Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп’ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»

В.о. зав. кафедрою БІСТ

Ольга МЕЛКОЗЬОРОВА

_____

« » 2023 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Дослідження та аналіз методів та засобів забезпечення безпеки інформаційних ресурсів в системах електронних платежів»

«Research and analysis of methods and means of ensuring the security of information resources in electronic payment systems»

оцінка « »

Голова ЕК

Олександр ЛЕМЕШКО _____

Керівник : к.т.н., доцент Єсіна М.В.

Рецензент : к.т.н. Бобух В. А.

Виконавець : студент(ка) групи КБ-61

Потапова З. Д.

Харків – 2023

РЕФЕРАТ

Дипломна робота другого (магістерського рівня) містить 79 сторінок, 4 рисунки та 1 таблиця. Перелік посилань нараховує 75 найменувань.

Актуальність роботи: Актуальність даного дослідження зумовлена розвитком систем електронних платежів та потребою у сучасних, швидких та безпечних методах захисту інформаційних ресурсів.

Мета роботи полягає у вивченні та аналізу наявних методів, засобів та заходів для забезпечення безпеки інформаційних ресурсів в системах електронних платежів.

Результати роботи та їхня новизна: результатом роботи є систематизація знань у сфері забезпечення безпеки інформаційних ресурсів та опис міжнародної нормативно-правової бази для подальшого використання зібраних даних у банківській інфраструктурі України.

Рекомендації щодо використання результатів роботи: Проаналізовані засоби, заходи та методи забезпечення безпеки можливо використати для створення більш захищеної системи електронних платежів. Використання досвіду країн-партнерок дозволить створити власну систему без повторення чужих помилок.

Значущість роботи та висновки: Стрімка популярність використання електронних платежів вимагає відповідного рівня безпеки даних, які використовуються в цих платежах. Окрім того, у 2022 році Україна зазнала значних кібератак у тому числі на фінансову систему, з чого випливає необхідність забезпечення максимального рівня безпеки інформаційних ресурсів в системах електронних платежів для захисту конфіденційних даних громадян.

Припущення про можливі напрямки розвитку: Проаналізовані методи та засоби захисту мають бути використані у наявних системах електронних платежів в майбутньому, як для передачі даних, так і для їхнього зберігання.

Об'єкт дослідження: Процес захисту інформаційних ресурсів в системах

електронних платежів.

Предмет дослідження: Методи захисту інформаційних ресурсів в системах електронних платежів.

Ключові слова (словосполучення): СИСТЕМИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ, ЕЛЕКТРОННІ ПЛАТЕЖІ, ОПЛАТА ЧЕРЕЗ ІНТЕРНЕТ, ЦИФРОВІ ПЛАТЕЖІ, ПЛАТЕЖІ.

ABSTRACT

The thesis of the second (master's) level contains 79 pages, 4 figures and 1 table. The list of references includes 75 items.

Relevance of the study: The relevance of this study is due to the development of electronic payment systems and the need for modern, fast and secure methods of protecting information resources.

The purpose of the work is to study and analyze the existing methods, tools and measures to ensure the security of information resources in electronic payment systems.

Results and novelty: The result of the work is the systematization of knowledge in the field of information resources security and a description of the international regulatory framework for further use of the collected data in the banking infrastructure of Ukraine.

Recommendations for using the results of the study: The analyzed security tools, measures and methods can be used to create a more secure electronic payment system. Using the experience of the partner countries will allow us to create our own system without repeating other people's mistakes.

Significance of the work and conclusions: The rapid popularity of electronic payments requires an appropriate level of security for the data used in these payments. In addition, in 2022, Ukraine suffered significant cyberattacks, including on the financial system, which implies the need to ensure the maximum level of security of information resources in electronic payment systems to protect confidential data of citizens.

Assumptions about possible directions of development: The analyzed methods and means of protection should be used in existing electronic payment systems in the future, both for data transmission and storage.

Object of research: The process of protecting information resources in the systems of electronic payment systems.

Subject of research: Methods of protecting information resources in electronic payment systems.

Keywords: ELECTRONIC PAYMENT SYSTEMS, ELECTRONIC PAYMENTS, PAYMENT VIA THE INTERNET, DIGITAL PAYMENTS, PAYMENTS.

ЗМІСТ

ЗМІСТ 6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 8

ВСТУП 10

1 ЕЛЕКТРОННІ ПЛАТЕЖІ ЯК ЯВИЩЕ 11

1.1 Що таке електронні платежі? 11

1.2 Типи електронних платежів 11

1.3 Історія та еволюція електронних платежів. 14

1.4 Електронні платежі зараз та в майбутньому 16

2 ДОСВІД ОКРЕМИХ КРАЇН У СФЕРІ ЕЛЕКТРОННИХ ПЛАТЕЖІВ 21

2.1 Естонія – найбільш цифровізована країна 21

2.2 Індія 23

2.3 Нігерія як країна, що розвивається 25

2.4 Досвід України 27

3 НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ У СФЕРІ ЕЛЕКТРОННИХ ПЛАТЕЖІВ 29

3.1 Стандарт PCI DSS 29

3.2 Рекомендації від Європейської Бізнес Асоціації 33

3.3 SWIFT CSCF 40

3.3.1 Загальний опис SWIFT CSCF 40

3.3.2 Рекомендаційні засоби безпеки від SWIFT 44

3.3.3 Аналіз рекомендаційних засобів безпеки від SWIFT 47

3.4 Нормативно-правова база в Україні 48

3.4.1 Огляд нормативно-правової бази України про забезпечення безпеки інформаційних ресурсів у сфері платіжних систем 48

3.4.2 Аналіз нормативно-правової бази України про забезпечення безпеки інформаційних ресурсів у сфері платіжних систем 49

4 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В СИСТЕМАХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ 52

4.1 Можливі загрози для систем електронних платежів 52

4.2 Проблеми електронних платежів 54

4.3 Вразливості систем електронних платежів 54

4.4 Підвищення безпеки електронних платежів 58

4.5 Методи забезпечення безпеки 59

4.6 Безпека в конкретних системах електронних платежів 61

4.6.1 PayPal 61

4.6.2 Мобільні гаманці 63

4.7 Блокчейн 67

ВИСНОВОК 69

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 70

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AES-GSM	Advanced Encryption Standard with Galois Counter Mode
B2B	Business-To-Business
BBPS	Bharat Bill Payment System
CSCF	Customer Security Controls Framework
CVV	Card Verification Value
DAN	Device Account Number
DDoS	Distributed Denial of Service
DMARC	Domain-Based Message Authentication, Reporting & Conformance
EBA	European Business Association
EDR	Endpoint Detection and Response
FIDO	Fast Identity Online
GEAR	Government E-Payment Adoption Ranking
HCE	Host Card Emulation
HIDS	Host-Based Intrusion Detection System
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IMPS	Immediate Payment Service
SO	International Organization for Standardization
KSI	Keyless Signature Infrastructure
KYC-SA	Know-Your-Customer Security Attestation
MMID	Mobile Money Identifier
MOTO	Mail Order Telephone Order
NETC	National Electronic Toll Collection
NFC	Near-Field Communication
NIBSS	Nigeria Inter-Bank Settlement System
NIDS	Network Intrusion Detection System

NPSC	National Payments System Committee
NPSV	National Payment System Vision
P2PE	Point-To-Point Encryption
PCI DSS	Payment Card Industry Data Security Standard
POI	Point of Interaction
POS	Point of Sale
PTS	PIN Transaction Security
QR	Quick Response
RFID	Radio-Frequency Identification
RMA	Relationship Management Applications
SCI	Serial Communications Interface
SE	Secure Element
SET	Secure Electronic Transaction
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	Single Sign-On
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UPI	Unified Payments Interface
VPA	Virtual Payment Address
XDR	Extended Detection And Response
XSS	Cross Site Scripting
СЕП	Система Електронних Платежів
ЦБЕ	Центральний Банк Естонії

ВСТУП

Актуальність роботи: Захист систем електронних платежів та їхніх інформаційних ресурсів – важлива тема для сьогодення. Наслідки пандемії COVID-19 призвели до стрімкого розвитку кібератак, які своєю чергою зіграли велику роль в погіршенні безпеки фінансових систем. За новітніми дослідженнями, тільки за 2022 рік системи електронних платежів зазнали збитків від шахрайства більш ніж на 40 мільярдів доларів, і при цьому, лише 34% з компаній вкладають гроші у заходи з запобігання або пом’якшення шахрайських дій. Окрім прямого шахрайства, великих збитків завдає витік даних, який становить загрозу як для клієнтів, так і для самих компаній. З усіх сфер, які постраждали від витоку даних, найбільше страждають системи фінансових послуг. Кількість осіб, що постраждали від витоку своїх даних, за рік збільшилася більше ніж на сто мільйонів. Така стрімка тенденція до витоку даних та шахрайства прямо говорить про необхідність покращення наявних методів захисту систем електронних платежів.

Мета кваліфікаційної роботи: систематизація та аналіз наявних знань про методи забезпечення безпеки інформаційних ресурсів в системах електронних платежів для пошуку оптимальних в плані безпеки, зручності та складності рішень для майбутнього їх використання в українських та міжнародних системах.

Результатом роботи буде систематизація знань та окреслення можливих рішень для розв’язання наявних проблем безпеки інформаційних ресурсів користувачів систем електронних платежів.

Публікації за темою роботи:

1 Потапова З. Д., Пономар В. А. Перспективи розвитку засобів безпеки в українських системах електронних платежів. *Захист інформації і безпека інформаційних систем* : Матеріали IX Міжнар. науково-техн. конф., м. Львів, 25–26 трав. 2023 р.

1 ЕЛЕКТРОННІ ПЛАТЕЖІ ЯК ЯВИЩЕ

1.1 Що таке електронні платежі?

За останні десятиліття системи електронних платежів привернули увагу як дослідників у сфері фінансів, бухгалтерського обліку та бізнес-технологій, так і розробників інформаційних систем через їхню вкрай важливу роль в сучасній електронній торгівлі. Через таку розбіжність у сферах досліджень виникли різні погляди на саме визначення електронних платежів. Так, у 2004 році вченим Денисом Абражевичем було надане наступне визначення систем електронних платежів: «Система електронних платежів – форма фінансової взаємодії, що включає продавця та покупця через використання електронних комунікацій» [5], а у 2011 вчені Лоренс Брукз та Остін Бріґз визначили системи електронних платежів як форми зв’язку між організаціями та окремими особами за допомогою банківських установ, що забезпечують електронний обмін грошима [14]. Однак, всі визначення зводяться до одного висновку: системи електронних платежів – це різні форми переказу коштів за допомогою Інтернету.

1.2 Типи електронних платежів

На цей час популярними системами електронних платежів є наступні.

Система електронних платежів на базі смарткарт: смарткарта – пластикова картка з інтегральним чіпом, що забезпечує мобільність та переносимість даних. [40] Ця картка об’єднує методи ідентифікації пластикових та магнітних карток, що дозволяє використовувати її для багатьох функцій та застосунків [63]. Система оплати смарткартами забезпечує механізм безпеки трифакторної автентифікації: ПІН-код, електронний підпис та біометричні дані. Також смарткарти використовують шифрування для забезпечення захисту інформації й розроблені таким чином, щоб бути стійкими до втручання. Цей механізм підвищує рівень безпеки цієї системи платежів [7], а популярними представниками електронних платежів на базі смарткарт є кредитні, дебетові та

картки передоплати. Процесор на картці містить базову операційну систему, що дозволяє зберігати, передавати та захищати дані. Працюють смарткартки наступним чином: мікропроцесори смарткарт обмінюються даними із пристроями для читання карток через SCI (Serial Communications Interface). Смарткарти «спілкуються» зі зчитувачами через прямий фізичний контакт або через RFID (Radio-Frequency Identification) чи інший стандарт бездротового підключення малого радіуса дії, після чого зчитувач передає дані зі смарткартки до місця призначення (зазвичай, до банківських платіжних систем чи до систем автентифікації) через мережеве з'єднання.

Існує декілька видів смарткарток:

– Контактні смарткарти: найпоширеніший вид смарткарт, що вставляються у зчитувач смарткарт, який своєю чергою з'єднується зі струмопровідною контактною пластиною на поверхні картки.

– Безконтактні картки: вид карток, які не потребують безпосереднього контакту зі зчитувачем. І картка, і зчитувач містять антену і «спілкуються» за допомогою радіочастот. У смарткарток антеною часто виступає мідний дріт, що огортає краї картки.

– Картки із подвійним інтерфейсом: вид смарткарт, які оснащені як контактними, так і безконтактними інтерфейсами.

– Гібридні смарткартки: вид смарткарт, які містять більше однієї технології смарткарт. Така картка може мати декілька мікросхем для різного використання, наприклад, безконтактний чіп використовується для контролю доступу, а контактний чіп – для автентифікації SSO (Single Sign-On).

Система онлайн-платежів: онлайн-платежі засновані на Інтернет-банкінгу та мають на меті переказ грошей або здійснення покупок через Інтернет. Користувачі можуть переказувати гроші іншим особам зі свого банківського рахунку або використовувати кредитні та дебетові картки для здійснення покупок в Інтернеті. Система онлайн-платежів дозволяє клієнтам банківських установ проводити фінансові операції на спеціальному захищеному вебсайті, яким керує ця установа [63]. Щоб мати доступ до онлайн-банкінгу банківської

установи, клієнт, який має доступ до Інтернету, повинен мати зареєстрований обліковий запис для перевірки.

Система електронних платежів на базі телефона: ця система дозволяє використовувати користувачам свій мобільний телефон для оплати транзакцій. Користувачі можуть відправляти смс-повідомлення, передавати пін-код, підтверджувати транзакцію у мобільному банкінгу або використовувати NFC для оплати. Мобільні платежі вже стали достойною альтернативою паперовим грошам, чекам, кредитним та дебетовим карткам, їх використовують для оплати рахунків, електронного переказу коштів, платежів через онлайн-банкінг та виставлення електронних рахунків [32]. За допомогою мобільного банкінгу банківські установи також інформують власників карток щоразу, як з їхньої картки була зроблена покупка, що допомагає запобігти можливому шахрайському використанню карток, оскільки власник картки буде інформований про кожний платіж з його картки.

Система електронних платежів на базі електронного гаманця: Електронний гаманець (e-wallet) забезпечує усі функції звичайного гаманця на одній смарткартці, що виключає необхідність використання декількох банківських карток. Електронний гаманець також забезпечує численні функції безпеки, що недоступні звичайним гаманцям [70]. Прикладом електронного гаманця є PayPal, який дозволяє здійснювати платежі та грошові перекази через Інтернет. За допомогою PayPal можна відправляти гроші без розкриття фінансової інформації та передавати кошти, маючи лише електронну пошту отримувача. Також новітніми представниками електронних гаманців стали запущені у 2015 році Google Pay, Samsung Pay та Apple Pay. Використання застосунків з електронними гаманцями стали настільки популярними, що у деяких країнах використання кредитних карток більше не є основним способом оплати.

Існує три види електронних гаманців:

– Мобільні гаманці, тобто ті, в яких роль гаманця виконує пристрій (наприклад, смартфон), щоб здійснити оплату. Прикладом такого гаманця є Google Pay.

– Онлайн-гаманці, тобто віртуальні гаманці, які зберігають гроші у цифровій формі та використовуються для оплати в Інтернеті або надсилання коштів іншим користувачам, наприклад, PayPal.

– Криптогаманці, які зберігають особисті ключі, які представляють право власності на цифрову валюту, наприклад, Біткоїн. Якщо користувач хоче оплатити товар чи послугу, або просто переказати кошти, особистий ключ використовується для підписання права власності на цю цифрову валюту іншому користувачу. Далі гаманець «транслює» цю транзакцію в мережу клієнтів, щоб перевірити транзакцію та включити її у блокчейн. Як тільки транзакція підтверджується в блокчейні, вважається, що платіж відбувся.

Переваги у використанні таких методів оплати є як для клієнтів, так і для продавців, оскільки використання альтернативних методів оплати є швидким, безпечним, такі методи оплати використовуються майже в усьому світі, а виконати оплату стає вкрай легко.

Цифрові гроші – технологія електронних платежів, яка може забезпечувати анонімні електронні платежі, приносить значні переваги фінансовим установам. Безпечна система електронних грошей може гарантувати анонімність користувачів, і при цьому забезпечувати відстеження відмитих та отриманих незаконним способом грошей. При цьому, якщо була присутня незаконна діяльність, анонімність цифрових грошей може бути скасована [34]. При цьому цифрові гроші можуть підвищити попит на продукти через простоту та безпеку каналів поширення. Цифрові гроші дозволяють відстежувати, хто незаконно відтворює та поширює інтелектуальні матеріали, захищені авторським правом [22].

1.3 Історія та еволюція електронних платежів.

Перш ніж розглянути електронні платежі детальніше, потрібно заглибитися у їх історію появи та еволюцію до тих видів та методів, які добре

нам знайомі. Роком першого прояву такого явища, як електронні платежі, можна назвати 1918 рік, коли Федеральний резервний банк США передав гроші між штатами за допомогою телеграфу. Однак, ця технологія не набула широкого використання, тож всім відома історія електронних платежів по всьому світу починається у 1990-х роках як відповідь на розвиток Інтернету та Інтернет-торгівлі. Спочатку платежі здійснювалися завдяки вже традиційним платіжним системам: банківськими переказами, використовувалася також післяплата та вкрай рідко використовували системи MOTO. MOTO (Mail Order Telephone Order) – перша форма дистанційної оплати, під час якої продавець запитував у клієнта дані картки телефоном, електронною поштою або факсом та вводив їх у фізичний термінал для завершення платежу замість клієнта. Цей спосіб не зазнав популярності через відсутність довіри клієнта до передачі даних своєї картки продавцю. Більшість онлайн-транзакцій проводилися за допомогою кредитних та дебетових карток, однак з поширенням популярності Інтернет-торгівлі зростала і потреба у появі більш безпечних та зручних методів оплати [33].

