-логіки банківських систем.

У лютому 2022 року Україну вразила масштабна DDoS-атака, яка стала найбільшою в історії країни. Ця атака була спрямована на урядові сайти та банківський сектор і мала на меті дестабілізувати ситуацію в країні. Атака була ретельно спланована і здійснена заздалегідь.

Особливо постраждали банки, зокрема ПриватБанк, Ощадбанк, Monobank, НеоБанк, Альфа-Банк та А-Банк. Було зафіксовано значний обсяг одночасних запитів до мобільних банкінгових додатків та веб-сайтів банків. Зловмисники маскували свої запити під звичайних користувачів, використовуючи ботів з усього світу. Атака була в 200 разів потужнішою, ніж щоденне навантаження від користувачів.

За словами Андрія Гриценюка, директора з інформаційних технологій Альфа-Банку, ця атака полягала у великій кількості одночасних запитів до мобільного банкінгу та веб-сайтів банків. Зловмисники маскували свої боти так, щоб запити виглядали як запити звичайних користувачів. В той ж вечір система доменних імен (DNS) gov.ua, де розміщені веб-сайти органів державної влади, також стала жертвою атаки. Джерелами атаки були як зарубіжні, так і українські IP-адреси, а пропускна здатність становила понад 150 гігабіт на секунду.

2.3.3 Програми вимагачі

Програми-вимагачі – це тип зловмисного програмного, призначеного для заборони доступу до комп’ютерної системи або даних, з вимогою сплатити викуп. Програми-вимагачі поширюються через фішингові електронні листи, шкідливу

рекламу, відвідування заражених веб-сайтів або використання вразливостей. Після зараження програма-вимагач може зашифрувати деякі або всі файли.

Після початкового зараження програмою-вимагачем, у примітці про викуп власнику пояснюється, що його файли недоступні. Зазвичай всі файли шифруються і їх зміст стає незрозумілий, тож жертва повинна надіслати викуп, щоб купити ключ дешифрування для розшифрування своїх файлів.

Інші програми-вимагачі у своєму повідомленні стверджують, що правоохоронні органи заблокували комп'ютер через використання піратського програмного забезпечення чи порнографію. Потім висувається вимога сплатити штраф за розблокування комп'ютера.

Остання статистика програм-вимагачів чітко показує, що фішинг є основним способом доставки програм-вимагачів. Нещодавній звіт показав, що 75% з 1400 опитаних організацій зазнали атаки програм-вимагачів, що підкреслює його постійну поширеність у діловому світі.

У 2020 році спостерігався значний сплеск атак програм-вимагачів, і ця тенденція продовжує зростати в 2021 році.За перші 6 місяців 2021 року кількість атак зросла на 151%, статистика показана на рисунку 2.3.

У 2021 році по всьому світу було зареєстровано 623,3 мільйона атак програм-вимагачів. А в 2022 році кількість атак програм-вимагачів впала на 23% порівняно з попереднім роком.

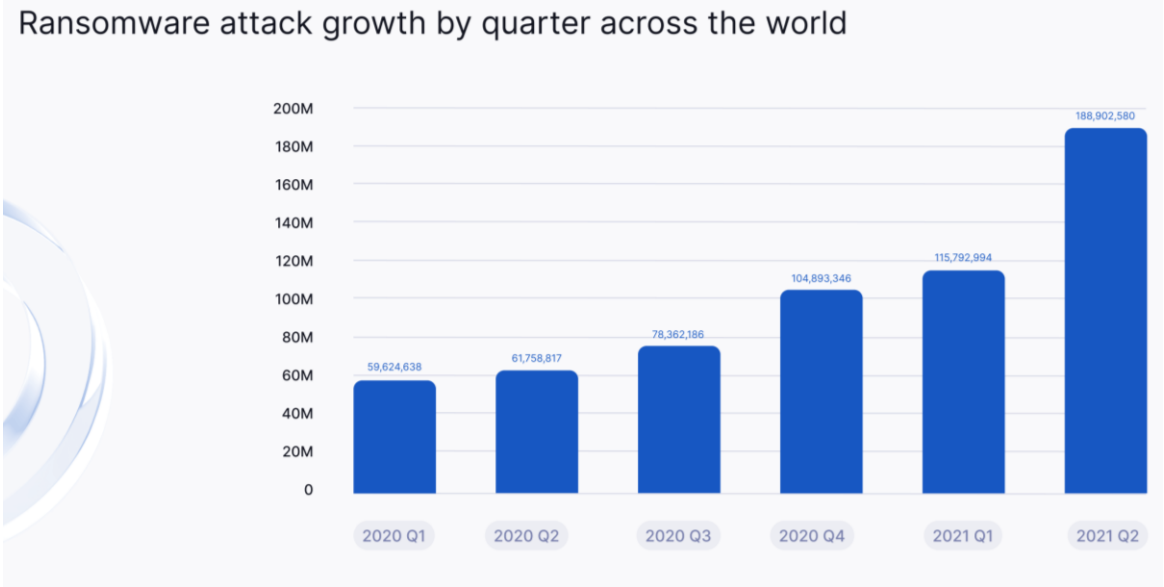

Рисунок 2.3 – Статистика атак програм-вимагачів

Однією з наймасштабніших можна вважати серію атак програм-вимагачів проти уряду Коста-Ріки у 2022 році. Це змусило уряд оголосити надзвичайний стан у країні, оскільки критично важливі системи були пошкоджені.

Кіберзлочинці здійснили дві атаки. Перша відбулася з середини квітня до травня, головними цілями були цифрова податкова служба та IT-системи, пов’язані з митним контролем. За оцінками, також постраждали 800 серверів і кілька терабайтів інформації в міністерстві фінансів.

Група програм-вимагачів Conti взяла на себе відповідальність за ці атаки, вимагаючи викуп у розмірі 10 мільйонів доларів.

Уряд Коста-Ріки відмовився платити викуп і намагався повернути системи та сервіси в Інтернет. Казначейство Коста-Ріки повідомило державним службовцям, що атака призупинила автоматичні платіжні послуги. Робітників попереджали, що уряд не може вчасно виплатити їм зарплату. Замість цього їм потрібно буде подати заявку на отримання зарплати електронною поштою або від руки на папері. Напад також вплинув на зовнішню торгівлю країни. Він порушив свою податкову та митну системи, що призвело до колапсу імпортної та експортної логістики. Збитки оцінюються десь між 38 і 125 мільйонами доларів США на день.

Друга атака була спрямована на Фонд соціального страхування Коста-Ріки, який займається охороною здоров'я країни. Більше половини серверів постраждали, що змусило лікарів перенести 7% зустрічей протягом першого тижня після атаки. У другій атаці звинуватили групу, яка використовує програму-вимагач HIVE.

Держдепартамент США запропонував винагороду в розмірі 10 мільйонів доларів за інформацію, яка допоможе знайти будь-кого, хто займає ключову керівну роль у банді Конті. США також запропонували 5 мільйонів доларів за «інформацію, яка призведе до арешту та/або засудження будь-якої особи в будь-якій країні, яка брала участь у інциденті з програмою-вимагачем Conti».

До інших відомих компаній які зазнали атак від програм вимагачів відносяться: Kia Motors, Acer, Cisco, Ferrari, SpiceJet, Nvidia.

Основні стратегії запобігання та пом’якшення наслідків:

– застосовувати багаторівневі заходи безпеки, такі як брандмауери, системи виявлення і запобігання вторгнень;

– постійно контролювати та оцінювати методи безпеки;

– регулярно встановлювати оновлення ПЗ та системи;

– використовуйте шифрування даних;

– впровадити програми підвищення обізнаності працівників щодо безпеки;

– створити детальний план реагування на інцидент;

– запровадити надійні процедури резервного копіювання та аварійного відновлення.

В Україні найбільш відома атака програми-вимагача сталась 27 червня 2017. Тоді потужний комп'ютерний вірус Petya паралізував роботу низки компаній у всьому світі [38].

Petya використовував вразливості в операційній системі Windows, відомі як EternalBlue та EternalRomance, щоб поширитися по мережі. Він зашифровував файли на зараженому комп'ютері, вимагаючи від користувачів викуп у розмірі 300 доларів в біткоінах. Однак в більшості випадків файли були пошкоджені без можливості відновлення, навіть якщо було сплачено викуп.

Україна була одною з найбільше постраждалих країн від атаки Petya. Банки, державні установи, енергетичні компанії та інші організації були серйозно уражені. В Україні було здійснено хакерську атаку з використанням програми для звітності та електронного документообігу M.E.doc. Було повідомлено про великі фінансові збитки та значні перерви в роботі.

На глобальному рівні NotPetya зашкодив багатьом великим компаніям, включаючи Maersk, FedEx і Merck. Загальні втрати від атаки NotPetya оцінюються в мільярди доларів.

