Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

Дипломної роботи
магістра
(назва освітньо-кваліфікаційного рівня)

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

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*
(назва освітньої програми)

освітньо-наукова програма *кібербезпека*

на тему: Захист даних платіжних карток при проведенні банківських операцій через інтернет-браузер

Виконавець: студент ІІ курсу, групи КБм-21

(підпис) **Луценко Владислав Володимирович** (прізвище ім'я по-батькові)

	Прізвище, ініціали	Оцінка	Підпис
Науковий керівник	Толюпа С.В.		
Рецензент	Степанов М.М.		
Нормоконтроль	Даков С.Ю.		

Київ 2022

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«__» _____ 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту КБм-21 (група) Луценку Владиславу Володимировичу (прізвище ім'я по-батькові)

Тема дипломної роботи Захист даних платіжних карток під час проведення банківських операцій через інтернет-браузер

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.2021

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес захисту даних платіжних карток від крадіжки.
Предмет досліджень	Методи захисту даних від витоку даних через дії хакерів
Мета	Розробка методу захисту від витоків даних платіжних карток при купівлі через інтернет-браузер.
Вихідні дані для проведення роботи	Методи захисту від витоку даних платіжних карток через інтернет-браузер.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна Удосконалення методу захисту даних платіжних карток за рахунок поєднання методів котрі впроваджені компаніями Visa, MasterCard, LiqPay

Практична цінність Покращення системи захисту даних платіжних карток під час банківських операцій в інтернеті.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Розробка плану для досягнення мети роботи	29.10.2021 – 23.01.2022
Аналіз літературних джерел	24.01.2022 – 14.02.2022
Розробка методу захисту від витоку даних платіжних карток через інтернет-браузер	15.02.2022 – 24.04.2022
Оформлення і друк пояснювальної записки	25.04.2022 – 19.05.2022

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження збитків через викрадення даних

Соціальний ефект Покращення технологій забезпечення захисту інформації як особисто так і на підприємствах.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____Луценко В.В._____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____Толюпа С.В.___
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____
Термін подання дипломної роботи до ЕК _____

УДК 004.492.2

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Захист даних платіжних карток при проведенні банківських операцій через інтернет-браузер»: 91 сторінка, 6 рисунків та 1 таблиця. 70 літературних джерел.

Об’єкт дослідження – процес захисту інформації від несанкціонованих витоків.

Мета роботи – розробка методу захисту даних платіжних карток від витоку через інтернет-браузер.

Методи дослідження – аналіз, класифікація, порівняння та опис.

У роботі досліджено сучасні загрози та методи протидії атакам задля отримання даних платіжних карток. Проведено аналіз наявних методів та засобів захисту з можливістю їх одночасного використання. Запропоновано метод захисту від втрати даних банківських карток.

Наукова новизна: запропоновано метод захисту від крадіжок даних пластикових карток під час використання через інтернет-браузері, за рахунок поєднання наявних методів захисту та виправлення недоліків при використанні.

Актуальність теми: Атаки з ціллю отримання даних платіжних карток є серйозною загрозою безпеки практично кожного громадянину та організації. Традиційний набір засобів захисту інформації не здатний протистояти наявним типам загроз. Поєднання та одночасне використання декількох методів захисту є найефективнішим механізмом виявлення такого типу загроз та протидії ним. Тому запропонований методу може використовуватися для покращення рівня безпеки онлайн платежів після впровадження його до інтернет-браузерів або банків-емітентів карток.

Ключові слова: банківські операції, пластикові картки, CVV2, Visa, MasterCard, соціальна інженерія, 3D Secure.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

PCI DSS - Payment Card Industry Data Security Standard

QSA - Qualified Security Assessor

SAQ - self-assessment questionnaires

НБУ - Національний банк України

НПС - національна платіжна система

НСД - несанкціонований доступ

НСМЕП - національна система масових електронних платежів

ІБ - інформаційна безпека

ІС - інформаційна система

ІТ - інформаційні технології

ОС - операційна система

ПЗ - програмне забезпечення

ПК - персональний комп'ютер

СЕК - система електронної комерції

СЕП - система електронних платежів

CMS - Content Management System

API - Application Programming Interface

ICSA - International Computer Security Association

DES - Data Encryption Standard

RADIUS - Remote Authntication Dial-In User Service

ЗМІСТ

РЕФЕРАТ 4
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 5
ВСТУП 8
РОЗДІЛ 1 МЕХАНІЗМИ ТА ПРИНЦИПИ ПРОВЕДЕННЯ БАНКІВСЬКИЇ ОПЕРАЦІЙ ЧЕРЕЗ ІНТЕРНЕТ-БРАУЗЕР 11
1.1 Витік інформації та порушення конфіденційності, цілісності та доступності інформації 11
1.2 Канали витоку конфіденційної інформації через інтернет-браузер 18
1.3 Основні загрози витоку даних в мережі інтернет 20
1.4 Принципи роботи банківських операцій в мережі інтернет 24
1.5 Загрози витоку платіжної інформації через інтернет-браузер 26
Висновки за розділом 1 31
РОЗДІЛ 2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ВІД ВИТОКІВ ДАНИХ ПЛАТІЖНИХ КАРТОК ТА АНАЛІЗ ЇХ ЕФЕКТИВНОСТІ 33
2.1 Аналіз та порівняння існуючих методів захисту 33
2.2 Основний перелік недоліків наявних методів та способів захисту даних платіжних карток 45
2.3 Оцінка ефективності та поширення методів захисту даних платіжних карток 51
Висновки за розділом 2 60
РОЗДІЛ 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ДАНИХ НА ОСНОВІ МОДЕЛІ ПОКРАЩЕНОГО МЕХАНІЗМУ ЗАХИСТУ 62
3.1 Сучасні методи захисту від витоків даних платіжних карток 62
3.2 Опис методів та засобів об’єднаного методу захисту платіжних карток 65

3.3 Аналіз ефективності даного методу та можливості його впровадження у банківську сферу 74

Висновки за розділом 3 77

ВИСНОВОК 79

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 85

ДОДАТОК А 91

ВСТУП

Актуальністю даної роботи є опис нового методу захисту інформації платіжних карток, котрі використовуються для оплати в мережі інтернет. Даний метод можливо буде впровадити та використовувати як для особистих карток так і для корпоративних, що значно поширює сферу застосування.

Основною задачею цієї кваліфікаційної роботи є знайти, розглянути, проаналізувати найефективніші та найбільш поширені варіанти захисту даних платіжних карток, визначаючи при цьому, яку інформацію можна віднести до інформації з обмеженим доступом та які інформацію слід захищати.

Науковою новизною цієї кваліфікаційної роботи є опис нового методу захисту котрий буде компіляцією існуючих методів захисту з мінімізацією недоліків під час використання за рахунок поєднання наявних технічних та організаційних способів захисту.

Мабуть кожна людина в якої є платіжна картка, хоча б один раз розраховувався нею в мережі інтернет. Здається що це дуже проста операція, може з точки зору користувача так воно і є, але насправді це дуже складна та багаторівнева система.

Об'єктом дослідження є процес захисту інформації від несанкціонованих витоків інформації, адже в наш час проблеми пов'язані з втратою даних або їх крадіжкою дуже актуальні та небезпечні, так як несанкціоновані дії користувачів призводять до виникнення загроз, а наявні методи захисту такі, як системи авторизації та автентифікації, спеціальні системи оплати, мережеві екрани, нажаль, не здатні забезпечити ефективний захист від такого типу загроз.

Предметом дослідження є методи захисту даних платіжних карток під час банківських операцій через інтернет браузер. Даними операціями можуть бути як і звичайні перекази з карти на карту, поповнення рахунків так і оплата комунальних або інших видів послуг.

Стрімкий розвиток інформаційних технологій та їх впровадження в усіх сферах діяльності значно удосконалює і прискорює багато бізнес процесів. Наявність або відсутність необхідної інформації, її збереження і захищеність від стороннього втручання істотно впливають на добробут компанії. Але з кожним роком все більше зростає кількість вірусів, мережевих атак, зловмисників, виникають загрози порушення конфіденційності інформації всередині компанії, що призводить до фінансових втрат. Вирішення питань захисту даних у сучасних інформаційних системах буде успішним лише за умови використання комплексного підходу до побудови системи забезпечення безпеки інформації.

Серед переваг інтернет-платежів є зручність оплати, економія часу, безпека платежів, широкий вибір можливостей для оплати послуг, для оплати потрібне лише підключення до мережі Інтернет.

У сучасному світі онлайн покупки стали дуже популярними, кожен день з’являються нові платіжні системи, за допомогою яких можна здійснювати процедури купівлі та продажу. Особливо з приходом карантину ми розуміємо на скільки важливими стали онлайн покупки.

Це не лише покупки в звичному розумінні, а іще всякі послуги такі як доставка, ремонт, прибирання, підписки на різні сервіси, та інше. В такому темпі розвитку особливо важливо приділяти увагу інформаційній безпеці.

Метою даної дипломної роботи є опис нового методу захисту, до якого буде входити перелік технічних та організаційних заходів, які необхідно впровадити емітентам карток або саме користувачам цих карток.

Багато людей розуміють що інтернет, а саме соціальні мережі, інтернет-браузери, веб-додатки, інтернет банкінг вже майже повністю проникли в наше життя.

Питання безпеки в мережі інтернет має беззаперечний рівень, адже майже кожен пристрій котрий ми маємо підтримує доступ до всесвітньої павутини. Телефони, комп’ютери, планшети, приставки, телевізори та багато іншого, все це потребує інтернету.

Знаходження дієвих методів способи нашого життя, в той час коли ми перебуваємо онлайн повинно бути обов’язковим.

Велика кількість людей думають що питання захисту в мережі є свого роду ілюзія, та бути надійно захищеним майже неможливо. Адже багато ресурсів збирають нашу конфіденційну та приватну інформацію. Однак, забезпечити такий захист цілком реально, хоча б для збереження не лише власний даних а й фінансових коштів.

Україна кожен рік потрапляє в анти рейтингові списки щодо піратства, розповсюдження шкідливого програмного забезпечення, DDoS атак та інше. Так, відповідно до дослідження корпорації Майкрософт, на 86% комп’ютерів в Україні встановлено неліцензійне програмне забезпечення [1].

Сформовані в результаті, теоретичні та практичні рекомендації можуть бути використані, як організаційна складова в процесі роботи над створенням та впровадження даного методу в банках та розробниками інтернет браузерів.

Описаний метод при подальшому дослідженні може бути використаний як додатковий ступінь захисту під час банківських операцій.

РОЗДІЛ 1
МЕХАНІЗМИ ТА ПРИНЦИПИ ПРОВЕДЕННЯ БАНКІВСЬКИЇ ОПЕРАЦІЙ ЧЕРЕЗ ІНТЕРНЕТ-БРАУЗЕР

1.1 Витік інформації та порушення конфіденційності, цілісності та доступності інформації

У глобальному масштабі регулюються не лише питання безпеки даних, а й питання безпеки цілих країн, оскільки національна безпека є одним із ключових понять не лише для України, а й для будь-якої іншої країни. Національна безпека є однією з головних умов нормального функціонування країни, адже вона має забезпечити все для безпечного життя. Вона охоплює велику кількість сфер життя кожного з нас.

Питаннями інформаційної безпеки займаються відповідні відділи інформаційної безпеки. Можна сказати, що це стан безпеки, при якому спеціальні інформаційні ресурси та активи не зазнають впливу внутрішніх і зовнішніх деструктивних факторів за рахунок спеціального обладнання та програмного забезпечення. На мою думку, це одна з найважливіших сфер національної безпеки, поряд з військовими та економічними.

Зараз війни йдуть не на полі бою, а в Інтернеті, фраза, яка чудово підкреслює важливість інформаційної безпеки.

Для того щоб ефективно захищати будь-які інформаційні ресурси потрібно визначити що таке інформація, які її види та властивості.

Поняття інформації неймовірно широке і трактується багатьма способами. У нормативно-правовій базі дається наступне визначення: інформація - будь-які відомості або дані, які можуть зберігатися на фізичних, електронних або іншого виду носіях[2].

Відповідно до Закону України "Про інформацію" [2] її розмежовують на:

- інформацію про особу - сукупність документованих або привселюдно повідомлених відомостей про особу;
- довідково-енциклопедичного характеру - систематизовані, задокументовані чи публічно відомі відомості про державне, суспільне життя та навколишнє природне середовище;
- науково-технічну - документовані чи привселюдно оголошені відомості про вітчизняні і закордонні досягнення науки, техніки, виробництва, що отримані в ході науково-дослідницької, проектно-технологічної, дослідно-конструкторської, виробничої і суспільної діяльності;
- статистичну - є офіційно задокументованою державною інформацією, що надає кількісно охарактеризує події та явища, котрі відбуваються в різних галузях життєдіяльності країни;
- масову - загальновідома думка та інформація котра поширена на відео, аудіо чи друкованими методами.

Захист інформації ведеться для підтримки таких властивостей інформації як: конфіденційність, цілісність та доступність. Це основоположні властивості інформації, які визначають напрями та аспекти захисту інформації.

Під конфіденційністю інформації розуміють неможливість розголосу та дотримання належної приватності при обробці та зберіганні інформації. Головною умовою конфіденційності є недопускання несанкціонованого доступу то інформації сторонніми особами [3].

Суть даної властивості полягає в тому, що необхідні інформаційні ресурси з’являються в тому вигляді, який потрібно користувачеві, де це потрібно користувачеві, і коли це потрібно користувачеві.

З розвитком інформаційного простору сформувалася так звана кіберзлочинність, метою якої є вторгнення, видалення або знищення інформаційного поля та воно стає мішенню кіберзлочинців.

За останні 10-15 років поняття «кіберзлочинність» трансформувалося в термін «кіберзлочинність» - поняття, яке охоплює фактичну кіберзлочинність та іншу незаконну діяльність, у якій комп'ютери є інструментами чи методами, авторське

право, громадську безпеку, етику. Таким чином, кіберзлочин є будь-яким злочином, котрий може бути скоєний за допомогою, всередині або проти інформації в комп'ютерній системі чи мережі. В принципі, він охоплює будь-який злочин, який можна вчинити в електронному середовищі [4].

Термін «кіберзлочинність» давно відомий у всьому світі, але зараз все частіше використовується в поєднанні з «комп'ютерна злочинність» і використовується як синонім.

В українській літературі найулюбленішим є поняття «комп'ютерна злочинність». Можливо, це пов'язано з тим, що більшість досліджень проводиться в криміналістичній чи процесуальній сферах. Крім того, частина XVI Кримінального кодексу України передбачає кримінальну відповідальність, яка спрямована на використання встановлених процедур автоматизованих систем [5].

Поняття кіберзлочинності багатогранне, тому на сьогодні немає чіткого визначення. Деякі тлумачать це як - протиправні дії, вчинені людьми, які використовують інформаційні технології у злочинних цілях, це визначення є досить абстрактним і не відповідає умовам сьогодення, оскільки все більше атак здійснюються за допомогою автоматичних систем. Натомість існують достатньо широкі поняття, такі як злочини у сфері комп'ютерної інформації [6].

У контексті розвитку інформаційного простору та всесвітньої мережі виникають такі поняття, як кібервійна. Його основним напрямком є порушення роботи інформаційних систем та доступу до інтернету державних установ, фінансових і великих приватних компаній, припинення та перешкоджання нормальному функціонуванню державних установ, які використовують глобальну мережу для вирішення різноманітних проблем.

Навіть конфлікти між воюючими сторонами все частіше проявляються у формі кібервійни через глобальну мережу. Можуть бути комп'ютерні атаки, мобільні атаки, пропаганда чи вандалізм.

Важко переоцінити, наскільки інтернет та інформаційні технології проникли в життя громадян і націй, оскільки не тільки атаки на мобільні пристрої, але й будь-який пристрій, який має доступ до інтернету, ваші дані можуть бути

скомпрометовані в усіх сферах життя. Війну слід розглядати як загрозу для всій національній безпеці.

Не дивно, що шпигуни в багатьох частинах світу використовують наявні діри в безпеці для шпигунства, саботажу та несанкціонованого доступу до інформації.

Західні експерти дійшли висновку, що домінуючими країнами у кібер-просторовій війні є Китай та США, представники яких категорично заперечують причетність державних органів до організації атаки [7]. Постійний розвиток сучасних технологій на мобільних пристроях постійно підвищує рівень кібервійни, яка з кожним днем стає все вищою та небезпечнішою.

Деякі країни виділяють достатні ресурси для запобігання кібервійні: організацію систем захисту, підтримку та підтримку спецпідрозділів, завданням яких є покращення та посилення інформаційної безпеки. Нині контроль і регулювання Інтернету визначає стан національної безпеки.

Ще наприкінці 2012 року в Дубаї відбувся Міжнародний саміт з кіберпростору, і суперечки про міжнародні телекомунікації наростають. Зокрема, США відмовилися підписати угоду про право всіх країн регулювати інтернет на користь понад 50 країн, у тому числі Франції, Великобританії та Канади.

З іншого боку Росія, Індія, Китай та інші країни, представники яких наголошують на рівноправності у всесвітній мережі. Тому підсумки цього саміту виявилися досить невтішними [8].

На даному етапі основним документом, що регулює міжнародне співробітництво у боротьбі з кіберзлочинністю, є Конвенція про кіберзлочинність. Даний документ визначає принципи вжиття заходів щодо боротьби з кіберзлочинністю на національному, міжнародному та міжнародному рівнях.

Міжнародне співробітництво допомагає вирішувати питання, пов’язані з екстрадицією кіберзлочинців, загальними принципами взаємодопомоги, отриманням інформації від іноземних конфіденційних органів, забезпеченням збереження інформації. Відповідно до даної Конвенції, видача осіб іншій стороні можлива за такі типи здійснених кібернетичних злочинів [9]:

- протизаконний доступ;

- неправомірне перехоплення;
- дія на дані функціонування системи;
- протизаконне використання пристроїв;
- фальшування та шахрайство з використанням комп'ютерних технологій;
- правопорушення, що пов'язані з дитячою порнографією;
- порушення авторських та суміжних прав.