Невідомо, що саме було першим проявом електронних платежів, однак найпопулярнішою теорією з цього приводу є те, що першим електронним платежем стала онлайн-покупка піци в популярній мережі Pizza Hut. У цьому ж році запускається Amazon, який тоді був книжковим магазином з можливістю онлайн-оплати товару. Очевидно, що потреби онлайн-бізнесу спонукали до розвитку методів електронних платежів, тому вже у 1995-1996 роках були запущені платіжні компанії Millicent, CyberCoin та ECash, однак справжня революція у сфері електронних платежів відбувається після заснування і виходу на ринку PayPal. PayPal пропонували дійсно революційні на той час рішення, наприклад, здійснення платежів за наявності однієї лише адреси електронної пошти. Вже у 1999 році компанії Ericsson та Telnor Mobil розробили на той момент новітню технологію, завдяки якій користувачі могли оплачувати з «мобільного гаманця» квитки в кінотеатр. «Мобільним гаманцем» ставала модель SIM-карток із функцією оплати від компанії Telnor Mobil, яку підтримували нові моделі телефонів від Ericsson [65]. У 2001 році Amazon

запустили мобільну версію свого сайту, що швидко підхопили інші компанії. Вже через два роки більш ніж 95 мільйонів людей по всьому світу здійснили свою першу мобільну покупку [6].

Окремо на початку 2000-х років компанії по всій Азії також починають стрімко розвиватися у сфері цифрових платежів. Так, в Китаї революція цифрових платежів починається з двох технологічних гігантів: Alibaba та Tencent. Alibaba була заснована у 1999 році як B2B майданчик для онлайн-оплати. У 2003 році Alibaba засновує свою систему для онлайн-оплати під назвою Alipay, яка мала б розв'язати проблему недовіру до онлайн-транзакцій. Після виконання транзакції клієнтом Alibaba утримувала гроші покупця до моменту підтвердження отримання товару клієнтом, щоб уникнути спроб шахрайства з боку магазинів. Своєю чергою, Tencent також засновує свою систему онлайн-платежів Tenpay, яку потім було інтегровано у найбільш популярну в Китаї соціальну мережу WeChat для переказу грошей прямо у месенджері.

В Індонезії на початку другого тисячоліття Центральний Банк Азії представив електронний та мобільний банкінг, ставши однією з перших установ, яка запровадила альтернативний спосіб здійснення фінансових операцій онлайн [6].

1.4 Електронні платежі зараз та в майбутньому

Ще у 2003 році в США електронні платежі обігнали за популярністю платежі чеками. Так, кількість електронних платежів в еквіваленті цього року склала 44,5 млрд доларів, поки кількість чеків в еквіваленті склала 36,7 млрд доларів, але найбільше на розвиток систем електронних платежів вплинула пандемія COVID-19. Удосконалення цифрової платіжної інфраструктури призвело до появи нових інноваційних форматів оплати, таких як QR-коди, цифрові гаманці та платежі з рахунку на рахунок, що своєю чергою призвело до спрощення користування клієнтами систем електронних платежів та поєднання різних методів оплати. Пандемія COVID-19 спонукала як клієнтів, так і компанії вплести цифрові технології у свою повсякденність. Так, наприклад, у країнах з

низьким або середнім рівнем доходу понад 40% дорослого населення, яке здійснювало онлайн-покупки, використали електронні платежі вперше. В Індії понад 80 мільйонів дорослого населення зробили свій перший електронний платіж після початку пандемії, в Китаї ця цифра досягла 100 млн. [20]. Серед споживачів послуг був помітний очевидний зріст використання безготівкових методів оплати, і за словами дослідницької компанії Capgemini, чий прогноз можна побачити на рис. 1.1, зростання безготівкових транзакцій з 2022 до 2026 років залишиться стійким [75].

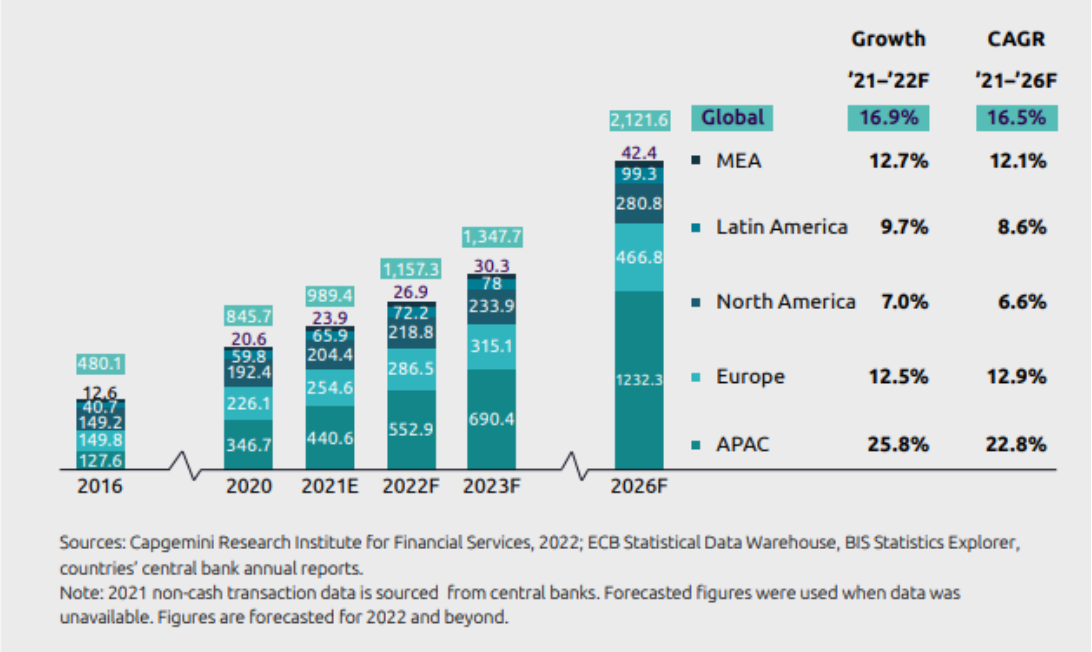

Рисунок 1.1 – Зростання безготівкових операцій по всьому світу до 2026 року

Порівняльний аналіз вказує на зростання популярності нових методів електронних платежів, таких як миттєві платежі, платежі за допомогою QR-коду, електронні гроші, мобільні та цифрові гаманці та оплата рахунок-рахунок. Наприклад, у 2021 році на традиційні методи оплати (кредитні картки, кредитні перекази та дебетування) припадали 83% від загального обсягу безготівкових транзакцій, а на нові методи оплати – 17%. За прогнозами, до 2026 року кількість транзакцій за допомогою нових методів оплати зросте до 28%. Наприклад, за дослідженням компанії Jupiter було підраховано, що у 2025 році кількість користувачів платежів за допомогою QR-коду може сягнути 2,2 мільярда

порівняно з 1.5 мільярдів у 2020 році, що означає, що приблизно 29% користувачів смартфонів до 2025 року буде користуватися даним видом платежів [53].

Окрім того, очікується, що завдяки зростанню впровадження електронних гаманців, кількість електронних платежів протягом періоду 2021-2026 років зросте приблизно на 27% і сягне 161 мільярда. За словами дослідників з організації Capgemini, у 2025 році кількість унікальних цифрових гаманців зросте приблизно в півтора раза та сягне 4.4 мільярда [75].

У цьому дослідження також можна прослідкувати зростання популярності електронних платежів у кожному регіоні.

Так, до 2026 року на Азійсько-Тихоокеанський регіон, вірогідно, буде припадати понад 50% від глобальної кількості безготівкових транзакцій через велику популярність мобільних гаманців. В Китаї 82% мають банківський рахунок і використовують його для здійснення цифрових платежів, в іншій частині цього регіону ця цифра складає приблизно 59%.

Через зростальну популярність миттєвих платежів у Північній Америці сукупний середньорічний темп зростання популярності безготівкових транзакцій за період 2021-2026 роки буде складати приблизно 7% [75].

У Латинській Америці важливу роль у розвитку безготівкових платежів зіграло впровадження миттєвих платежів. Так, бразильська система миттєвих платежів PIX стала настільки популярною за три роки (запуск PIX відбувся у листопаді 2020 року), що на цей момент її використовують приблизно 60% населення Бразилії. За рік кількість користувачів досягла цифри у 107 мільйонів користувачів, а сума переведених за допомогою цієї системи грошей склала понад 700 мільярдів доларів. Варто зазначити, що кількість користувачів PIX в Бразилії перевищила кількість власників кредитних карток по всій країні. PIX був спрямований більшою мірою на дрібні покупки, але став вкрай популярним, оскільки більша частина дорослого населення Бразилії не працює офіційно, і відповідно, значна кількість населення не має банківського рахунку. Зараз PIX є цілою екосистемою фінансових послуг [68].

Також очікується зростання популярності платіжних додатків завдяки електронним гаманцям, а спрощення транскордонних транзакцій очікується завдяки EU Digital Identity Wallet. З 2018 до 2021 року кількість електронних платежів в ЄС зросла більш ніж на 30%. Так, організація Statista у 2020 році проводила дослідження про різні методи оплати від загального обсягу електронних платежів [12]. На рис. 1.2. можна побачити графік з цього дослідження та зробити висновок, що до 2024 року обсяг електронних платежів за допомогою електронних гаманців збільшиться приблизно на 8% у порівнянні з 2020 роком.

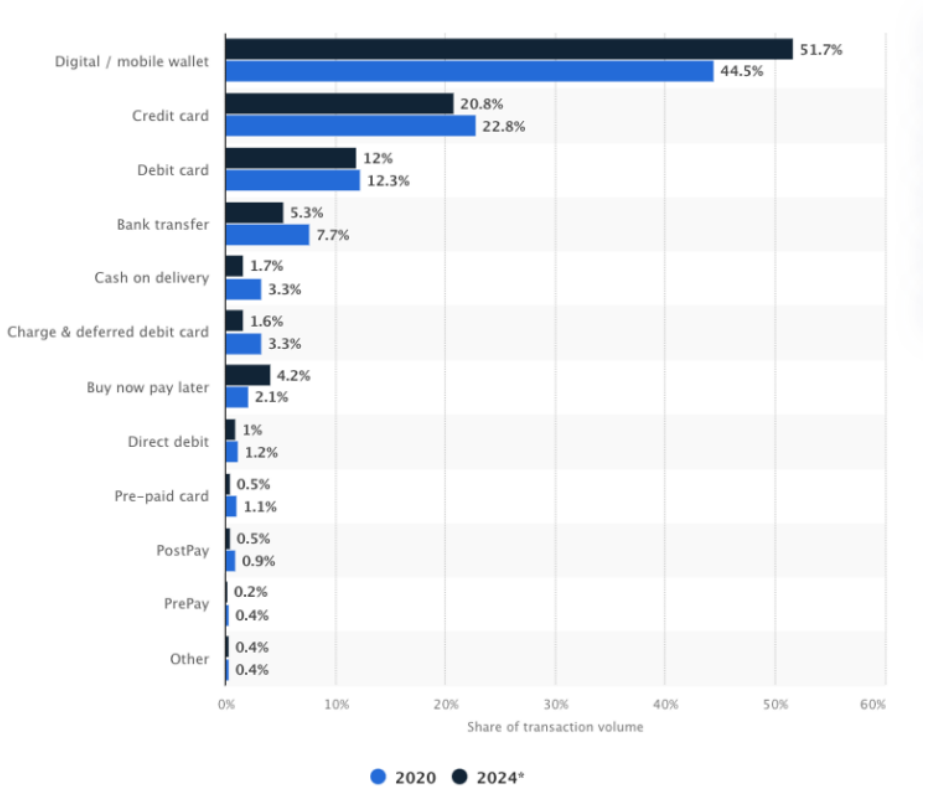

Рисунок 1.2 – Ринкова частка способів оплати в загальній вартості транзакцій електронної комерції в усьому світі у 2020 році з прогнозом на 2024 рік

У 2021 Європейський центральний банк замовив дослідження нових електронних платежів з метою розуміння переваг даних методів та вивчення особливостей, які зроблять дані методи більш привабливими для населення. Результати дослідження показали, що більш технічно підковані люди

використовували цілу низку методів електронних платежів, однак, більшість людей, що брали участь у дослідженні, вказали дебетові картки як найпоширеніший спосіб повсякденних покупок. Велику роль також зіграв технологічний розвиток: в країнах з високим рівнем цифровізації та більш інноваційним ринком електронних платежів учасники обирали більший набір платіжних інструментів.

Однак, нові платіжні інструменти не отримали великої популярності, оскільки більшість учасників вважали, що вже присутні платіжні методи повністю відповідають їхнім потребам. Найпопулярнішими методами цифрової оплати виявилися мобільні платежі та дебетові картки. Мобільні платежі у більшості використовували у більш технологічно розвинутих країнах, наприклад, у Фінляндії та Естонії. У Португалії більшість учасників опитування зазначили, що вони навіть не мають гаманця з грошима та повністю покладаються на оплату за допомогою мобільного телефону.

Проте, немає особливої різниці, чи люди користуються новітніми платіжними інструментами, такими як оплата через QR-код, чи продовжують користуватися електронними гаманцями. В обох випадках готівка відходить на задній план, а електронні платіжні системи стають все більш популярними через свою швидкість, зручність та безпеку. Використання електронних платежів підвищує ефективність транзакцій, а прозорість таких систем полегшує відстежувати відмивання грошей та шахрайство.

2 ДОСВІД ОКРЕМИХ КРАЇН У СФЕРІ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

2.1 Естонія – найбільш цифровізована країна

На цю мить Естонія є однією з країн-лідерок у сфері електронних платежів. На початку 1990-х років міжбанківські розрахунки в Естонії здійснювалися за допомогою кореспондентських рахунків у клірингновому відділенні Центрального банку Естонії (ЦБЕ). Цей процес був досить трудомістким, оскільки платіжні документи доходили до ЦБЕ на папері, після чого дані переносилися на перфокарту і завантажувалися на комп'ютер. Виписки з рахунків доходили до банку наступного дня, а розрахунки із віддаленими відділеннями тривали кілька днів. Оскільки такий формат не міг існувати довго, під час грошової реформи в Естонії були написані нові правила для розрахунків та з 1 квітня по 1 жовтня 1992 року діяв перехідний період для переходу банків від паперових розрахунків до електронних [67].

Всього за декілька років після отримання незалежності Естонія створила з нуля фінансову і платіжну інфраструктуру з використанням найновітніших технологій у цій сфері. Державний проєкт Tiigrihüpe («Стрибок тигра»), що був запущений у 1996 році, був спрямований на розвиток та розширення електронних мереж обміну даними. У тому ж році в Естонії з'явився електронний кабінет та послуги електронного банкінгу. Послуги банку стали доступними 24/7 у будь-якому куточку країни. Мобільний банкінг з'явився у 2000 році, у 2002 році були введені e-ID та електронні підписи. За даними сайту Invest in Estonia [30] Естонія на 99% є безготівковою країною та лише 1% відходить до неелектронних варіантів, таких як готівкові платежі, паперові платіжні доручення та чеки, і це один з найвищих показників у світі. За даними дослідницької компанії Statista [69], приблизно 7 з 10 опитаних естонців назвали Visa та Mastercard найбільш вподобаним способом оплати. Наступним за популярністю методом платежу назвали банківський переказ, після якого йде банківська картка, електронний гаманець, мобільний платіжний застосунок,

післяплата та інші види банківських карток. Детальніше результати цього опитування можна розглянути на рис. 2.1.

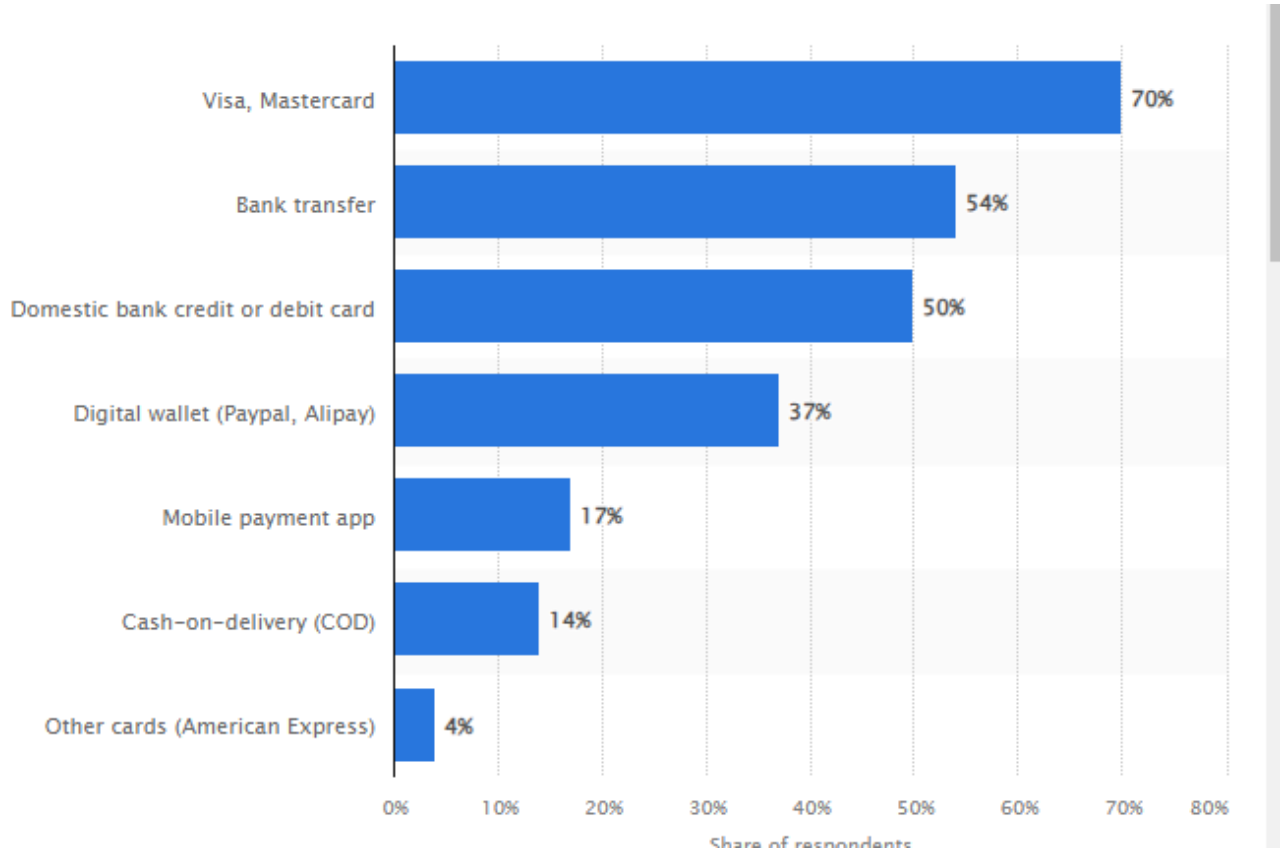

Рисунок 2.1 – Найпопулярніші електронні методи оплати в Естонії

Частка електронних платежів зростала щороку і вже з 2001 року перевищувала 90% від усієї кількості платежів [10]. Такого результату вдалося досягти через велику інтегрованість суспільства у цифрові технології: банки починають вчити дітей цифровому банкінгу та користуванню банківськими картками ще з шестирічного віку, а людей похилого віку інтегрують в електронні платежі за допомогою систематичних курсів, окрім того, всі виплати для пенсіонерів, такі як пенсії та соціальні виплати, виплачуються лише в електронному вигляді [19].