Для запобігання цієї атаки антивірусні експерти з Symantec, відомої американської компанії, радять симулювати інфекцію комп'ютерів вірусом Petya для його запобігання. В їхніх вказівках, що були оприлюднені 28 червня, вони зазначають, що під час атаки, вірус Petya перевіряє наявність файлу C:\Windows\perfc

в системі. Якщо цей файл вже існує, вірус припиняє свою активність і не інфікує систему. Спеціалісти Symantec радять користувачам самостійно створити цей файл за допомогою стандартної програми "Блокнот" з розширенням .dll (або без будь-якого розширення) і захистити його від змін [37].

2.4 Технології захисту електронних банківських послуг

Незважаючи на те, що форми електронних платежів можуть бути різними (оплата за допомогою банківської картки, системи інтернет-банкінгу, платіжного терміналу, SMS тощо), з точки зору законодавства США, все це є однією і тією ж операцією - переказом коштів. Послуги з переказу коштів надає оператор - банк, власник платіжних терміналів тощо. Оператор, у свою чергу, користується послугами однієї з систем онлайн-платежів - Visa, MasterCard, PayPal тощо.

Різні форми цифрових платежів мають свої нюанси. При використанні банківської картки платник переказує кошти зі свого банківського рахунку. Картка є "ключем" для доступу до банківського рахунку і може бути використана для оплати двома способами: за допомогою спеціального терміналу (в банкоматі або касі магазину) і за допомогою веб-сайту. При оплаті через термінал особу платника підтверджує він сам, а також картка (точніше, інформація, записана на її магнітній смузі або чіпі) і ПІН-код, який не знає ніхто, крім платника. При оплаті через сайт підтвердженням платежу є інформація, нанесена на картку (номер картки, ім'я власника, термін дії та CVC/CVV код підтвердження), яку платник повинен ввести у відповідні поля веб-форми. При цьому CVC/CVV код є паролем, який не повинен знати ніхто, крім платника.

У системах дистанційного банківського обслуговування (ДБО) клієнту доступні різні форми платежів:

– разові платежі;

– шаблонні платежі (клієнт один раз заповнює шаблонну форму, вказуючи реквізити отримувача, в подальшому необхідно вказувати лише суму платежу);

– автоматичні платежі (шаблонні платежі, які автоматично здійснюються з певною періодичністю - наприклад, щомісяця).

Розвиток схем, якими користуються шахраї, у свою чергу сприяє покращенню систем безпеки фінансових установ. Великі банки використовують передові платформи для боротьби з шахрайством з використанням алгоритмів на основі штучного інтелекту.

Двофакторна автентифікація — це метод ідентифікації користувача в службі (зазвичай в Інтернеті) шляхом запиту двох різних типів даних автентифікації, що забезпечує дворівневий і, отже, більш ефективний захист облікового запису від неавторизованого входу. На практиці зазвичай це виглядає так: перша межа - це логін і пароль, а друга - спеціальний код, який приходить через SMS або електронну пошту. Це один із найпопулярніших способів забезпечення безпеки онлайн-платежів.

Токенізація - це тип шифрування. В онлайн-транзакціях він використовується для захисту даних банківської картки. Наприклад, якщо ви хочете оплатити вибраний інтернет-магазин або оплатити комунальні послуги, введіть номер картки, термін дії та CVV у спеціальному полі. На цьому етапі ви повідомляєте інформацію про карту сторонньому ресурсу, який може її зберігати. Але технологія токенізації підвищує безпеку платежів в Інтернет-середовищі. Вона захищає дані користувачів під час онлайн-транзакцій, будь то оплата карткою чи смартфоном.

SSL (Secure Sockets Layer) — стандартна технологія безпеки для встановлення зашифрованого з’єднання між веб-сервером і клієнтом (веб-браузером). SSL використовується для захисту онлайн-транзакцій і гарантує, що конфіденційна інформація (наприклад, дані кредитної картки, облікові дані користувача та особисті дані) шифрується та безпечно передається. Щоб захистити свій ресурс за допомогою SSL, ви повинні отримати сертифікат SSL від ЦС (центру сертифікації) і встановити його на своєму сервері. Веб-сайт із захистом SSL починається з HTTPS, а не HTTP. На початку це може здатися незручним, але це розумно, якщо ви справді прагнете забезпечити безпеку онлайн-платежів.

Методи цифрової перевірки особи, такі як біометрична перевірка, розпізнавання обличчя та цифрова перевірка ідентифікатора, можуть допомогти компаніям, урядам і фінансовим установам підтвердити особу людини в Інтернеті.

Систему особистої перевірки можна використовувати, коли особа та її документ, що посвідчує особу, фізично відсутні. Цифрове підтвердження особи є ключовим кроком у відкритті рахунку та залученні клієнта. Після перевірки особи заявника фінансові установи можуть провести перевірку, щоб переконатися, що заявник не є шахраєм, злочинцем, зловмисником або намагається вчинити шахрайство.

2.4.1 Етапи розвитку технологій захисту електронних банківських послуг

Розвиток технологій захисту електронних банківських послуг є важливою темою в сучасному світі фінансів і кібербезпеки. З появою електронних платежів 1990-х роках було важливо захистити передачу даних. Шифрування стало ключовою технологією для забезпечення конфіденційності та цілісності банківських транзакцій.

Про електронні платежі в Україні вперше почули в 1993 році, саме 5 січня 1993 року вперше запустили систему електронних платежів СЕП та провели перші міжбанківські операції через систему електронних платежів. В Україні на початку 1994 року були повністю скасовані паперові і телеграфні авізо, що були офіційними письмовими повідомленнями між контрагентами про розрахункові операції та зміни у взаєморозрахунках. Замість цього, з появою системи електронних платежів (СЕП), банки почали обробляти значну кількість платежів щодня. За оцінками банків, СЕП обробляє середньо 1,6 мільйонів платежів на суму близько 200 мільярдів гривень за день. Однак, потенціал цієї системи перевищує поточні обсяги в декілька разів.

У 1996 році в Україні відбулися значні події у галузі банківських послуг, такі як випуск перших банківських карток та встановлення банкоматів та PoS-терміналів. Вісім вітчизняних банків стали першими учасниками міжнародної платіжної системи Visa Europay. Зараз платіжні картки випускають близько 70 банків, а на руках у

населення знаходиться понад 40 мільйонів активних карток. Існує близько 19 тисяч банкоматів та 400 тисяч торгових PoS-терміналів, на яких можна здійснити платежі.

У 2001 році була запущена перша онлайн-система інтернет-банкінгу. В даний час всі універсальні банки пропонують багатофункціональні системи віддаленого банкінгу, і загальна кількість користувачів онлайн-банкінгу становить приблизно 20 мільйонів клієнтів. Більшість клієнтів використовують мобільні банківські додатки для керування своїми коштами.

Перше впровадження безпеки платіжних карток шляхом застосування чипу відбулося у 2003 році. Було запроваджено стандарт безпеки для платіжних карток та платіжних терміналів EMV. Основна мета стандарту EMV полягає в заміні традиційних магнітно-смужкових карток на "розумні" чіпові картки. Ці картки містять вбудований мікропроцесор, що забезпечує безпеку та автентифікацію під час здійснення платежів. Стандарт EMV був розроблений з метою зменшення шахрайства та підвищення безпеки платіжних транзакцій. Він став широко використовуваним по всьому світу і є стандартом безпеки для багатьох платіжних систем та країн. На початок червня, за даними Національного банку України, майже 18 мільйонів активних платіжних карток були оснащені мікрочіпами. Це становить половину від загальної кількості функціонуючих карток.

У 2005 році була запущена Національна система масових електронних платежів (НСМЕП). Відмінною особливістю цієї системи було те, що всі картки в ній були чіповими. Незважаючи на просунуту технологію, НСМЕП не стала значним конкурентом для міжнародних платіжних систем (МПС), і навіть спроба перезапуску системи в 2015 році під новим брендом "Простір" не принесла бажаних результатів.

У 2007 році в Україні з'явилися вуличні платіжні термінали. Ці термінали були установлені як банками, так і небанківськими установами. Наприкінці першої чверті 2021 року в Україні було застосовано приблизно 50 тисяч програмно-технічних комплексів самообслуговування (ПТКС), через які було здійснено платежі на суму майже 140 мільярдів гривень [13].

У 2008 році було введено перший банківський мобільний додаток в Україні. Ця версія додатку була розроблена для платформи iOS.

У 2010 році був представлений перший мобільний додаток для платформи Android. Згідно з оцінками, до весни 2021 року приблизно 70% користувачів уже використовують мобільні додатки, що суттєво перевершує за популярністю веб-версію [13].