Допускається також видача осіб іншим державам, у випадку замаху, співучасті чи підбурювання до здійснення вищевказаних злочинів. Видача осіб, які здійснили злочини, можлива за наявності у двох сторін передбаченого покарання у вигляді позбавлення волі, максимальний термін якого визначається не менше як один рік.

Суттєве значення в рамках Організації Об'єднаних Націй має «Резолюція про боротьбу з використанням інформаційних технологій», прийнята на початку XXI століття у 2001 році, яка вказувала на необхідність співпраці держави та приватного сектора у боротьбі з використанням інформаційних технологій [10].

Співпраця у боротьбі зі злочинністю у сфері інформаційних технологій має захищати комп'ютерні системи шляхом закріплення відповідальності за інформаційні злочини до закону, транснаціонального співробітництва правоохоронних органів, міжнародного обміну інформацією щодо використання інформаційних технологій злочинності, шкідливих програм на усіх пристроях, навчання діяльності правоохоронців в інформаційному суспільстві та захист комп'ютерних систем від несанкціонованого втручання, забезпечення збереження інформаційних даних та своєчасного збору доказів у кримінальних справах.

У пункті 1 Резолюції вказано, що інформаційні технології мають розроблятися таким чином, щоб сприяти попередженню та виявленню випадків злочинного використання шкідливого програмного забезпечення на мобільних пристроях, відстеженню злочинців та збиранню доказів [9].

Цей пункт надає правоохоронним органам окремої країни право здійснити виявлення та затримання злочинців у короткий термін з більшою ефективністю. Але існує можливість неправомірного доступу злочинців до вищевказаних технологій з

використанням замаскованих можливостей систем, з метою здійснення інформаційних злочинів, таких як крадіжка персональних даних.

Ще у 1996 році країнами Великої Вісімки було прийнято рішення про створення спеціальної групи по боротьбі з міжнародними злочинами у сфері високих технологій - «Ліонська група» [11].

В цей же час керівники цих країн схвалили прийняття плану, що складається з десяти пунктів, по протидії кіберзлочинам. З найбільш важливих пунктів документу, варто відмітити [11]:

- створення в кожній країні контактного центру, працюючого 24 години на добу, для співпраці у боротьбі з інформаційними злочинами;
- надання допомоги кваліфікованими співробітниками правоохоронних органів іншим державам;
- розробку і використання сумісних стандартів для отримання і перевірки достовірності електронних даних у ході судового розслідування;
- ознайомлення із законодавчими методами боротьби з комп'ютерними правопорушеннями країн учасниць даного договору.

На щорічній сесії країн НАТО, що проходила наприкінці 2000-х років, була підготовлена доповідь - «НАТО і кіберзахист». У доповіді були наявні основні засади які сприяють ефективному захисту від можливих кібернетичних загроз. Так, на міжнародному рівні, було запропоновано ввести в законодавства країн, такі терміни: «кібервійна», «кібератака», «кібертероризм» [12].

Додатково була відмічена необхідність тісного співробітництва країн з приватними організаціями й компаніями, які надають послуги інтернету для забезпечення захисту.

Крім того, у рамках розвитку заходів по кіберзахисту країн НАТО, було рекомендовано сприяти Росії, Китаю, Бразилії і Індії, до швидкого їх приєднання до «Конвенції про кіберзлочинність» [12]. Блоком країн НАТО, в Талліні у 2008 році був відкритий сучасний центр по проведенню досліджень і навчань в області кіберзахисту та веденню військових дій у кіберпросторі [13].

У рамках співпраці держав-учасників СНД, ще у далекому 2001 році було вироблено угоду по боротьбі із злочинами у сфері комп'ютерної інформації, за якою, сторони здійснюють співпрацю у формах [13]:

- обміну інформацією;
- проведення розслідувань в області комп'ютерної інформації;
- сприяння в підготовці кадрів;
- проведення спільних наукових досліджень;
- створення інформаційних систем(ІС);
- обмін нормативно-правовими актами і науково-технічної літератури по боротьбі з комп'ютерними злочинами.

Також у цьому документі було сказано, що країни СНД здійснюють спільну роботу на підставі запитів компетентних органів про сприяння, а час на його виконання не повинен перевищувати 30 діб з дня його отримання. Відмова в його виконанні допустима, у разі, якщо його виконання суперечить національному законодавству запрошеної сторони.

Але Російська Федерація прийняла угоду з обмовкою - відмова у виконанні запиту допустима, якщо його виконання може завдати збитку суверенітету або безпеці РФ [14].

Міжнародне законодавство грає дуже важливу роль у боротьбі з кіберзлочинами. Такі кроки як, створення цілодобових центрів реагування, законодавче визначення понять «кіберзлочини», видача осіб, що їх вчинили, міжнародна взаємодія співробітників компетентних органів, проведення навчань та обмін інформацією, сприяють здійсненню ефективних методів реагування і боротьби з міжнародними злочинами, що здійснюються в кіберпросторі.

Розвиток сучасних інформаційних технологій для користувачів сучасних мобільних пристроїв має тенденції до все більшого прискорення, тому нормативно-правова база має не тільки встигати за ним, але й змінюватися, задовольняючи у цьому всі нагальні проблеми людини, суспільства і міжнародного співтовариства у сфері інформаційної безпеки [14].

Нажаль навіть у концепції про кіберзлочинність ми на знайдемо чіткого визначення «кіберзлочинності», проте в ній вказано що за такого типу протиправні дії повинно бути передбачене кримінальне покарання а також на необхідність створення систем та заходів задня її протидії.

1.2 Канали витоку конфіденційної інформації через інтернет-браузер

В реаліях сучасного світу ми живемо в просторі який переповнений різноманітною інформацією, яка описує: явища, предмети, відчуття, тощо. Ми обмінюємося своєю особистою інформацією, інформацією стосовно своїх близьких чи колег, розповідаємо як у нас справи на роботі та чим ми були зайняті. У всьому цьому різноманітті інформації встає питання необхідності класифікації інформації за формою доступу.

Згідно із Законом України "Про інформацію" [2], за режимом доступу інформація поділяється на відкриту та з обмеженим доступом.

Відкрита інформація - це інформація, яка доступна для користування всіх, виходячи з ціни, зрозумілості і простоти у викладі. Подібна інформація повинна систематично публікуватися в офіційних друкованих виданнях, поширюватися засобами масової інформації, безпосередньо надаватися зацікавленим громадянам, державним органам та юридичним особам.

Згідно Закону України «Про державну таємницю» перша стаття має визначення державної таємниці такою як - різновид секретної інформації, яка містить в собі деталі у сфері оборони, захисту, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку, безпеки громадян країни. Розголос таких даних завдає пряму загрозу для важливих інтересів інтересам України, таких що були визначені у порядку, встановленому таким законом, державною таємницею та підлягають охороні державою [15].

Відповідними державними органами визначаються правила обігу таємної інформації та її захисту за умови дотримання вимог, встановлених цим законом.

Одним із специфічних видів конфіденційної інформації можна виділити конфіденційну інформацію про особу. Її правовий статус визначається Законом України "Про інформацію", а офіційне тлумачення викладене у Рішенні Конституційного Суду України № 5 від 30 жовтня 1997 року.

Аналіз їх матеріалів дає підстави віднести до конфіденційної інформації про особу також дані про: інтимні сторони життя, захворювання, неблаговидні вчинки.

В ході роботи багатьох організацій вони оперують переважно конфіденційною та особистою інформацією, адже для роботи з інформацією під грифами секретності необхідна відповідна акредитація від Служби безпеки України. Тому в переважній більшості компаній стає питання захисту саме конфіденційної інформації.

Каналом витоку інформації можна вважати можливість передачі інформації будь-яким способом. При обробці інформації мобільними пристроями завжди є обмін інформацією між різними елементами інформаційного поля, тому можна казати про наявність каналів обміну або каналів витоку інформації.

Загалом, канал витоку інформації - це певна сукупність джерел інформації, певного носія інформації або середовища розповсюдження сигналу, котрий переносить в собі інформацію, і засіб виділення інформації з сигналу або носія.

Це зокрема розглядається як вірогідність некерованого розповсюдження інформації, яка призводить до отримання інформації неправовим методом [16].

Якщо даний аспект розглядати як захист інформації, каналів або інформаційних потоків, то вони можуть бути законними або незаконними. Незаконний інформаційний потік створює витік інформації і, зокрема цим порушує приватність та секретність або, можливо, цілісність та прозорість даних.

Служба інформаційної безпеки повинна контролювати всі відомі канали витоку. Загалом, в будь-якій системі можна виділити відкриті канали витоку, тобто ті, які вдалося ідентифікувати і які контролюються засобами захисту і приховані, в яких витік відбувається шляхом, який не контролюється засобами захисту.

Загалом, канали витоку інформації класифікують за такими групами, перша група каналів, які пов’язані з доступом до елементів системи обробки даних, але такі, що не потребують зміни компонентів системи.

Друга група каналів пов’язана з доступом до елементів системи і зміною структури її елементів.

До третьої групи каналів включають незаконне підключення спеціальної реєструючої апаратури до пристроїв системи або ліній зв’язку чи виведення з ладу механізмів захисту.

До четвертої групи можна віднести несанкціоноване одержання інформації шляхом підкупу або шантажу посадових осіб відповідних служб.

1.3 Основні загрози витоку даних в мережі інтернет

Наразі інтернет-браузери здобули нечувану популярність через свою величезну кількість і можливість встановлення на велику кількість пристроїв.

Результати останніх досліджень було виявлено, що трафік через інтернет-браузери становить 52% використання Інтернету у світі.

На основі проведеного дослідження можна спрогнозувати модель типового користувача інтернет-браузеру - це особо середнього віку, від 16 до 40 років, які проживають в обласний та районних центрах України там мають вищу або середню освіту [17].

З багатьох причин недосвідчені або неуважні користувачі інтернет-браузерів завантажують та встановлюють зловмисне програмне забезпечення, яке може нанести шкоду, чи принести збитки компанії, в якій вони працевлаштовані. Зловмисник зможе отримати доступ до соціальних мереж, особистої та корпоративної пошти, даних платіжних карток, списку контактів, фотографій, даних які зберігаються на хмарних сховищах. Хакери зможуть вимагати грошові кошти або повністю заблокувати пристрій, чи використовувати його для атак по мережі.

Особливу небезпеку для захисту інформації несуть відкриті Wi-Fi мережі, адже кожен має змогу підключення до них та зможе виконувати необхідні зловмисні дії.

Також небезпеку становлять і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись прочитавши пароль з чеку чи дізнавшись

його у працівника, тобто у зловмисника не повинно виникати складнощів у пошуку цього паролю.

Особлива небезпека спідкає користувачів, коли ненадійний або стандартний пароль використовується для панелі адміністрування, в такому випадку всі пристрої піддаються ризику стати ціллю хакерської атаки. Майже третина користувачів використовують в якості пароля слова або словосполучення з переліку - 10 000 паролів.

На рисунку 1.1 зображено кількість успішних атак хакерами під час проведення банківських операція в інтернет браузері.

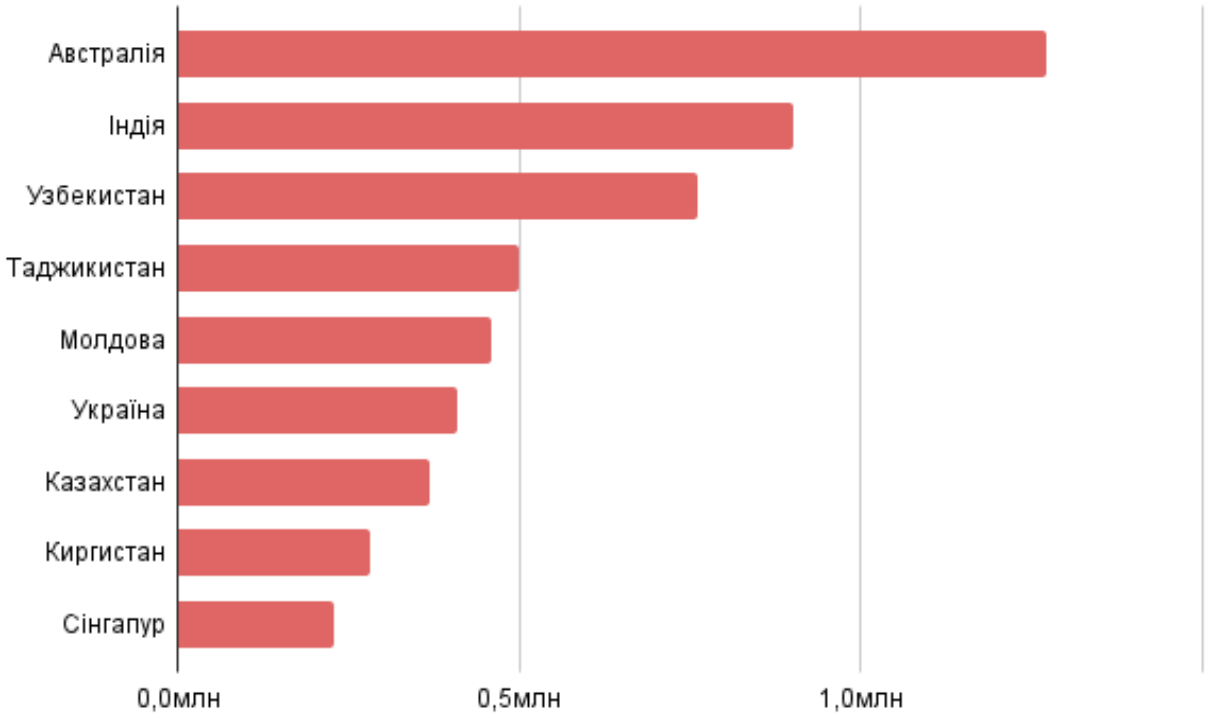

Рисунок 1.1 – Кількість успішних атак в банківському секторі онлайн

Ще однією причиною серйозних хакерських атак в останній час є мала надійність. Після підключиться до мережі зловмисник отримує доступ абсолютно до всіх пристроїв які мають активне інтернет з’єднання з цією точкою доступу.

Програми для злому паролів, засновані на словниках, в першу чергу аналізують найпоширеніші варіації серед яких , зазвичай, і опиняються подібні версії. У кращому випадку, це може збільшить час злому і надасть додаткові

можливості для того, щоб система захисту змогла ідентифікувати атаку, якщо вона є.

Більшість компаній виявляють проблему шкідливого програмного забезпечення на пристроях протягом одного дня 37,3%. Протягом однієї години це вдається зробити в 11,5% організацій, та близько тижня необхідно для 31,5% компаній. Іншим компаніям потрібно більше часу. Збитки, нанесені в результаті кібератак, виражаються переважно в перебоях роботи системи 58,4%, втраті даних 25,2% та неавторизованому доступ до конфіденційної інформації 14,9%. Крім того, не потрібно забувати про репутаційні та часові витрати, коли в результаті дій зловмисників фахівці втрачали час та не могли скористатися необхідним обладнанням [18].

На рисунку 1.2 більш детально проілюстрована дана інформація.

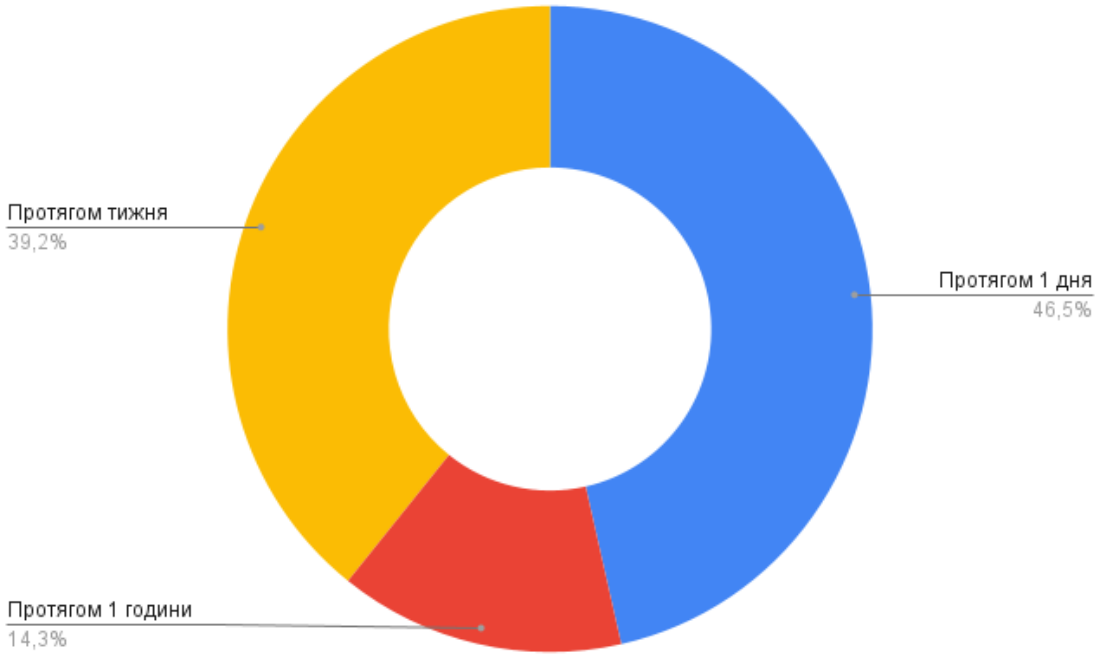

Рисунок 1.2 – Швидкість реакції на шкідливе ПЗ

Варто розуміти, що для мобільних пристроїв притаманні дуже схожі загрози, що і для повноцінних комп’ютерів, тому що телефон це і є комп’ютер, тільки зменшений та з операційною системою, яка була створена для роботи на мобільних пристроях.

Це обумовлює і можливість запуску шкідливого програмного забезпечення на мобільних пристроях, і шпигунства за власниками мобільних пристроїв, і крадіжку конфіденційної інформації, крадіжку грошей з мобільних рахунків, крадіжку коштів за банківських рахунків та крадіжку даних, які можуть зберігатися на мобільному пристрої.