У 2014 році Естонія стала членом SEPA, тобто членом Єдиної зони платежів у євро, що дозволило людям здійснювати міжнародні платежі з тією ж швидкістю, що і всередині країни. Безконтактні банківські картки з’явилися в Естонії у 2016 році, і, якщо спочатку їх можна було використовувати для платежів на суму до 10 євро, то зараз ця сума зросла до 50 євро.

Однак, через високу швидкість переказу коштів, яка була впроваджена за допомогою SEPA, банкам довелося вводити окремі заходи для запобігання шахрайству. Системи e-ID та електронного підпису допомагають боротися з шахрайством як універсальна надійна автентифікація клієнтів, якими користуються громадяни та е-резиденти. Завдяки системі електронних посвідчень і передових технологій мобільних банків клієнти не відвідують банки фізично, а проводять всі операції у цифровому вигляді.

2.2 Індія

Індія є однією з країн-лідерок світової цифрової економіки. У 2022 році в Індії було оброблено приблизно 70 мільярдів цифрових платежів, і, за даними порталу збору даних Statista, це досить суттєве збільшення у порівнянні з 44 мільярдами у 2021 році [35]. Щодня Індія обробляє приблизно 280 мільйонів електронних транзакцій. Вже у 2018 році Індія посіла 28 місце у списку GEAR (Government E-payment Adoption Ranking) серед 73 країн [31]. Хоча готівка все ще домінує як спосіб оплати, кількість електронних платежів стрімко зростає. Так, з 30 листопада 2020 по 6 серпня 2021 року кількість електронних платежів по країні зросла на 80% [24].

Уряд активно сприяє перетворенню Індії на безготівкове суспільство, зокрема, урядом у 2015 році була запроваджена флагманська програма «Цифрова Індія». Слоган цієї програми – «Faceless, Paperless, Cashless», тобто «без облич, без паперів, без готівки» [16]. Міністерство електроніки та IT Індії також інтенсивно поширює серед населення ідеї електронних платежів. У рамках цієї програми в Індії доступні безліч способів цифрових платежів і наборів режимів електронних платежів, такі як UPI (Уніфікований інтерфейс платежів), IMPS (Служба миттєвих платежів), NETC (Національне електронне стягнення дорожнього мита), BBPS (Система оплати рахунків Бгарат), що активно зміцнюють платіжну екосистему Індії. Наприклад, UPI – система, яка об’єднує кілька банківських рахунків в єдину мобільну програму, об’єднує їхні банківські функції та полегшує проведення торговельних платежів. Для реєстрації потрібен лише телефон і картка одного з банків, активація послуги проводиться за п’ять

хвилин і є безплатною. Для переказу грошей потрібен лише номер телефону отримувача або його віртуальна платіжна адреса (VPA). UPI – це розширена версія IMPS, яка призначена для переказу коштів з використанням: переказу через віртуальну платіжну адресу; переказу через номер рахунку; переказу через номер мобільного телефона; переказу через MMID (ідентифікатор мобільних грошей) та переказу через номер Aadhaar, тобто, через ідентифікаційний номер людини.

Однак, хоч і кількість цифрових методів оплати стрімко зростає, Індія все ще стикається з певними проблемами, наприклад, дрібні продавці не наважуються використовувати POS-термінали на своїх точках продажу через їхню високу вартість, недостатню обізнаність і проблеми з підключенням. Так, на один POS-термінал в Індії приходить 358 осіб [23]. Проте, в Індії була заснована компанія Paytm, яка спеціалізується на електронних платежах, і яка зокрема запровадила опцію Paytm QR, що дозволяє покупцям просканувати QR-код продавця та оплатити покупку. Індійська дослідниця Рупа Ніцуре у своєму дослідженні зазначила, що однією із проблем впровадження електронних платежів у Індії є низький рівень залученості суспільства в електронні платежі. Однією з нагальних проблем є можливе виникнення цифрового розколу, оскільки бідна частина населення виключена з Інтернету, а отже, і з фінансової системи [44]. Однак, Резервний банк Індії оголосив про новий вид електронних платежів – так звані «розмовні платежі». Користувачі UPI зможуть промовляти усні інструкції щодо переказу коштів у свій телефон, які пізніше будуть оброблятися за допомогою штучного інтелекту (ШІ) для ініціювання транзакцій. Цей сервіс було розроблено Індійським технологічним інститутом Мадраса, він використовує мовні інструменти ШІ із відкритим кодом, та спочатку буде працювати лише з англійською мовою та хінді. Щоб уникнути проблем із відсутністю Інтернету, також була введена технологія «зв’язку ближнього поля». Ця система використовується в операціях безконтактними картками, і тепер вона дозволить створити з’єднання між двома розташованими поруч телефонами. Це допоможе проводити деякі платежі в ситуаціях, коли Інтернет слабкий або

недоступний. За словами керівника Національної платіжної корпорації Індії, ці заходи допоможуть сприяти зростанню цифрових платежів за межами найбільших міст Індії. Однак, такі нововведення вже зазнали критики, оскільки за словами громадськості, зростання цифрової інфраструктури Індії випереджає захист даних користувачів [49].

Згідно із дослідженням компанії PYMNTS, майже половина роздрібних транзакцій відбувається через платформу UPI. PYMNTS зазначили, що через «новаторську природу Індії, місцеві споживачі використовують більше функцій цифрових платежів, аніж люди в Сполучених Штатах або Великій Британії» [36]. За дослідженнями, на Індію припадає 46% світових платежів в режимі реального часу, і вона здійснює більше цифрових транзакцій, ніж будь-яка інша країна [52]. Електронні платежі в Індії сприяли економічному зростанню в країні, що, своєю чергою, позиціює Індію як лідера світової економіки у сфері електронних платежів.

2.3 Нігерія як країна, що розвивається

Однак, усі вищенаведені приклади стосуються розвинутих країн, і варто пам’ятати, що у країнах, що розвиваються, введення електронних платежів відбувалося інакше, що можна розглянути на прикладі Нігерії. Влада Нігерії за останні двадцять років приймала значні кроки до модернізації платіжної системи, оскільки до цього система мала купу проблем та не користувалася довірою населення, починаючи від відсутності адекватної правової підтримки, довіри до людського фактора, цілісності передавання даних та завершуючи відсутністю функціональної сумісності. Системи платежів в Нігерії були засновані на готівці як через позитивні причини, так і через негативні, де до позитивних причин можна віднести миттєву конвертацію грошей в інші форми вартості без посередництва фінансових установ, а до негативних – відсутність як грамотності населення, так і розуміння інших безготівкових інструментів [48]. Перехід від суспільства, в якому 90% готівки зберігається за межами банківських установ до безготівкового суспільства – це велика зміна, тому на плечі влади лягла задача зробити так, щоб ця система стала економічно вигідною.

Результатом цієї модернізації стали видатні зміни: перехід від рудиментарних систем платежів до новітніх систем електронних платежів, а темпи розвитку описують як вкрай високі, враховуючи наявні проблеми в країні та короткі терміни. Для прикладу, картки із пін-кодом, які наразі широко використовуються, були наявні в Нігерії за п’ять років до їхньої появи в США.

У пошуках надійної та ефективної платіжної системи, яка мала на меті збільшити розвиток платіжних інструментів, які могли б відповідати потребам користувачів, був створений Комітет національних платіжних систем (National Payments System Committee (NPSC)) для сприяння розвитку платіжних систем Нігерії. Розвиток електронних платежів у Нігерії почався з 2009 року, коли владою була підписана директива, через яку усі платежі в державних установах мали проводитися в електронному виді, після чого були створені конкретні правила та процедури. Однак, ці правила регулярно змінювалися в міру зміни ситуації в країні та надходження скарг від населення [14].

У 2011 році федеральне керівництво пропонує перехід до цифрової економіки, який був реалізований у 2012 році в рамках NPSV (National Payment System Vision 2020), метою якого було створення безпечного, ефективного та дієвого механізму для зручного здійснення платежів, та своєчасне отримання цих платежів з будь-якого місця через цифрові платформи Нігерії. До 2014 року ця політика безготівкової оплати була ефективно та успішно реалізована в Абуджі, столиці Нігерії та деяких окремих штатах Нігерії, таких як Ріверс, Абіа, Кано та Огун, та набирала обертів з поширенням Інтернету. В Нігерії за сприяння NIBSS (Система міжбанківських розрахунків Нігерії) були впроваджені наступні методи електронних платежів: банкомати, електронний переказ коштів NIBSS, миттєвий платіжний переказ NIBSS, PoS-термінали, послуги автоматичних платежів NIBSS, смарткарти, електронні чеки й так далі [25].

З роками цифрова платіжна система Нігерії досягла такого рівня, що користувачі все частіше віддають перевагу проведенню грошових операцій без відвідування банків офлайн. Дослідження Одіор та Банусо [46], Ечекоба та Езу [25], та Нкванко [45] показують, що цифрова платіжна система змогла завоювати

визнання користувачів попри наявні проблеми. Нові платіжні системи зросли у популярності; так, сума транзакцій у банкоматах складала 399,7 млрд найр у 2010 році, і у 2019 зросла до 6512 млрд найр, а сума мобільних платежів зросла з 6,65 млрд до 5,080 трлн за той же період [17].

Однак, попри наявний успіх введення та розвитку електронних платежів в Нігерії, проблема відсутності комп'ютерної та цифрової грамотності населення, низькі доходи населення та великий обсяг готівкових транзакцій все ще постають досить великою проблемою. На цей рік лише 47% населення має доступ до Інтернету, що сильно впливає на поширеність електронних платежів. Серйозною проблемою також є нестабільність нігерійської найри щодо долара США.

А все таки, підтримка держави та дефіцит паперових грошей каталізували електронні платежі. Система банківських переказів в Нігерії працює цілодобово, а нові альтернативні методи оплати через мобільні платформи пропонують ще більше можливостей для клієнтів, а отже, сприяють зростанню електронних платежів. Цифровий прогрес Нігерії не обмежився лише її кордонами, а позитивно впливає на розвиток усього регіону Західної Африки, стимулюючи введення електронних платежів у своїх країнах.

2.4 Досвід України

На початку 1990-х років всі розрахунки між українськими банками велися виключно за допомогою паперових документів, що призводило до великих затримок, оскільки на це витрачалося дуже багато часу, а через підроблені авізо (тобто, через фальшиві повідомлення про розрахункові операції) збитки від шахрайства ставали все більшими. Через це виникла серйозна потреба у створенні своєї системи електронних платежів, яку створив Національний банк України (НБУ) у 1992 році, яку так і назвали – Система Електронних Платежів (СЕП) [3]. У 1994 році ця система запрацювала на повну потужність, і дозволяла ефективніше використовувати ресурси банків, а проходження платежів займало приблизно один день. Так Україна стала першою з пострадянських країн, яка мала власну державну систему електронних міжбанківських розрахунків. Досить швидко постало питання захисту даних в СЕП, тож вже в 1996 році були

впровадженні електронні підписи, які використовувалися під час транспортування електронних платіжних документів. У 2006 році СЕП була трансформована в СЕП-2, яка містила новітні технології та могла обробляти значно більшу кількість платежів. У 2017 році відбувся перехід на СЕП-3, яка у порівнянні із СЕП-2 мала більшу продуктивність, відмовостійкість та безпеку, а з 1 квітня 2023 року в Україні працює СЕП-4, створена на базі стандарту ISO 20022. СЕП-4 створена для майбутнього приєднання України до вищезгаданої SEPA, а також для можливості швидкого та цілодобового функціонування (оскільки СЕП-3 працювала лише 23 години на добу).

В Україні працюють сорок дві системи електронних платежів, серед яких як міжнародні карткові системи платежів (MasterCard, Visa), так і системи переказу грошей UnionPay та Western Union. У 2019 році за статистикою НБУ стало відомо, що в Україні найбільша кількість платежів здійснюється через карткові платіжні системи, а за допомогою СЕП – найменша. Це відбувається у тому числі через монополізацію ринку міжнародними платіжними системами.

Окрім того, існує декілька проблем з використанням систем електронних платежів в Україні, серед яких недостатньо розвинене законодавство, яке має покращити статус українських платіжних систем на ринку, та відсутність фінансової та ІТ-грамотності у населення, які через недолік знань випадають з новітньої фінансової сфери. З усім тим, навіть ситуація в країні не заважає продовжувати розвиток СЕП і фінансувати навчання з фінансової та ІТ грамотності для населення, що означає неминучий розвиток функціонування платіжних систем і більш стійку позицію України на фінансовому світовому ринку.

3 НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ У СФЕРІ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

3.1 Стандарт PCI DSS

Стандарт PCI DSS (Payment Card Industry Data Security Standard) – це сукупність вимог щодо забезпечення безпеки даних власників платіжних карток, які зберігаються, передаються та/або обробляються в інформаційній інфраструктурі організацій. Цей стандарт – загальноприйнятий в усіх країнах ЄС та є обов'язковим для законного ведення бізнесу та був розроблений для заохочення та підвищення безпеки і сприяння широкому впровадженню узгоджених заходів безпеки даних по всьому світу. Основне завдання стандарту PCI DSS – це забезпечення безпеки мережевої інфраструктури й захист даних власників платіжних карток, що зберігаються, оскільки це найбільш вразливі місця, що безпосередньо загрожують конфіденційності та втраті коштів. Для того, щоб мати гарантію безпеки збереження коштів своїх клієнтів, такі компанії, як, наприклад, Visa і MasterCard вимагають від торгових підприємств і різних постачальників послуг, які приймають платежі від покупців через дані платіжні системи, відповідати стандарту PCI DSS. Іншими словами, без наявності у компанії сертифіката PCI DSS банки не стануть надавати послуги з приймання платежів за допомогою платіжних карток, а отже, клієнти не зможуть розрахуватися за послуги прямо на сайті.

Рада стандартів безпеки PCI (PCI SSC) – це глобальний форум, який об'єднується для розробки, поширення та надання допомоги в розумінні стандартів безпеки для захисту платіжних рахунків. PCI SSC підтримує, розвиває та просуває стандарти безпеки індустрії платіжних карток, та надає важливі інструменти, необхідні для провадження стандартів, такі як: анкети для оцінки, програми сертифікації, інструменти для навчання. PCI SCC очолює виконавчий комітет, до складу якого входять представники наступних компаній: America Express, JBC International, Mastercard, UnionPay, Visa Inc. і т.д.

Стандарт PCI DSS містить в собі всього 12 точних, деталізованих вимог [1]:

- Захист локальної мережі;
- Конфігурація компонентів інформаційної структури;
- Захист збережених даних власників карток;
- Захист переданих даних власників карток;
- Антивірусний захист інформаційної інфраструктури;
- Розробка і підтримка інформаційних систем;
- Управління доступом до даних власників карток;
- Механізми автентифікації;
- Фізичний захист інформаційної інфраструктури;
- Управління інформаційною безпекою;
- Ведення журналу подій і процесів;
- Контроль захищеності інформаційної інфраструктури.

Для захисту платіжного рахунку за допомогою PCI DSS виконуються чотири кроки:

1) Оцінка – визначення усіх місць розташування даних платіжних рахунків, проведення інвентаризації усіх IT-активів та бізнес-процесів, пов’язаних з обробкою платежів, їхній аналіз на наявність вразливостей, які можуть розкрити дані платіжних рахунків, впровадження або оновлення необхідних заходів контролю.

2) Усунення – виявлення та усунення будь-яких прогалин у сфері безпеки, усунення виявлених вразливостей, безпечне видалення непотрібних сховищ платіжних даних, впровадження безпечних бізнес-процесів.

3) Звіт – документування деталей оцінки та виправлення, а також подання звітів про відповідність організації, що приймає вимоги (зазвичай це банк-еквайр або платіжний бренд).

4) Моніторинг та підтримка – підтвердження того, що впроваджені для захисту даних платіжного рахунку та середовища заходи безпеки продовжують ефективно та належним чином функціонувати протягом року. Ці процеси мають

бути впроваджені як частина загальної стратегії безпеки організації, щоб допомогти забезпечити захист на постійній основі.