2010 рік, НБУ легалізував електронні гроші. Постановою №481 від 4 листопада 2010 року, затверджена Національним банком, встановлено "Положення про електронні гроші в Україні". У той же місяць було видано відповідні ліцензії двом банківським системам електронних грошей, затвердивши їх правила функціонування. Незаконні системи електронних грошей наявні в Україні протягом щонайменше семи років до цього часу. Згідно з інформацією, наданою Національним банком України, в 2020 році банками-емітентами було підвищено обсяги операцій з використанням електронних грошей до 19,3 мільйонів гривень, а обсяги електронних гаманців зросли до 79 мільйонів штук.

У 2011 році MasterCard було здійснено першу в країнах СНД та Україні NFC-транзакцію. NFC (Near Field Communication) - це бездротова технологія зв'язку короткого діапазону, яка даєможливість обміну даними між пристроями, що знаходяться в безпосередній близькості (зазвичай до 4 сантиметрів). Вона базується на радіочастотній ідентифікації (RFID) і дозволяє безконтактно передавати інформацію між двома пристроями, які підтримують цю технологію. Завдяки NFC можна здійснювати різні типи безконтактних операцій, включаючи безконтактні платежі, обмін контактами, передачу файлів, запуск додатків та інше. Зазвичай NFC використовується в мобільних пристроях, таких як смартфони, для зручного та швидкого обміну даними з іншими пристроями або зчитування інформації з безконтактних карток. На сьогоднішній день в Україні випущено майже 15 мільйонів безконтактних платіжних карток. Згідно з даними Українського процесингового центру (UPC), у другому кварталі 2021 року безконтактна оплата становила 64,4% від загальної кількості покупок [13].

2014 рік, запроваджено безконтактні платежі за допомогою телефонів годинників та інших гаджетів з чипом NFC. На сьогодні в Україні кількість гаджетів, які замінили платіжні картки, перевищує 4,5 мільйона. Відповідно до даних

Національного банку України, у першому кварталі поточного року гаджети використовувалися для здійснення близько 25% всіх платежів через PoS-термінали.

У Київському метрополітені на початку 2015 року впроваджено систему безконтактних платежів [13].

2017 рік в Україні було створено перший банк, котрий функціонує виключно в онлайн-режимі. Зараз український банківський сектор поповнився сімома віртуальними банками, які працюють виключно в онлайн-середовищі. Ці цифрові банки, зокрема Monobank, Sport Bank, todo bank, Neobank, O.Bank, IZi та Власний Рахунок, доступні переважно через мобільні додатки, без наявності браузерних версій або фізичних відділень. Вони створюють конкуренцію провідним банками України.

Цікавим фактом є, що в Києві в 2017 році відбулася історична подія - перша у світі продаж квартири за криптовалюту. Ця трансатлантична угода відбулася з використанням блокчейна Ethereum та смарт-контракту, розрахунок було здійснене криптовалютою Ethereum. Загальна сума угоди становила приблизно 60 000 доларів або 212,5 ETH. Цей подія підтверджує росту популярності криптовалют та їх використання в різних галузях, включаючи нерухомість.

Шифрування стало ключовою технологією для забезпечення конфіденційності та цілісності банківських транзакцій. Захист від несанкціонованого доступу до банківських рахунків зазнав поліпшень з впровадженням двофакторної аутентифікації. Додатковий рівень захисту був досягнутий через комбінацію факторів, таких як пароль, одноразовий код, відбиток пальця тощо. У новітніх технологіях захисту використовуються біометричні дані, такі як сканування відбитка пальця, розпізнавання обличчя або сканування сітківки ока. Це дозволяє підвищити рівень безпеки та унікальності ідентифікації користувача. Сучасні технології захисту базуються на аналізі великих обсягів даних та використанні алгоритмів машинного навчання для виявлення підозрілих активностей та атак. Це дозволяє банкам реагувати на загрози в реальному часі та запобігати шахрайству.

2.5 Протоколи безпеки онлайн-транзакцій кредитних і дебетових карток

Протоколи безпеки для онлайн-транзакцій кредитних і дебетових карток відіграють важливу роль у забезпеченні безпеки платіжних операцій у цифровому середовищі. Ці протоколи розроблені з метою захисту конфіденційної інформації користувачів та запобігання несанкціонованому доступу до їх фінансових ресурсів.

Одним з найпоширеніших протоколів безпеки є 3D Secure. Цей протокол забезпечує додатковий рівень аутентифікації під час онлайн-транзакцій, вимагаючи введення додаткового пароля або одноразового коду, який відправляється на мобільний пристрій користувача. Це дозволяє перевірити, що особа, яка здійснює платіж, є власником картки. Принцип роботи показано на рисунку 2.4

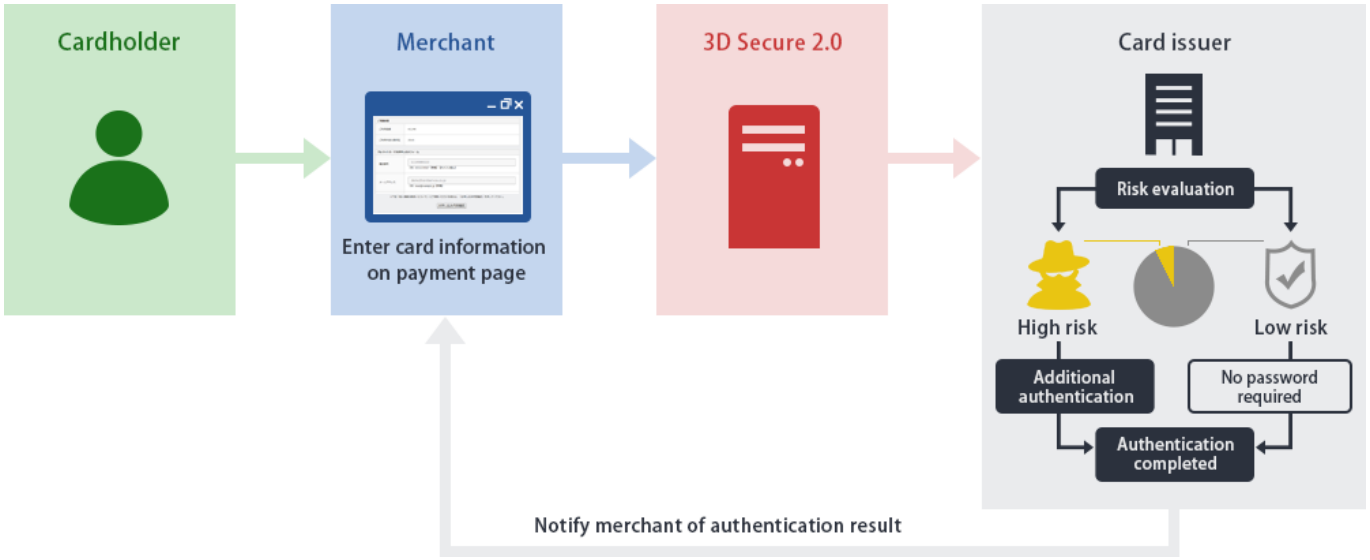

Рисунок 2.4 – Принцип роботи 3D Secure 2

3D Secure був створений компанією Arcot Systems (тепер CA Technologies) і вперше використаний компанією Visa для забезпечення покращення безпеки Інтернет-платежів [19].

3DS забезпечує обмін даними або повідомленнями між продавцем і емітентом для автентифікації споживача та схвалення транзакції. Дані містять інформацію про транзакцію, спосіб оплати та пристрій. Використовуючи ці дані, емітенти можуть швидко й точно виявляти та запобігати шахрайським транзакціям із картками, не

додаючи непотрібних труднощів у процес оплати, що часто призводить до відмови від покупок.

3D Secure використовує обмін повідомленнями XML і зв'язок SSL для захисту та автентифікації транзакцій.

Назва 3D походить від моделі трьох доменів, які використовуються для забезпечення додаткового рівня безпечної автентифікації між процесом фінансової авторизації та процесом онлайн-автентифікації.

Домен покупця: банк і продавець, які отримують оплату транзакції.

Домен емітента: банк, який випустив кредитну або дебетову картку, використану для транзакції.

Домен сумісності: інфраструктура, надана для картки, яка використовується для підтримки протоколу 3D Secure.

Протокол безпеки 3D Secure пропонує високий рівень захищеності для онлайн-транзакцій з картками, забезпечуючи автентифікацію власника карти та запобігаючи несанкціонованому використанню.

Застосування цих технологій у 3D Secure забезпечує впевненість клієнтів та банків у безпеці їхніх платежів та знижує ризик шахрайства.