Розглянемо проблему троянських програм більш детально. На жаль, більшість громадян не замислюються над безпекою мобільних пристроїв.

Сьогодні існує величезна кількість загроз: троянські програми, віруси, мережеві хробаки, рекламні модулі, модулі інтеграції, котрі спрямовані на зовсім різні платформи для мобільних пристроїв. Також є окремий клас шпигунських програм, які відносяться до так званих легальних шпигунських програм [19].

Встановлення подібної програми на пристрій користувача, дозволяє встановити стеження за ним всюди, адже хоча б один з пристроїв практично завжди з власником та майже завжди має доступ до інтернету. Слідкувати можна не лише в плані дій в самому пристрої, але і за безпосереднім оточенням користувача - реальним життям, де він перебуває, які місця він відвідує, яке у нього коло оточення і звісно за його витратами.

На основі досліджень, які проводились, можна зробити висновок, що класичні віруси майже не вивчаються та не розробляються. Зокрема для мобільних гаджетів розробляють так звані троянські програми, рекламний модуль, бекдор програм [20].

Слід зрозуміти, що такі вірусні програми створюються майже для всіх операційних систем, на які можна встановити додаткове програмне забезпечення. Це означає що, якщо на ваш мобільний пристрій або сам інтернет-браузер можна встановити додаткову програму, це автоматично означає, що туди можуть потрапити шкідливі програми. Але коли ця програма не потрапляє туди самостійно, то тут вже сам користувач завантажує її автоматично, використовуючи існуючи засоби новітніх методів сучасних соціальних технологій [20].

Наприклад, користувачу інтернет-браузеру запропонують встановити цікаву гру або додаток але після встановлення виявляється, що це не лише гра чи додаток, а й шкідлива програма. Або взагалі ці програми не маскуються, а просто почнуть

виконувати зловмисні дії. Тільки пристрої з повною забороною на встановлення додаткового програмного забезпечення є захищеними.

1.4 Принципи роботи банківських операцій в мережі інтернет

Загальні засади функціонування платіжного ринку, відносини у сфері надання платіжних послуг користувачам регулюються Конституцією України, Законом України про платіжні системи та перерахування коштів в Україні від 05.04.2001 року № 2346-III, Законом України про платіжні послуги № 1591-IX від 30.06.2021 року, іншими законами України та прийнятими на їх основі нормативно-правовими актами.

Проведення банківських операцій змінило наше повсякденне життя і продовжує змінювати. На рисунку 1.3 можна побачити як з року в рік зростала кількість онлайн платежів [21].

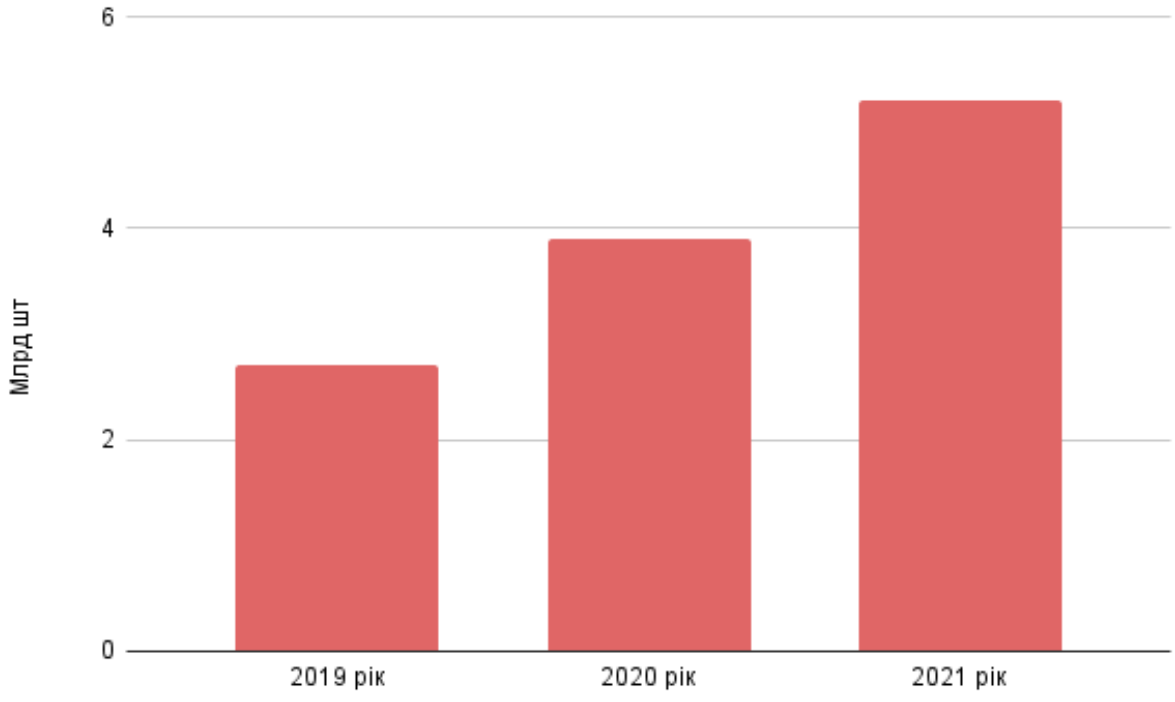

Рисунок 1.3 - кількість онлайн-платежів в Україні

В Україні існує основна система онлайн-платежів електронних платежів НБУ (СЕП) - загальнодержавна платіжна система, яка є забезпеченням для здійснення

розрахунків між банківськими установами, органами державного казначейства із застосуванням електронних засобів приймання, обробки, передавання та захисту інформації, та іншими учасниками фінансового ринку.

Термін, протягом якого погоджують платіжний документ між учасниками розрахунку коливається в розрізі від 10 хв. до 2 год. Система СЕП працює в режимі реального часу , що дає змогу завершити розрахунки між учасниками фінансового ринку протягом операційного дня. Загалом на протязі робочого операційного дня система може здійснити декілька, частіше це здійснює 2-3-разовий обіг коштів по рахунках банків, а в період найбільш активних платіжних днів, економічна активність системи може сягати аж до вісьми оборотів на день [22].

Інтернет-еквайринг - це найпопулярніший спосіб здійснення онлайн-платежів. Являє собою переказ коштів з банківської картки покупця на рахунок продавця за участю банку та процесингової компанії.

Процесингова компанія надає інтерфейс для здійснення покупки онлайн та проводить процедуру списання або зарахування коштів. Вона може належати банку чи бути незалежною стороною.

Якщо говорити про захист від несанкціонованих перекладів СЕП загалом, то незалежно від рівня кожної конкретної моделі до них діють однакові вимоги.

При роботі звісно виникають вразливості безпеки, котрі змушують банки та операторів забезпечувати захист трафіку при пересиланні даних та розробляти моделі автентифікації відправника та одержувача коштів.

Серед найбільш уразливих місць є інтернет-трафік між учасниками обміну електронними повідомленнями фінансових установ таких як: банки, операторами платіжних гаманців, страхові компанії та обробка інформації всередині банку або оператора.

При цьому у роботі банку можуть виникати такі проблеми [23]:

- визначення взаємної справжності учасників трансакції під час встановлення з'єднання;
- забезпечення конфіденційності та справжності платіжних доручень, що надсилаються через інтернет;

- захист процесу відправлення, формування доказів відправлення та отримання документів.

Банк та оператор СЕП зобов'язані реалізувати механізми захисту клієнтів від несанкціонованих списань грошових коштів, конкретні вимоги до яких визначаються політиками операторів та регламентами НБУ.

Серед таких регламентів варто виділити [24]:

- управління доступом клієнта, співробітників оператора та одержувача, створення механізму аутентифікації;
- контроль справжності та цілісності інформації у повідомленні;
- забезпечення конфіденційності відомостей у процесі передачі;
- неможливість відмовитися від авторства доручення на надсилання коштів або повідомлення;
- гарантії доступу до ресурсів та збереження повідомлення в дорозі;
- неможливість оператора чи банку відмовитися від виконання доручення на переказ чи платіж;
- збереження даних за дорученнями та повідомленнями.

Для здійснення платежів за допомогою банківських карток міжнародні системи переказів застосовують власні заходи ІБ міжкарткових переказів.

Платіжна система - це спосіб здійснювати фінансові транзакції без використання готівки, за допомогою банківських карток та електронних грошей.

1.5 Загрози витоку платіжної інформації через інтернет-браузер

Проаналізувавши загрози котрі можуть підстерігати користувачів пластикових карток та злочини у сфері банківських крадіжок можна виявити певні схеми або типову поведінку зловмисників чи шкідливих програм.

Вказані схеми шахраї застосовують найчастіше, видаючи себе за «покупців» товарів, які виставлені на продаж в мережі Інтернет. Іноді шахраї обирають людину із відомим їм номером телефону.

Наприклад, шукають на сайті приватних оголошень, де зазвичай продавці вказують свої мобільні номери [25].

Якщо шахрай видає себе за покупця, то найчастіше зловмисник прагне вивідати секретні реквізити картки продавця, аргументуючи необхідність здійснення передоплати за товар. Шахраї можуть працювати в парі: один запитує у продавця номер картки, а другий дзвонить нібито від імені банку, повідомляє про надходження грошей на картку, які, проте потрібно ще нарахувати, а для цього продавець повинен повідомити секретні реквізити своєї картки.

Шахрай, який видає себе за покупця, або його напарник видає себе за співробітника банку може відправити продавця до банкомату, нібито для того, щоб «допомогти нарахувати» передоплату на товар. У банкоматі користувач може перевести гроші лише з власної картки на чужу, а не навпаки. Шахрай буде намагатися заплутати свою жертву, щоб вона власними руками допомогла йому.

В іншому випадку зловмисник видає себе за продавця, тоді злочинці, видаючи себе за продавців, зазвичай пропонують покупцям придбати неіснуючий товар.

Незалежно від типу товару, є загальні ознаки для всіх злочинних схем [26]:

- шахраї пропонують товар за більш низькою ціною, ніж інші продавці. Наявність і якість неіснуючого товару підтверджується за допомогою знайдених в Інтернеті фото, до речі, покупець може знайти джерело фото за допомогою можливостей пошукової системи Google й таким чином зрозуміти, продавець товару сфотографував пральну машинку, яку продає, або товару у нього насправді не існує;
- шахраї вигадують різні приводи, чому покупцеві слід перевести всю вартість товару відразу або зробити значну передоплату, в якості аргументів може використовуватися будь-яка причина, в тому числі, загроза, що товар купить хтось інший;
- шахраї можуть спробувати дізнатися секретні дані вашої картки, нібито для здійснення платежу з неї за цією схемою шахраї також можуть діяти в парі, коли один видає себе за продавця, а інший - за співробітника банку «через який проходить платіж», аргументи зазвичай зводяться до того, що при нарахуванні грошей саме на «картку такого типу», як у продавця.

Будьте уважні, якщо продавець товару поводиться дивно, не хоче надсилати нові фото товару, а вимагає передоплату або повну оплату вартості товару.

Ніколи не робіть повну оплату товару до того, як отримали його. Обирайте функцію післяоплати. Скористайтеся послугою «Безпечна угода» від компанії «Нова пошта». Вона передбачає оплату карткою, суму, що дорівнює вартості товару, «блокується» на карті покупця. Після отримання товару сума переводиться на карту продавця. У такому випадку, захищені від шахрайства обидві сторони угоди.

Окремою сферою у злочинців існують фішингові сайти та сервіси. Зловмисники створюють сайти, що як дві краплі води схожі на сайти легітимних сервісів для грошових переказів і поповнення мобільного телефону, з ціллю дізнатися секретні дані банківської картки користувача.

Даний тип шахрайства називається шахрайством за допомогою фішингових сайтів. Такі сайти роблять привабливою оплату карткою через інтернет для клієнтів, а саме [27]:

- пропонують більш вигідні послуги, наприклад, з нульовою комісією;
- дизайн сайту схожий на популярний сервіс;
- за допомогою платної реклами шахраї навіть піднімають рейтинг веб-ресурсу і він потрапляє в перші рядки пошукової видачі по тематичних запитах.

Фішингові сервіси пропонують клієнтам заповнити платіжну форму. Користувач повинен ввести конфіденційні дані власної картки: номер, термін дії картки, тризначний код безпеки зі зворотного боку картки, код CVC2, в окремих випадках - підтверджує операцію кодом з sms від банку. Шахраї використовують отриману інформацію, щоб вкрасти гроші з рахунку.

Також хакери створюють веб-ресурси для продажу дешевих авіаквитків або підроблені онлайн-сервіси для отримання кредиту, на них теж треба вказати дані своєї картки. При спробі купити, наприклад, авіаквиток через фішингових сайтів клієнт може навіть «отримати його на руки»: користувач вводить секретні дані своєї картки в платіжній формі, отримує підтвердження про нібито придбання квитка і навіть, в окремих випадках, може його роздрукувати.

Однак насправді квиток виявляється недійсним. Тим часом дані вашої картки шахраї можуть використати для крадіжки грошей з рахунку. Для безпечної оплати в Інтернеті завжди перевіряйте репутацію обраного сервісу.

Комп'ютерні віруси та троянські програми котрі користувач може завантажувати з інтернету можуть знаходиться у будь-яких підозрілих та неперевірених програмах. Такі програми можуть стати вірусами, вони захоплюють контроль над комп'ютером, видаляють і встановлюють інші програми.

Проте найнебезпечніше є те, що вони можуть «зливати» особисту інформацію. Так звані мережеві атаки діють методом пошуку вразливих місць в операційних системах комп'ютерів і крадуть ваші дані для різних цілей, серед який [28]:

- злом комп'ютера та відключення від соціальної мережі, якщо девайс - це сервер, який надає інтернет-сервіс клієнтам;
- установка шкідливих програм та крадіжки особистих даних;
- блокування певних програм та додавання комп'ютера під небезпечний ботнет.

Ще одна величезна сфера за допомогою якої зловмисники отримують доступ до ваших даних це - соціальна інженерія.

Працює це приблизно так, людині дзвонить шахрай, представляється родичем, співробітником банку або інших установ, і випитує особисті дані, якими ніхто не ділився б з незнайомим. Кількість прийомів, які вигадали шахраї, безліч. Вони дзвонять, пишуть повідомлення на телефон або e-mail, надсилають файли, що виявляються вірусами.

Небезпеку також становлять сайти які змушують оформити розсилку для них. Дані ресурси схожі або повністю копіюють відомі сайти, щоб користуватися довірою клієнта. На даних ресурсах жертви вводять свої дані, щоб увійти до свого облікового запису, таким чином і відбувається витік інформації.

Звісно, мало хто замислюється над мінімізацією публікації особистої інформації до інтернету. Дана небезпека стосується людей, які люблять ділитися у соцмережах інформацією про свої плани. Наприклад, пишуть про заплановані подорожі, а шахраї бачать у цьому інформацію - коли квартира буде порожня і її

можна пограбувати або ж які покупки ви можете здійснити у найближчому майбутньому.

Існує велике різноманіття шляхів через які хакери атакують користувачів. На рисунку 1.4 зображено джерела, котрі використовують зловмисники для атак [29].

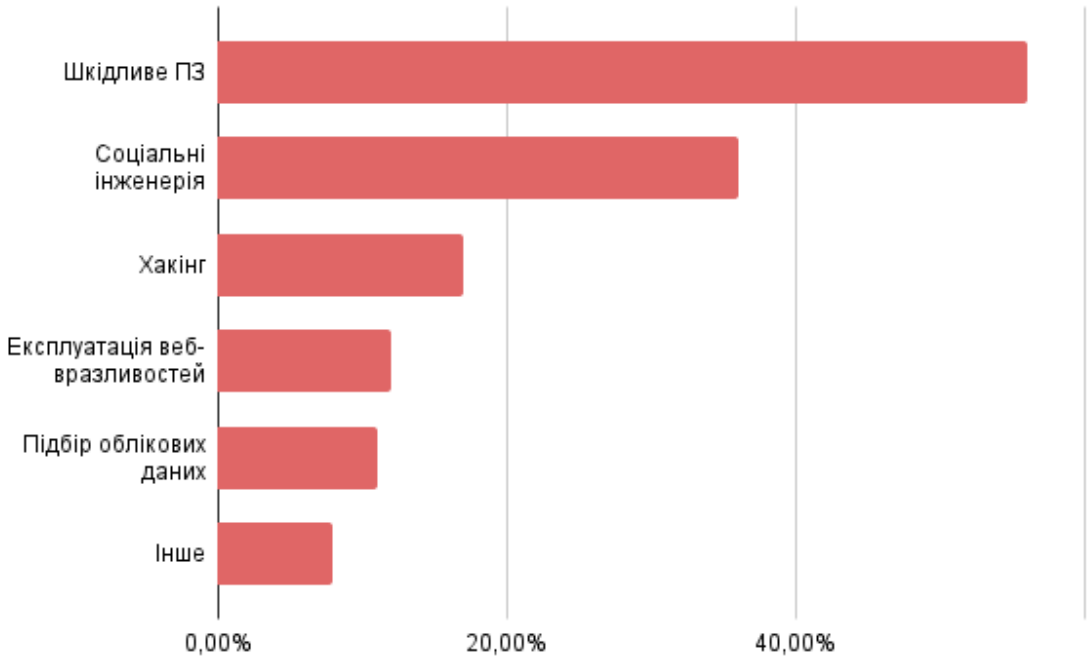

Рисунок 1.4 – Шляхи якими діють шахраї під час злочинних дій

Система для оплати через інтернет функціонує постійно і на неї спрямована величезна кількість загроз. Серед основних чинників, котрі впливають на стан інформаційної безпеки у зв'язку із використанням загальнодоступних та соціально орієнтованих ресурсів мережі Інтернет:

1. Сьогоднішня ситуація у країні та як наслідок масовані кібератаки, масштабні проти українські інформаційні кампанії, а саме психологічний вплив на українських користувачів всесвітньою павутиною, отримання несанкціонованого доступу до конфіденційної інформації або інших таємних даних з електронних поштових, скриньок або соціальних мереж.