Стандарти безпеки PCI підвищують безпеку платежів завдяки надійним комплексним вимогам до контролю безпеки, процедурам оцінки та допоміжним матеріалам. Стандарти визначають засоби контролю безпеки та процеси для суб'єктів, залучених до платіжної екосистеми, а також вимоги до розробників постачальників рішень щодо створення та безпечного керування платіжними пристроями, програмним забезпеченням рішень для індустрії платежів. Частину стандартів безпеки PCI можна описати наступним чином.

Стандарт безпеки даних PCI – ефективна структура для розробки надійного процесу безпеки даних платіжного рахунку, включаючи запобігання, виявлення та відповідне реагування на інциденти безпеки.

Безпека транзакцій PIN-коду (PTS – PIN Transaction Security) – вимоги безпеки, зосереджені на характеристиках управління пристроями, які використовуються для захисту PIN-кодів власників карток (персональних ідентифікаційних номерів) та інших конфіденційних платіжних даних. Стандарт PTS Point of Interaction (POI) охоплює пристрої, включаючи PIN-термінали, POS-пристрої та платіжні термінали без нагляду. Стандарт PTS Hardware Security Module (HSM) визначає вимоги безпеки для HSM для забезпечення конфіденційності та цілісності даних під час таких дій, як фінансові операції та персоналізація платіжних карток.

Software Security Framework – набір стандартів програм для безпечного проєктування, розробки та обслуговування чинного та майбутнього платіжного програмного забезпечення. Включає стандарт безпечного життєвого циклу програмного забезпечення (Secure SLC) та стандарт безпечного програмного забезпечення.

Шифрування «точка-точка» (P2PE) – комплексний набір вимог безпеки для перевірки рішень P2PE, щоб захистити дані платіжного рахунку за допомогою шифрування, починаючи з місця, де вони фіксуються в платіжному терміналі, допоки не будуть розшифровані в середовищі постачальника рішення.

Мобільні стандарти – включають стандарти безконтактних платежів на COTS (CPoC) програмного введення PIN-коду на COTS (SPoC) для рішень приймання мобільних платежів на комерційних готових (COTS) пристроях (наприклад, смартфонах або планшетах) у середовище, яке відвідує торговець.

Інші стандарти – стандарти PCI, що визначають контроль вимоги до тестування для безпеки PIN-коду, виробництва та надання фізичних логічних карток, постачальників послуг маркерів безпеки доступу (3D Secure).

PCI DSS було розроблено для заохочення та підвищення безпеки платіжних рахунків і сприяння широкому впровадженню узгоджених заходів безпеки даних у всьому світі. PCI DSS надає базові технічні та операційні вимоги, призначені для захисту даних платіжних рахунків [51].

Таблиця 3.1 – Вимоги PCI DSS

Мета	Вимоги PCI DSS
Створити та обслуговувати безпечну мережу та системи	1) Встановіть та підтримуйте засоби контролю безпеки мереж. 2) Застосуйте безпечну конфігурацію до усіх компонентів системи.
Захистити дані облікового запису	3) Захистіть збережені облікові дані. 4) Захистіть дані власника за допомогою надійної криптографії під час передачі даних.
Підтримати програму керування вразливостями	5) Захистіть усі системи та мережі від шкідливого ПЗ. 6) Розробіть та підтримайте безпечні системи та ПЗ.
Впровадити суворі заходи контролю доступу	7) Обмежте доступ бізнесу до компонентів системи та даних про власника картки. 8) Ідентифікуйте користувачів та проведіть автентифікацію доступу до компонентів системи.

Продовження таблиці 3.1 – Вимоги PCI DSS

Впровадити суворі заходи контролю доступу	9) Обмежте фізичний доступ до даних власника картки.
Впровадити суворі заходи контролю доступу	10) Обмежте доступ бізнесу до компонентів системи та даних про власника картки. 11) Ідентифікуйте користувачів та проведіть автентифікацію доступу до компонентів системи. 12) Обмежте фізичний доступ до даних власника картки.
Регулярно перевіряти та тестувати мережі	13) Реєструйте та відстежуйте доступи до компонентів системи та даних власників карток. 14) Регулярно перевіряйте безпеку систем мережі.
Дотримуватися політики інформаційної безпеки	15) Дотримуйтеся інформаційної безпеки за допомогою організаційної політики.

3.2 Рекомендації від Європейської Бізнес Асоціації

У 2014 році EBA (Європейська Бізнес Асоціація) випустила консультаційний документ щодо рекомендацій до безпеки Інтернет-платежів під назвою «Final guidelines on the security of internet payments». Ці рекомендації базувалися на рекомендаціях, що були опубліковані Європейським форумом з безпеки роздрібних платежів (SecuRe Pay). Конвертація до рекомендацій EBA мала на меті забезпечити міцну правову базу до послідовного впровадження вимог у всіх країнах-учасницях ЄС. У другому розділі даного документу зазначені наступні рекомендації [29]:

Управління: Постачальники платіжних послуг повинні впроваджувати та переглядати офіційну політику безпеки для Інтернет-платежів на регулярній основі – політика безпеки повинна бути належним чином задокументована, регулярно переглядатися та затверджуватися вищим керівництвом і має визначати цілі безпеки та схильність до ризику.

Оцінка ризику: Постачальники послуг мають проводити та документувати ретельну оцінку ризику щодо безпеки Інтернет-платежів як до встановлення послуги, так і після цього – постачальники послуг через свою функцію управління ризиками повинні проводити та документувати детальну оцінку ризиків для Інтернет-платежів та пов'язаних послуг. Постачальники платіжних послуг мають враховувати результати постійного моніторингу загроз безпеці, пов'язаних з платіжними послугами в Інтернеті, беручи до уваги технологічні рішення, які вони використовують, послуги, передані зовнішнім постачальникам та технічне середовище клієнтів. Постачальники послуг також мають оцінювати ризики, пов'язані з вибраними технологічними платформами, архітектурою застосунків, процедурами та методами програмування на своєму боці (таких як SQL-ін'єкції, XSS, переповнення буфера тощо) та боці клієнтів (наприклад, ризики, пов'язані з використанням плагінів браузера, зовнішніх посилань та мультимедійних програм), а також результати моніторингу інцидентів безпеки. Після цього постачальники платіжних послуг повинні визначити, чи потрібні зміни в наявних заходах безпеки та використаних технологіях і, якщо так, то якою мірою. Оцінка ризиків повинна враховувати необхідність захисту та безпеки конфіденційних платіжних даних. Загальний перегляд оцінки ризику повинен проводитися щонайменше раз на рік.

Моніторинг інцидентів: Постачальники повинні забезпечувати постійний моніторинг, обробку та подальші дії у зв'язку з інцидентами безпеки, включно зі скаргами клієнтів, що пов'язані з безпекою. Постачальники платіжних послуг мають встановити процедуру звітування про такі інциденти керівництву, а у разі великих інцидентів порушення безпеки – у компетентні органи. Постачальники платіжних послуг повинні мати процес моніторингу, обробки та подальших дій щодо інцидентів безпеки та скарг клієнтів, пов'язаних з безпекою, повідомляти про такі інциденти керівництву і мати процедуру негайного сповіщення компетентних органів (тобто органів нагляду та захисту даних), у разі серйозних інцидентів безпеки платежів щодо наданих платіжних послуг, а у випадку

виникнення таких інцидентів мати процедуру співпраці з компетентними органами.

Контроль пом’якшення ризиків: Постачальники платіжних послуг повинні впроваджувати заходи безпеки відповідно до своєї політики безпеки, щоб зменшити виявлені ризики. Ці заходи повинні включати декілька рівнів оборони, де при провалі одного рівня буде впроваджений наступний – при створенні, розробці та обслуговуванні послуг для Інтернет-платежів постачальники платіжних послуг повинні приділяти особливу увагу адекватному розподілу обов’язків у середовищах ІТ-технологій, та належному впровадженні принципу «найменших привілеїв» як основу для надійної ідентифікації та управління доступом, де принцип «найменших привілеїв» означає, що кожна програма та кожен привілейований користувач системи має працювати, використовуючи найменшу кількість привілеїв, необхідну для виконання завдання [56]. Також постачальники платіжних послуг повинні мати відповідні рішення безпеки для захисту мереж, вебсайтів, серверів та каналів зв’язку від атак, та позбавити сервери усіх зайвих функцій, щоб мінімізувати вразливі місця. Доступ різних програм до потрібних даних та ресурсів має бути зведений до мінімуму відповідно до принципу «найменших привілеїв». Для обмеження використання шахрайських вебсайтів, транзакційні вебсайти, що пропонують послуги Інтернет-платежів, мають ідентифікуватися за допомогою розширених сертифікатів або інших методів автентифікації. Постачальники платіжних послуг повинні мати процеси для моніторингу, відстеження та обмеження доступу до конфіденційних платіжних даних і фізичних критичних ресурсів та створювати, зберігати та аналізувати журнали аудиту. Заходи безпеки для платіжних Інтернет-сервісів мають тестуватися під наглядом функції управління ризиками, щоб переконатися у їхній надійності та ефективності, а усі зміни мають підлягати офіційному процесу управління змінами, який гарантує планування, перевірку, документування та функціонування змін. На основі внесених змін та помічених загроз, тести слід регулярно повторювати й включати сценарії відомих потенційних атак. Окрім цього, якщо постачальник

платіжних послуг дізнається, що продавець не має необхідних заходів безпеки, він повинен вжити заходів для забезпечення виконання цього договірного зобов'язання або розірвати договір.

Відстежуваність: Постачальники платіжних послуг повинні мати процеси, що гарантують, що усі транзакції та електронне доручення належним чином відстежуються – постачальники платіжних послуг повинні гарантувати, що їхні послуги включають механізми для детального запису даних транзакцій та електронних доручень, включно із порядковим номером транзакції та часовими мітками, а також впровадити файли журналів, які дозволяють відстежувати будь-яке додавання, зміну або видалення даних транзакцій. Програми для аналізу та оцінки файлів журналів мають бути доступні лише авторизованому персоналу.

Первинна ідентифікація клієнта: Клієнти повинні бути належним чином ідентифіковані згідно з Європейським законодавством про боротьбу з відмиванням грошей (наприклад, згідно з Директивою (ЄС) 2015/849 Європейського Парламенту та Ради від 20 травня 2015 року про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму, яка вносить зміни до Регламенту (ЄС) № 648/2012 Європейського Парламенту та Ради та скасування Директиви 2005/60/ЄС Європейського Парламенту та Ради та Директиви Комісії 2006/70/ЄС), та мають належним чином підтвердити свою готовність здійснити Інтернет-платежі, перш ніж отримати доступ до послуг. Постачальники платіжних послуг повинні надавати клієнту адекватну «попередню», «регулярну», або, де це можливо, «спеціальну» інформацію про необхідні вимоги для здійснення безпечних платіжних транзакцій в Інтернеті та властиві цьому ризики – Постачальники платіжних послуг повинні переконатися, що клієнт пройшов процедури перевірки клієнта та надав належні документи, що посвідчують особу (наприклад, паспорт, ID-карту або електронний підпис), перш ніж отримати доступ до Інтернет-платежів. Постачальники платіжних послуг також мають переконатися, що клієнту були надані усі конкретні відомості щодо Інтернет-платежів (інформація про необхідне програмне забезпечення, покроковий опис

процедури клієнта для авторизації платіжної операції, вказівки щодо безпечного використання усього наданого клієнту забезпечення), та перевірити, що у контракті з клієнтом вказано про можливість заблокування платіжної операції/інструменту з міркувань безпеки, та як клієнт може звернутися до постачальника, щоб розблокувати транзакцію.

Надійна автентифікація клієнта: Ініціалізація Інтернет-платежів, та доступ до конфіденційних платіжних даних повинні бути захищені надійною автентифікацією клієнтів. Постачальники послуг повинні мати відповідну надійну процедуру автентифікації клієнта – постачальники платіжних послуг повинні виконувати надійну автентифікацію клієнта для авторизації клієнтом платіжних транзакцій в Інтернеті, але за необхідності розглянути альтернативні заходи автентифікації клієнта для транзакцій між двома рахунками одного клієнта та переказів у межах одного постачальника послуг. Для отримання доступу до конфіденційних платіжних даних або для їхньої зміни, потрібна надійна автентифікація клієнта. Усі випущені картки мають бути технічно готовими до використання із надійною автентифікацією. Постачальники платіжних послуг у випадку електронних гаманців мають підтримувати надійну автентифікацію клієнтів, коли клієнти входять до платіжних служб гаманця або здійснюють операції з карткою через Інтернет. Використання альтернативних засобів автентифікації можливе для заздалегідь визначених категорій транзакцій з низьким рівнем ризику. Для віртуальних карток початкова реєстрація має відбуватися у безпечному та надійному середовищі, а для генерації даних віртуальних карток повинна бути присутня надійна автентифікація клієнта. Постачальники платіжних послуг також мають забезпечити належну двосторонню автентифікацію під час спілкування з продавцями з метою ініціювання Інтернет-платежів та доступу до конфіденційних платіжних даних, де двостороння автентифікація – метод автентифікації, в якому сервер автентифікує себе для клієнта, а клієнт для сервера, щоб встановити безпечний зашифрований канал між клієнтом та сервером [74].

Реєстрація та надання інструментів автентифікації та/або програмного забезпечення, що надається клієнту: Постачальники платіжних послуг мають впевнитися, що реєстрація клієнта та початкове надання інструментів автентифікації, необхідних для користування послугою Інтернет-платежів та/або доставлення необхідного для оплати програмного забезпечення, здійснюється безпечно – відповідні процедури мають відбуватися у безпечному та надійному середовищі, беручі до уваги можливі ризики, що пов’язані з пристроями, які постачальники платіжних послуг не контролюють. Процедури доставлення програмного забезпечення, персоналізованих пристроїв для оплати та даних облікових записів мають відбуватися швидко та безпечно, а програмне забезпечення, що передається через Інтернет, має містити електронний підпис постачальника платіжних послуг, щоб клієнт міг перевірити його автентичність та незмінність.

Спроби входу, тайм-аут сеансу, дійсність автентифікації: Постачальники платіжних послуг мають обмежити кількість спроб автентифікації або входу в систему, визначити правила для тайм-ауту сеансу платіжної послуги та встановити часові обмеження для дійсності автентифікації – постачальники платіжних послуг мають переконатися, що термін дії одноразових паролів (якщо такі використовуються) обмежений суворо необхідним мінімумом, встановити максимальну кількість невдалих спроб входу та ідентифікації, після якої доступ до послуг Інтернет-платежів блокується та максимальний період, після якого неактивний сеанс автоматично припиняється.

Моніторинг транзакцій: Механізми моніторингу транзакцій, призначенні для виявлення, запобігання та блокування шахрайських платіжних транзакцій, повинні працювати до остаточної авторизації постачальника платіжних послуг; підозріла операція або операція з високим ризиком повинна підлягати спеціальній процедурі перевірки та оцінки. Еквівалентні механізми моніторингу безпеки та авторизації також повинні бути на місці видачі електронних доручень – постачальники платіжних послуг повинні використовувати системи виявлення та запобігання шахрайству для виявлення підозрілих транзакцій. Ці системи

мають базуватися на певних правилах (наприклад, містити чорні списки викрадених даних карток), та відстежувати ненормальну поведінку клієнта або його пристрою (наприклад, зміна IP-адреси або нестандартні дані транзакції). Такі системи мають мати можливість виявити ознаки зараження зловмисним ПЗ та відстежити відомі сценарії шахрайства. Постачальники платіжних послуг мають виконувати перевірку цими системами протягом відповідного часу, щоб не затримувати виконання транзакції. Якщо транзакція була визнана як потенційно шахрайська та заблокована, постачальники платіжних послуг мають розблокувати цю транзакцію якомога швидше після розв'язання проблем безпеки.

Захист конфіденційних платіжних даних: Конфіденційні платіжні дані повинні бути захищені під час зберігання, обробки та передачі – усі дані, що використовуються для ідентифікації та автентифікації клієнта, повинні бути належним чином захищені від крадіжки або несанкціонованої модифікації. Постачальники послуг також повинні забезпечити безпечне наскрізне шифрування під час сеансу обміну конфіденційними даними між сторонами, з метою забезпечення конфіденційності та цілісності даних, використовуючи надійні та визнані методи шифрування. Наскрізне шифрування – той вид шифрування, під час якого доступ до переданої інформації має лише відправник та отримувач. При відправленні повідомлення шифрується, а розшифровується при надходженні до одержувача [4].

Навчання та спілкування з клієнтами: Постачальники платіжних послуг повинні надавати допомогу та вказівки клієнтам, якщо це необхідно, щодо безпечного використання платіжних послуг. Постачальники повинні спілкуватися зі своїми клієнтами таким чином, щоб запевнити їх у достовірності отриманих повідомлень – постачальники платіжних послуг мають мати щонайменше один захищений канал зв'язку з клієнтами щодо безпечного та правильного використання послуг Інтернет-платежів та повинні інформувати клієнтів про цей канал зв'язку. Постачальники платіжних послуг повинні пояснити клієнту процедуру повідомлення зі сторони клієнтів про шахрайські

інциденти та аномалії під час сеансу платіжних послуг, процедуру інформування клієнта про шахрайські транзакції з боку клієнта або попередження клієнта про можливі шахрайські атаки. Постачальники послуг повинні надавати допомогу клієнтам у їхніх скаргах, запитах та питаннях про аномалії та інциденти, що пов'язані з Інтернет-платежами, та ініціювати програми навчання та обізнаності клієнтів щодо необхідності захисту своїх конфіденційних даних, належного рівня безпеки свого пристрою та можливих видів загроз та ризиків [29].

Дані рекомендації були впроваджені в ЄС з 1 серпня 2015 року і застосовуються до державних органів платіжних схем та усіх постачальників платіжних послуг в ЄС. Ці рекомендації були інтегровані у вже наявні системи нагляду за платіжними схемами та розглядаються як мінімальні вимоги до послуг Інтернет-платежів.