У жовтні 2016 року EMVCo опублікувала специфікацію для 3-D Secure 2.0. Вона розроблена так, щоб бути менш нав'язливою, ніж перша версія, дозволяючи надсилати більше контекстних даних емітенту картки клієнта (включаючи поштові адреси та історію транзакцій) для перевірки та оцінки ризику транзакції. Клієнт повинен буде пройти перевірку автентифікації, тільки якщо буде визначено, що його транзакція несе високий ризик. Крім того, процес автентифікації тепер розроблений таким чином, що він більше не потребує переспрямування на окрему сторінку, а також можна використати автентифікацію через мобільний додаток банку [20].

Крім 3D Secure, існують інші протоколи безпеки, такі як Tokenization (токенізація) і Encryption (шифрування). Токенізація замінює справжні дані картки на унікальний токен, що використовується під час транзакцій, що дозволяє зберігати фінансові дані в зашифрованому вигляді. Шифрування захищає передачу даних між

користувачем, продавцем та платіжною системою, забезпечуючи їх конфіденційність та цілісність.

EMV (Europay, Mastercard, Visa): Це міжнародний стандарт безпеки, що використовується для забезпечення безпечних платежів з використанням чіп-карток. Він базується на шифруванні даних та аутентифікації мікросхеми, що міститься на картці.

Tokenization: Цей протокол використовує технологію заміни конфіденційної інформації, такої як номер картки, на унікальний ідентифікатор або токен. Таким чином, справжні дані не використовуються під час транзакції, що забезпечує вищий рівень безпеки.

SSL/TLS (Secure Sockets Layer/Transport Layer Security): Ці протоколи використовуються для шифрування даних, які передаються між веб-сайтом та клієнтом. Вони гарантують конфіденційність та цілісність інформації під час переказу.

SecureCode та Verified by Visa: Ці протоколи є аналогами 3D Secure і використовуються для підтвердження та автентифікації користувачів під час онлайн-платежів з використанням кредитних і дебетових карток.

Забезпечення високого рівня безпеки в онлайн-транзакціях з кредитними і дебетовими картками є пріоритетним завданням для фінансових установ, платіжних систем та користувачів. Це обумовлено постійно зростаючими загрозами в сфері кібербезпеки.

Висновки за розділом 2

У цьому розділі було проаналізовано найбільш поширені ризики, пов'язані з використанням електронних банківських послуг, такі як зловмисне програмне забезпечення, незахищені громадські точки доступу Wi-Fi, вразливості додатків та ідентифікаторів.

Також було визначено найбільш поширені кібератаки на банківську систему. До них відносяться фішинг, DDoS-атаки та програми вимагачі. Згідно зі статистикою,

майже 50% усіх зафіксованих фішингових атак були пов'язані зі сектором фінансових послуг. А за даними IBM та Ponemon Institute, середня вартість витоку даних у фінансовому секторі у 2021 році становила 5,72 мільйона доларів. Це підкреслює високий ризик для банківських систем і необхідність прийняття ефективних заходів безпеки для захисту від цих атак.

Крім того, було проведено дослідження протоколу безпеки для онлайн-транзакцій платіжних карток 3D Secure, який забезпечує додатковий рівень аутентифікації та дозволяє переконатися, що особа, яка здійснює платіж, є власником картки.

У цьому розділі основна увага приділялась технологіям захисту електронних банківських послуг, тож у підсумку можна зауважити, що для забезпечення безпеки даних держателів карток і мережевих систем в банківській сфері необхідно встановлювати брандмауер, шифрувати передачу даних, обмежувати доступ та регулярно оновлювати програмне забезпечення. Також важливо аутентифікувати доступ, контролювати мережевий доступ та підтримувати політику інформаційної безпеки. Виконання цих заходів допомагає запобігти зловживанням та зберегти довіру клієнтів до банківських послуг.

РОЗДІЛ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ ВДОСКОНАЛЕННЯ ЗАХИСТУ ЕЛЕКТРОННИХ БАНКІВСЬКИХ ПОСЛУГ

3.1 Обґрунтування вибору біометричної автентифікації як інструменту безпеки

В умовах стрімкого розвитку цифрових технологій, кібербезпека в банківській сфері вимагає все більше уваги. Основним завданням банку є захист інформації та активів своїх клієнтів. У цьому контексті біометрична автентифікація виступає одним з найбільш ефективних інструментів.

Відповідно до Закону України «Про електронні довірчі послуги» від 5 жовтня 2017 року, автентифікація – електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних [14].

Автентифікація – це будь-який процес, за допомогою якого система перевіряє особу користувача, який бажає отримати доступ до системи. Оскільки контроль доступу зазвичай базується на ідентифікації користувача, який вимагає доступу до ресурсу.

Біометрія – сукупність автоматизованих методів і засобів аутентифікації людини, заснованих на її фізіологічній або поведінковій характеристиці [15].

Біометрична автентифікація дозволяє використовувати унікальні фізичні або поведінкові характеристики особи для підтвердження її особи. Це можуть бути відбитки пальців, риси обличчя, сканування сітківки ока, голосові особливості та інші. Порівняно з традиційними методами автентифікації, такими як паролі та PIN-коди, біометрична автентифікація забезпечує вищий рівень безпеки та зручності.

Переваги та недоліки використання біометричної ідентифікації наведено в таблиці 3.1

Таблиця 3.1 - Переваги та недоліки використання БІ

Переваги	*Недоліки*
гарантована безпека та достовірність	ризик витоку даних
позитивний користувацький досвід	біометричні пристрої можуть обмежувати конфіденційність користувачів
висока стійкість до фальсифікації	помилки та відмови

Головна перевага біометричної автентифікації полягає в тому, що вона практично неможлива для копіювання, викрадення або взлому. Крім того, вона є значно більш зручною для клієнтів, оскільки вони не мають запам'ятовувати складні паролі або носити з собою спеціальні пристрої для генерації одноразових паролів.

Попри всі переваги біометрії, є важливі виклики, які потребують розгляду при впровадженні біометричних систем. Потрібно розуміти й зважувати ці потенційні проблеми в процесі розробки та впровадження біометричних систем безпеки.

Більшість сучасних методів біометричної автентифікації використовують лише часткові дані для підтвердження особи користувача. Наприклад, при використанні мобільного біометричного пристрою, на етапі реєстрації проводиться сканування всього відбитка пальця, який потім перетворюється в числові дані. Проте при подальшій біометричній перевірці використовується лише частина цього відбитка, що пришвидшує процес.

При оцінці ефективності роботи будь-якої системи ідентифікації використовуються деякі параметри або характеристики, які характеризують роботу си-стеми з того чи іншого боку. Звичайно системи біометричної ідентифікації ма-ть наступні параметри:

1. Помилка першого виду FRR (False Reject Rate) – ймовірність того, щосистема ідентифікації не зможе ідентифікувати зареєстрованого користувача (або часто говорять, що система приймає «свого» за «чужого»).

2. Помилка другого роду FAR (False Accept Rate) – ймовірність того, щосистема ідентифікації ідентифікує не зареєстрованого користувача(тобто прийме «чужого» за «свого»).

3. Час спрацьовування – показує скільки проходить часу з моменту надання біометричного ідентифікатора і до моменту надання доступуабо відмови у доступі.

4. Тип зчитувача біометричного ідентифікатора – контактний або дистанційний.

5. Кількість біометричних ознак, які використовуються для ідентифікації.

6. Стійкість системи до муляжів (штучні копії біометричних ідентифікаторів).

7. Автономність – характеризує функціональну незалежність системи від апаратно-програмних засобів.

8. Можливість централізовано керувати значною кількістю територіально розподілених пристроїв ідентифікації.

Взагалі параметри FAR та FRR дуже тісно пов’язані один з одним, цілкомзрозуміло, що більш критичним параметром є FAR, бо відмова в доступі «своєму» не нанесе такої значної шкоди ніж надання доступу «чужому». Тому привпровадженні системи цілком зрозуміло, що значення FAR повинно бути якможна меншим, проте зменшення значення FAR призводить до різкого збіль-шення значення FRR, тобто система починає масово відмовляти у доступі зареєстрованим користувачам, що також не є хорошим показником роботи.

3.2 Порівняння біометричних інформаційних систем розпізнавання обличчя

Технологія розпізнавання обличчя зараз є одним з найбільш активно розвинених напрямків в біометрії. Зростаюча кількість камер в нашому житті, будь то аеропорти, вокзали або вулиці міст, стимулює інтенсивність розвитку цього сектору біометрії.

Всі ключові технології розпізнавання обличчя розробляються з метою здійснення пошуку в режимі "один до багатьох", що означає ідентифікацію певного обличчя серед тисяч інших, зафіксованих в базі даних.

Ця технологія викликає особливий інтерес через свою схожість з тим, як люди впізнають одне одного. Додатковою перевагою є безконтактність такого розпізнавання.