2. Загрози державним органам, а саме фінансовим установам, міністерствам, відомствам, через використання працівниками у службовій діяльності та

повсякденному житті програмного забезпечення та програмного забезпечення неперевіреного походження іноземного виробництва.

3. Маніпулювати медіа та соціальними мережами, щоб охопити більшу аудиторію, використовуючи методи соціальної інженерії.

4. Використання соціальних мереж для поширення недостовірної або деструктивної інформації та маніпулятивного впливу на суспільну свідомість користувачів української частини мережі Інтернет.

Для забезпечення мінімального рівню захищеності доцільно дотримуватись мінімальних правил користування мережею через інтернет-браузер, а саме [30]:

- не варто вмикати геолокацію та функцію пошуку вашого акаунта через соціальній мережі за номером мобільного телефону або поштовою скринькою;
- регулярно перевіряйте список друзів у соціальних мережах. Якщо в них є незнайомі або підозрілі люди чи акаунти, то їх слід видалити, оскільки статус «друг» зазвичай відкриває доступ до більш приватної особистої інформації;
- ви повинні буди обережні, додаючи нових користувачів до списку друзів;
- налаштувати двофакторну автентифікацію на всіх облікових записах.
- не відповідати незнайомим користувачам;
- у підозрілих ситуаціях встановіть сервіси VPN;
- не встановлюйте жодних програм, які рекомендують в інтернеті. Це необхідно робити лише з перевірених джерел.

Доцільним є довіра лише до перевірених ресурсів та сервісів. Якщо ви почули новину про якусь акцію чи вигідні умови купівлі в інтернеті, перш за все переконайтесь чи вона правдива. Вивчення правила безпеки в мережі зможу значно знизити ймовірність стати жертвою шахраїв.

Висновки за розділом 1

Наразі важко переоцінити, який вплив онлайн платежів мають на наше життя. Сучасні способи оплати стали невід’ємною частиною нашого життя, але окрім

зручності та багатьох технічних можливостей вони можуть стати причиною втрати не лише ваших даних, а й фінансових коштів.

Платіжна система є невід'ємною частиною фінансової інфраструктури ринкової економіки та має ключове значення для грошово-кредитного регулювання, забезпечення ефективного платіжного обслуговування фінансової систем держави й реального сектору економіки.

Платіжну систему як один з інструментів безготівкової форми розрахунків доцільно розглядати в двох аспектах: функціональному та інституціональному. З точки зору функціонального аспекту платіжна система є сукупністю механізмів, форм, методів, принципів організації переказу коштів від однієї особи іншій за законами, правилами та стандартами, що визначають права, обов'язки та відповідальність учасників. Інституціональний аспект дозволяє розглядати платіжну систему як сукупність інститутів, що законодавчо регулюються та забезпечують виконання боргових зобов'язань, які виникають в процесі економічної діяльності [31].

Кожного дня користуючись інтернет-браузерами ми наражаємо себе на небезпеку. Користувачі не лише читають новини, дивляться прогноз погоди, передивляються відеоролик, а й ведуть розрахунки банківськими картками.

Перелік послуг чи товарів котрі ми можемо оплатити або придбати через мережу інтернет майже нескінченний. Проте, нажаль мало хто замислюється над тим які ризики це за собою веде чи яку свою особисту інформації ви наражаєте на небезпеку.

Щоб навчитися правильно захищати не лише свою інформацію, а й фінанси необхідно розуміти механізми захисту котрі все наявні та можливі для використання на вашому пристрої, банківській картці чи інтернет-браузері.

Під час купівлі чи оплати через інтернет-браузер ви можете зіштовхнутися із загрозами одразу з декількох джерел, а саме: операційна система пристрою, інтернет-браузер, загрози банківської системи та навколишні чинники.

РОЗДІЛ 2
МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ВІД ВИТОКІВ ДАНИХ ПЛАТІЖНИХ КАРТОК ТА АНАЛІЗ ЇХ ЕФЕКТИВНОСТІ

2.1 Аналіз та порівняння існуючих методів захисту

Питання захисту даних платіжних карток завжди було одним з основних під час роботи банківських установ, а згодом і для розробників програмного забезпечення.

Такі компанії, як Apple, Bank of America, Google, PrivatBank, OTP, Samsung, Visa, MasterCard, American Express та інші давно працюють над цим.

Наразі існую досить багато методів та сервісів котрі можуть гарантувати безпеку під час онлайн оплат через інтернет-браузер.

Однією з провідних систем, котра забезпечує безпеку інтернет-платежів є система 3D Secure.

Автор протоколу 3D Secure (3DS) - міжнародна платіжна система Visa, програма Verified by Visa. 3DS підтримується ключовими світовими платіжними системами: MasterCard SecureCode та J-Secure від JCB International [32].

Основне завдання 3DS - захистити платників та підприємства від шахраїв. Підтримка протоколу 3DS практично ліквідує небезпеку здійснення шахрайських операцій за допомогою банківської картки, оскільки є ще одним способом підтвердження особи платника.

3D Secure допоможе захистити себе від шахрайства завдяки надійним механізмам захисту. Коли ви робити покупки, перераховуєте гроші, то ваші особисті дані можуть бути розкриті, або навіть викрадені. Тільки в Європі 60% шахрайства з картками пов’язана з онлайн-транзакціями.

Дана технологія розшифровується як 3-Domain Secure (3DS), це протокол безпеки, який підвищує надійність карткових переказів через мережу Інтернет. Як виходить із назви, 3D Secure поєднує три сторони, які беруть участь в онлайн-транзакції, а саме [33]:

- отримувач платежу;
- емітент карти;
- платіжна мережа.

Принцип, який лежить в основі 3D Secure, досить простий, вашому банку необхідно підтвердити вашу особистість, щоб авторизувати платіж. Після вводу платіжних даних вас перенаправлять на сторінку аутентифікації вашого банку. На даному етапі вам необхідно буде підтвердити свою особистість.

Підтвердження особистості може бути виконане різними способами. Зазвичай вас просять ввести пароль або унікальний код, який вам було відправлено по SMS. Іноді просять підтвердити платіж в додатку вашого банку, алгоритм роботи 3D Secure для вашої карти залежить від вашого банку. Наприклад, візьмем один з найбільших банків України УкрСиббанк.

Така ідентифікація забезпечується шляхом обов'язкового введення тримача картки одноразового паролю, який під час проведення операції автоматично направляється банком в SMS-повідомленні на номер мобільного телефону такого тримача, який підключений до послуги SMS-інформування.

Розглянемо перелік дій для оплати товарів і послуг онлайн за допомогою картки з технологією 3D Secure на сайтах торгово-сервісних компаній, що підтримують цю технологію [33]:

1. Клієнт оформлює платіж і вказує необхідні реквізити платіжної карти на сайті торгово-сервісного підприємства.

2. Автоматично відбувається переадресація на захищений сайт УкрСиббанка з одночасною відправкою клієнту SMS-повідомлення від Банка з одноразовим паролем (пароль діє 10 хвилин).

3. Клієнт вказує пароль, отриманий в повідомленні, в спеціальній формі на сайті Банка.

4. Проводиться автоматичне повернення до сайту підприємства та оплата платежу.

Отримання та введення одноразового пароля - це додаткова ідентифікація власника платіжної картки, окрім факту володіння її реквізитами, і разом з

перевіркою строку дії карти, гарантує мінімальний ризик проведення несанкціонованих транзакцій в Інтернеті.

Дослідивши механізм роботи 3D Secure можна виділити деякі переваги під час її використання.

Однією з них є гарантована безпека, адже платежі підтверджуються одноразовим паролем, який у доступі лише власника картки і діє лише протягом 10 хвилин і тільки для однієї операції.. На ввод пароля пропонується три спроби. При необхідності є можливість отримати новий одноразовий пароль.

Відносна простота впровадження, адже підключать 3D Secure не потрібно, технологія стає доступною автоматично при умові активного.

Зручність при використанні, адже на картках, котрі підключені до 3D Secure, для здійснення покупок в інтернеті встановлені ліміти. Це дозволяє мінімізувати необхідність звернень до довідкової служби для отримання доступу на проведення інтернет-операції. Не потрібно пам'ятати пароль, тому що він пароль надсилається кожен раз при здійсненні операції.

Але якщо ж, картка підключена до 3D Secure, але інтернет-сайт не підтримує технологію 3D Secure, то операція проводиться в стандратному режимі. Тобто без використання одноразового пароля, але з використанням лімітів для карт з 3D Secure.

На сайтах, котрі підтримають технологію 3D Secure, як правило, присутні відповідні логотипи.

Використання 3DS продавцями і банками знижує ризик шахрайства при онлайн оплаті, забезпечує кращий захист фінансових даних та забезпечує більш безпечні міжнародні транзакції.

Важливо! Якщо карта підключена до 3D Secure, але Інтернет-торговець не підтримує технологію 3D Secure, то операція здійснюється в стандартному режимі.

Традиційно електронні платіжні системи обслуговують кілька видів кредитних карток. Зазвичай це Visa, MasterCard, American Express і Diners Club. Дві найпоширеніші системи - це CyberPlat і VeriSign. Перший більш популярний в країнах СНД. Другий більш затребуваний на Заході та в США. Вони підтримують

не лише зазначені вище кредитні картки, а й деякі інші кредитні картки, зокрема національні, наприклад, НСМЕП України, платежі [34].

Сьогодні український ринок електронних платіжних систем можна з упевненістю назвати розвиваючим, адже у цій сфері все ще працює близько 10 систем, але з невеликим успіхом.

Вибір правильної платіжної системи може забезпечити надійних захист, правильну та легку її інтеграцію задля ваших потреб. Для цієї задачі можна виділити декілька аспектів.

Основне завдання платіжної системи - полегшити оплату для клієнтів. Географія та переваги клієнтів є найважливішими факторами. Перш ніж вибрати платіжну систему, слід провести дослідження ринку. Відомо, що в Україні найпоширенішим сервісом є LiqPay, до якого входить Приват-24, наприклад, у США стає популярним Amazon Pay, але міцного зв’язку з банком немає. Не менш важливий є ваш спосіб життя. Незалежно від регіону світу, можливо вам буде зручно використовувати класичний PayPal або Masterpass - ще один електронний гаманець, який є ідеальним рішенням для тих, хто має багато різних банківських карт.

Наступним аспектом є кількість та періодичність витрат у клієнту. Виконання різних операцій коштуватиме фіксований відсоток або може бути безкоштовним, у тому числі за певних умов. Тарифи на всі послуги постійно змінюються, але завжди вказані на офіційному сайті, і перед тим, як вибрати одну з них, варто порівняти вартість.

Легкість впровадження має велике значення. Практично всі платіжні ресурси та сервіси мають або забезпечені готовими модулями та пристроями, що дають можливість бути підключеними до практичних та сучасних CMS і API, що дозволяє працювати з більш складнішими операціями. Більшість організацій, які пропонують такі послуги здебільшого завжди йдуть на зустріч своїм клієнтам та допомагають їм у підключені до системи онлайн-оплат, шляхом залучення до цього процесу своїх фахівців. Як правило це основним чином великі об’ємні та великі сервіси: ідея його

дуже проста – банк має мало клієнтів, але вірогідність отримати складності в момент інтегрування дуже висока.

Чітке і вірне, адже дуже добре, коли ваші клієнти можуть оплатити замовлення буквально у декілька кліків, та насамперед система повинна гарантувати вам безперешкодження, щоб отримати свої кошти назад.

В Україні всі ліцензовані та спеціальні сервіси в більшості своєму спрацьовують дуже швидко, але у випадку проведення готівкових розрахунків з рахунків PayPal , або будь-яких других електронних ресурсів відбувається не так швидко, іноді навіть з ускладненнями. Але це загальна територіальна проблема, яка має свої особливості, і якщо ви вирішили працювати з тією або іншою системою, треба врахувати такі особливості.

Для розуміння роботи платіжних систем, доцільно проаналізувати та порівняти одні з найпопулярніших в Україні.

Але як загалом працюють дані платіжні системи. В більшості випадків алгоритм роботи виглядає приблизно так.

Якщо клієнт зупинився на оплаті онлайн, платіжна система відразу отримає його індивідуальний особливий номер, і покупець автоматично потрапляє на сайт сервісу.

На даному етапі покупець може бути впевнений у захисті своїх даних, що обрати спосіб, яким він хоче здійснити оплату, та в тому, що відповідні дані, які необхідні для здійснення операції, можна вводити безпечно. Це такі дані, як номер карти, строк дії такої карти та унікальний cvv-код.

Система співставляє в режимі цілковитої таємності та захисту даних інформацію, і тільки тоді сервіс має намір провести операцію. Результат такої транзакції потрапляє на сервер [35].

Покупець, автоматично знову повертається на сайт продавця в любій ситуації, та отримає інформацію про стан транзакції: вона або відмінена, або проведена. Продавець так само отримає таке повідомлення.

Основний гарант в проведенні транзакції є те, що операція або буде успішною і кошти будуть списані з рахунка покупця на рахунок продавця, або вона буде

відмінена. І в такому випадку грошові кошти не списуються, операція буде вважатися такою, що не закінчена.

Системи для платежів – новітні рішення, які ускладнені новітніми технологіями. Їх головне завдання - транзакції для вас та ваших клієнтів повинні бути безпечними. Для цього сервіс або інтернет-магазин, який ви маєте намір підключити, мають бути відповідними до низки правил та вимог.

Насамперед, безумовно, це технічний аспект: хостинг, де розташований домен, має бути статичною IP-адресою, доменне ім'я сайту має бути з захищеним протоколом https, який має другий рівень захисту. Будь-які інші вимоги, які можуть з’явитись стосуються вже до наповнення сторінок. Сайт, щоб мати достатньо інформації для прийняття рішення про купівлю кількістю інформаційного змісту і діючим внутрішніми повідомленням повинен містити наступні критерії [36]:

- докладну та повну інформацію про компанію-продавця – її місцезнаходження (реєстраційна та фізична адреса), контакти, електронну пошту;
- способи сплати, умови доставки;
- обов’язкова інформація, яка гарантує захист персональних даних; інформаційні умови в правовому полі при співпраці;
- вартісні показники мають бути вказані в національній валюті.

Обов’язковою умовою для підключення платіжного сервісу є розміщення логотипу платіжної системи на сайті.

Розглянемо один іх сервісів, а саме Liqpay. На сьогодні це один з популярніших в Україні сервіс інтернет-еквайрингу. Це розробка самого мабуть великого банку - ПриватБанку, але її використовують сьогодні найбільші маркетплейси і найпопулярніші роздрібні магазини в країні.

При підключенні до сервісу ви залучаєтесь до інтеграції з Приват24 і Google Pay, а також маєте можливість генерувати QR-коди для сплати і оплаті в месенджерах і соцмережах. У Liqpay існують готові інтеграції з CMS Magento, OpenCart, 1С-Бітрікс і декількома іншими, а з liqpay api його просто підключити і до сайтів на інших платформах.

Здійснити онлайн-оплату на сайтах є можливість у сервісах інтернет-еквайрингу, платіжних шлюзах і операторів електронних грошових коштів, а також у агрегаторів. Вибір системи, з урахуванням переваг та недоліків кожного варіанту, залежить лише від завдань, які ви ставите перед собою, та цільової аудиторії, на яку ви маєте намір працювати.

В таблиці 2.1 наведено порівняльну характеристику трьох популярних платіжних систем в Україні [37].

Таблиця 2.1

Порівняльна характеристика платіжних систем

Система	WayForPay	LiqPay	Portmone
Вид	Інтернет-еквайринг	Інтернет-еквайринг	Платіжний шлюз
Простота впровадження	Готові API для виставлення рахунків, міжкарткових переказів, онлайн-кредитування, мобільного поповнення, оплати QR-кодом.	Програмні модулі для онлайн-еквайрингу, P2P-платежів, ботів у Telegram, платежів карткою, обліковим записом, телефоном або електронною поштою.	Програмні модулі для всіх базових завдань і SDK для вирішення складних на популярних мовах програмування.
Підтримка Apple та Google Pay	Так	Ні	Так
Додатковий функціонал	Особистий кабінет та додаток.	Утримання та автоматичні списання. Регулярні платежі за допомогою токенів або підписок. Ви можете налаштувати віджет	Особистий кабінет для b2b клієнтів. Автоматичні платежі, предавторизація, оплата по sms і e-mail.

		оплати.	

Іншою системою котра має широку популярність на території України є IPay.ua. Віна пропонує потенційним клієнтам користуватись нею для онлайн-сплати на сайті і через термінали в звичних магазинах. Ви можете завантажити фірмове ПО на свої термінали, інше обладнання, касу і РРО в оренду у провайдера послуг.

Принцип роботи Електронного гаманця з банківським рахунком дуже схожий, але при цьому Електронний гаманець є альтернативним варіантом. Вам однаково треба буде укласти договір, але на цей раз лише з оператором і направити систему оплат на свій сайт. Однозначно самою вагомою перевагою методу є практично відсутність труднощів для клієнтів, які користуються електронним гаманцем, незалежно від їх місцеперебування, в будь-якій країні світу. Але при цьому значним недоліком є можливість зняти з рахунку лише певну суму, або всі кошти, які були отримані за певний проміжок часу.

На рисунку 2.1 зображено результати опитування, котрі показують популярність платіжних сервісів на території СНД [38].