3.3 SWIFT CSCF

3.3.1 Загальний опис SWIFT CSCF

Однак, вищезгадані рекомендації стосуються виключно Європейського союзу, тож варто розглянути систему електронних платежів, що поширена по всьому світу. Такою системою є міжнародна міжбанківська система SWIFT (Society for Worldwide Interbank Financial Telecommunications). Ця система призначена для швидких транскордонних платежів. До системи SWIFT доєдналися більш ніж 11 тисяч банківських установ з 200 країн. У 2016 році у відповідь на збільшення кількості кібератак на користувачів SWIFT була запущена програма CSP (Customer Security Program), мета якої – підтримувати відповідний рівень кібербезпеки для всіх користувачів, знизити ризик кібератак та мінімізувати фінансові наслідки шахрайських операцій CSP також встановлює набір засобів контролю безпеки клієнтів Customer Security Controls Framework (CSCF), який містить набір обов'язкових та рекомендаційних заходів безпеки для користувачів SWIFT. Обов'язкові заходи безпеки встановлюють базовий рівень безпеки та повинні бути реалізовані усіма користувачами SWIFT. Рекомендаційні засоби безпеки не є обов'язковими та лише рекомендовані для

застосування, однак зі змінами засобів контролю такі заходи можуть теж стати обов’язковими.

SWIFT CSCF базується на міжнародних стандартах інформаційної безпеки, таких як NIST Cybersecurity Framework v1.1, ISO 27002 та PCI DSS 3.2.1. Через мінливий характер загроз та впровадження нових технологій, засоби контролю регулярно оновлюються, змінюються та публікуються у нових версіях документа CSCF, останнє таке оновлення відбулося 7 липня 2023 року. SWIFT рекомендує користувачам користуватися саме останньою версією, а щоб підтримати впровадження заходів безпеки, був розроблений процес, який вимагає від користувачів підтвердити відповідність обов’язковим засобам безпеки. Щороку користувачі мають пройти атестацію безпеки за допомогою застосунку KYC-SA (KYC Security Attestation).

Засоби контролю безпеки ґрунтуються на трьох основних структурних цілях, що підтримуються сімома принципами безпеки. Принципи детально описують найбільш пріоритетні напрямки в межах кожної цілі. 32 засоби контролю безпеки (з яких 25 – обов’язкові засоби контролю, а 7 – рекомендаційні, які виділені *курсивом*) лежать в основі цих цілей та принципів. Цілі, принципи та відповідні заходи безпеки виглядають наступним чином:

1) Захистити своє середовище:
   - A Обмежити доступ до Інтернету та відокремити критичні системи від загального IT-середовища
     a) Захист середовища SWIFT
     b) Контроль привілейованих облікових записів операційної системи
     c) Віртуалізація або захист хмарної платформи
     d) Обмеження доступу до Інтернету
     e) Захист середовища споживача
   - B Зменшити ділянку атаки та кількість вразливостей.
     a) Безпека внутрішнього потоку даних
     b) Оновлення безпеки

c) Посилення системи

d) Безпека потоку даних бек-офісу

e) Захист даних зовнішньої передачі

f) Конфіденційність та цілісність сеансу оператора

g) Сканування вразливостей

h) Захист критичних дій при передачі стороннім виконавцям

i) Засоби контролю транзакцій

j) Посилення застосунку

k) Контроль діяльності RMA (Relationship Management Applications)

C Фізично захистити середовище.

a) Фізичний захист

2) Знати та обмежувати доступ:

A Запобігти компрометації облікових даних.

a) Політика паролів

b) Багатофакторна автентифікація

B Керувати ідентифікаторами та розділяти привілеї.

a) Логічний контроль доступу

b) Керування токенами

c) Процес перевірки персоналу

d) Фізичний та логічний захист сховища паролів.

3) Виявляти та реагувати:

A Виявляти аномальні активності в системі або записах про транзакції

a) Захист від шкідливих програм

b) Цілісність програмного забезпечення

c) Цілісність бази даних

d) Ведення журналу та моніторинг

e) Виявлення вторгнень

B Скласти план реагування на інциденти та обміни інформацією.

a) Планування реагування на кіберінциденти

b) Навчання та підвищення рівня безпеки

c) Тестування на проникнення

d) Оцінка ризику на основі сценарію

SWIFT задокументували найпоширеніші чинники ризику у межах кожного засобу контролю безпеки. Усунення цих ризиків спрямоване на запобігання або мінімізацію потенційних шахрайських бізнес-наслідків, таких як:

- Несанкціоноване надсилання або модифікація фінансових операцій.
- Обробка змінених або неавторизованих вхідних транзакцій SWIFT.
- Операції з неавторизованим контрагентом.
- Порушення конфіденційності.
- Порушення цілісності.

Наступні компоненти входять у сферу дії засобів контролю безпеки:

1) Інфраструктура користувача SWIFT – колекція локальних або віддалених специфічних компонентів SWIFT, якими керують користувачі. Прикладами налаштування інфраструктури користувача SWIFT можна назвати зону безпеки SWIFT (зона, що відокремлює системи, пов’язані зі SWIFT від ширшого корпоративного середовища), інтерфейс обміну повідомлення (ПЗ, що підтримує використання стандартів повідомлень через служби обміну миттєвими повідомленнями) та інтерфейс зв’язку (ПЗ, що забезпечує зв’язок між мережею SWIFTNet та програмним забезпеченням інтерфейсу обміну повідомленнями).

2) Оператор – кінцеві користувачі та адміністратори, що безпосередньо взаємодіють з інфраструктурою користувача SWIFT на рівні програми або операційної системи.

3) ПК оператора – обчислювальний пристрій кінцевого користувача або адміністратора, який використовується для виконання своїх обов’язків оператора або користувача.

4) Рівень обміну даними – транспортування даних між пов’язаними зі SWIFT компонентами.

5) Сервер проміжного локального забезпечення – реалізація локальних систем проміжного програмного забезпечення, таких як сервер та бек-офіс користувача.

6) Сервер передачі файлів – сервер, що використовується для обміну файлами між пов’язаними зі SWIFT компонентами.

Засоби безпеки не застосовуються до цих компонентів:

1) Бек-офіс користувача – системи, відповідальні за бізнес-логіку, створення транзакцій та інші дії, що відбуваються перед передачею користувача у SWIFT.

2) Загальне корпоративне IT-середовище – інфраструктура, що використовується для підтримки ширшої організації.

3.3.2 Рекомендаційні засоби безпеки від SWIFT

SWIFT CSCF містить детальний опис кожного із засобів контролю безпеки, компоненти, на які впливає цей засіб безпеки, керівництво з впровадження цього засобу безпеки та додаткові заходи з вдосконалення цього засобу безпеки, однак, ми вважаємо за доцільне розглянути лише ті засоби безпеки, які SWIFT виділили як «рекомендаційні», тобто ті, що не обов’язкові для імплементації клієнтом у свою систему. Першим таким засобом контролю безпеки є безпека потоку даних бек-офісу. Метою цього засобу є забезпечення конфіденційності, цілісності та взаємної автентичності даних, що передаються між локальними або віддаленими компонентами інфраструктури SWIFT та бек-офісами, до яких вони підключаються. Цей засіб контролю безпеки безпосередньо впливає на обмін даними про бізнес-транзакції між локальними або віддаленими ланками бек-офісу, до яких вони відключені або безпосередньо, або через деяку кількість серверів-мостів. SWIFT пропонує користувачам захистити обмін даних за допомогою налаштування інвентаризації потоків даних між компонентами, пов’язаними зі SWIFT, оцінити безпеку кожного потоку, а для потоків, які не захищені належним чином, визначити план, ґрунтуючись на можливих ризиках. Можливими рішеннями можуть бути впровадження безпечних механізмів та протоколів та перенесення застарілих потоків до

безпечних механізмів та протоколів. У випадку впровадження наскрізного захисту між першим переходом бек-офісу та компонентом безпечної зони рекомендується впровадити захисний механізм для забезпечення цілісності, конфіденційності та автентифікацію даних (наприклад AES-GSM), та врахувати механізм виявлення можливих атак повторного відтворення. Атака повторного відтворення – підвид атаки man-in-the-middle, під час якого зловмисник з несанкціонованим доступом перехоплює трафік та надсилає повідомлення до початкового пункту призначення під виглядом автентичних повідомлень.

Наступним засобом контролю безпеки є захист даних зовнішньої передачі, мета якого – захист конфіденційності конфіденційних даних, пов’язаних зі SWIFT, які передаються або зберігаються за межами безпечної зони як частина операційних процесів, наприклад, резервних копій, деталей бізнес операцій та облікових даних. У випадку відсутності даного заходу контролю безпеки можлива компрометація надійних резервних даних та втрата конфіденційності конфіденційних даних. Найпростішим способом захисту таких даних є забезпечення шифрування даних на рівні сховища, в якому будуть зберігатися ці дані.

Третій рекомендаційний засіб контролю безпеки – контроль діяльності RMA. RMA – сервіс застосунків від SWIFT, який дозволяє фінансовим установам, що обмінюються даними, контролювати ці обміни. Мета впровадження даного заходу контролю безпеки – максимально обмежити транзакційну діяльність з перевіреними та затвердженими контрагентами. Це необхідно для зменшення можливості надсилання та отримання шахрайських транзакцій.

Наступний консультаційний засіб контролю безпеки – процес перевірки персоналу, щоб, наскільки це максимально можливо, забезпечити надійність персоналу, який керує середовищем SWIFT, регулярно перевіряючи персонал для зниження ризику внутрішніх загроз. Ці перевірки можуть включати як підтвердження особи, кваліфікації цієї особи та підтвердження минулої трудової

діяльності, так і перевірки кримінальних проваджень особи та участі у бізнесах, які можуть призвести до конфлікту інтересів.

П’ятий консультаційний засіб контролю безпеки – виявлення вторгнень, мета якого – виявлення та стримання аномальної мережевої активності у локальному або віддаленому середовищі SWIFT. Впровадити даний засіб контролю безпеки можливо завдяки системі виявлення вторгнень, яка може охоплювати методи NIDS, HIDS, EDR, XDR або комбінації цих методів. NIDS – система виявлення вторгнень на мережу – встановлює базову лінію нормальної роботи та надсилає сповіщення про виявлення ненормальної активності в мережах. HIDS (система виявлення вторгнень на хост) призначена для захисту окремої системи, на якій вони реалізовані. Кінцеве та розширене виявлення та реагування (EDR та XDR) – частина технології, яка вирішує потребу в постійному моніторингу шляхом виявлення підозрілих дій та інших проблем на кінцевих точках.

Шостий консультаційний засіб контролю безпеки – тестування на проникнення, ціллю якого є перевірка робочої конфігурації безпеки та виявлення прогалин у безпеці за допомогою penetration test, тобто тесту на проникнення. Тест на проникнення – симуляція атак на систему з використанням тих технологій, які використовуються в реальних атаках, що здійснюється для визначення слабких місць, якими можуть скористатися зловмисники, щоб отримати доступ до цільового середовища.

Останній рекомендований засіб контролю безпеки – оцінка ризику на основі сценарію, що означає оцінку ризиків та готовність організації до можливих сценаріїв кібератак. Оцінка ризиків на основі сценаріїв містить тестові атаки на наявні системи та технічні вправи, що виконуються в рамках процесу управління ризиками. Діяльність з оцінки та планування проводиться щонайменше раз на рік та оновлюється з урахуванням здійснення значних технологічних змін або, коли стає відомо про зміни у можливостях або мотиваціях зловмисників [64].

3.3.3 Аналіз рекомендаційних засобів безпеки від SWIFT

Проаналізувавши усі консультаційні засоби контролю безпеки за версією CSCF, можна зробити висновок, що деякі з цих засобів варто зробити обов'язковими, оскільки їхня відсутність може сильно вплинути на конфіденційну інформацію, що міститься в системі. Так, наприклад, відсутність тестування на проникнення ставить під загрозу безпеку всієї системи. Варто зазначити, що усі засоби контролю безпеки стосуються не безпосередньо SWIFT, а користувачів послуг SWIFT, тобто фінансових установ, саме тому в CSCF наголошується, що тестування на проникнення проводиться тільки на систему клієнта, а не на центральні служби SWIFT. Проте, тестування на проникнення – вкрай важлива складова забезпечення безпеки як конфіденційних даних, так і системи в цілому, оскільки тестування на проникнення виходить за рамки стандартного захисту системи компанії, створюючи реальний сценарій, в якому показує, наскільки поточний захист компанії буде ефективним у випадку кібератаки. CSCF рекомендує проводити тестування на проникнення мінімум раз на два роки та у випадку великих оновлень системи, але насправді тестування на проникнення варто починати проводити з самого створення системи та продовжувати регулярно, оскільки кіберзлочинці розвиваються та знаходять нові вразливості ледь не щодня. Якщо проводити тестування на проникнення раз на два роки, можна дізнатися про наявну вразливість в системі через занадто довгий проміжок часу, коли цими вразливостями вже скористалися шахраї. Рекомендації CSCF стосуються банківських установ, що означає велику кількість конфіденційної інформації, яка щоденно проходить крізь систему, і відсутність тестування на проникнення потенційно ставить під загрозу усю цю інформацію, тож вважається за доцільне у наступному оновленні CSCF засіб контролю безпеки «тестування на проникнення» зробити обов'язковим для усіх клієнтів SWIFT та переглянути рекомендації щодо регулярності тестування.

Вкрай важливим засобом контролю безпеки також є безпека потоку даних бек-офісу. Оскільки можливими ризиками при відсутності даного засобу контролю безпеки є як втрата конфіденційності та цілісності конфіденційних

даних, так і несанкціонований доступ до системи, цей засіб контролю безпеки має стати обов'язковим, що SWIFT і планує зробити в наступних оновленнях CSCF. Перехід до обов'язкової фази відбудеться у два етапи, де під час першого етапу буде обов'язковим захист нових потоків «точка-точка» та серверів-мостів, які забезпечують обмін даними, після чого у наступному оновленні стане обов'язковим захист успадкованих потоків.

3.4 Нормативно-правова база в Україні

3.4.1 Огляд нормативно-правової бази України про забезпечення безпеки інформаційних ресурсів у сфері платіжних систем

Україна керується своїми власними законами для забезпечення інформаційної безпеки в платіжних системах. Головним документом можна назвати Постанову Національного Банку України (НБУ) № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України». Поштовхом до створення даної Постанови стали масивні кібератаки на українські організації вірусом родини Petya у 2017 році [72]. Суть цієї постанови – затвердити мінімальні необхідні заходи для забезпечення безпеки й кіберзахисту та визначити вимоги то систем електронних платежів для криптографічного захисту інформаційних ресурсів. Цим Положенням затверджуються такі методи захисту як використання TLS та SSL, про роботу яких буде детальніше розказано в розділі 4. Також встановлюються мінімальні вимоги до криптографічних наборів захисту, а саме, в системах електронних платежів мають використовуватися симетричні криптографічні алгоритми, довжина ключа яких має бути не менша ніж 128 біт.

Якщо казати не про технічну сторону забезпечення безпеки інформаційних ресурсів, то цим Положенням банк зобов'язаний створити та регулярно оновлювати свою політику інформаційної безпеки, суть якої в систематизації принципів, правил та вимог інформаційної безпеки в платіжній системі. Банківська установа має мати окремий кіберпідрозділ, основна мета яких – розслідування інцидентів з безпекою інформаційних ресурсів та контроль виконання заходів інформаційної безпеки.

Окремий пункт даної Постанови відведений під СУБД, а саме про облікові записи користувачів СУБД та про повноваження кожного з цих користувачів. Важливим уточненням цих повноважень є так званий принцип надання мінімально необхідних повноважень для усіх користувачів, суть якого в обмеженні користувачів рівно тими правами, які їм необхідні для виконання їхніх дій з цією СУБД.

В електронній платіжній системі також мають бути використані новітні оновлення для усіх програм та засобів, які використовує ця система, оскільки застарілі версії програм та засобів можуть містити вразливості до певного роду зловмисних дій, які у нових версіях вже були виправлені. Електронна платіжна система має мати перевірку від зловмисного коду різними програмними засобами.

Дана Постанова була затверджена у 2017 році та дотримується фінансовими установами України по цей день. Кожен банк розробляє власну політику інформаційної безпеки згідно з Постановою № 95.

3.4.2 Аналіз нормативно-правової бази України про забезпечення безпеки інформаційних ресурсів у сфері платіжних систем

Розглянувши Постанову Національного Банку України (НБУ) № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» (надалі також «Постанова НБУ № 95»), можна сказати, що вона є достатньо сучасною та відповідає мінімальним вимогам міжнародної нормативно-правової бази. У даному Положенні досить детально описати необхідні вимоги для забезпечення інформаційної безпеки. Так, для криптографічного захисту виділено окремий розділ, в якому детально описані можливі криптографічні алгоритми, які зобов’язані використовувати платіжні системи, та вказані необхідні параметри для використання цих алгоритмів. Так, наприклад, якщо фінансова установа використовує для електронних підписів та/або ключів шифрування алгоритм RSA, цією Постановою затверджено, що мінімальна довжина модуля має складати не менше ніж 2048 біт. Канадський центр кібербезпеки, що є частиною канадського

уряду, у своєму новому дослідженні зазначив, що на цей момент алгоритм RSA з довжиною модуля 2048 біт є безпечним і буде залишатися безпечним приблизно до кінця 2030-х років [15], з чого можна зробити висновок, що в плані криптографічного захисту Постанова НБУ № 95 є сучасною та тою, що відповідає міжнародним вимогам.

Це Положення містить корисні поради щодо оновлень програмного забезпечення або перевірки усього трафіку на випадок зловмисного коду, але в даному Положенні не вистачає пари досить важливих пунктів:

Перевірка персоналу: в даній Постанові є окремий пункт про заходи для підвищення обізнаності та навченості персоналу щодо інформаційної безпеки, однак, перевірка персоналу є вкрай важливим моментом для фінансової системи. У Постанові зазначено, що персонал фінансової системи має лише мінімально необхідні для виконання обов'язків повноваження, але, якщо особа з персоналу, яка має конфлікт інтересів або минулі кримінальні провадження за шахрайство, матиме достатній рівень повноважень, щоб вчиняти шахрайські дії, це може призвести до серйозних наслідків.