Розглядаючи технологію в цілому, процес ідентифікації особи відбувається в два етапи. На першому етапі визначається місцезнаходження особи на зображенні. Для цього початкове зображення сканується з допомогою вікна меншого розміру, і після кожного сканування робиться оцінка ступеня схожості зображення у вікні з обличчям потрібної особи. Цей етап є найбільш складним з точки зору обчислень, оскільки потребує повного сканування зображення для різних розмірів вікна та визначення рівня схожості між зображенням в вікні та певною особою після кожного сканування.

Наразі можна виділити такі методи розпізнавання обличчя [16]:

- методика аналізу «власне обличчя» або «eigenface»;
- методика аналізу відмінних рис;
- методика аналізу на основі нейромереж;
- методика аналізу автоматичної обробки зображення облич.

Метод Eigenface використовує 2D зображення у відтінках сірого, які відображають характерні особливості обличчя. Цей метод часто служить базою для інших методів розпізнавання. Коли обличчя особи вводиться в систему, воно представляється як набір коефіцієнтів. Під час спроби розпізнати особу, "живий" зразок порівнюється з шаблоном, що був раніше внесений в базу, і визначаються коефіцієнти відмінності. На основі ступеня відмінності визначається, чи є особи подібними чи ні. Цю технологію краще використовувати в добре освітлених приміщеннях та коли обличчя можна сканувати анфас.

Методика аналізу відмінних рис є найбільш поширеною. Вона досить схожа на "eigenface", але краще адаптована до змін обличчя людини (усмішка, гнів, смуток). У цій технології є визначений набір параметрів, що описують характеристики різних частин обличчя. У поєднанні ці параметри унікально ідентифікують особливості людського обличчя. Динамічність людського обличчя суттєво ускладнює процес ідентифікації. В результаті мімічних змін положення деяких частин обличчя

зміщується відносно шаблону, внесеного в систему, тому ця технологія вимагає великих ресурсів і коштовного, високоякісного обладнання.

Методика аналізу на основі нейромереж схожа на інші за своїм алгоритмом роботи - характеристики обличчя зі зразка порівнюються з шаблоном на збіги. Але завдяки нейронним мережам можна порівняти максимально можливу кількість параметрів. Перевагою є те, що після звичайної перевірки на розбіжності між зразком і шаблоном, запускається механізм, який використовує вагові коефіцієнти для визначення відповідності параметрів зразка і шаблону. Метод аналізу на основі нейронних мереж можна використовувати в умовах, що перешкоджають якісній ідентифікації.

Метод автоматичної обробки зображень обличчя досить простий. Він базується на використанні відстаней та відношень між точками на обличчі, такими як ніс, брови, губи. Цей метод не є таким ефективним, як інші, але він може бути використаний для ідентифікації зображень в погано освітлених приміщеннях. На рис. 3.1 можна побачити області, які використовуються для ідентифікації.

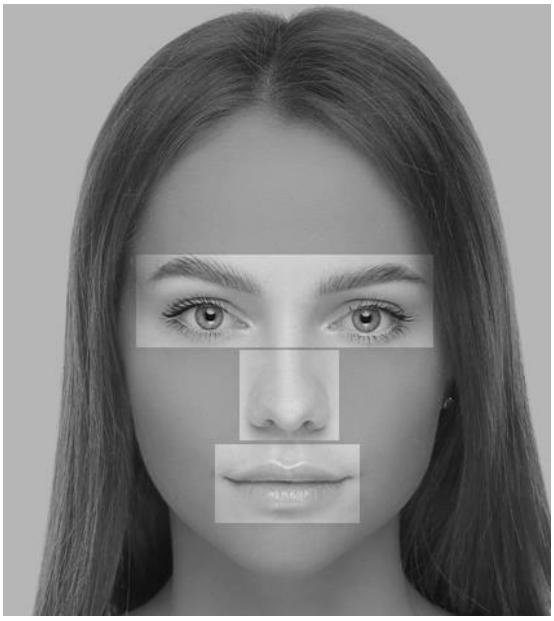

Рисунок 3.1 – Порівнювальні області

Технології розпізнавання обличчя стали широко розповсюдженими в різних сферах, починаючи від безпеки до споживчих сервісів. Хоча вони представляють собою потужний інструмент, вони мають свої переваги та недоліки.

До переваг технологій розпізнавання обличчя можна віднести:

– Вдосконалену точність та швидкість. Сучасні системи розпізнавання обличь використовують штучний інтелект та машинне навчання для поліпшення точності та швидкості розпізнавання.

– Пасивність та ненав'язливість. Системи розпізнавання обличь можуть працювати у фоновому режимі без активної участі людини, зменшуючи необхідність вмішування.

– Використання існуючих матеріалів. Системи можуть працювати з вже існуючими фото або відеозаписами, що зменшує необхідність фізичної присутності особи.

– Автоматизація. Вони здатні автоматизувати процеси, що раніше вимагали значних людських ресурсів, такі як моніторинг відеокамер безпеки.

– Широке соціальне прийняття. Багато людей вже звикли до використання технологій розпізнавання обличь, наприклад, для розблокування своїх смартфонів або для автоматичного тегування на фотографіях у соціальних мережах.

Недоліки технологій розпізнавання обличь включають:

– Питання приватності. Використання технологій розпізнавання обличчя може порушувати приватність осіб, особливо якщо їх використовують без відповідного дозволу або інформованості.

– Ризик зловживань та кримінальних дій:. Технологія може бути використана для злочинних цілей, таких як стеження, шахрайство або навіть кіберзлочини.

– Технологічна недосконаліть. Хоча технологія розпізнавання обличь вдосконалюється, ще залишаються проблеми, пов'язані з точністю, особливо в умовах поганого освітлення, різного кута зйомки або змінами в зовнішності людини.

– Можливість обходу системи. Технологія не є непомічною для обходу, особливо якщо зловмисник має доступ до високоякісних зображень особи, яку він намагається імітувати.

3.3 Обґрунтування використання біометричної аутентифікації з використанням системи розпізнавання обличчя для вдосконалення захисту електронних банківських послуг

Сьогодні більшість українських банків використовують для підтвердження онлайн платежу технологію 3D Secure. 3DS вимагає від покупця додаткового підтвердження того, що він є законним власником карти. Після введення даних картки, її власник перенаправляється на сторінку свого банку-емітента, де йому необхідно ввести додатковий пароль або SMS-код, щоб підтвердити транзакцію.

Однак у цьому процесі беруть участь обидві сторони: і банк-емітент, і банк-еквайер (банк продавця). Еквайер відправляє запит до емітента про здійснення перевірки 3D Secure, а емітент надає підтвердження після того, як від користувача отримано необхідну інформацію [23].

Незважаючи на додатковий рівень безпеки, який надає протокол 3D Secure, він має деякі недоліки:

Дискомфорт - додатковий етап аутентифікації може бути незручним для користувачів, що може призвести до втрати продажів через відмову від завершення процесу покупки і відповідно до зниження конверсії.

Несумісність - не всі карти підтримують 3D Secure, і не всі банки пропонують цю опцію для своїх клієнтів.

Труднощі в розумінні - не всі користувачі можуть зрозуміти, що від них вимагається, коли вони стикаються з 3D Secure, особливо якщо вони вперше роблять покупку в Інтернеті.

Технічні складнощі - іноді можуть виникати проблеми з підключенням до сервера 3D Secure, що призводить до відмови в операції.

Безпека - хоча 3D Secure і зменшує ризик шахрайства, він не є 100% надійним. Шахраї можуть використовувати тактику "phishing" для отримання доступу до особистих даних користувача.

На рисунку 3.2 зображено процес проходження автентифікації з використанням одноразового пароля.