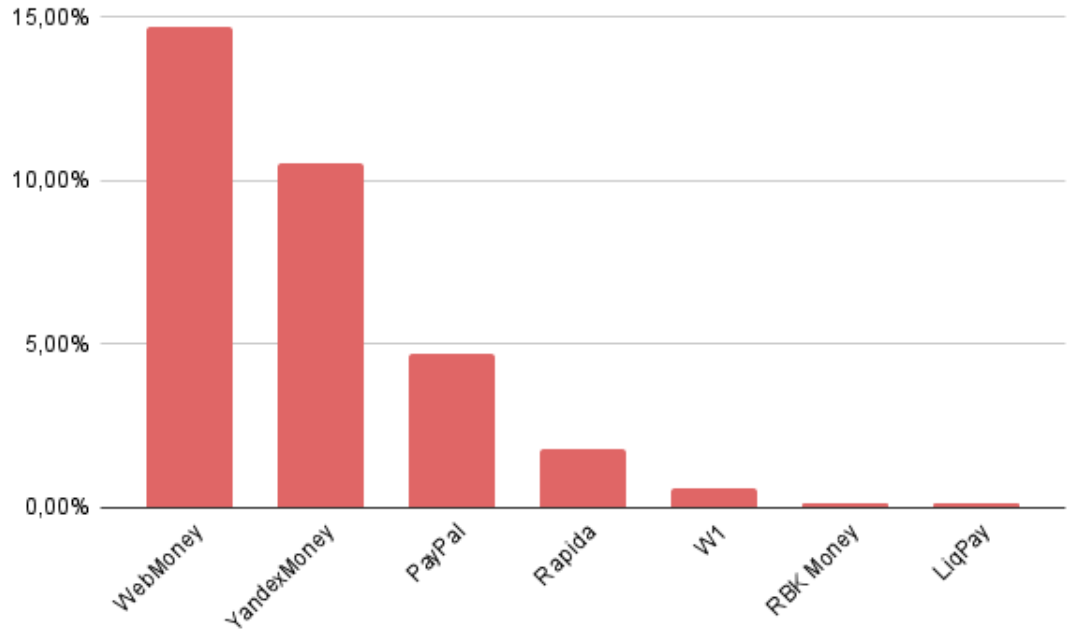

Рисунок 2.1 – Популярність платіжних сервісів у країнах СНД

Для порівняння візьмемо найпопулярніша міжнародна платіжна система у світі, це – PayPal.

Сервіс Masterpass від компанії MasterCard працює вже більше як у нас 15 років і не втрачає при цьому своєї популярності по всьому світу. До цього електронного сервісу можна підключати карти різного типу, а також та інших платіжних систем.

Покупцю потрібно лише підтвердити свої дані на сайті, і відразу клієнту стане доступна оплата схожа на Apple і Google Pay – з технологією FaceID, TouchID, з пін-кодом або індивідуальним паролем. Зокрема, у даній системі відсутній головний недолік, притаманний операторам електронних грошей – на ваш рахунок грошові кошти надходять протягом доби, тобто не пізніше 24 годин [39].

Також доцільним можна виділити використання платіжних шлюзі – це такі собі допоміжні універсальні посередники, сервіси, головним завданням яких є направити відповідну операцію-транзакцію до вашого банку.

Розглянемо сервіс Opayo, який користується дуже великою популярністю в таких країнах як Великобританія та Ірландія, та інших країнах ЄС. Сервіс дотримується усіх мережевих стандартів та критеріїв RTS, які забезпечують захист персональних даних, при цьому ви сплачуєте саму меншу комісію за операцію.

Також на ринку України присутній такий сервіс, як Portmone, який є дуже популярний та успішний. Кредитна схема цього сервісу та система платежів відбувається через електронну доставку і сплату рахунків з картами типу Visa, MasterCard.

Також задля проведення платежів в мережі інтернет були створені так звані платіжні агрегатори, або як ще їх називають сервіси-посередники. Вони, на відміну від шлюзів спершу приймають гроші покупця на свій рахунок, а потім передають за вимогою. При тому, що їх легко підключить, існує безумовний мінус праці з таким сервісом: ви сплачуєте практично подвійну комісію як для банка так і для агрегатору, при цьому захист операцій практично відсутній.

Платіжна система для інтернет-браузеру повинна підходити вам та відповідати вашим потребам. Дізнайтеся переваги, порівняйте тарифи та умови різних сервісів. Також ви повинні бути впевнені в тому, що сайт належним чином

задовольнить вимоги платіжної системи, а платіжна система повинна відповідати вашим потребам.

Система LiqPay – це сервіс для платежів Банків, який зазвичай використовується для зручності розрахунків між різними учасниками ринку, такими як і юридичні особи, фізичні особи-підприємці, або звичайні фізичні особи. Такі розрахунки проводяться з використанням новітніх гаджетів та пристроїв, або звичайних мобільних засобів. Банк надає користувачу платіжний сервіс для спрощення проведення розрахунків у мережі. Банк здійснює дистанційне обслуговування, надає послуги із забезпечення виконання операцій, ініційованих з використанням реквізитів платіжних карток з метою здійснення ініціювання й виконання переказів від фізичних осіб на користь клієнту або навпаки від клієнту на користь фізичних осіб (масові виплати), здійснення розрахунків (оплати) у безготівковій формі.

Дана система забезпечує технологічне обслуговування прийому платежів або перерахування грошових коштів в порядку, визначеному законодавством, в свою чергу покупець-користувач повинен сплатити закладу або фінансовій установі таке собі комісію, яка встановлена згідно договору та відповідає тарифам.

Для того щоб відповідний сайт мав змогу під єднатися до системи LIQPAY, він повинен відповідати певним умовам.

Перша з них це те що для отримання фінансового відшкодування в системі LiqPay , вони повинні відповідають реквізитам поточного рахунку клієнта в банку.

Отримувач ще до початку роботи із системою LiqPay має активний поточний рахунок у банку, а так само клієнт ідентифікований і верифікований відповідно до вимог законодавства та внутрішніх положень банку.

Серед додаткових вимог можна виділити необхідність роботи на сайті інтернет-магазину або зареєстрованої торгової марки. Номер телефону, на який зареєстровано обліковий запис у системі LiqPay, відповідає номеру телефону, зазначеного в реквізитах клієнта в банку як фінансовий номер фізичної особи.

Інтернет-магазин або сайт повинен успішно пройти перевірку на відсутність заборонених послуг або товарів.

Сайт може пройти таку перевірку лише за наявність необхідного функціоналу для здійснення покупок, а саме [40]:

- опис товару або послуги на сайті;
- наявність товару та цін;
- встановлена оплата через систему LiqPay;
- відсутність додаткових комісій;
- наявність контактних даних на сайті;
- наявність договору й умови конфіденційності;
- прописані умови та правила оплати, доставки та повернень;
- торгові марки брендів Visa і MasterCard в повному кольорі;
- бренди товарів та послуг написані без помилок;
- наявність інформації про відповідність стандарту PCI DSS, якщо введення карткових даних клієнтів відбувається на сайті не через платіжну сторінку LiqPay.

Банк має право встановити магазину статус «Без відшкодування» в таких випадках [41]:

- відсутність актуальних ідентифікаційних даних клієнта;
- відсутність актуальних ліцензій та дозволів на продаж певних категорій товарі та послуг;
- невиконання вимог до web-сайту клієнта за всіма або декількома пунктами;

При такому статусі платники можуть відправляти платежі за товари та послуги. Ці кошти списуються з рахунків платників, але утримуються на транзитному рахунку банку та не перераховуються клієнту до виконання вимог для активації з відшкодуванням.

Якщо магазин не буде активовано з відшкодуванням, через 90 днів кошти повертаються на рахунки платників.

Для активації магазину зі статусом “Без відшкодування” сервіс зобов’язується на запит до банку надати запитувану інформацію (підтверджувальні документи) для проведення належної перевірки та налаштування інтернет-сайту. Запит

направляється користувачу на електронну пошту, вказану при реєстрації в системі LiqPay.

При первинній реєстрації банк має право відмовити в наданні послуг, а також повернути платіж без виконання, якщо платіж не пройшов перевірку безпеки.

У межах своїх внутрішніх правил та політики ведення бізнесу з метою мінімізації можливих ризиків і збитків від шахрайської діяльності, недотримання вимог законодавства, в односторонньому порядку встановлювати або змінювати максимальну суму операції з надання банком послуги клієнту на підставі договору.

Також банк залишає за собою право без узгодження з клієнтом обмежити загальну суму транзакцій за електронним платіжним засобом за один день на користь клієнта, а також банк має право встановити обмеження за сумою транзакції з одного електронного платіжного засобу за один день щодо кожного або будь-якого залученого клієнтом підприємства.

При виникненні претензій з боку платника або його банка-емітента з приводу необґрунтованості списання коштів з його рахунку на користь сайту, банк вживає заходів щодо врегулювання спірних питань, керуючись вимогами міжнародних та Національних платіжних систем і чинного законодавства України. Клієнт зобов’язаний відшкодувати банку суму оспорюваної транзакції у встановленому порядку.

Під час підключення до системи необхідно вказувати правильні реквізити, на які буде здійснюватися перерахування грошових коштів. Банк не несе відповідальності за повноту й достовірність наданих реквізитів.

Забезпечити конфіденційність і нерозголошення інформації про операції, персональні дані платників, транзакції це також є обов’язком компанії [42].

Відразу, але не пізніше 24 годин повинно бути забезпечено збереження всієї інформації у всіх можливих для фіксації джерелах, що стосується фактів компрометації, зокрема:

- забезпечити збереження та захист усіх потенційних доказів, що мають відношення до судової експертизи;
- ізолювати зламані системи з мережі;

- зберегти всі системи виявлення вторгнень, захист від вторгнень, журнали Prevention System, усі брандмауери, Web, бази даних і журнали подій;
- задокументувати всі дії реагування на інциденти, а також утримуватися від перезавантаження скомпрометованої, потенційно зараженої системи або від прийняття еквівалентних дій, які можуть мати ефект усунення або знищення інформації, яка потенційно може свідчити про подію.

З метою виявлення операцій, що викликають підозру щодо їхньої правомірності та вжиття заходів для запобігання шахрайських операцій із картками, банк має право здійснювати моніторинг сайтів та інтернет-магазинів залучених клієнтом підприємств, а також аналіз транзакцій та інформації, що міститься в дистанційних розпорядженнях, які підпадають під регулювання на предмет відповідності вимогам, положень законодавства України, правил міжнародних та Національних платіжних систем, умов надання банківських послуг.

Банк має право в односторонньому порядку встановлювати обмеження й ліміти надання послуги за кожним із каналів оплати (наприклад, максимальну суму транзакції за кожним каналом оплати) без обов'язкового попереднього повідомлення власнику сайту. Продовження співпраці при змінених умовах є підтвердженням власників інтерне-сторінки про ознайомлення та про прийняття змінених умов.

Сайт несе відповідальність за нерозголошення і збереження конфіденційності даних, що використовуються для авторизації користувача в системі LiqPay [43].

Також він несе повну відповідальність за будь-які дії осіб, яким були передані дані, які використовуються для авторизації в системі LiqPay для підключення користувача до системи LiqPay або внесення зміни в умови надання послуг.

2.2 Основний перелік недоліків наявних методів та способів захисту даних платіжних карток

Платіжні системи мають досить високий рівень небезпеки. В різних сферах. Це пов'язано з досить великими обсягами та значними об'ємами транзакцій, які

виконуються в системі. Ця небезпека рівна як і для тих, хто переказує кошти, так і для самого оператора.

Вивчання небезпек платіжної системи потрібно починати з вивчення самого поділу ризику, виходячи з того, в якій сфері вони виникають, які засоби розрахунку використовуються, проміжок часу використання. Такий аналіз дає змогу оцінити кожен окремий вид та його ступені фінансових ризиків, а це, в свою чергу здійснює та вивчає можливі варіанти засобів керування цих ризиків.

Фінансові ризики в платіжних системах виникають в разі настання невизначеної ситуації щодо можливості остаточного розрахунку. Фінансовий ризик платіжної системи ґрунтується як вірогідність складної ситуації, настання якої непередбачуване, і яка пов’язана з роботою усіх членів розрахунків на розрахунковій стадії транзакції, а це, в свою чергу наражає до погіршення грошового потоку через неясність та непрозорість вибору для кінцевого розрахунку платіжних вимог [44].

Так як фінансова небезпека такий собі результат виконання зобов’язань у період проведення переказів коштів, аж надто особливо коли це стосується зобов’язання банку або іншої фінансової установи, яка виконує роль фінансового посередника, дуже часто саме ці ризики є небезпеками платіжних систем.

Можна виділити наступні критерії, які притаманні фінансовим ризикам [44]:

- ризики ліквідності;
- кредитний ризик;
- розрахунковий ризик;
- системний ризик;
- моральний ризик.

Кредитний ризик – це ризик того, що учасник операції, який має виплатити кошти, виявиться не в змозі виконати розрахунок за своїми зобов’язаннями у визначений термін внаслідок свої повної або часткової неплатоспроможності.

В контексті платіжної системи основна увага приділяється саме ризику невиконання платіжних зобов’язань. Окрім цього, кредитний ризик може також виникати на кожному етапі платіжного процесу, оскільки банківські установи або

клієнти їх, що позичають кошти під час платіжного процесу, можуть виявитись нездатними повернути кошти з причин, що не пов’язані з їх платіжною діяльністю

Ризик ліквідності суттєво відрізняється від кредитного ризику, оскільки кредитний ризик пов’язаний з можливістю збитків, які можуть бути розподілені між тими, хто вступав у відносини з учасником платіжної системи, який не виконує своїх зобов’язань.

Ризик ліквідності переважно означає відсутність достатніх коштів. Ризик ліквідності виникає у тому разі, коли учасник операції, що заборгував грошові кошти, ймовірно не зможе виконати свої зобов’язання у повній мірі у визначений термін внаслідок недостатньої кількості високоліквідних активів.

Розрахунковий ризик утворюється в системах, які працюють із використанням взаємозаліку платежів. Ним передбачається можлива відсутність коштів при врегулюванні чистих позицій учасників, що утворилися протягом дня. Оскільки в умовах глобалізації посилюються інтеграційні процеси, особливу увагу при визначенні ризиків набуває системний рик.

Неспроможність одного з учасників системи своєчасно виконати розрахунок за своїми зобов’язаннями може спричинити невиконання зобов’язань іншими учасниками. Саме такий вид ризику зумовлює загрозу для всієї платіжної системи. У випадку, коли учасники системи не вживатимуть ніяких заходів для зниження рівня ризику або сподіваються на те, що інші учасники чи центральний банк як гарант покриє їхні зобов’язання без належного забезпечення настає моральний ризик.

Одним із різновидів не фінансових ризиків є правові ризики. До таких ризиків належать недосконала правова база, підроблення фінансових документів, шахрайство, помилки. Операційні ризики виникають через можливість порушень системи обробки даних, оскільки діяльність платіжних систем залежить від захищеності, безпеки та безперебійності функціонування систем обробки та передачі даних.

Зростання автоматизації операцій призводить до зростання залежності від технологічного забезпечення та більш високого рівня вразливості у випадках

технічних порушень. Ефективна платіжна система, що передбачає визначені права й обов'язки користувача, повинна скоротити ризики до мінімуму.

Найбільш розповсюдженими у платіжних системах розвинутих країн існують два підходи щодо обмеження ризику, що спрямовані на: обмеження обсягу розрахунків та забезпечення надійності розрахунків.

Стосовно обмеження обсягу розрахунків виокремлюють юридичні та процедурні підходи. Юридичний підхід сприяє забезпеченню визначеності правового статусу кінцевої чистої позиції. За допомогою раціональної правової процедури взаємозаліку можна гарантувати ситуацію, за якої належна до розрахунку сума узгоджується з чистою позицією в межах системи [45].

Обмеження також можуть встановлюватись на двосторонній основі двома учасниками або на багатосторонній основі між одним учасником та всіма іншими учасниками системи. Можливим є також комбінований підхід, коли сумарна дебетова позиція обмежується певною сумою, розподіл якої між різними учасниками контролюється за допомогою двосторонніх лімітів.

Перевага використання двосторонніх лімітів полягає у тому, що учасники можуть самостійно регулювати розміри ризику потенційних збитків, які вони готові допустити стосовно різних учасників.

Процес менеджменту ризиків передбачає ідентифікацію, оцінку ризиків, вибір методів управління ризиком та їх застосування, кінцевою метою чого є досягнення оптимального для підприємця співвідношення прибутку і ризику.

Серед способів управління ризиками, залежно від спеціальних прийомів, можна виділити дві групи: організаційно-технічні способи управління, які охоплюють заходи уникнення ризику, зниження його рівня та фінансово-договірні способи самостійного протистояння ризикам, передавання ризику, страхування ризиків і, як наслідок, забезпечення інформаційної безпеки платіжної системи.

У процесі розроблення та реалізації заходів щодо мінімізації ризиків у платіжних системах керуються загальними принципами. До них належать, зокрема можуть належати [46]:

- рішення мають відповідати ринковим вимогам;

- ризиком повинні управляти ті, хто має найкращі можливості робити це з мінімальними витратами;
- потрібно виявляти гнучкість у визначенні шляхів досягнення поставленої мети;
- вирішення технічних питань, за винятком визначення стандартів та відносин із центральним банком, краще залишити на розсуд учасників.

Технічні стандарти не можна нав'язувати [46]:

- використані заходи повинні стимулювати найбільш економічні вирішення проблеми управління ризиком;
- бажані оприлюднення частоти помилок, їх характерних особливостей, випадків шахрайства, а також централізований аналіз параметрів та причин помилок;
- жодна окрема особа не повинна мати повноваження затверджувати (вводити) і надсилати платіжні інструкції;
- варто звести до мінімуму можливості вносити зміни в платіжні інструкції та платіжну інформацію;
- необхідна періодична перевірка заходів протидії шахрайству із внесенням необхідних змін у платіжний процес.

З метою захисту своїх членів платіжна система здійснює оцінку наступних видів ризиків, а саме ризик держави члена платіжної системи, ризик члена платіжної системи, ризик виду карток платіжної системи, ризик торгової марки та ризик клірингу і взаєморозрахунків.

За допомогою системи рейтингових оцінок потенційного ризику держави члена платіжної системи оцінюється ризик держави. Ризик членів оцінюється за допомогою платіжної системи для нових членів, які отримують основну ліцензію або у випадку зміни статусу асоційованого члена на основного.

Ризики видів платіжних карток залежать від різноманітності дебетових та кредитних платіжних інструментів, які використовує член платіжної системи. Ризики клірингу і розрахунків оцінюються відповідно до обраної технології розрахунків.