Тестування на проникнення: дане тестування є важливим пунктом забезпечення безпеки інформаційних ресурсів, оскільки без реальної перевірки системи на наявність вразливостей дізнатися про ці вразливості можна буде вже під час зловмисної атаки. Тестування на проникнення може мінімізувати такі атаки, оскільки, якщо віднайти усі вразливості під час тестування, і, що важливо, прибрати їх, реальна зловмисна атака може не мати успіху. Законодавство України, зокрема, Постанова НБУ № 95, не регулює тестування на проникнення взагалі, але конкретна система електронних платежів може замовити для себе цю послугу у компетентних компаній.

Якщо порівняти Постанову НБУ «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» та SWIFT CSCF, можна помітити, що Постанова НБУ містить майже всі засоби безпеки, що і SWIFT CSCF, що є одним з еталонних прикладів нормативно-правової бази системи електронних платежів. Приведений вище

приклад про тестування на проникнення у SWIFT CSCF теж є необов’язковим до виконання, тобто, деякі системи електронних платежів можуть не дотримуватися цієї вимоги.

Якщо порівняти Постанову НБУ № 95 із PCI DSS, можна помітити, що обидва ці документи засновані на стандарті ISO/IEC 27001. Це означає, що вони є досить схожими, різниця тільки в тому, що Постанова НБУ № 95 є більш конкретною та більш адаптованою для українських платіжних систем, в той час як PCI DSS є більш загальною. За дослідженнями української компанії GetPCI, PCI DSS та Постанова НБУ № 95 схожі приблизно на 60% [2], а ті 40%, що лишилися, стосуються безпосередньо українських аспектів та продуктів на кшталт українських криптоалгоритмів «Калина» та «Купина». Враховуючи той факт, що дотримання PCI DSS вимагають майже всі провідні системи електронних платежів, можна зробити висновок, що українська законодавча база також відповідає сучасним вимогам до систем електронних платежів.

4 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В СИСТЕМАХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

4.1 Можливі загрози для систем електронних платежів

Системи електронних платежів містять величезну кількість конфіденційної та банківської інформації, яка приваблює зловмисників, а проблеми безпеки, що загрожують системам електронних платежів, змінюються постійно і зазвичай вкрай швидко. Зловмисник може легко атакувати платіжну систему банківської установи для здійснення шахрайських цілей. Існують безліч видів вторгнення в банківські системи, які потенційно можуть призвести до втрати захищених даних. Розглянемо деякі з них:

1) DoS-атаки. Denial of Service, тобто «відмова в обслуговуванні», вважається однією з найбільш небезпечних атак через потенційну велику втрату грошей через втрату клієнтів та великі затрати для відновлення заподіяної системі шкоди. Поширеним типом цієї атаки для платіжних систем є DDoS (Distributed Denial of Service) атака, суть якої полягає в створенні сотень комп'ютерів-«зомбі», які відправляють в банківську систему велику кількість пакетів одночасно, через що справжні пакети будуть відкидуватися через тайм-аут, тобто великий час обробки. Цей тип атаки впливає на доступність та безперервність системи, оскільки платіжна система не може проводити транзакції з клієнтами та партнерами.

2) Витік даних – одна з загроз, яка може вплинути на систему безпеки фінансової установи, суть якої полягає у витоку інформації з системи, що робить її доступною іншим людям. Зазвичай, у випадку витоку даних мова йде про конфіденційні та секретні дані, які можуть бути викрадені або використані кимось, хто не повинен мати до них доступ. Зазичай витік даних відбувається тоді, коли в системі є лазівки, що дозволяють неавторизованій особі отримати доступ до системи. Це пов'язано з поганою системою безпеки та відсутністю оцінок безпеки. Втрата ідентифікаційної інформації внаслідок витоку даних –

прямий шлях зловмиснику до отримання автентифікації, яку він може використати для власної вигоди.

3) Підміна TCP/IP – поширена форма онлайн-шахрайства. При підміні IP-адреси зловмисник отримує несанкціонований доступ до мережі, удаючи, що зловмисне повідомлення прийшло з довіреного пристрою. Цей метод дозволяє зловмиснику відправляти пакети мережею без блокування з боку брандмауера. Зазвичай брандмауер фільтрує зовнішні IP-адреси, які намагаються з ним зв’язатися, однак у випадку підміни IP зловмисник удає, що він належить до внутрішньої мережі та тим самим обходить фільтри брандмауера. Мета цього методу – надання зловмиснику можливості отримати root-доступ до сервера банківської системи за допомогою відправок пакетів, що можуть містити зловмисне ПЗ, яке направлене на викрадення конфіденційних даних.

4) Зловмисне ПЗ – програма, призначена для зміни та модифікації системи без дозволу користувача або власника. Атаки зловмисного ПЗ можуть вплинути на конфіденційність, цілісність та доступність банківської системи. Шкідливе ПЗ, що атакує конфіденційність, направлене на перехват натискань клавіш для перехвату паролів та номерів кредитних карт, завантаження файлів та стеження за всім, що відбувається на екрані. Відомим прикладом такого шкідливого ПЗ є трояни, які збирають конфіденційні дані на заражених комп’ютерах, при цьому маскуючись під корисні застосунки. Один із найвідоміших троянів Zeus, що спричинив збитків більше, ніж на 100 мільйонів доларів і заразив понад 200 тисяч комп’ютерів [73], був спрямований на викрадення банківської інформації та отримував дані різними способами, наприклад, викрадав паролі, що зберігалися у браузерах за допомогою функції зберігання паролів, та відстежував дії користувача, і, якщо користувач відвідував банківський сайт, то використовував захоплення натискань клавіш клавіатури або захоплення форм браузера, щоб перехопити логіни та паролі користувачів [11]. Своєю чергою, атаки на цілісність теж шкодять системі, наприклад, завантаживши туди заражений файл або пошкодивши файли даних чи змінивши файли конфігурації.

4.2 Проблеми електронних платежів

Проте, електронні платежі мають наступні проблеми:

- Цілісність: переконатися, що фінансова інформація, що передається, не змінилася при її транспортуванні.
- Відсутність репутації: переконатися, що усі сторони мають неспростовні докази передачі та отримання платежу.
- Конфіденційність: переконатися, що транзакції захищені від можливих перехоплювачів.
- Надійність: переконатися, що відсутність відмови платежу зменшується.
- Авторизація: переконатися, що усі учасники розпізнані та їм надані бажані права та привілеї.

Окрім того, деякі системи електронних платежів знаходяться на стадії свого розвитку і потребують великого обсягу відкритої інформації та обізнаності населення, щоб користувачі могли оцінити дане нововведення. Також існує проблема відсутності законодавства, яке зобов'язувало банки використовувати спільну програмну платформу, через що банки використовують будь-яку платформу, яка може надавати послуги електронних платежів, що, своєю чергою, викликає проблеми при забезпеченні грошових переказів з одного банку до іншого. Великою проблемою постає питання безпеки, а саме забезпечення безпеки від різноманітних загроз.

4.3 Вразливості систем електронних платежів

Міцні та довготривалі ділові відносини завжди залежали від довіри. Електронні платежі не досягли б свого успіху без довіри користувачів, а їхня довіра базується на достатній безпеці своїх платежів. Вищезгаданий МОТО, хоч і був одним з альтернатив для онлайн-оплати покупок, не досяг успіху через абсолютну відсутність безпеки платіжних даних покупця, що могло призводити до великої кількості шахрайських дій. Для здійснення електронного платежу клієнти мають надати дані кредитної картки, а також свої персональні дані, що

може легко використати зловмисник для викрадення грошей. Дані платіжних карток є ціллю номер один для шахраїв: так, за даними звіту Verizon, 84% випадків витоку даних стосувалися саме даних платіжних карток [50]. За оцінками Cybersecurity Ventures, шкода, спричинена кіберзлочинами до 2025 року сягне 10,5 трильйонів доларів [26]. Витоки даних стаються у таких компаній-гігантів, як Yahoo, Adobe, eBay, Uber та інших [55]. Так, американська компанія Target витратила щонайменше 18,5 мільйонів доларів на розслідування найбільшого витоку даних близько 42 мільйонів клієнтів даної мережі [42].

Вразливості можуть з’явитися будь-де в екосистемі обробки платіжних систем, включаючи:

- торгові пристрої;
- хмарні системи;
- мобільні пристрої, комп’ютери та сервери;
- бездротові точки доступу;
- застосунки для вебпокупок;
- паперові системи зберігання;
- передача даних власника картки постачальникам послуг;
- підключення до віддаленого доступу.

Вразливості можуть поширюватися також на фінансові установи, які ініціюють та підтримують відносини із продавцями, які приймають платежі.

Наприклад, мобільні платежі стали новою формою електронних платежів, які здійснюються або через СМС, або через Інтернет, або через спеціалізовані застосунки на смартфонах. Хоча і банки, і клієнти отримують свої переваги від електронних платежів, вони мають слідкувати за безпекою, щоб зручна альтернатива готівковим платежам не стала катастрофою. Безпека є найбільш важливим фактором, що негативно впливає на потенційних користувачів електронних платежів, оскільки клієнти часто чують про хакерів, комп’ютерні віруси та фішингові атаки [8]. Загалом, безпека – це набір процедур, механізмів та програм для автентифікації джерела інформації та гарантування цілісності та конфіденційності інформації. Користувачі вимагають конфіденційності,

автентифікації, цілісності даних, та неспростовності як основних потреб для здійснення безпечних розрахунків за допомогою Інтернету, і очевидно, що системи електронних платежів мають мати усі вказані атрибути захисту, оскільки користувачі не будуть покладатися на незахищену систему електронних платежів [13, 58].

Для подолання викликів безпеки система повинна реалізувати властивості безпеки електронних платежів, які будуть детальніше розглянуті нижче:

1) Авторизація – електронні платежі мають бути доступними виключно для авторизованих клієнтів. Система має перевірити, чи може користувач провести транзакцію та підтвердити, що кожен учасник транзакції може її здійснити, оскільки, якщо авторизація проводиться неналежним чином, хакер може перехопити платіжну інформацію клієнтів без перевірки і лишитися анонімним [37].

2) Конфіденційність – гарантія того, що інформація про користувача надається виключно уповноваженим особам і є недоступною для інших користувачів електронного банкінгу. Лише авторизований користувач має мати можливість отримати зашифроване повідомлення, щоб інші користувачі не могли переглядати його вміст [59]. Система має захищати конфіденційну інформацію від будь-якої неавторизованої особи, процесу та пристрою.

3) Цілісність – використовується, щоб переконатися у точності інформації для своїх потреб та пов’язана із правдивістю інформаційних ресурсів. Інформація має бути автентичною та повною, і цілісність має гарантувати, що інформація не буде замінена або пошкоджена під час передачі [41].

4) Автентифікація – процедура підтвердження ідентичності процедури чи пристрою. Основна проблема електронних платіжних систем – подбати про автентифікацію, яка гарантує, що клієнт є тим, ким він обіцяє бути. Процес автентифікації використовується, щоб дозволити особі увійти до свого облікового запису, і, якщо він збігається із наявним, то особа є перевіреним користувачем і їй дозволено увійти в систему. Однак, було виявлено, що один фактор авторизації не є надійним для забезпечення достатнього рівня безпеки,

через що було створено багатофакторну автентифікацію, яка перевіряє дійсність особи. Багатофакторна автентифікація містить біометричні дані та пристрої-токени разом зі смарткарткою [28]. Це як підвищує рівень безпеки, так і додатково використовує ідентифікацію, підтвердження та верифікацію, щоб гарантувати повноваження клієнта [47].

5) Неспростовність – механізм, який гарантує, що користувач з'єднується з автентичним сервером, а сервер – з автентичним користувачем, щоб ніхто не міг пізніше заперечити обробку даних [43].

6) Надійність – з трансформацією електронних платежів існує потреба у змінах та розвитку. Надійність є однією із важливих критеріїв для успіху системи. Заходи безпеки повинні перевірятися під функцією моніторингу загроз, щоб переконатися у їхній надійності та ефективності.

7) Ефективність – одна із позитивних характеристик систем електронних платежів. Забезпечення високої ефективності у здійсненні транзакцій призводить до поширення електронних гаманців серед клієнтів [66]. Ефективність також можна поширити, зменшивши витрати на транзакції для клієнтів.

8) Доступність – баланс між потребами безпеки клієнтів і їхнім комфортом. Доступність дозволяє користувачу завершити покупку у зручний для клієнта час та визначає доступ до джерел інформації, що своєю чергою забезпечує своєчасне та повне виконання розпочатої транзакції [38].

У сфері електронних платежів найбільш небезпечною загрозою, без сумніву, можна назвати фішинг – метод збору конфіденційної інформації під виглядом іншої організації. Фішингові атаки, зазвичай, використовують листи на електронну пошту або шкідливі вебсайти для збору інформації. Клієнт банку отримує лист від облікового запису, що видає себе за банківську установу, яка запрошує інформацію про кредитні картки та/або обліковий запис клієнта в цьому банку. Коли користувачі надають цю інформацію, зловмисники використовують її, щоб отримати доступ до їхніх облікових записів і їхніх коштів [18].

4.4 Підвищення безпеки електронних платежів

Система електронних платежів має мати достатні рівні безпеки, оскільки система електронних платежів без належної безпеки не отримає довіри клієнтів. У спробах досягнути високого рівня захисту були створені різні методи забезпечення безпеки електронних платежів, які, однак, не завжди сприймалися належно, наприклад, Secure Electronic Transaction (SET) – відкритий стандарт від Visa та MasterCard, суть якого полягала у наданні обом учасникам транзакції цифрового сертифіката для забезпечення захисту транзакції. Цей метод не був сприйнятий користувачами через потребу завантажувати додаткове програмне забезпечення, після чого SET було перероблено в 3D Secure, який не вимагає наявності додаткового програмного забезпечення для перевірки [71].

Для безпеки онлайн-платежів також були створені різні протоколи безпеки, найпоширенішим з яких є Secure Sockets Layer (SSL) – це протокол, що використовується для підтримки автентифікації клієнта та сервера. Про його наявність на сайті свідчить присутність символу замка біля адресного рядка сайту. В SSL зв’язок між сервером та клієнтом шифрується за допомогою їхніх сертифікатів. Таке шифрування створює віртуальну інформацію, яку не можуть зламати зловмисники. Алгоритм роботи SSL зображений на рис. 3.1.

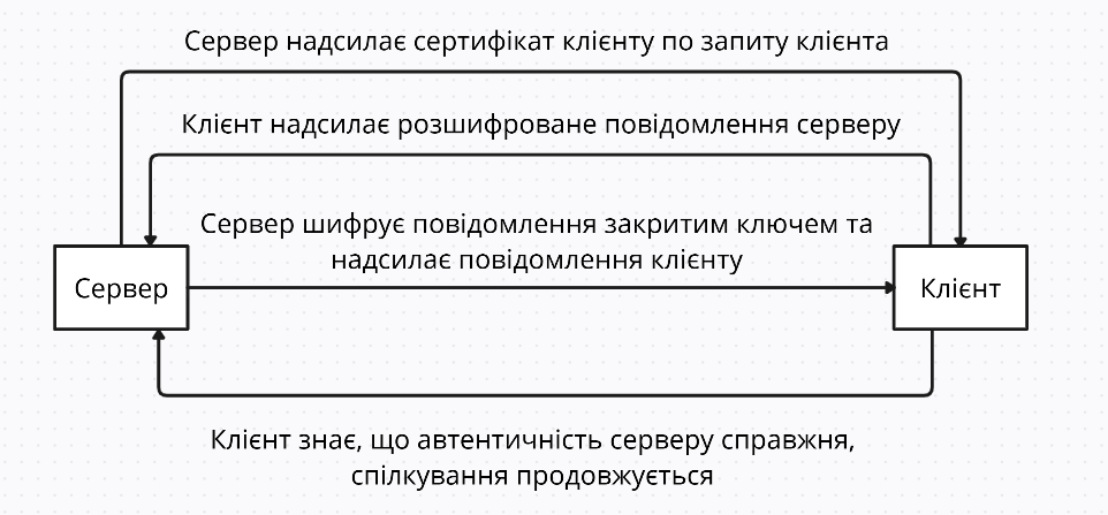

Рисунок 3.1 – Алгоритм роботи SSL

Мета SSL – забезпечити безпечний зв’язок між обома сторонами, але при цьому одна зі сторін має мати сертифікат, якому довіряє, щоб запобігти атакам

типу «man in the middle». SSL використовує протокол рукостискання, суть якого полягає в наступному алгоритмі:

- Клієнт надсилає на сервер повідомлення.
- Сервер після отримання повідомлення підтверджує його, надіславши клієнту відповідне повідомлення. Також сервер надсилає клієнту свій сертифікат і запитує сертифікат клієнта.
- Клієнт надсилає свій сертифікат, повідомлення про обмін ключами та повідомлення перевірки сертифіката.
- Клієнт та сервер надсилають повідомлення про зміну специфікації шифру, щоб сповістити один одного про те, що наступні повідомлення будуть захищені відповідно до ключів.
- Клієнт та сервер надсилають готові повідомлення для завершення рукостискання [61].

Вебсайт реалізує SSL за допомогою HTTPS, що означає протокол передачі гіпертексту через рівень захищених сокетів. SSL також підтримує використання цифрових сертифікатів X.509 з сервера, тобто користувач за необхідності може автентифікувати відправника [62].