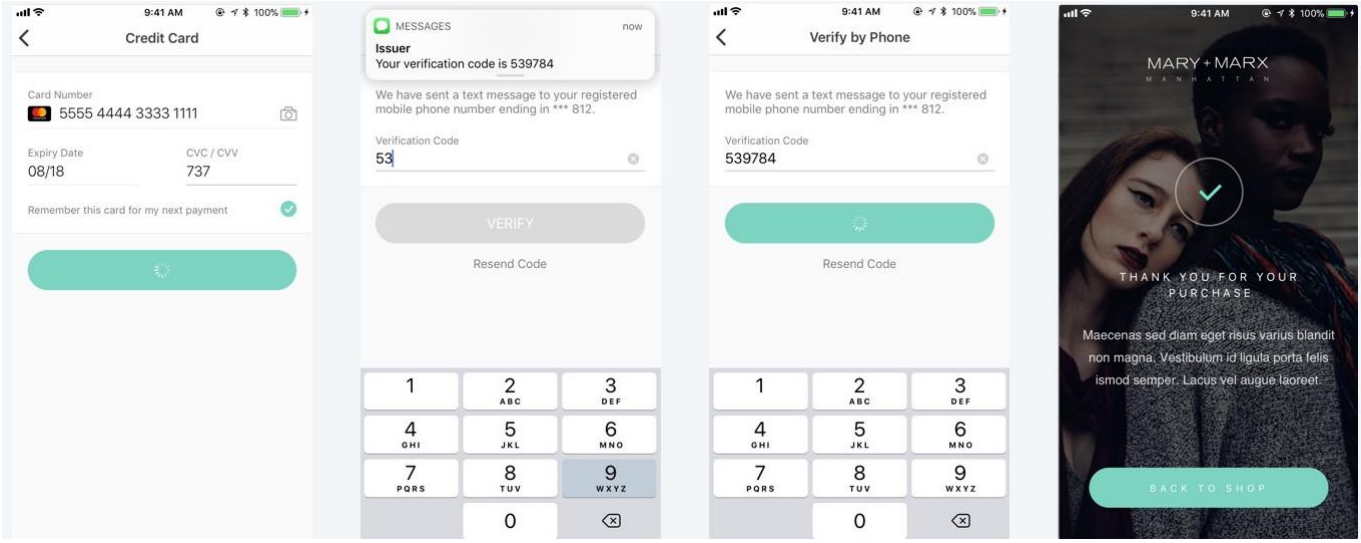

Рисунок 3.2 – Приклад аутентифікації одноразовим паролем

У відповідь на ці проблеми, була створена нова версія протоколу - 3D Secure 2, яка вирішує багато з цих недоліків, зокрема, підвищує зручність користувачів і знижує ризик відмови від покупки.

3D Secure 2 використовує додаткові дані покупця для більш глибокого аналізу. Це можуть бути історія попередніх покупок, тип пристрою, з якого вони працюють, місцезнаходження, поведінка користувача та інші подібні відомості. Це дозволяє краще виявляти підозрілу поведінку і зменшує кількість помилкових спрацьовувань.

Додаткова інформація, яка збирається в 3D Secure 2, також допомагає зменшити кількість випадків, коли покупцю потрібно вводити додатковий SMS-код для, щоб підтвердження транзакції. Це робить процес покупки швидшим і зручнішим. На рисунку 3.3 показано що не потрібно робити ніяких додаткових підтверджень для оплати. Технологія 3DS2 аналізує платіжну поведінку, щоб визначити, чи є якісь порушення чи аномалії в транзакції і якщо таких не виявлено, дозволяє проводити платіж без додаткових підтверджень.

Високий ризик вимагає додаткової перевірки клієнта, як правило це до 5% транзакцій, а низький ризик не потребує додаткової перевірки клієнта і становить 95% транзакцій.

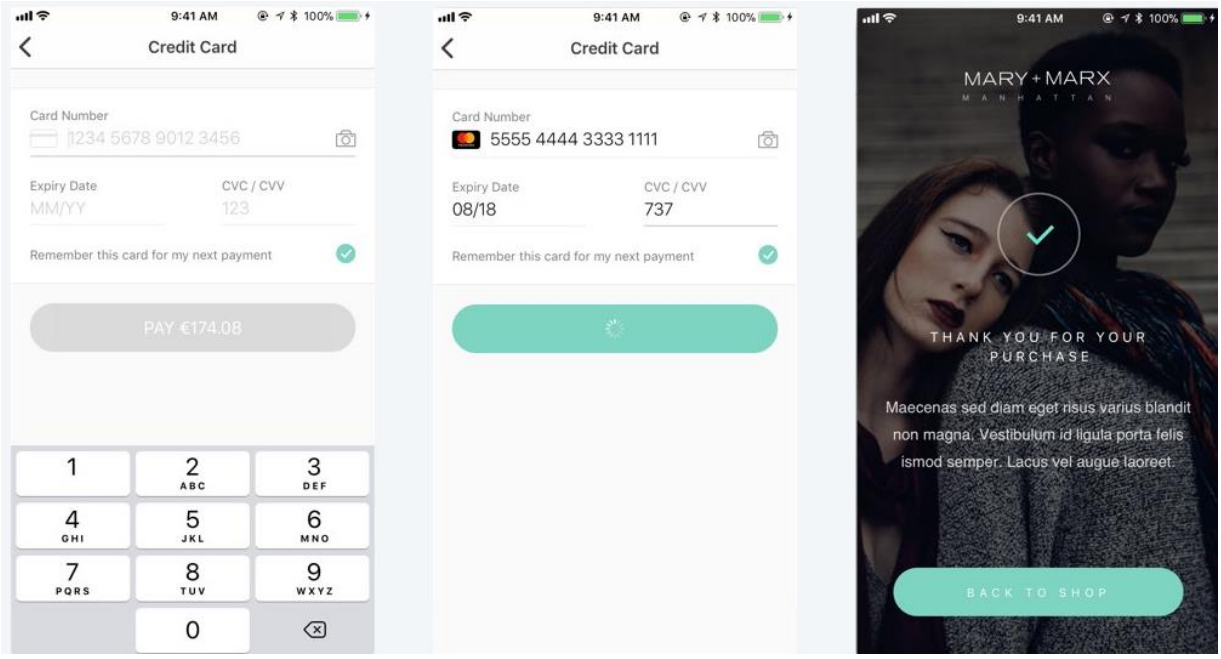

Рисунок 3.3 – Приклад аутентифікації без залучення користувача

Впровадження аутентифікації без залучення користувача дозволяє подолати зростаючу тенденцію відмови від онлайн-оплати карткою і створити кращий досвід електронної комерції для користувачів, одночасно сприяючи зростанню коефіцієнтів конверсії. 3D Secure 2 також пропонує більш гнучкі опції автентифікації, такі як біометричні дані, одноразові паролі, або навіть аутентифікація на основі мобільних додатків. При виявленні підвищеного ризику, нетипових дій або інших аномалій, система переводить нас до традиційних методів підтвердження особистості, таких як використання одноразового коду підтвердження.Але вони можуть бути перехоплені чи скомпрометовані, а їхній формат часом вводить користувача в оману, посилюючи недовіру до таких схем. Це особливо актуально в контексті шахрайських схем, які намагаються імітувати процеси підтвердження.

Тому, враховуючи ці недоліки, я пропоную розглянути більш прогресивні та надійні методи автентифікації. Саме біометрична аутентифікації з використанням системи розпізнавання обличчя може стати ефективним рішенням. Ці системи вже знайомі великій кількості користувачів, завдяки широкому використанню в смартфонах та інших пристроях. Крім того, ця технологія демонструє високу точність і надійність. Додатково, використання такої системи може поліпшити користувацький досвід, роблячи процес підтвердження більш зручним і неперервним.

Однак, важливо враховувати можливі питання конфіденційності та захисту даних, пов'язаних з такими системами.

Аутентифікація з використанням системи розпізнавання обличчя є статичним методом, при застосуванні якого будується двовимірний або тривимірний образ обличчя людини. За допомогою камери і спеціалізованого програмного забезпечення на зображенні або наборі зображень особи виділяються контури брів, очей, носа, губ і т. д., обчислюються відстані між ними й інші параметри, залежно від алгоритму, що використовується. За цими даними будується образ, що перетворюється в цифрову форму для порівняння. Причому кількість, якість і різноманітність образів (різні кути повороту голови, зміни нижньої частини обличчя при вимові ключового слова і т. д.) може варіюватися залежно від алгоритмів і функцій системи, що реалізує даний метод.

Отже, кожного індивідуума можна описати за допомогою унікального набору параметрів, причому навіть із деяким надлишком. Для ідентифікації з високим ступенем точності потрібно не більше 40 характерних точок лиця, тоді як система зазвичай може виокремити близько двох тисяч оціночних параметрів. Це дає змогу забезпечити високу надійність ідентифікації незалежно від положення голови, наявності окулярів, косметики. Фотозображення та цифровий опис обличчя кожного індивідуума (шаблон обличчя) вносяться в спеціальну базу даних, за якою згодом здійснюється пошук і розпізнавання осіб.

3D-системи розпізнання осіб за обличчям можуть ефективно ідентифікувати людей за різних кутів повороту голови й аж до вигляду в профіль. Традиційні 2D-системи досить непогано працюють із зображеннями в анфас і за повороту голови на кут до двадцяти градусів

Дослідження показало, що до 2027 року сумарна вартість електронних мобільних платежів з біометричною автентифікацією сягне 1,2 трильйона доларів США, збільшившись із 332 мільярдів доларів у 2022 році. Зростання на 365% зумовлене нещодавніми нормативними змінами, завдяки введенню SCA (Strong Customer Authentication), що сприяє більш широкому застосуванню біометрії.