Кліринг та розрахунки можуть виконуватись центральним процесингом платіжної системи без розподілу на внутрішній та міжнародний клірингі і міжбанківські розрахунки, або з розподілом на кліринг та розрахунки за міжнародними та на кліринг і розрахунки за внутрішніми трансакціями.

Потенційний ризик емісії розраховується як загальна сума за всіма трансакціями, яку повинен емітент відшкодувати еквайру з врахуванням кількості днів, що потрібно для повного розрахунку з банком-еквайром. Потенційний ризик еквайрингу визначають із розрахунку того, що при банкрутстві еквайра його підприємства повинні отримати кошти за всіма здійсненими ними трансакціями.

Оцінка потенційного ризику розраховується виходячи із середньої кількості днів, що необхідні для розрахунків еквайра з підприємствами торгівлі та послуг. У даному випадку необхідним є врахування національних термінів перерахування коштів та категорії ризиків торговців за сферами їх діяльності.

Потенційний ризик повернень визначається із розрахунку загальної суми коштів, яку повинен еквайр повернути емітенту за неакцептовані трансакції з врахуванням кількості днів, що потрібні для повного розрахунку з банком-емітентом. Таким чином, зазначимо, що в умовах сьогодення платіжні організації застосовують різноманітні засоби з метою захисту від ризиків [47].

Проте, з метою запобігання кредитних ризиків здійснюють:

- перевірку платоспроможності суб’єкта;
- проводять реструктуризацію боргу; коригування параметрів угоди;
- зменшують ліміт кредитування;
- відмовляються від здійснення активних операцій.

Щодо зниження ризику ліквідності засобами захисту можна виділити залучення довгострокових пасивів, зниження питомої ваги ризикових активів, рефінансування зі сторони центрального банку та утримання заставного забезпечення; використання міжбанківських позик.

З метою захисту від системного ризику відбувається встановлення відкритих правил платіжних систем та здійснюється контроль за діяльністю учасників платіжних систем, визначаються обмеження для учасників з низькою довірою.

Платіжні організації, щоб захистити свою діяльність від морального ризику здійснюють напрацювання норм відповідальності за порушення умов розрахунків, а саме встановлюють обмеження використання коштів центрального банку при гарантуванні розрахунків.

Зменшити ймовірність виникнення ризиків платіжних систем можливо з використанням таких заходів безпеки [48]:

- удосконалення законодавства стосовно відповідальності кредитора за своєчасне погашення власних зобов'язань;
- збільшити забезпечення майбутніх зобов'язань зі збільшенням обсягів платежів;
- зменшити обсяги рефінансування банківських установ зі сторони Національного банку України та впровадити взаємо кредитування в межах платіжної системи;
- покращити регулювання та нагляд за діяльністю учасників розрахунків;
- застосовувати економіко-математичні методи в процесі прогнозування фінансового стану учасників та ймовірності виникнення ризиків платіжних систем.

Платіжна система котра впроваджена та використовується в інтернет-браузері повинна мати добре продуману стратегію захисту інформації. Необхідно зосередити увагу на тому, що розроблення заходів охорони, технологічних та програмно-апаратних засобів захисту здійснюється платіжною організацією відповідної платіжної системи, її членами або іншими установами на їх замовлення.

2.3 Оцінка ефективності та поширення методів захисту даних платіжних карток

З лютого 2022 року Національний банк України вдосконалив процедури проведення операцій з використанням електронних платіжних методів. Це сприятиме підвищенню рівня захисту прав власників банківських карток та посиленню контролю за дотриманням еквайерами правил платіжної системи а також вимог від законодавства.

Дані зміни передбачені постановою Ради директорів Національного банку України від 08.02.2022 р. № 13, а саме «Внесення змін до Положення про затвердження операцій з випуску та використання електронних способів платежу», яка набула чинності 10 лютого 2022 року [49].

Еквайр - юридична особа, банк або інша установа, що надає технічні та інформаційні послуги для розрахунків за операціями в платіжних системах з використанням банківських карток.

Аналіз експертів зі США показав, що 88% втрати конфіденційності інформації з мережі інтернет є наслідком зловмисної поведінки персоналу, а інша частина – наслідком перехоплення технічними засобами інформаційного потоку.

Експерти з шифрування визнають, що майже всі комерційні системи шифрування не мають захисту від активних атак з боку зловмисників, тактика яких полягає у перехопленні трафіку веб-сайтів, а потім надсилає на нього до 1 мільйона повідомлень. Аналіз відповіді сервера на такі повідомлення може виявити конфіденційну інформацію.

У системі електронної комерції всі транзакції дуже короткі та прості за структурою, що очевидно для таких даних, атрибутів платежу чи банківських рахунків. Тому коротку і прозору інформацію в її структурі відповідно легше розшифрувати. Упакування таких транзакцій дозволяє легше уникнути природної структури даних. Така ситуація типова для архітектури клієнт-сервер з віддаленим доступом до бази даних.

Майже усі СУБД котрі впроваджені у бізнес секторі є реляційними. А отже є результатом реляційного запиту до бази SQL-запиту, тому на виході ми маємо чітко структуровану інформацію. Провідні методи шифрування повинні враховувати дані особливості інформації.

Методи шифрування поділяються на 2 групи, а саме симетричні та асиметричні методи.

Симетричні методи засновані на принципі, що всі сторони використовують один ключ для шифрування і дешифрування. Очевидно, що тривале використання ключа збільшує ризик ідентифікації ключа, тому його слід регулярно замінювати.

Якщо новий ключ потрібно передати віддаленій системі або людині, ця ситуація є окремою проблемою, тобто зміна його є критичним процесом.

Використовуються асиметричні методи або стандарти відкритих ключів, загалом, за такими схемами [50]:

• у одержувача є 2 ключі, які неможливо отримати від іншої сторони, а саме відкритий та закритий. Відкриті ключі знаходяться у відкритому доступі та розміщуються на веб-сайтах;

• відправник шифрує дані за допомогою відкритого ключа, секретний ключ знає тільки система шифрування;

• одержувач використовує закритий ключ для розшифровки отриманих і зашифрованих даних.

Новітня криптографічна система Cramer-Shoup, яка ще не є галузевим стандартом, але має певні переваги, подвійне шифрування інформації, надісланої з інтернет-сайтів. Відповіді сервера на команди адміністрації веб-сайту та на будь-які запити від сервера шифруються.

Такий підхід ускладнює зловмисникам визначення ключів до захищеної системи, і IBM вже використовує цей підхід у своїх криптосистемах [51].

DES (Data Encryption Standard) це сучасний федеральний стандарт у США, подібний до міжнародного комітету ISO 8372-87, що характерно для симетричного шифрування. Він був розроблений корпорацією IBM ще в 1970 році.

Даний стандарт має наступні режими роботи [51]:

- електронна кодова книга;
- зашифрований текст або вихідний зворотний зв’язок;
- блокчейн.

Стандарт визначає, скільки разів він встановлюється під час генерації ключа і скільки разів він використовується. Сьогодні для 64-розрядних блоків зазвичай використовуються 56-розрядні ключі, але багато експертів вважають таку довжину ключів недостатньою і рекомендують переходити на 112-розрядні або більше ключів, що, звичайно, сповільнить цей стандарт.

Так званий потрійний DES – це послідовність шифрування та дешифрування різними ключами. Американська банківська асоціація (ABA) використовує DES як галузевий стандарт.

SET (Secure Electronic Transaction), який використовується для встановлення безпечного з'єднання в мережі, як правило, між банком або компанією, що володіє картковою системою, і банком, який обслуговує клієнта.

Secure Multipurpose Mail Extensions — це протокол електронної пошти, який шифрує та підписує повідомлення цифровим способом. Розроблено RSA як модифікація електронної пошти MIME.

Дані листа шифруються за допомогою одноразового ключа, створеного симетричним методом, і надсилаються за схемою відкритого ключа: шифрування відкритим ключем.

SSL на даний момент є найпоширенішим протоколом інформаційної безпеки в Інтернеті, розробленим RSA Data Security. Дозволяє аутентифікувати всіх учасників обробки інформації.

Це електронний центр сертифікації, який видає електронні сертифікати у вигляді цифрових підписів кожному, хто звертається за ним. Під час роботи обидві сторони можуть перевірити справжність іншої сторони.

Сертифікат – це відкритий ключ, який «підписаний» центром сертифікації закритим ключем.

X509 являє собою специфікацію електронного підпису, котра широко поширена в мережі. Перша версія була в створена і впроваджена комітетами ITU-T та ISO, ще у 1988 році, а остання версія вийшла у 1996 році.

Існує виділений порядок дій для перевірки інформації на достовірність. Після отримання інформації цей напрямок поширюється на службу аутентифікації для отримання відкритого ключа, який розшифровує електронний підпис – отримує дайджест повідомлення. Ви також можете перевірити дійсність сертифіката.

Справжню надійність шифрування за допомогою алгоритму DES з 56-бітовим ключем можна оцінити на основі офіційних конкурсних даних дешифрування, які регулярно заплановані RSA для шифрування даних за допомогою цього алгоритму.

Одним з обов’язкових методів захисту, який необхідно впровадити, є аутентифікація об’єктів і суб’єктів, які звертаються до інформації.

Варто призначити для використання наступні методи [52]:

- одностороння аутентифікація, коли клієнт системи доступу до інформації доводить її достовірність;
- двостороння аутентифікація, якщо система не є клієнтом, вона повинна підтвердити свою автентичність;
- тристороння аутентифікація, так звані послуги нотаріальної аутентифікації, використовуються для підтвердження автентичності кожного партнера при обміні інформацією.

Розглянемо технології, що підтримують безпеку передачі інформації. Одним із перспективних способів захисту транзакцій є зчитування унікального номера процесора комп’ютера, який ініціював транзакцію, і передача його в систему аутентифікації. Всі інші параметри мережі логічні, вони встановлюються під час налаштування програмного забезпечення і зазвичай можуть бути змінені без перезавантаження системи. Але для найпоширеніших процесорів Intel і сумісних системних команд Pentium III надає таку можливість.

Технологія RADIUS є розробкою компанії Livingston Enterprises, вона аутентифікує віддалений доступ до мережевих ресурсів. Після того, як сервер віддаленого доступу або брандмауер отримує запит від віддаленого користувача, він зв’язується з сервером RADIUS, щоб ідентифікувати користувача за ім’ям та паролем.

Ця технологія дозволяє отримати доступ з будь-якої точки планети за допомогою єдиного пароля та імені користувача.

Використання біометричних параметрів у системах інформаційної безпеки є обов’язковим, оскільки цей метод в основному базується на деяких біометричних параметрах людини, які підтверджують автентифікацію власників кредитних або депозитних карток чи адміністраторів програмного забезпечення, унікальність яких доведена та є доволі простою, швидкою та відносно дешевою. Серед цих параметрів пріоритетним є райдужна оболонка ока людини і капілярний рисунок на пальцях.

Початкове сканування райдужної оболонки для внесення еталону у відповідну базу банку займає всього 1-2 хвилини. Після цього власник картки може більше не пам’ятати ідентифікаційний код.

Банкомат просканує очі клієнта та дозволить операцію. Пошук у базі даних на поточному рівні апаратних і програмних можливостей відбувається зі швидкістю мільйони зображень в секунду.

Надійність цього порівняння вже досить висока — одна з 30 мільйонів спроб не вдасться визначити «правильного» клієнта. Навіть клієнти, які використовують контактні лінзи під час сканування окулярів, зроблять лише 1% помилки.

Щоразу, коли користувач має намір здійснити транзакцію, браузер за допомогою протоколу надсилає копію сертифіката продавцеві, щоб перевірити дійсність кредитної картки користувача.

SET — це технологія та програма аутентифікації, розроблена Visa і MasterCard. Протокол підтримується Verisign, Cybercash і First Virtual, які контролюють дозволи користувачів для продавців і банків. Він є основним протоколом безпеки для використання банківських карток онлайн, але це лише специфікація, а не повний продукт безпеки [53].

Відсутність єдиного стандарту призвело до появи безлічі встановлених протоколів шифрування фінансових операцій з різним ступенем стабільності. Жоден з них не відповідає головній вимозі, що відображає природу всесвітньої павутини, а саме вимозі відкритості.

Ця ситуація змінилася лише з появою протоколу SET. Він дозволяє здійснювати безпечні платежі пластиковими картками у відкритих мережах. Розроблятися даний протокол почався в 1996 році, а в червні 1997 року вже була випущена специфікація його останньої версії SET 1.0. Нині у світі існують десятки систем електронної комерції, які працюють на основі протоколу SET і об’єднують сотні банківських установ, інтернет-магазинів та бізнес-центрів.

SET на даний момент є основним протоколом інформаційної безпеки в онлайн частині банківської сфери. Протокол підтримує більшість платіжних систем, таких як VISA, EuroCard, MasterCard, American Express, Diners Club, JCB, CyberCash і Digi

Cash, а також провідні комп'ютерні компанії, наприклад AT&T, HP, IBM, Microsoft, Northern Telekom, RSA, що автоматично забезпечує високу довіру мільйонам клієнтів [54].

Слід зазначити, що він дозволяє використовувати різні методи шифрування інформації, котрі регламентовані регіональними стандартами і відповідають вимогам SET.

Взаємодія між інтернетом та різноманітними платіжними системами створює певний шлюз, тобто апаратно-програмний комплекс, котрий керується банківською установою, уповноваженою організацією чи процесинговим центром.

Даний протокол описує наступний порядок дій під час покупки товарів чи послуг [55]:

1. Клієнт аналізує список товарів на сайті або на будь-якому іншому носії, такому як папір, CD-ROM чи іншому.

2. Клієнт обирає необхідні йому товари.

3. Клієнт отримує від продавця електронне замовлення або автоматично створену електронну таблицю, що містить детальну фінансову інформацію та умови придбання товару.

4. Клієнт обирає спосіб оплати покупки.

5. Клієнт надсилає виконане замовлення разом із платіжним дорученням продавцю. Ці документи зашифровані та засвідчені електронним підписом клієнту.

6. Продавець надсилає запит на авторизацію до банку-сервісу, а банк-сервіс надсилає запит на авторизацію банку-емітенту через мережу обраної платіжної системи.

7. Компанія, отримавши додаткову відповідь, надсилає покупцю підтвердження замовлення.

8. Продавець доставляє покупцю товар чи надає послугу.

9. Банк клієнту відшкодовує продавцю вартість покупки.

У додатку на основі SET-протоколів покупець не знає платіжних даних продавця, продавець не бачить номер картки покупця, а банк не має інформації про замовлення. Це забезпечує високий ступінь анонімності транзакцій.

SET заснований на багатьох передових досягненнях сучасної криптографії. Під час обміну фінансовою інформацією вона шифрується за симетричним алгоритмом з використанням динамічно згенерованого ключа, а потім передається власнику даних у зашифрованому вигляді за допомогою відкритого ключа відправника. До цього часу сторони угоди під час обміну цифровими сертифікатами проходять аутентифікацію.

Система цифрових сертифікатів є однією з головних особливостей SET. Вони доступні для всіх сторін угоди, а саме: платіжних шлюзів, банків-емітентів, власників карток, продавців, банків-еквайрів, сертифікаторів і всієї платіжної системи.

Провідну роль відіграє так званий кореневий ключ системи, відомий всім сторонам протоколу. Його буде визначати та регулярно змінювати організація, котра об’єднує VISA, EuroCard, MasterCard, American Express та JCB.

Орган, який видає ключ іншим учасникам системи повинен підписати його своїм електронним підписом. Отже, знаючи один кореневий ключ за допомогою ланцюжку автентичності, ви можете перевірити кожний сертифіката на оригінальність.

Кожна сторона протоколу має два цифрових сертифіката, один, котрий підтверджує відкритий ключ, який використовується для обміну ключами, а інший – відкритий ключ, що використовується для електронних підписів. Окрім цього, дані ключі несуть різну інформацію про учасників системи.

Спрощені системи видачі та розрахунку сертифікатів тільки починають з’являтися. Тому всім зацікавленим власникам карток знадобиться багато часу, щоб отримати цифровий сертифікат від свого банку або платіжної системи. Крім того, вони потребують програмного забезпечення, сумісного з SET.

Це найбільша перешкода для швидкого розвитку та зростання кількості транзакцій SET. Як компроміс, SET дозволяє покупцеві працювати в не автентифікованому режимі, тобто обмін інформацією між покупцями та продавцями в даній сфері відбувається за спрощеним варіантом. Однак передбачається, що покупець використовує програмне забезпечення, сумісне з SET.

Інший істотний мінус SET це вузький спектр спеціалізацій для оплати банківськими картками. Він не регулює організацію мікроплатежів чи розрахунків цифровими готівковими чеками. Однак, незважаючи на деякі недоліки, SET-Protocol за короткий час зумів стати галузевим стандартом.

Використовувати пластикові картки для створення несумісної з SET системи електронних платежів в мережі зараз не має сенсу. З виходом специфікації SET 1.0 багато компаній розробили на її основі системи бізнес-розрахунків.

Варто розглянути таке поняття як, віртуальний гаманець покупця, так званий vWallet. Він є додатком, інтегрованим у браузер покупця, сумісний з Netscape Navigator та Microsoft Інтернет Explorer, починаючи з версії 3.

В порівнянні з стандартним гаманцем, vWallet може містити дані про банківські картки та персональні цифрові сертифікати, до того ж окремо для кожного з користувачів комп'ютера. Окремий пароль буде надавати захист кожному з гаманців. Додаток проводить приховану для клієнту процедуру шифрування транзакцій та роботу із сертифікатами безпеки.

Дана технологія доволі гнучко налаштовується задля потреб банківських установ або магазинів, що їх розповсюджують. Обов'язкова наявність бази даних та опції щодо створення детальних звітів про платежі за обраний період часу [56].

Якщо не надто звертати на складність, що існує всередині, то vWallet досить приємній у користуванні, вражає своєю зручністю та легкістю. Його розповсюджують або майже безкоштовно, або за таку собі цілком символічну комісійну платню для банків-еквaєрам. Також його можуть надавати так званим процесинговими центрами, при цьому використовують Інтернет-продукт VeriFone.