Сильною стороною SSL є здатність запобігання типовим атакам, однак у нього є свої недоліки, як повторне узгодження головного ключа. Після встановлення з’єднання один і той самий головний ключ буде використовуватися протягом усього з’єднання, і це може бути серйозним недоліком, якщо SSL міститься під тривалим з’єднанням. Одним із можливих рішень цієї вади є повторне узгодження головного ключа через певний час.

Також існує Transaction Layer Security (TLS), що заснований на SSL. TLS має певні зміни у своєму MAC, має чіткіші та точніші специфікації, чистішу обробку через відсутність сертифіката клієнта та більшу гнучкість.

4.5 Методи забезпечення безпеки

Є різні причини для забезпечення безпеки процесу електронних платежів:

- Захистити конфіденційну інформацію
- Уникнути шахрайства

- Отримати довіру клієнтів
- Захистити репутацію компанії

І для досягнення усіх цих причин першочерговим є забезпечення високого рівня захисту систем електронних платежів. Для цього існують різні методи, які будуть розглянуті нижче.

1) Дотримання нормативно-правової бази, яка підходить для конкретної системи електронних платежів.

Більшість компаній ставляться до нормативно-правової бази, як до непотрібних папірців, які не впливають на роботу платіжної системи. З усім тим, чітке дотримання мінімальних вимог, наприклад, PCI DSS (або у випадку з інтеграцією SWIFT у свою систему електронних платежів – SWIFT CSCF) знизить вірогідність шахрайства з боку зловмисників. Це як захист даних, які зберігаються та передаються під час здійснення платежу, забезпечення швидких і захищених механізмів автентифікації, щоб уникнути проникнення в систему неавтентифікованого користувача (зловмисника), так і ведення журналу подій і його захист, щоб мати можливість швидко відстежити несанкціоновані та підозрілі дії користувачів в системі.

2) Шифрування даних

Під час здійснення електронного платежу конфіденційна інформація платника передається через Інтернет, і цю інформацію може легко перехопити зловмисник, та, якщо ця інформація не зашифрована, легко використати її в зловмисних цілях. Для шифрування даних в системах електронних платежів використовують вищезгаданий TLS, який захищає з’єднання між клієнтом та вебсайтом, що гарантує неможливість перехоплення інформації, що передається.

3) Використання багатофакторної автентифікації

Використання багатофакторної автентифікації знижує ризик можливого шахрайства з боку клієнта. Викрадення конфіденційної інформації користувача, такої як PIN або пароль до системи електронних платежів може призвести до шахрайства з боку зловмисника. В такому випадку використовується багатофакторна автентифікація, наприклад, одноразовий пароль, який надходить

на електронну пошту або на номер телефону, оскільки можливість того, що зловмисник матиме одночасно доступ і до даних входу, і до телефону або електронної пошти досить мала. Однак, ця вірогідність все ще існує, тому також використовується біометрична автентифікація. Біометрична автентифікація – вид автентифікації, під час якої використовується сам користувач, наприклад, відбиток пальця, сканування обличчя або голос. Чим більше рівнів автентифікації – тим вищий рівень безпеки, оскільки зловмисникам стає все важче скомпрометувати усі елементи автентифікації.

4) Використання токенів

Останнім часом системи електронних платежів активно використовують систему токенів, про яку детальніше буде розказано нижче. Якщо коротко, токени використовуються для здійснення платежу без передачі конфіденційної платіжної інформації. Використання токенів дозволяє уникнути витоку даних.

5) Освіченість користувачів

Варто зазначити, що усі перераховані вище методи безпеки не будуть працювати, якщо користувачі недостатньо освічені у сфері безпеки. Для прикладу, зловмиснику не доведеться витрачати час на знаходження даних для проходження багатофакторної автентифікації, якщо користувач перейде за шахрайським посиланням та сам введе свої конфіденційні дані.

4.6 Безпека в конкретних системах електронних платежів

4.6.1 PayPal

Через велику популярність Інтернет-покупок люди потребують безпечної системи онлайн-платежів, якій вони зможуть довіряти. Такою системою став PayPal, який є однією з найбільших систем онлайн-платежів у світі. Все, що потрібно мати користувачу – обліковий запис PayPal, після чого користувач буде готовий безпечно отримувати та надсилати платежі онлайн. PayPal використовує ті технології та механізми безпеки, що і більшість сайтів. Так, PayPal використовує HTTPS та SSL для шифрування потоку даних, коли користувач встановлює сеанс із сайтом PayPal. Механізми безпеки, які PayPal використовує для захисту своїх баз даних клієнтів, не оголошують широкому загалу

користувачів, оскільки за останні 10 років на PayPal було організовано декілька кібератак, а відкриття інформації про механізми безпеки дозволить хакерам швидше знайти протидію або недоліки в цих механізмах. Згідно з інформацією на сайті PayPal, PayPal у 2016 році оновив сертифікати SSL і, якщо раніше вони були підписані за допомогою SHA-1, то тепер відбулося оновлення до більш надійного алгоритму SHA-256. Окрім того, з боку PayPal відбулося оновлення, після якого PayPal не підтримує захищені з'єднання, у яких для підтвердження довіри потрібен кореневий сертифікат VeriSign G2. Тепер до успішного безпечного з'єднання призведе лише з'єднання, в якому сертифікат буде підписаний кореневим сертифікатом VeriSign G5 [60].

Окрім цього, PayPal була однією із перших компаній, яка використала технологію токенізації для захисту особистих даних клієнтів під час транзакції. Токенізація замінює фінансову інформацію платника набором певних чисел, які підтверджують для отримувача платежу справжність цього платежу, при цьому не розкриваючи дані платника. Також, PayPal вкрай обережно ставиться до кібербезпеки: так, PayPal став членом-засновником альянсу Fast Identity Online (FIDO), суть якого полягає у пошуку нових методів автентифікації, суть яких полягає у відході звичайних паролів і переході на біометричні дані.

Очевидно, що при всіх зусиллях жодна компанія не може знайти усі вразливості у своїй системі самостійно, тому у 2012 році PayPal заснував програму винагород, яка спонукає користувачів повідомляти про вразливості, співпрацювати із PayPal щодо їх виправлення та своєю чергою отримувати винагороду. Зараз ця програма нараховує більш ніж 1500 учасників, яким було виплачено понад 2 мільйони доларів [21].

Однією з найбільших проблем безпеки для PayPal стали види шахрайства через електронні листи. Велика кількість користувачів отримували електронні листи, начебто від PayPal, із закликом перейти через посилання в цьому листі та увійти до своїх облікових записів. Таким чином хакери отримують дані облікових записів користувачів, видаючи себе за PayPal, входять у ці облікові записи та крадуть гроші. Також є види шахрайства, у яких користувачу навіть не

потрібно переходити за фішинговими посиланнями, оскільки лист виглядає як форма для входу в PayPal, а лист говорить, що при відмові входити у PayPal обліковий запис користувача буде заблоковано. Зазвичай такі форми та фішингові сайти відрізняються декількома символами в URL-рядку, а вигляд вони мають майже ідентичний з оригінальним. Запобігти такому шахрайству можуть допомогти клієнтські сертифікати, але їх нечасто використовують в такого роду сайтах. Окрім того, сам PayPal активно працює у сфері запобігання такого типу шахрайства. Так, у 2014 PayPal заснував технологію Domain-based Message Authentication, Reporting & Conformance (DMARC), тобто технологію автентифікації, звітування та відповідності повідомлень на основі домену. Ця технологія допомогла заблокувати понад 180 мільйонів шкідливих електронних листів із фішинговими посиланнями [21].

4.6.2 Мобільні гаманці

Також великої популярності серед населення набирають мобільні гаманці, такі як Apple Pay та Google Pay. Розглянемо кожен з них детальніше.

4.6.2.1 Apple Pay

Apple Pay – сервіс від Apple для мобільних платежів за допомогою пристроїв на iOS, який поєднує низку технологій безпеки та засобів контролю для здійснення клієнтами платіжних транзакцій. Процес реєстрації картки в Apple Pay відбувається з введення даних картки в застосунок, після чого ці дані надсилаються через безпечне з’єднання на сервери Apple разом з іншими даними користувача, відомостями про пристрій та місцеперебуванням користувача. Банк отримує цю інформацію та приймає рішення про дійсність картки. Якщо картку прийнято, банк зв’язується з постачальником платіжної мережі, щоб створити унікальний токен. Токен зіставляється з відповідним номером картки та зберігається у таблиці пошуку токенів, що зберігається у безпечній базі даних. Після цього створюється DAN (Device Account Number), який Apple отримує разом із криптограмою (одноразовий зашифрований рядок, що представляє інформацію про транзакцію та продавця) та за допомогою якого пізніше будуть створюватися коди безпеки для підтвердження платежу.

Процес платежу за допомогою Apple Pay починається з розміщення пристрою біля термінала NFC. Наступне, що має зробити користувач – ідентифікувати себе за допомогою відбитка пальця, FaceID або PIN-коду. Мета цього контролю безпеки – обмежити дії зловмисника із викраденим пристроєм. Після вибору картки її DAN завантажується в так званий SE (Secure Element). SE – захищений від несанкціонованого доступу чіп із захищеним мікроконтролером, призначений для надійного зберігання конфіденційних і криптографічних даних. Продавець надсилає необхідну інформацію банку, який отримує плату за транзакцію, який своєю чергою перевіряє банківський ідентифікаційний номер та надсилає банку-емітенту. Банк-емітент перевіряє дані та авторизує або відхиляє транзакцію, після чого відправляє сповіщення банку, який проводить транзакцію, який своєю чергою відправляє його продавцю. Окрім автентифікації користувача, є важливою автентифікація пристрою. Кожна транзакція, проведена через Apple Pay, створює унікальне значення, яке гарантує, що транзакція проводиться з авторизованого пристрою. Цей унікальний ідентифікатор разом із токеном та криптограмою гарантують, що, навіть, якщо токен буде викрадено, його не можна буде використовувати з іншого пристрою, оскільки токен має надходити з пристрою, на якому він був зареєстрований. Окрім того, токен вираховується із сумою транзакції, тож навіть у випадку викрадення зловмисник не зможе його використати для іншої покупки.

Щодо захисту даних Apple Pay використовує різні засоби:

- Токенізація – під час реєстрації картки створюється токен, який зберігається на пристрої та використовується під час платіжних операцій. Під час оплати ніколи не використовується справжній номер картки та CVV (Card Verification Value), що допомагає мінімізувати розкриття реальних конфіденційних даних та обмежує можливість атак з боку ненадійних продавців, оскільки вони не бачать справжнього номера картки та CVV.
- Використання SE – Secure Element, присутній в пристроях Apple, є високозахищеним чіпом, який захищений від несанкціонованого доступу. Якщо

буде виявлено спроби прочитати його вміст, він автоматично обнуляє пам’ять, що виключає будь-яку можливість викрадення ключів.

- Дані кредитної або дебетової картки надсилається платіжною мережею в зашифрованому вигляді за допомогою платіжних аплетів, які знаходяться в SE.

4.6.2.2 Google Pay

Google Pay (G Pay, раніше відомий як Android Pay) – схожа на Apple Pay система мобільних платежів, яка дозволяє здійснювати оплату за покупки за допомогою мобільного пристрою на платформі Android. Щоб додати картку в Google Pay, необхідно обрати платіжну картку, яка збережена в обліковому записі Google, або, за необхідності, ввести дані картки вручну та підтвердити свій спосіб оплати. Підтвердити спосіб оплати можна декількома способами:

- Електронною поштою або текстовим повідомленням – банк надсилає клієнту електронний лист/текстове повідомлення з кодом підтвердження.
- Телефоном – клієнт може зателефонувати в банк і запитати код підтвердження.
- Верифікація через банківський застосунок – при наявності банківського застосунку на пристрої клієнт може увійти в нього та підтвердити картку.
- «Тимчасова сплата» – з користувача буде стягнуто невелику тимчасову плату, яка буде містити код підтвердження, який треба ввести у Google Pay.

Раніше Google Pay використовував SE, але у 2014 році було прийняте рішення перейти на хмарні технології з використанням HCE (Host Card Emulation). Ця система дозволяє Android емулювати платіжну картку та спілкуватися безпосередньо з NFC зчитувачем.

Щоб здійснити оплату за допомогою Google Pay, необхідно пройти автентифікацію користувача за допомогою FaceID, відбитка пальця або PIN-коду, після чого розташувати пристрій біля точки NFC (наприклад, POS-термінал). Перед початком оплати пристрій підключається до серверів Google та отримує низку платіжних токенів. Після розташування пристрою біля POS-термінала, контролер NFC на пристрої запитує один з цих токенів та відправляє

токен та криптограму на POS-термінал. Продавець пересилає інформацію банку-отримувачу, який своєю чергою пересилає токен та криптограму банку-емітенту через платіжну мережу. Платіжна мережа запитує справжній номер картки у постачальника послуг токенів та пересилає його банку-емітенту. Банк-емітент авторизує або відхиляє транзакцію і надсилає сповіщення банку-отримувачу, який, своєю чергою, надсилає його продавцю. Варто зазначити, що Google Pay не працює на пристроях, на яких ввімкнено адміністративний контроль, також відомий як root-доступ. Зазначається, що HCE зберігає дані картки в базах даних, що розміщені в безпечному хмарному середовищі.

Запобігання несанкціонованого доступу до HCE залежить від чотирьох стовпів безпеки:

- Ключі безпеки обмеженого використання – термін дії закінчується досить швидко, що запобігає їхньому зловживанню.
- Токенізація – зменшення ризику за допомогою заміни справжніх даних картки на дані обмеженого використання, які своєю чергою проходять крізь платіжну систему.
- Відбитки пальців на пристрої – підтвердження пристрою.
- Аналіз ризиків транзакцій – забезпечення оцінки транзакцій в реальному часі для виявлення незвичних дій.

Однак, серйозна проблема безпеки Google Pay полягає у великій різноманітності пристроїв з системою Android, які мають різні засоби забезпечення безпеки. Так, у 2021 році стало відомо про серйозний недолік смартфонів Samsung серії S: всі смартфони використовували один ключ для шифрування та дозволяли повторне використання вхідних даних для шифрування [54]. Ця вразливість дозволила вченим вкрасти конфіденційну інформацію з пристроїв Samsung, яка нібито була захищена на апаратному рівні та обійти автентифікацію, щоб отримати доступ до паролів. Інша нещодавня новина полягає у вразливості пристрою, якщо на смартфоні ввімкнений NFC та функція закріплення застосунків. Вразливість полягає у тому, що, якщо NFC-зчитувач опиниться біля такого смартфона в режимі блокування екрана, на нього

без необхідності автентифікації користувача відправиться повна інформація про банківську картку, а у випадку із POS-терміналом можлива навіть транзакція без участі користувача смартфона. Хоч вірогідність проходження всіх необхідних кроків з боку користувача малоймовірна, ця вразливість існує і є досить небезпечною [57]. Обидві ці вразливості були вже виправлені в оновленнях ПЗ.

4.7 Блокчейн

Блокчейн – «ланцюжок блоків» – така собі розподілена база даних транзакцій. Блокчейн може бути застосований для перевірки оновлень, боротьби з DDoS, захисту ланцюжків поставок, контролю цілісності політик і конфігурацій, а також для управління ідентифікаційними даними. Перевага блокчейну полягає в пов’язаності блоків між собою: наступний ланцюжок містить геш-значення попереднього блоку, що унеможливлює зміну або видалення якогось із блоків.

В системах електронних платежів блокчейн є новітньою системою, яку починають використовувати через зашифровані розподілені реєстри, які дозволяють перевіряти транзакції на справжність без посередників. Деталі транзакції зберігаються в блокчейні, їх не можна змінити або видалити непомітно.

Звичайно, впровадження блокчейну несе свої проблеми: якщо казати за технічні аспекти, неповне або неправильне впровадження блокчейну може нести серйозні проблеми. Найбільшою проблемою блокчейну також є обмежена пропускна здатність, а у випадку із системами електронних платежів ця проблема постає вкрай гостро, оскільки користувачі не будуть користуватися системою, яка працює з затримками, якщо навколо є купа альтернатив, які працюють швидше.

З цією ж проблемою зіткнулася й Естонія, про яку було згадано у розділі 2. Оскільки головною проблемою країни було переосмислення теперішніх систем, щоб отримати максимальну правильність та захищеність даних. Ще у 2008 році компанія Guardtime розробила систему електронного підпису на основі технології KSI Blockchain, яку активно впровадили в системи електронних

платежів. Система, що існувала до того, хоч і була успішною, але через складність та вартість перевірки ключів реалізація перевірки була вкрай ускладнена. Своєю чергою, KSI Blockchain дозволяє криптографічно довести правильність даних та інформації, яка переміщується в системах [39]. Після того, як цю систему випробував уряд у сфері охорони здоров'я, KSI Blockchain швидко підхопили банківські установи Естонії. Як було згадано, пропускна здатність блокчейну є вкрай великою проблемою для платіжних систем, але Guardtime за підтримки уряду Естонії зуміли модернізувати блокчейн. Так, у 2021 році Центральний Банк Естонії випустив дослідження, в якому зазначено, що нове рішення, засноване на блокчейні, може одночасно обробляти понад триста тисяч платежів, а користувачі отримували гроші менше ніж за дві секунди [27]. Окрім того, було розглянуто, чи можна поєднати блокчейн-рішення з компонентами цифрової ідентифікації. В Естонії таким компонентом є eID, та дослідження показало, що використання eID допомагає підтримувати основні принципи, такі як конфіденційність, безпека, доступність, ринкова нейтральність та допомагає оптимізувати процес.

Проаналізувавши дане дослідження, можна зробити висновок, що використання блокчейну в українських системах електронних платежів також є можливим. Як було зазначено, використання блокчейну Національним Банком Естонії витримало усі перевірки та тести, що означає, що блокчейн можна використовувати й Національним Банком України, як для зберігання даних в банківській системі, так і для передачі даних в міжбанківських і не тільки розрахунках. Системою замість eID може виступити українська система ідентифікації BankID [9].