Інститут кібербезпеки Entrust опитав 1450 споживачів у всьому світі, щоб вивчити їхній досвід використання автентифікації без пароля та гібридних ідентифікацій. Це дослідження показало, що користувачі хочуть більше зручності, коли йдеться про верифікацію. 51% респондентів скидають пароль принаймні раз на місяць, тому що не можуть його згадати. 15% користувачів відповіли, що роблять це принаймні раз на тиждень.

Оскільки споживачі прагнуть більшої зручності та безпеки, біометрія повинна замінити паролі. Якщо вибрати між біометричними даними чи паролем, 74% респондентів оберуть біометричні дані в половині чи частіше випадків. Третина завжди вибере біометричні дані, якщо така можливість існує.

Дослідження також вказують, що впровадження технології розпізнавання облич сприяє поширенню використання біометрії в мобільних платежах та стимулює майже повсемісне поширення можливостей розпізнавання облич для безперешкодного здійснення онлайн покупок.

Зі зростанням використання розпізнавання обличчя, ця технологія стане мішенню для зловмисників, які використовують сучасні методи підміни та спуфінг

Тому під час розробки потрібно приділяти першочергову увагу вдосконаленню та впровадженню методів виявлення живої присутності та боротьби з спуфінгом, щоб протистояти шахрайству, яке постійно розвивається, і не допустити порушення безпеки.

Криптовалютна індустрія – це ще одна сфера, яка за останні роки пережила величезний сплеск популярності. Як правило, ті, хто використовує криптовалюти, роблять це для транзакцій на великі суми. Станом на 2020 рік середня транзакція у валюті біткойн становила 25 000 доларів США .

Крипто-транзакції, як і будь-які фінансові транзакції, вимагають високого рівня безпеки, особливо з огляду на пов’язані транзакції великого обсягу та вартості. Основним способом зберігання, доступу та керування криптовалютними біржами та електронниим гаманцями є закритий ключ. Запровадження біометричної автентифікації, для доступу до криптовалютних бірж та електронних гаманців

виглядає наступним логічним кроком. Це допоможе забезпечити додатковий рівень безпеки для зберігання та керування криптовалютою.

Згідно з прогнозом Juniper Research, до 2025 року близько 1,4 мільярда людей використовуватимуть технологію розпізнавання облич для автентифікації платежу, що більш ніж удвічі зросте порівняно з 671 мільйоном у 2020 році.

3.4 Рекомендації по оновленню нормативно-правової бази банку для підтримки впровадження біометричної автентифікації в Україні

Деякі члени цивільної спільноти стурбовані тим, як використовуються біометричні дані. Зокрема, у несекретному звіті оборонної наукової ради Сполучених Штатів із оборонної біометрії зазначено, що розумно захищати, а інколи навіть маскувати справжній обсяг можливостей у сферах, безпосередньо пов'язаних із забезпеченням безпеки. що стосується і біометрії. Йдеться про те, що це класична риса розвідки та військових операцій.

Оскільки біометрична автентифікація стосується обробки персональних даних користувачів, важливо забезпечити її відповідність законодавчим вимогам. Банкам необхідно ретельно переглянути їхню політику приватності і додати необхідні положення про обробку біометричних даних. Це включає оновлення політик і процедур, які стосуються збору, зберігання та обробки біометричних даних. Також, важливо визначити механізми відповідальності та відшкодування у разі порушень безпеки. Доцільно переглянути і внести відповідні зміни в угоди з клієнтами та інші документи, що регулюють взаємовідносини між банком та користувачами.

Крім того, необхідно вдосконалити та актуалізувати корпоративні правила і нормативи, щоб вони включали використання біометричної автентифікації. Можливо, банку знадобиться провести аудит безпеки, щоб визначити, які зміни необхідні для підтримки нової системи автентифікації.

Важливо також забезпечити відповідність міжнародним документам. Друга директива про платіжні послуги PSD2 (Payment Services Directive 2) є ключовим правовим актом, що регулює платіжний сектор в Європейському союзі, включаючи

Україну. Його головною метою є забезпечення безпеки та захисту платіжних транзакцій, а також підвищення довіри клієнтів до цифрових платіжних послуг.

PSD2 встановлює правові вимоги для платіжних послуг, що надаються в рамках Європейського союзу. Вона спрямована на просування конкуренції, інновацій та захисту інтересів клієнтів. Згідно з цією директивою, банки та інші постачальники платіжних послуг повинні забезпечити відкритий доступ до своїх систем для сприяння новій хвилі фінтех-інновацій, а також впровадити засоби автентифікації, що відповідають стандартам SCA.

SCA (Strong Customer Authentication) є методом автентифікації, який базується на використанні двох або більше факторів ідентифікації, які повинні бути незалежними один від одного. Це можуть бути такі фактори, як щось, що клієнт знає (наприклад, пароль), щось, що клієнт має (наприклад, мобільний пристрій), або щось, що клієнт є (наприклад, біометричні дані, такі як розпізнавання обличчя або відбиток пальця). Це забезпечить більшу надійність та безпеку під час автентифікації клієнтів під час здійснення платіжних операцій.

Оновлення нормативно-правової бази банку для підтримки впровадження біометричної автентифікації в Україні передбачає врахування вимог та стандартів SCA та PSD2. Це означає, що банки повинні забезпечити використання сильної автентифікації з використанням біометричних даних, як одного з факторів ідентифікації клієнта. Крім того, вони повинні забезпечити безпеку та захист платіжних транзакцій, включаючи застосування методів виявлення живої присутності та боротьби з спуфінгом.

Такі оновлення нормативно-правової бази допоможуть банкам відповідати вимогам міжнародних стандартів та забезпечити впровадження біометричної автентифікації відповідно до найвищих стандартів безпеки та захисту даних. Це покращить впевненість клієнтів у безпеці їхніх фінансових операцій та сприятиме розвитку цифрового банкінгу та інноваційних рішень в Україні.

Можна зробити висновок про те, що впровадження методу біометричної автентифікації — це складний процес, який вимагає певної підготовки, але він може принести значні переваги в плані захисту банківських послуг від кіберзлочинності.

Висновки за розділом 3

Найбільша увага в третьому розділі приділена розробці рекомендацій щодо впровадження біометричної автентифікації для вдосконалення захисту електронних банківських послуг.

Біометрична автентифікація є ефективним інструментом безпеки в банківській сфері. Вона забезпечує гарантовану безпеку та достовірність, позитивний користувацький досвід і високу стійкість до фальсифікації.

При впровадженні біометричної автентифікації важливо обрати правильний тип біометричних характеристик, які будуть використовуватись. Це можуть бути відбитки пальців, риси обличчя, сканування сітківки ока, голосові особливості тощо. Вибір залежить від конкретних потреб і контексту використання.

Комбінування різних методів автентифікації допомагає забезпечити більш надійний і складніший процес перевірки особи але втомлює користувачів. Тому біометрична аутентифікація з використанням системи розпізнавання обличчя може стати ефективним рішенням. Ця технологія демонструє високу точність та надійність і вже знайома великій кількості користувачів, завдяки широкому використанню в смартфонах та інших пристроях.

Дослідження показують, що 51% респондентів скидають пароль принаймні раз на місяць, тому що не можуть його згадати. 15% користувачів відповіли, що роблять це принаймні раз на тиждень. Якщо вибрати між біометричними даними чи паролем, 74% респондентів оберуть біометричні дані в половині чи частіше випадків. Третина завжди вибере біометричні дані, якщо така можливість існує. А згідно з прогнозом Juniper Research, до 2025 року близько 1,4 мільярда людей використовуватимуть технологію розпізнавання облич для автентифікації платежу.

Результати цих досліджень свідчать про те, що майбутнє саме за біометричною аутентифікацією. Біометрична аутентифікація з використанням технології розпізнавання облич є перспективною, зручною, прогресивною та надійною технологією.

ВИСНОВКИ

У кваліфікаційній роботі було розроблено рекомендаці щодо впровадження біометричної автентифікації для вдосконалення захисту електронних банківських послуг в Україні, а також представлено рекомендації по оновленню нормативно-правової бази банку для підтримки впровадження біометричної автентифікації в Україні.

У першій частині кваліфікаційної роботи було проведено аналіз сучасного стану використання електронних банківських послуг. Аналіз складався з дослідження нормативно-правової бази, що стосується безготівкових розрахунків. Було проаналізовано статистику використання безготівкових розрахунків в Україні та досліджено переваги використання електронних банківських послуг.