Враховуючи малу ємність шлюзу, для збільшення обсягу інтернет-транзакцій в найближчі кілька років та знизити високу вартість системи, в нашій країні достатньо організувати платіжний шлюз, яким можуть використовувати усі банківські установи.

Відомо, що багато українських інтернет-провайдерів переповнені в районі, який надає лише послуги доступу до інтернету. Все більше компаній починають надавати різноманітні інформаційні послуги, в тому числі бізнес-послуги.

З цією метою бажано надати клієнтам можливість безпечно оплачувати ці послуги онлайн. Для багатьох продавців організація та підтримка віртуального магазину самостійно або в поєднанні з існуючою структурою, стане хорошим козирем у конкурентній боротьбі та забезпечить додатковий потік доходу за рахунок платежів [57].

Інтернет-магазин може легко організувати багато компаній з веб-сайтами. Особливо це стосується комп'ютерних компаній, туристичних агентств, квиткових кас, різних операторів, редакцій та видавництв. Все, що їм потрібно зробити, це встановити vPos на своєму веб-сайті або сайті провайдера та розробити сторінки інтернет-магазину.

Висновки за розділом 2

Максимальний комфорт і безпека, дистанційна розстрочка платежів і можливість оплати всього в два кліки – все це лише основні переваги для клієнтів, які використовують платіжну систему через інтернет-браузер.

Для власників магазинів переваг не менше, адже через неможливість оплати в інтернеті компанії можуть втратити багатьох потенційних покупців, котрі будуть звертатися до конкурентів, а пошукові системи не будуть показувати рекламні інтеграції, як мінімум в розділі в деяких розділах для широкої аудиторія.

Електронна платіжна система, здатна приймати оплату за послуги та товари – це електронна послуга, яка дозволяє споживачеві купувати пропоновані йому товари, послуги за допомогою звичайного доступу до мережі та номера банківської картки.

Ще пару років том назад людина, яка розраховувалась карткою в терміналі магазину, викликала незадоволення у людей в черзі, а сьогодні, хіба що невеликі магазини не мають терміналів. Тому, кому, як не нам з вами, самій активній частині інтернет-спільноти, направляти розвиток електронної комерції в потрібне русло.
Не бійтеся експериментувати, платити в інтернеті і підключати оплату картками до своїх мерчантам або стартапам. Раптом це виявиться зручно та дешево.

В наш час багато провідних компаній для захисту своїх клієнтів використовують провідні світові технології та стандарти у сфері кібербезпеки, щоб захистити кошти та карти своїх клієнтів. Це декілька рівнів захисту, які зупиняють шахраїв та не заважають платежу добропорядних покупців.

РОЗДІЛ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ДАНИХ НА ОСНОВІ МОДЕЛІ ПОКРАЩЕНОГО МЕХАНІЗМУ ЗАХИСТУ

3.1 Сучасні методи захисту від витоків даних платіжних карток

В основі нового методу захисту повинні об’єднуватися правила та вимоги до банківських установ та клієнтів, неухильне дотримання яких зможе збільшити рівень безпеки під час проведення банківських операцій через інтернет браузер.

Серед основних організаційних правил щодо захисту платіжних карток слід визначити такі [58]:

1. Не потрібно залишати без нагляду банківські картки та не передавайте їх іншим недовіреним особам.
2. Ніколи не повідомляйте свій пароль для служб, які дозволяють керувати грошима, наприклад, онлайн-банкінг або електронні гаманці.
3. Не зберігайте PIN-код своєї картки разом із самою карткою.
4. Ніколи не повідомляйте свій CVC2-код нікому за межами процесу онлайн-платежів, оскільки це потрібно для завершення трансакції.
5. Ніколи не відповідайте на особисту інформацію електронною поштою. У вас ніколи не запитуватиметься пароль доступу в жодному банку чи службі.
6. Регулярно перевіряйте стан свого рахунку на платіжних системах і картках. Якщо у вашому банку є SMS-сервіс – обов’язково підключіть його, оскільки це найшвидший спосіб отримати інформацію про те, що відбувається з вашим рахунком.
7. Ніколи не кладіть всі гроші на банківську картку.
8. Створіть спеціальну картку для інтернет-платежів та оплат.
9. Під час скидання пароля приділяйте більше уваги і розповідайте про інформацію, яку ви використовуєте, щоб відповісти на друге секретне запитання.
10. Ніколи не використовуйте електронну платіжну систему для карткових операцій у магазині, якому ви не довіряєте чи бачите вперше. Особливо якщо вони

не мають ознак платіжних систем та інших організацій, що борються з шахрайством.

11. Якщо вас попросять надіслати PIN-коди або інші дані картки, не надсилайте їх, а зателефонуйте в кол-центр банку і переконайтеся, що це не дії хакерів або шахраїв.

Одна з перших на що необхідно завжди звертати увагу при покупці товарів через інтернет це репутація та добросовісність продавця. Основною метою продавця є прагнення реалізувати свій товар. Аби привернути увагу споживачів та зацікавити своїм товаром в інтернеті, продавець створює сайт або сторінку в соцмережі.

При цьому покупець не знає, хто є дійсним власником товару. Цю інформацію він може отримати лише за наявності реальних контактних даних.

Якщо вся інформація про продавця доступна, це дає можливість перевірити його наявність у Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань.

Також за необхідності це дає змогу зв’язатися з ним, запросити додаткові документи, а вразі отримання неякісного товару або неповернення коштів надіслати на його адресу претензію, а за необхідності звернутися до суду. Адже якщо на сайті є лише номер телефону і назва сайту, то ви не зможете ні повернути товар, ні кошти, оскільки невідомо, з кого вимагати усунення порушень ваших прав.

Перш за все, зберігайте свій PIN-код у безпеці та закривайте клавіатуру під час його введення, щоб ви не могли прочитати його за допомогою шахрайської крихітної камери.

Ніколи не встановлюйте будь-які віддалено доступні програми чи програми на вимогу абонентів та співробітників банку.

Не виконуйте команди USSD на прохання абонентів і агентів банку.

Ні в якому разі не перераховуйте свої кошти на рахунки інших або третіх осіб на вимогу абонентів та банківських агентів.

Необхідно створювати стійкі паролі до електронної пошти, соціальних мереж та інтернет-банкінгу.

Не розкривайте всі реквізити платіжної картки та контролюйте рух коштів на своєму рахунку. Єдине, що можна повідомити за телефоном: 16-значний номер картки; можна, але не обов'язково прізвище, ім'я та по-батькові.

Конфіденційність: три цифри на зворотному боці картки, код банку та мобільного оператора, тобто одноразовий пароль; пароль для онлайн-банкінгу; код банку.

Підключіть текстові повідомлення про операції з платіжними картками. Використовуйте свою платіжну картку, щоб встановити особистий ліміт транзакцій.

Якщо ви дізналися, що ви випадково розкрили дані своєї платіжної картки шахраю, або що з вашою карткою відбулася підозріла транзакція, вам слід негайно заблокувати картку та отримати доступ до онлайн-банкінгу за номером телефону, вказаним на звороті вашої картки.

Якщо, на жаль, ви вже стали жертвою шахраїв – напишіть заяву до кіберполіції, або повідомне про ваш випадок по телефону.

У вас є можливість перевіряти відгуки які можуть вказати на надійність сайтів, продавців чи інтернет-магазинів через інтернет-браузер.

Обов'язково необхідно захистити телефонний номер, котрий прив'язаний до вашої пластикової картки. Не варто використовуйте даний номер у соцмережах, оголошеннях та для контактів з контрагентами або клієнтами.

Для збільшення рівня безпеки свого фінансового номеру слід дотримуватись таких рекомендацій [59]:

- краще перейти на контракт з мобільним оператором;
- відключити послугу віддаленої заміни сім-карти у свого мобільного оператора;
- тримати в секреті логін на пароль до онлайн-кабінету мобільного оператора, смс-коди операторів;
- нікому не повідомляти puk-код та серійний номер сім-картки.

3.2 Опис методів та засобів об’єднаного методу захисту платіжних карток

Платіжні системи розглядають інтернет тільки як місце проведення транзакції . І це призводить до деякої плутанини при кардхолдера з банком, який випустив карту.

Ствердження співробітника кол-центру про те, що карта відкрита для виплати в інтернеті, так само вірне як і те, що вона закрита, може не відповідати дійсності. Наприклад, емітент в цілях безпеки може дозволити до авторизації тільки транзакції типу e-commerce з вводом CVV2, в той час як деякі сайти не мають запитів CVV2 та формують транзакцию як Mail-Phone order [60].

В останньому випадку оплата не відбудеться. Чи банківська установа котра випустила картку може заборонити використання e-commerce, втім не заблокувати Mail та Phone order, тоді оплата в деяких інтернет-магазинах буде дозволена. Тому буди до кінця впевненими в тому, що платіж відбудеться при тих чи інших умовах, може бути хіба що працівник процесингово центру ПО.

Культура користування особистими картками в нашій країні розвинута доволі слабо, тому треба бути завжди обережними зі своїми зарплатними, кредитними та й будь-якою іншою карткою, на якій є доступні кошти.

На превеликий жаль кількість атак на дані платіжних карток через інтернет браузер з кожним роком буде тільки збільшуватись. Ми можемо лише впроваджувати та використовувати все більш прогресивне механізми та засоби захисту. На рисунку 3.1 зображено прогнозований рівень атак під час онлайн розрахунків [61].

В першу чергу варто не часто використовувати картку в мережі, не дивлячись на явну зручність. Також не відкривати та не давати у вільний доступ номер картки та зворотню сторону з CVV2 в чергах у терміналах та не випускати картку з поля зору, коли ви передаєте її працівнику чи касиру або іншому обслуговуючому персоналу.

В деяких випадках сума з картки може бути списана навіть без вводу CVV2. Тобто зловмисникам буде достатньо підглядіти номер вашої картки та термін дії, щоб виконати платіж в інтернеті.

Для здійснення виплат в інтернеті краще взагалі завести окрему картку або використовувати дебітову, постійно контролюючи на ній вільний доступний залишок грошових коштів, наприклад підключивши послугу sms-сповіщення. Також, якщо банк-емітент пропонує таку послугу, бажано встановити на картку індивідуальний ліміт платежів в інтернеті.

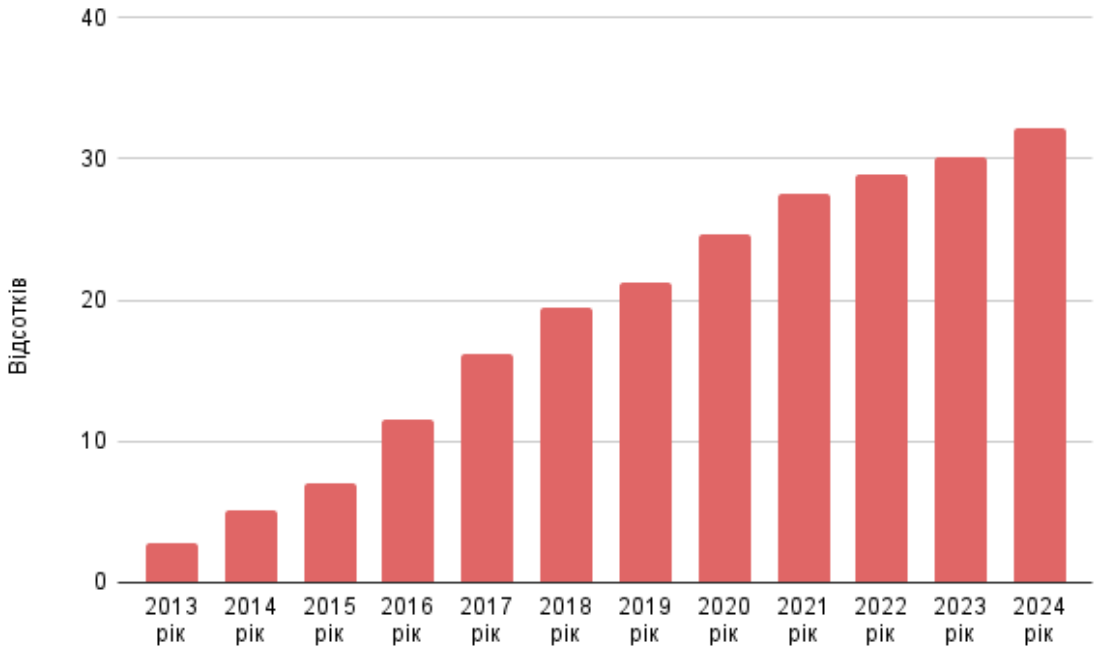

Рисунок 3.1 – Ймовірність загроз під час проведення банківських операцій онлайн

Крім описаних вище методів та засобів, одним із засобів захисту картки, тепер вже технічним, є , протокол 3D Secure.

Не дивлячись на спроби просування платіжними системами протокола 3D Secure, банки на території України та СНГ не квапляться його вивчати і як і раніше вигадують свої методи захисту від шахраїв.

Здавалося б, очевидним , що головна ціль протокола 3D Secure - захистити кардхолдера від несанкціонованого використання його карти. Але насправді в повній мірі це працює лише в тому випадку, коли і банк-еквайєр і банк-

емітентпідпримують один і той самий протокол. Тобто якщо шахрай спробує розрахуватись вашою карткою, яка підключена до 3D Secure, в торговій мережі, яка не підтримує його, захист не спрацює.

Так як більшість мерчантов в СНГ та Україні все ще не підтримують протокол 3D Secure або підтримують лише на словах, то користі від такого захисту мало. У випадку несанкціонованого використання захищеної карти в мерчанте, який не підтримується 3D Secure, відповідальність за шахрайство переходить на банк, який обслуговує торгову точку. Хоча в такому випадку кардхолдер може повністю розраховувати на повернення грошових коштів, це мало втішає, тому що ми знаєм як по часу затягується волокита з претензіями в наших банках. Таким чином, головна перевага

3D Secure на даному етапі розвитку електронної комерції в Україні та в країнах СНГ - це перенос відповідальності на банк, який обслуговує торгову точку [62].

Варто розглянути такий поширений і доволі суворий стандарт безпеки, як PCI DSS. Щоб отримати PCI DSS сертифікацію, організаціям, які бажають впровадити таку систему, необхідно проходити щорічний незалежний QSA-аудит та ASV-сканування кожні три місяці.

Ці компанії мають відповідати PCI DSS Level 1. Це підтверджує, що сервіс безпечно зберігає данні та захищає фінансову інформацію клієнтів на самому високому рівні світової індустрії платіжних карток.

Директива PSD2, котра займається регулюванням платіжних послуги в Європейському Союзі. Він призначений для підвищення безпеки, зменшення шахрайства та розширення можливостей споживачів.

Дотримуючись цього правила, компанії можуть приймати платежі з Європи, знаючи, що вони є суворо аутентифікованими користувачами під час будь-якої транзакції. А саме ваші транзакції будуть відповідати всім вимогам законодавства.

Всі транзакції проходять через систему Antifraud. Це самонавчальна система, яка перевіряє платежі по більш ніж 300 факторів та співставляє кожну транзакцію з патером поведінки шахраїв [63].

Аналіз даних дозволяє антифроду вираховувати як чисте шахрайство, так і спроби зламу аккаунтів або використання крадених карт. Пригадайте, як при сплаті онлайн-послуг або товарів на сайті система просила вас вести пароль із повідомлення для перевірки даних карти. Це і є технологія 3DS.

В сучасних і більш технологічних компаніях пішли ще далі. Там використовують Smart 3DS. Якщо говорити просто, ці компанії рекомендують коли вам використовувати авторизацію платіжної карти з 3D Secure, а коли - ні. Таким чином, частка успішних онлайн-оплат за ваш товар чи послугу зростає.

Технологія SecureCode від Mastercard дозволяє бути впевненим, що оплата відбувається безпосередньо тримачем карти. Працює все просто: коли людина здійснює покупку онлайн, тримачу карти на ваш пристрій надходить тимчасовий пароль. Оплата може бути здійснена лише після введення коду на спеціальній захисній сторінці.

Оригінальна технологія захисту, яку використовує платіжна система Visa, розроблена спеціально для оплати товарів та послуг в інтернеті. Цей протокол захисту додає додаткову аутентифікацію тримача карти.

Після вводу даних карти користувач буде направлений на захищену сторінку для вводу пароля, якій знає тільки він та банк-емітент. Пароль може бути або постійним, або одноразовим.

Ці компанії повинні відповідати Загальному регламенту захисту даних, який регулює збір, уніфікацію і використання персональних даних користувача. Це обов’язковий стандарт для компаній, які надають послуги в Європі.

Підтримка протоколу HTTPS означає, що всі дані, передані між пристроєм користувача та сайтом будуть передаватися у зашифрованому вигляді та будуть конфіденційними. Окрім цього даний протокол гарантує, що усі ваші дані будуть надійно збережені в повному обсязі, а сам користувач перебуває дійсно на тому сервісі, котрий він шукав, а не на сторінці хакерів.

Portmone.com - перша компанія в Україні, що пройшла міжнародний аудит безпеки за стандартом PCI DSS. Це означає, що власники банківських карток

можуть бути спокійні за збереження своїх даних при проведенні фінансових операцій.

Коли бізнес приймає рішення підключити до своїх сервісів платіжну систему для прийому онлайн-платежів, перше, на що важливо звернути увагу, це безпека. Щоб користувач міг здійснювати онлайн-оплати з повною гарантією безпеки своїх коштів, всі платіжні послуги в Україні зобов'язані проходити сертифікацію за міжнародним стандартом PCI DSS.

Payment Card Industry Data Security Standard- це міжнародний стандарт безпеки даних індустрії платіжних карток, який розроблений платіжними системами Visa та MasterCard, American Express, JCB та Discover. Він є переліком 12 деталізованих вимог щодо забезпечення безпеки даних про власників платіжних карток. Ці дані повинні передаватися, зберігатися та оброблятися в інформаційних інфраструктурах організацій [64].