ВИСНОВОК

Системи електронних платежів є невіддільною частиною нинішнього життя. Пандемія COVID-19 зі своїми наслідками у вигляді карантину та неможливості населення ходити по банківських установах призвела до стрімкого розвитку технологій, у тому числі технологій електронних платежів. У майбутньому електронні платежі ставатимуть все більш популярними, а отже, питання безпеки систем електронних платежів ставатиме все гостріше. По всьому світу кількість шахрайств, пов’язаних з електронними платежами лише збільшується, що означає сильну необхідність у розвитку методів забезпечення безпеки систем електронних платежів.

Проаналізовані в роботі методи показують, що захист інформаційних ресурсів в системах електронних платежів є вкрай важливою задачею по всьому світу. Як міжнародні компанії, так і уряди окремих країн роблять все можливе, щоб інформаційні ресурси користувачів були максимально захищені. Якщо виокремити Україну, то наша країна, попри масивні кібератаки, постійно вдосконалюється у сфері захисту інформаційних ресурсів. Українське законодавство є сучасним та таким, що відповідає міжнародним стандартам. Головна мета на майбутні роки – продовжувати оновлювати свою нормативно-правову базу та системи електронних платежів, щоб вони відповідали сучасним нормам захисту, оскільки кібершахраї щодня покращують свої шахрайські методи. Також є важливим залучити співпрацю із країнами-партнерками, щоб об’єднати зусилля та отримати більш захищену систему електронних платежів, або використовувати їхній вже наявний досвід для покращення власних систем електронних платежів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Сертифікація | GetPCI. URL: https://getpci.com/ (дата звернення: 13.09.2023).
2. Сертифікація PCI DSS допоможе виконати більшість вимог Постанови НБУ №95. GetPCI. URL: https://getpci.com/pci-dss-certification-will-help-to-fulfill-most-of-the-requirements-of-nbu-resolution-no-95. (дата звернення: 20.11.2023).
3. Система електронних платежів. Національний банк України. URL: https://bank.gov.ua/ua/payments/sep (дата звернення: 21.11.2023).
4. Що таке end-to-end шифрування, яке часто згадують, говорячи про месенджери? Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/sho-take-end-to-end-shifruvannya-yake-chasto-zgaduyut-govoryachi-pro-mesendzheri. (дата звернення: 10.11.2023).
5. Abrazhevich D. Electronic payment systems : a user-centered perspective and interaction design : Phd dissertation. Eindhoven, 2004. 189 c. URL: https://doi.org/10.6100/IR575913 (дата звернення: 04.09.2023)
6. A brief history of online payments - where electronic payments began. Ayoconnect - Southeast Asias Largest Open Finance Platform. URL: https://www.ayoconnect.com/blog/brief-history-of-online-payments-where-electronic-payments-began (дата звернення: 13.09.2023).
7. Aigbe P., Akpojaro J. Analysis of security issues in electronic payment systems. International journal of computer applications. 2014. Vol. 108, no. 10. P. 10–14. URL: https://doi.org/10.5120/18946-9993 (дата звернення: 11.09.2023).
8. Angelakopoulos G., Mihiotis A. E-banking: challenges and opportunities in the Greek banking sector. Electronic commerce research. 2011. Vol. 11, no.

3. P. 297–319. URL: https://doi.org/10.1007/s10660-011-9076-2 (дата звернення: 20.09.2023).

9. BankID НБУ. Національний банк України. URL: https://bank.gov.ua/ua/bank-id-nbu. (дата звернення: 10.10.2023).
10. Bank of Estonia notes increasing electronic payments - Central Banking. Central Banking. URL: https://www.centralbanking.com/central-banking/news/2171050/bank-estonia-reports-electronic-payments-methods (дата звернення: 15.09.2023).
11. Belcic I. The zeus trojan: what it is, how it works, and how to stay safe. Avast. URL: https://www.avast.com/c-zeus (дата звернення: 25.09.2023).
12. Best R. E-commerce payment methods market share 2026 | Statista. Statista. URL: https://www.statista.com/statistics/1111233/payment-method-usage-transaction-volume-share-worldwide/ (дата звернення: 15.09.2023).
13. Bezovski Z. The future of the mobile payment as electronic payment system. European journal of business and management. 2016. Vol. 8, no. 8. P. 127–132. URL: https://eprints.ugd.edu.mk/id/eprint/15691. (дата звернення: 21.09.2023).
14. Briggs A., Brooks L. Electronic payment systems development in a developing country: the role of institutional arrangements. The electronic journal of information systems in developing countries. 2011. Vol. 3, no. 49. P. 1–16. URL: https://doi.org/10.1002/j.1681-4835.2011.tb00347.x (дата звернення: 05.09.2023).
15. Canadian Centre for Cyber Security. Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information. 2022. URL: https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111. (дата звернення: 19.11.2023).
16. Cashless India. Government of India. URL: http://cashlessindia.gov.in/ (дата звернення: 19.09.2023).

17. Central Bank of Nigeria. 2020 Statistical bulletin financial sector - Payments system statistics. 2020.
18. Considerations regarding the security and protection of E-banking services consumers' interests. Amfiteatru Economic. 2010. Vol. 12, no. 28. P. 388–403.
19. Country profile: digital and instant payments are the norm in Estonia. European Payments Council. URL: https://www.europeanpaymentscouncil.eu/news-insights/insight/country-profile-digital-and-instant-payments-are-norm-estonia (дата звернення: 15.09.2023).
20. COVID-19 drives global surge in use of digital payments. The World Bank. URL: https://www.worldbank.org/en/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments (дата звернення: 16.09.2023).
21. Cybersecurity | PayPal. PayPal Government Relations. URL: https://publicpolicy.paypal-corp.com/issues/cybersecurity (дата звернення: 29.09.2023).
22. Deok-Gyu Lee, Hyung-Geun Oh, Im-Yeong Lee. A study on contents distribution using electronic cash system. IEEE international conference on e-technology, e-commerce and e-service, 2004. EEE '04. 2004, Taipei, Taiwan, 31 March 2004. 2004. URL: https://doi.org/10.1109/eee.2004.1287331 (дата звернення: 15.09.2023).
23. Digital drawback: Only one PoS terminal in India for every 358 people. Deccan Herald. URL: https://www.deccanherald.com/national/digital-drawback-only-one-pos-terminal-in-india-for-every-358-people-808112.html (дата звернення:: 19.09.2023).
24. Digital payments continue to grow; significant growth in tier II, III towns. Business Standart. URL: https://mybs.in/2Zgdhrk. (дата звернення:: 21.09.2023).

25. Echekoba F. N., Ezu G. K. Electronic retail payment systems : user acceptability and payment problems in Nigeria. Oman chapter of arabian journal of business and management review. 2012. Vol. 1, no. 6. P. 18–35. URL: https://doi.org/10.12816/0002106 (дата звернення: 19.09.2023).
26. Economic impact of cybercrime on business predicted to reach $10.5 trillion by 2025: Cybersecurity Ventures. Reinsurance News. URL: https://www.reinsurancene.ws/economic-impact-of-cybercrime-on-business-predicted-to-reach-10-5-trillion-by-2025-cybersecurity-ventures/. (дата звернення: 04.10.2023).
27. Eesti Pank. Work stream 3: A New Solution – Blockchain & eID. 2021. URL: https://www.eestipank.ee/en/publications/varia/2021/work-stream-3-new-solution-blockchain-and-eid. (дата звернення: 15.11.2023).
28. Electronic banking security andcustomer satisfaction in commercial banks / F. Komb et al. Journal of security and sustainability issues. 2016. Vol. 5, no. 3. P. 411–422. URL: https://doi.org/10.9770/jssi.2016.5.3(9) (дата звернення: 23.09.2023).
29. European Banking Authority. Final guidelines on the security of internet payments. 2014. URL: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/934179/f27bf266-580a-4ad0-aaec-59ce52286af0/EBA-GL-2014-12%20(Guidelines%20on%20the%20security%20of%20internet%20payments)_Rev1.pdf. (дата звернення: 07.10.2023).
30. FinTech – invest in Estonia. Invest in Estonia. URL: https://investinestonia.com/business-opportunities/fintech/ (дата звернення: 15.09.2023).
31. Government e-Payments Adoption Ranking - GKToday. GKToday- Current Affairs, GK (General Knowledge), General Studies for UPSC, IAS, Banking / IBPS, SSC and States Civil Services Examinations. URL: https://www.gktoday.in/topics/government-e-payments-adoption-ranking/ (дата звернення: 19.09.2023).

32. Goyal V., Pandey U., Batra S. Mobile banking in India: Practices,challenges and security issues. International journal of advanced trends in computer science and engineering. 2012. Vol. 1, no. 2. URL: https://warse.org/pdfs/ijatcse03122012.pdf (дата звернення: 06.09.2023).
33. History of the web and online payments. Axerve. URL: https://www.axerve.com/en/learn/insights/history-web-online-payments (дата звернення: 13.09.2023).
34. Hyun Ju Lee, Mun Suk Choi, Chung Sei Rhee. Traceability of double spending in secure electronic cash system. 2003 international conference on computer networks and mobile computing. ICCNMC 2003, Shanghai, China. URL: https://doi.org/10.1109/iccnmc.2003.1243063 (дата звернення: 15.09.2023).
35. India: number of digital payments 2023 | Statista. Statista. URL: https://www.statista.com/statistics/1251321/india-total-volume-of-digital-payments/ (дата звернення: 19.09.2023).
36. India writes the playbook for mobile payments innovation. Pymnts.com. URL: https://www.pymnts.com/news/ecommerce/2023/india-writes-the-playbook-for-mobile-payments-innovation/ (дата звернення: 19.09.2023).
37. Kang J. Mobile payment in Fintech environment: trends, security challenges, and services. Human-centric computing and information sciences. 2018. Vol. 8, no. 1. URL: https://doi.org/10.1186/s13673-018-0155-4 (дата звернення: 23.09.2023).
38. Khrais L. T. Highlighting the vulnerabilities of online banking system. The journal of internet banking and commerce. 2015. Vol. 20, no. 3. URL: https://doi.org/10.4172/1204-5357.1000120 (дата звернення: 23.09.2023).
39. KSI Blockchain - e-Estonia. e-Estonia. URL: https://e-estonia.com/solutions/cyber-security/ksi-blockchain/. (дата звернення: 30.09.2023).
40. Lutkevich B., Rosencrance L., Cobb M. What is smart card? | Definition from TechTarget. Security. URL:

https://www.techtarget.com/searchsecurity/definition/smart-card (дата звернення: 13.09.2023).

41. Mahmadi F., Zaaba Z., Osman A. Computer security issues in online banking: an assessment from the context of usable security. IOP conference series: materials science and engineering. 2016. Vol. 160. P. 012107. URL: https://doi.org/10.1088/1757-899x/160/1/012107 (дата звернення: 23.09.2023).
42. McCoy K. Target to pay $18.5M for 2013 data breach that affected 41 million consumers. USA Today. URL: https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/. (дата звернення: 03.10.2023).
43. National Institute of Standards and Technology. Guide for developing security plans for federal information systems. Gaithersburg, 2006.
44. Nitsure R. R. E-Banking: challenges and opportunities. Economic and political weekly. 2003. Vol. 38, no. 51-52. URL: https://doi.org/10.2307/4414436. (дата звернення: 21.09.2023).
45. Nwankwo O., Eze O. R. Electronic payment in cashless economy of Nigeria: problems and prospect. Journal of management research. 2012. Vol. 5, no. 1. URL: https://doi.org/10.5296/jmr.v5i1.2650 (дата звернення: 20.09.2023).
46. Odior E., Banuso F. Cashless banking in nigeria: challenges, benefits and policy implications. European scientific journal. 2012. Vol. 8, no. 12.
47. Omariba Z., Masese N. B., Wanyembi G. W. Security and privacy of electronic banking. International journal of computer science issues. 2012. Vol. 9, no. 4. URL: https://www.researchgate.net/publication/268060917_Security_and_Privacy_of_Electronic_Banking. (дата звернення: 20.09.2023).
48. Ovia J. Enhancing the efficiency of the Nigerian payments system. *Central bank of Nigeria bulletin*. 2003. Vol. 1, no. 29.

49. Parkin B. India to expand digital payments with AI-powered voice transactions. Financial Times. URL: https://www.ft.com/content/a9a11275-a0f5-4f40-99e2-4c532afd77d4 (дата звернення: 19.09.2023).
50. Payment card security: what the 2022 Verizon data breach investigation report can teach us about current threats. Curbstone. URL: https://curbstone.com/2022-verizon-data-breach-investigation-report/ (дата звернення: 13.09.2023).
51. PCI DSS 4.0. Official edition. 2022. URL: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf. (дата звернення: 06.10.2023).
52. PYMNTS.com. 2023 global digital shopping index: India edition – August 2023|pymnts.com. *Pymnts.com*. URL: https://www.pymnts.com/study/2023-global-digital-shopping-india-ecommerce-retail-payments/?cache=skip#wpcf7-f1594900-o1?download=true (дата звернення: 19.09.2023).
53. QR code payment users to reach 2.2 billion globally by 2025. Juniper Research: Experts in Fintech, Telecoms & IoT Markets. URL: https://www.juniperresearch.com/press/qr-code-payment-users-to-reach-2-2-billion (дата звернення: 15.09.2023).
54. Rogers J. Android warning as Google Pay security flaw leaves millions of phones at risk. The US Sun. URL: https://www.the-sun.com/money/4783370/android-samsung-security-warning-google-pay/ (дата звернення: 09.10.2023).
55. Rooney K. $1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do. CNBC. URL: https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html (дата звернення: 20.09.2023).
56. Saltzer J. H. Protection and the control of information sharing in multics. Communications of the ACM. 1974. Vol. 17, no. 7. P. 388–402. URL: https://doi.org/10.1145/361011.361067 (дата звернення: 25.09.2023).

57. Sarangapurkar V. Recent Google Wallet vulnerability could expose credit card information. Android Central. URL: https://www.androidcentral.com/apps-software/google-wallet-vulnerability-exposes-card-information (дата звернення: 09.10.2023).
58. Sharma M. K. Electronic cash over the internet and security solutions. International journal of advanced research in computer science. 2017. Vol. 8, no. 1. URL: http://www.ijarcs.info/index.php/Ijarcs/article/view/2891. (дата звернення: 10.10.2023).
59. Shukur Z., Salameh N. Review of user authentication methods in online examination. Asian journal of information technology. 2015. Vol. 5, no. 14. URL: https://www.researchgate.net/publication/284895765_Review_of_user_authentication_methods_in_online_examination. (дата звернення: 22.09.2023).
60. SSL certificate upgrade - PayPal. PayPal Konto | Digitale Mobile Wallet | PayPal DE. URL: https://www.paypal.com/in/webapps/mpp/ssl-upgrade
61. SSL: Intercepted today, decrypted tomorrow | Netcraft. Netcraft | Leader in Phishing Detection, Cybercrime Disruption and Website Takedown. URL: https://www.netcraft.com/blog/ssl-intercepted-today-decrypted-tomorrow/
62. SSL/TLS in detail. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785811(v=ws.10)?redirectedfrom=MSDN (дата звернення: 09.10.2023).
63. Sumanjeet S. Emergence of payment systems in the age of electronic commerce: the state of art. Global journal of international business research. 2009. Vol. 2, no. 2. URL: https://ssrn.com/abstract=1536620 (дата звернення: 07.09.2023).
64. Swift customer security controls framework v2024. SWIFT. URL: https://www2.swift.com/knowledgecentre/rest/v1/publications/cscf_dd/48.0/CSCF_v2024_20230707.pdf?logDownload=true (дата звернення: 02.10.2023).

65. Telenor and Ericsson launch the "mobile wallet". Telenor Group - Telenor Group. URL: https://www.telenor.com/media/newsroom/archive/telenor-and-ericsson-launch-the-mobile-wallet/ (дата звернення: 13.09.2023).
66. Teoh T. T., Hoo C. Y., Lee T. H. E-wallet adoption: a case in Malaysia. International journal of research in commerce and management studies. 2020. Vol. 2, no. 2.
67. The development of settlement systems in Estonia. Eesti Pank. URL: https://www.eestipank.ee/en/payments/development-settlement-systems-estonia (дата звернення: 13.09.2023).
68. The future of payments in Latin America is instant | EBANX Blog. EBANX. URL: https://blog.ebanx.com/en/the-future-of-payments-in-latin-america-is-instant/ (дата звернення: 15.09.2023).
69. Top e-commerce payment methods Estonia 2022 | Statista. Statista. URL: https://www.statista.com/statistics/1373842/top-e-commerce-payment-methods-estonia/ (дата звернення: 15.09.2023).
70. Uddin M. S., Akhi A. Y. E-Wallet system for Bangladesh an electronic payment system. International journal of modeling and optimization. 2014. Vol. 4, no. 3. URL: http://www.ijmo.org/papers/376-A1015.pdf. (дата звернення: 15.09.2023).
71. United Nations Economic Commission for Africa. E-Payment: challenges and opportunities in Ethiopia. 2005. URL: https://www.ethioconstruction.net/sites/default/files/Law/Files/ePayment%20Study.pdf. (дата звернення: 18.09.2023).
72. What are Petya and NotPetya Ransomware? | Malwarebytes. Malwarebytes. URL: https://www.malwarebytes.com/petya-and-notpetya. (дата звернення: 15.11.2023).
73. What is GameOver Zeus? - GOZ botnet explained | proofpoint US. Proofpoint. URL: https://www.proofpoint.com/us/threat-reference/gameover-zeus-goz (дата звернення: 25.09.2023).

74. What is mutual authentication?. Home - Visa Developer Community. URL: https://community.developer.visa.com/t5/Tutorials/What-is-Mutual-Authentication/ba-p/5757 (дата звернення: 25.09.2023).
75. World payments report 2023. Capgemini. URL: https://www.capgemini.com/insights/research-library/world-payments-report/ (дата звернення: 15.09.2023).