У другій частині кваліфікаційної роботи було визначено найбільш поширені кібератаки на банківську систему. До них відносяться фішинг, DDoS-атаки та програми вимагачі. Також проведено огляд найбільш поширених ризиків, пов'язаних з використанням електронних банківських послуг, таких як: зловмисне програмне забезпечення, незахищені громадські точки доступу Wi-Fi, вразливості додатків та ідентифікаторів.

Крім того, було проведено дослідження протоколу безпеки для онлайн-транзакцій платіжних карток 3D Secure, який забезпечує додатковий рівень аутентифікації та дозволяє переконатися, що особа, яка здійснює платіж, є власником картки.

На основі зібраних даних із першої та другої частин у третій частині кваліфікаційної роботи було розроблено рекомендацій щодо впровадження біометричної автентифікації для вдосконалення захисту електронних банківських послуг в Україні. Також представлено рекомендації по оновленню нормативно-правової бази банку для підтримки впровадження біометричної автентифікації в Україні.

Виходячи із поставленої мети кваліфікаційної роботи були виконані наступні завдання:

– проведено аналіз нормативно-правового забезпечення надання електронних банківських послуг;

– досліджено ризики використання електронних банківських послуг;

– досліджено сучасні кібератаки на банківську систему;

– досліджено протокол безпеки для онлайн-транзакцій платіжних карток;

– розроблено рекомендації щодо підвищення рівня захищеності електронних банківських послуг.

Всі задачі було виконано в повному обсязі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію [Електронний ресурс]: Закон України від 21.12.2019 № 2657-XII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

2. Безготівкові розрахунки [Електронний ресурс] – Режим доступу до ресурсу: https://bank.gov.ua/ua/payments/nocash.

3. Про затвердження Положення про порядок емісії та еквайрингу платіжних інструментів [Електронний ресурс] // Постанова від 29.07.2022 № 164 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0164500-22#Text.

4. Про Національний банк України [Електронний ресурс] // Закон України від 20.05.1999 № 679-XIV – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/679-14#Text.

5. Про захист інформації в інформаційно-комунікаційних системах [Електронний ресурс]: Закон України від 16.12.2020 № 1089-IX. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

6. Про захист персональних даних [Електронний ресурс]: Закон України від 16.12.2021 № 1971-IX. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

7. Олійник О.В. Стан забезпечення інформаційної безпеки в Україні / О.В. Олійник // Юридичний вісник. – 2014. – № 2(31). – С. 59-65.

8. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] // Закон України від 05.10.2017 № 2163-VIII – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

9. Особливості правового забезпечення кібербезпеки банківської системи у сучасних умовах / Е. С. Дмитренко // Актуальні проблеми управління інформаційною безпекою держави / Е. С. Дмитренко. – Київ, 2019. – (Електронне видання). – С. 206–208.

10. Про затвердження Положення про використання засобів криптографічного захисту інформації Національного банку України [Електронний

ресурс] // Постанова від 14.04.2023 № 49 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0049500-23#n17.

11. Про доступ до публічної інформації [Електронний ресурс]: Закон України від 01.12.2019 № 2939-VI. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17

12. Cashless-розрахунки в Україні стабільно зростають [Електронний ресурс] // Національний банк України. – 2022. – Режим доступу до ресурсу: https://bank.gov.ua/ua/news/all/cashless-rozrahunki-v-ukrayini-stabilno-zrostayut.

13. Банківські технології [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://new.minfin.com.ua/ua/bankovskie-tehnologii-3-0#1996.

14. Про електронні довірчі послуги [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text

15. Горошко М.П. Біометрія: навч. посібн. / М.П. Горошко, С. І. Миклуш, П. Г. Хомюк – Львів: Камула, 2004. – 236 с.

16. Скобцов Ю.А. Методи визначення біометричних характеристик для створення автоматизованої системи надання доступу до даних [Електронний ресурс] / Ю.А. Скобцов, Ф.С. Фоменко // IV міжнародна науково-технічна конференція студентів, аспірантів та молодих вчених «Інформаційні управляючі системи та комп'ютерний моніторинг». – Том 1. – Режим доступу: http://masters.donntu.org/2013/fknt/fomenko/library/article1.htm

17. Clarke R. Human identification in information systems: Management challenges and public policy issues [Electronic resource]/ Clarke Roger // Information T & P. – 1994. – № 7 (4). – P. 6 – 37. – Access: https://www.deepdyve.com/lp/emerald-publishing/human-identification-in-information-systems-management-challenges-and-PHQXBfPuvo

18. Динамічний ринок платіжних карток в Україні: аналіз показників за перший квартал 2023 року [Електронний ресурс] // upc. – 2023. – Режим доступу до ресурсу: https://upc.ua/dinamichniy-rinok-platizhnikh-kartok-v-ukraini-analiz-pokaznikiv-za-pershiy-kvartal-2023-roku/.

19. EMV 3-D Secure [Електронний ресурс] – Режим доступу до ресурсу: https://www.emvco.com/emv-technologies/3-d-secure/.

20. PCI DSS v4.0 [Електронний ресурс] – Режим доступу до ресурсу: https://getpci.com/.

21. Here is what you should understand about PCI DSS Compliance [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://fortytwo.nl/understand-pci-dss-compliance/.

22. Chaudhari R.D. The Historical Development of Biometric Authentication Techniques [Electronic resource] / R.D. Chaudhari, A.A. Pawar, R.S Deore // International Journal of Engineering Research & Technology. – 2013. – №2. – P. 3921 –3928. – Access: https://www.ijert.org/research/the-historical-development-of-biometric-authentication-techniques-a-recent-overview-IJERTV2IS101132.pdf

23. What is 3-D Secure Authentication, and Why Do I Need It? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.tokenex.com/blog/what-is-3-d-secure-authentication-and-why-do-i-need-it/.

24. Companies Affected by Ransomware [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://heimdalsecurity.com/blog/companies-affected-by-ransomware/.

25. Kost E. The 6 Biggest Cyber Threats for Financial Services in 2023 [Електронний ресурс] / Edward Kost. – 2023. – Режим доступу до ресурсу: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services#toc-2.

26. Duncan C. Cyber Security in Banking [Електронний ресурс] / Caroline Duncan. – 2022. – Режим доступу до ресурсу: https://www.alert-software.com/blog/cybersecurity-in-banking.

27. Атаки на системи Дистанційного банківського обслуговування (ДБО) [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://cyberpolice.gov.ua/article/ataky-na-systemy-364/.

28. Про затвердження Положення про використання засобів криптографічного захисту інформації Національного банку України [Електронний ресурс]: Постанова Правління Національного Банку України від 14.04.2023 № 49 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0049500-23#Text.

29. Про затвердження Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи [Електронний ресурс]: Постанова від 04.07.2007 N 243 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0955-07#Text.

30. Про затвердження Положення про використання засобів криптографічного захисту інформації Національного банку України [Електронний ресурс] // ПОСТАНОВА від 14.04.2023 № 49 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0049500-23#Texthttps://zakon.rada.gov.ua/laws/show/v0049500-23#Text%D0%BC.

31. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс] // Постанова від 28.09.2017 № 95 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text.

32. Про затвердження Положення про застосування цифрового власноручного підпису в банківській системі України [Електронний ресурс] // Постанова від 13.12.2019 № 151 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0151500-19#Text.

33. Про затвердження Положення про Систему BankID Національного банку України [Електронний ресурс] // Постанова від 17.03.2020 № 32 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0032500-20#Text.

34. As payments systems go digital, they are changing global finance [Електронний ресурс] // TheEeconomist – Режим доступу до ресурсу: https://www.economist.com/special-report/2023/05/15/as-payments-systems-go-digital-they-are-changing-global-finance.

35. The Latest 2023 Ransomware Statistics [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://aag-it.com/the-latest-ransomware-statistics/.

36. Khantimirov R. DDoS Attack Wave on Banks: How can Companies Protect Themselves? [Електронний ресурс] / Ramil Khantimirov – Режим доступу до ресурсу: https://cyberprotection-magazine.com/ddos-attack-wave-on-banks-how-can-companies-protect-themselves.

37. Petya and NotPetya [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Petya_and_NotPetya.

38. На сайти органів влади здійснена чергова масова DDoS-атака. [Електронний ресурс] – Режим доступу до ресурсу: https://www.ukrinform.ua/rubric-technology/3410542-sajti-bankiv-ta-organiv-vladi-zaznali-masovoi-ddosataki.html.

39. How Exactly Does Online Payment Work? [Електронний ресурс] // 2020 – Режим доступу до ресурсу: https://www.ccv.eu/en/2020/how-exactly-does-online-payment-work/.

40. Кумченко Ю.О. Інформаційна технологія ідентифікації персоналу на основі комплексу біометричних параметрів: дис. …канд. тех. наук: 05.13.06 / Юрій Олександрович Кумченко; Криворізький національний університет. – Кривий Ріг, 2017. – 44 с.