При обміні інформацією з користувачами Portmone.com застосовує індустріальний стандарт TLS 1.2 шифрування з використанням стійкої криптографії, довжина ключа до 256 біт. Цей сертифікат засвідчено міжнародним сертифікаційним агентством GeoTrust.

Процес оплати в інтернеті товарів або послуг за допомогою банківських карток передбачає передачу коштів за допомогою введення персональних даних платіжних карток. І якщо на сайті не встановлений спеціальний захист щодо відстеження можливих шахрайських операцій - зростає ризик кіберзлочинності. Тому компанія, яка приймає та обробляє дані банківських карток на своєму сайті, зобов'язана щорічно проходити міжнародний аудит безпеки PCI DSS.

Це означає, що компанія виконує всі вимоги міжнародних платіжних систем VISA та Mastercard - вони стосуються правил проведення платежів та засобів захисту даних. Їх ще називають PCI DSS Visa та Mastercard PCI DSS.

При передачі даних користувача забезпечується їхнє надійне шифрування. Встановлюються жорсткі вимоги до процесу розробки, тестування та впровадження програмного забезпечення з багатоступінчастим контролем безпеки обробки даних.

Відбувається регулярне сканування системи с метою виявлення вразливостей та їх ліквідації.

Контроль захищеності даних користувача відбувається як у момент виконання фінансових операцій, і при зберіганні його даних у системі. Програмне забезпечення повинно постійно оновлюватися та використовуватися лише за останньою версією.

Окремо стоять такі технології оплати як Apple Pay. Це простий, безпечний та конфіденційний спосіб оплати покупок у магазинах, програмах та в Інтернеті. Крім того, через Apple Pay можна обмінюватися коштами з друзями та близькими прямо у програмі «Повідомлення», нажаль працює лише у США. А безконтактні бонусні картки у програмі Wallet дозволяють отримувати та погашати бонуси при оплаті за допомогою Apple Pay.

Система Apple Pay розроблена з урахуванням безпеки та конфіденційності користувачів, завдяки чому здійснювати платежі через неї зручніше та безпечніше, ніж використовувати фізичні кредитні, дебетові та передплачені картки.

Захист транзакцій у Apple Pay забезпечується за рахунок функцій безпеки, вбудованих в апаратне та програмне забезпечення вашого пристрою. Крім того, для використання Apple Pay на пристрої необхідно задати пароль і, за бажанням, налаштувати Face ID або Touch ID. Можна використовувати простий пароль або більш складний, щоб підвищити рівень безпеки.

Система Apple Pay також призначена для захисту особистих даних користувача. Компанія Apple не зберігає вихідні номери кредитних, дебетових або передплачених карток, доданих до Apple Pay, і не має доступу до них.

При використанні кредитної, дебетової або передоплаченої картки в системі Apple Pay компанія Apple не збирає жодних відомостей про транзакцію, які б дозволили визначити вашу особу: всі транзакції проводяться між вами, організацією торгівлі або розробником і банком або емітентом картки [65].

Коли ви додаєте до Apple Pay кредитну чи дебетову картку, то дані, введені на пристрої, шифруються і в такому вигляді відправляються на сервери Apple. Якщо дані картки вводяться за допомогою камери, вони ніколи не зберігаються в пам'яті пристрою або медіатеці. Компанія Apple розшифровує дані, визначає платіжну систему картки та

повторно шифрує інформацію за допомогою ключа, який можна розблокувати лише в цій системі, або лише на стороні постачальника, авторизованого емітентом картки для надання послуг з підготовки та виділення токенів.

Відомості, які ви надаєте про свою карту, про активацію певних настройок пристрою та про характер його використання, наприклад, відсоток часу, протягом якого пристрій перебуває в русі, та приблизна кількість викликів на тиждень, можуть надсилатися до Apple з метою визначення правомочності використання Apple Pay.

Компанія Apple також може надсилати інформацію емітенту картки, до платіжної системи або постачальникам, які мають дозвіл емітента картки на використання Apple Pay, з метою визначення правомочності вашої картки, її налаштування в Apple Pay та запобігання шахрайству.

Після підтвердження картки банк, авторизований банком постачальник послуг або емітент карти створює унікальний номер облікового запису пристрою, шифрує його та передає разом з іншими даними, наприклад, ключем для створення унікальних динамічних кодів безпеки для кожної транзакції, на сервери компанії Apple.

Apple не може розшифрувати номер облікового запису пристрою, але зберігає його в модулі Secure Element - це сертифікована відповідно до галузевих стандартів мікросхема для безпечного зберігання платіжної інформації на самому пристрої. На відміну від звичайних ситуацій з номерами кредитних або дебетових карток, емітент може заборонити використання цього номера на картках з магнітною смугою, телефоном або веб-сайтами. Номер облікового запису пристрою у модулі Secure Element ізольований від ОС iOS, watchOS та macOS, а також ніколи не зберігається на серверах Apple та в резервній копії iCloud.

Компанія Apple не зберігає вихідні номери кредитних, дебетових або передплачених карток, доданих до Apple Pay, і не має доступу до них. У системі Apple Pay зберігаються лише фрагменти фактичних номерів карток та облікових записів пристроїв, а також описи карток. Карти прив'язуються до вашого ідентифікатора Apple ID, що спрощує їх додавання на різних пристроях та керування ними [66].

Крім того, iCloud захищає дані у програмі Wallet, наприклад квитки та відомості про транзакції, шифруючи їх при пересиланні через Інтернет і зберігаючи в такому вигляді на серверах Apple [66].

При оплаті покупок за допомогою Apple Pay у магазинах, які приймають безконтактні платежі, Apple Pay передає дані між пристроєм та платіжним терміналом за стандартом NFC. NFC - це стандартна безконтактна технологія, створена для роботи лише на близьких відстанях.

Якщо увімкнений iPhone виявляє поле NFC, відображається вікно з номером картки за замовчуванням. Щоб надіслати платіжну інформацію, необхідно пройти автентифікацію за допомогою Face ID, Touch ID або пароля, крім Японії, якщо картка Suica використовується як транспортна експрес-картка.

При використанні Face ID або годинника Apple Watch необхідно двічі натиснути бічну кнопку на розблокованому пристрої, щоб активувати карту для оплати.

Після підтвердження транзакції Secure Element надсилає терміналу в місці продажу номер облікового запису пристрою та динамічний код безпеки транзакції, а також додаткову інформацію, необхідну для здійснення цієї транзакції. Як і в інших випадках, ні компанія Apple, ні пристрій не передають до іншої системи фактичний номер платіжної картки.

До підтвердження оплати банк, емітент картки або платіжна система може перевірити вашу платіжну інформацію за допомогою динамічного коду безпеки, щоб підтвердити його унікальність та зв'язок з вашим пристроєм.

Під час використання програми або веб-сайту з підтримкою Apple Pay в ОС iOS, watchOS або macOS програма або веб-сайт може перевірити, чи активовано службу Apple Pay на вашому пристрої.

Щоб забезпечити безпечну передачу платіжної інформації при оплаті в програмах та на веб-сайтах, служба Apple Pay отримує зашифровані відомості про транзакції та повторно шифрує їх за допомогою ключа, прив'язаного до певного розробника, перед надсиланням цієї інформації йому або обробнику платежів.

Завдяки цьому ключу до зашифрованої платіжної інформації може отримати доступ лише програма або веб-сайт, де ви робите покупку. Якщо веб-сайт пропонує як спосіб оплати Apple Pay, він щоразу проходить перевірку домену.

Як і при покупках в магазині, Apple відправляє програмі або веб-сайту номер облікового запису пристрою разом з динамічним кодом безпеки транзакції. Ні компанія Apple, ні пристрій не передають у програму фактичний номер платіжної картки.

Apple зберігає анонімні відомості про транзакції, включаючи приблизну суму покупки, відомості про розробника та назву програми, приблизну дату та час, а також інформацію про успішне завершення транзакції.

Ці дані використовуються для покращення роботи Apple Pay, а також інших продуктів та служб Apple. Компанія Apple також вимагає, щоб програми та веб-сайти в браузері Safari, на яких використовується Apple Pay, надавали користувачеві можливість ознайомитися з положеннями та умовами політики конфіденційності, де перераховуються особливості використання даних.

При використанні Apple Pay на iPhone або Apple Watch для підтвердження покупки, здійсненої в браузері Safari на комп'ютері Mac, комп'ютер Mac і авторизуючий пристрій обмінюються даними зашифрованим каналом через сервери Apple. Компанія Apple не зберігає цю інформацію у формі, яка припускає ідентифікацію особи користувача [67].

При додаванні бонусних карток у Wallet вся інформація зберігається на вашому пристрої та шифрується за допомогою заданого пароля. Можна настроїти автоматичне пред'явлення бонусної картки для оплати покупок за допомогою Apple Pay у магазинах торгової організації або вимкнути цю функцію у програмі Wallet. Компанія Apple вимагає, щоб усі дані передавалися на платіжний термінал у зашифрованому вигляді. Дані бонусної картки надсилаються лише після авторизації користувача. Компанія Apple не отримує жодних відомостей про операцію з бонусами, крім тих, що вказані у картці транзакції. Для резервного копіювання даних бонусних карток та їх синхронізації на кількох пристроях можна використовувати службу iCloud.

Якщо ви реєструєтеся для отримання бонусної картки та надаєте організації торгівлі інформацію про себе, в тому числі ім'я, поштовий індекс, адресу електронної

пошти та номер телефону, Apple отримає повідомлення про реєстрацію, але надана вами інформація буде надіслана організації торгівлі безпосередньо з пристрою та оброблена в відповідно до політики конфіденційності цієї організації.

Якщо ж ваш пристрій було викрадено але на ньому було увімкнено службу Знайти iPhone, можна зупинити роботу Apple Pay, перевівши пристрій у режим зникнення, щоб не анулювати карти відразу. Якщо ви знайдете пристрій, ви зможете повторно активувати Apple Pay.

Заборонити здійснення платежів за допомогою кредитних, дебетових та передплачених карток, які використовувалися в Apple Pay на пристрої, можна на сторінці облікового запису Apple ID.

При стиранні пристрою у дистанційному режимі за допомогою служби «Знайти iPhone» можливість оплати за допомогою карток, які використовувалися в Apple Pay, також блокується. Банк, авторизований банком постачальник послуг, емітент картки або авторизований цим емітентом постачальник послуг можуть призупинити обслуговування кредитних, дебетових та передплачених карток у Apple Pay, навіть якщо пристрій знаходиться в режимі офлайн і не підключено до мережі або мережі Wi-Fi.

Якщо ви знайдете свій пристрій, зможете повторно додати карти у програмі Wallet.

Крім того, можна звернутися до банку або емітенту картки для припинення обслуговування кредитної, дебетової або передплаченої картки з Apple Pay.

3.3 Аналіз ефективності даного методу та можливості його впровадження у банківську сферу

Протягом останніх років спостерігається швидкий розвиток ринку платіжних систем в Україні. Кількісне зростання показників цього ринку одночасно супроводжується і його якісним розвитком. Зокрема, активно впроваджуються нові платіжні послуги та операції.

Усе більшої популярності набувають електронні гроші. Зростає частка розрахунків, які здійснюються через мережу Інтернет.

Емітуються мобільні платіжні інструменти, які дають змогу контролювати та управляти банківським рахунком, а також здійснювати платежі за допомогою мобільного телефону.

Поняття безпеки фахівцями платіжних систем трактується з багатьох точок зору. Як користувач, незалежно від механізму захисту, система повинна бути простою, сучасною та надійною, забезпечувати нестандартні рішення складних проблем. Час передачі та сприйняття даних системою має бути коротким, щоб користувачі могли використовувати всі функції системи.

Якщо ж розглядати з точки зору обслуговуючого персоналу системи, то він повинен нести відповідальність за надійну та правильну роботу системи, тому його розуміння безпеки системи є іншим явищем. Для того, щоб мати можливість керувати роботою системи та дотримуватись вимог безпеки необхідно надати кожному користувачу визначені ресурси системи [68].

З цією метою необхідними є надійні механізми ідентифікації та встановлення прав доступу користувачів. При модифікації системи для підвищення сервісної функції системи, системний експерт повинен передбачити майбутні зміни потреб користувача.

Дослідивши різні трактування поняття “безпека” зазначимо, що під безпекою платіжних систем розуміють запобігання несанкціонованого доступу до інформації, несанкціонованого зміни інформації, несанкціонованих операцій з використанням функцій платіжної системи.

Безпеку платіжної системи можна розглядати як зовнішню та внутрішню безпеку. Зовнішня безпека включає захист систем від втрати або модифікації інформації в разі стихійного лиха, а також запобігання зловмисникам із зовні від крадіжки, отримання інформації або вимкнення системи.

Метою внутрішньої безпеки є забезпечення надійного та зручного механізму регулювання діяльності всіх користувачів і співробітників та підтримки правил доступу до ресурсів системи.

Створення надійної системи захисту розподіляють на наступні етапи [63]:

- аналіз можливих загроз;

- розробка системи захисту;
- реалізація системи захисту;
- супроводження системи захисту під час експлуатації платіжної системи.

Всі ці етапи взаємопов'язані. під час реалізації і для роботи платіжної системи необхідно постійно аналізувати адекватність системи захисту і можливість загроз, не врахованих на першому етапі.

Тому процес створення системи захисту є безперервним і вимагає уваги та постійного ретельного аналізу платіжних систем.

Розпочавши розроблення системи захисту для платіжної системи необхідним є аналіз можливих загроз. Важливою загрозою безпеки є несанкціонований доступ, тобто користувач отримує доступ до об’єктів, на які він не має дозволу.

Для досягнення несанкціонованого доступу використовуються два методи: подолання захисту процесів або систем моніторингу та аналіз інформації.

Наступний етап, з точки зору розвитку системи захисту, має форму єдиного заходу різних планів боротьби з можливими загрозами.

Дана система включає [64]:

- законодавчі акти, укази та інші нормативні документи, що регулюють правила роботи з обробки, накопичення та зберігання платіжної інформації в системі, а також відповідальність за порушення даних вимог;
- етико-моральні, тобто розрахунок кодексів поведінки учасників та обслуговуючого персоналу;
- заходи управління, а саме організаційні заходи щодо регулювання роботи системи обробки платіжної інформації, використання її ресурсів, діяльності працівників;
- заходи фізичного захисту, котрі включаючи охорону приміщень, обладнання та персоналу платіжної системи;
- програмно-апаратні засоби захисту, що забезпечують функції захисту самостійно або в поєднанні з іншими засобами: ідентифікація користувача, розподіл доступу, реєстрація основних системних подій, функції пароля.

Розгляд основних принципів, яких необхідно дотримуватись при створенні системи захисту, оцінки ризиків, які можуть виникати при здійсненні загроз внаслідок порушень системи захисту зі сторони різних елементів платіжної системи здійснюється при розроблені політики безпеки. В даному контексті політика безпеки визначається як набір законів, правил та практичних рекомендацій, на основі яких здійснюється керування, захист і розподіл критичної інфраструктури.

Висновки за розділом 3

Не зважаючи на постійні спроби захисту спеціалістів з безпеки, кількість загроз та атак задля отримання доступу до платіжної інформації зростає з кожним роком.

Підводячи підсумки, як вберегти себе від дій шахраїв, адже не всі ж користуються простими правилами, як не заразити комп'ютер вірусами, як не пустити грабіжника в квартиру, так і виконання правил користування картами немає нічого важкого:

- не світити карту в громадських місцях;
- не губити із поля зору карту при оплаті товарів чи послуг;
- користуватися в інтернеті тільки картками, які ви спеціально відкрили для таких цілей;
- стежити за залишками на картах (бажано через sms-повідомлення);
- встановити на інтернет-картку індивідуальний ліміт платежів в інтернеті;
- підключити карту до протоколу 3D Secure;
- вводити дані з картки тільки на перевірених сайтах, по можливості з логотипами Visa Secure та Mastercard SecureCode;
- не передавати данні карти третім особам (навіть родичам та друзям);

Не дивлячись на, здавалося б сумну ситуацію з захистом платіжних карток в інтернеті, все не так вже й погано.

Платіжні системи Visa і Mastercard регламентують цілісні правила ведення претензійної роботи, які зазвичай захищають кардхолдера, та гарантують

повернення грошей при шахрайстві, якщо не виявлено факт компрометації або передачі даних сторонній особі чи організації.

Можливо, це не завжди працює в нашій правовій державі, але є значною перевагою перед неповерненими локальними віртуальними платіжними системами. Крім того, платіжні картки широко використовуються у всьому світі, і для нас лише питання часу та швидкості як буде розвиватися культура безготівкових розрахунків.

ВИСНОВОК

На сьогодні у сфері інформаційної безпеки вже склалася певна база та створена система боротьби зі злочинами у кіберпросторі. Дослідження світових компаній показує що кількість атак задля отримання даних кредитних карток збільшується з кожним роком, а ефективність захисту залишається на минулому рівні. Отже дослідження методів та засобів пошуку і нейтралізації загроз від витоків інформації банківських карток є актуальною темою для досліджень у майбутньому.

Дослідження ефективності міжнародних платіжних систем в умовах сучасних інформаційних технологій дозволило зробити ряд характеристичних висновків щодо її роботи.

Загалом платіжні системи як один з інструментів безготівкової форми розрахунків доцільно розглядати в двох аспектах: функціональному та інституціональному. З погляду функціонального аспекту платіжна система є сукупністю механізмів, форм, методів, принципів організації переказу коштів від однієї особи іншій за законами, правилами та стандартами, що визначають права, обов’язки та відповідальність учасників.

Інституціональний аспект дозволяє розглядати платіжну систему як сукупність інститутів, що законодавчо регулюються та забезпечують виконання боргових зобов’язань, які виникають у процесі економічної діяльності та формують у рамках системи умови для використання банківських платіжних карток обумовленого стандарту як платіжний засіб.

Відповідно до нашого законодавства, насамперед, Закону України «Про українські платіжні системи та перекази коштів», електронні та паперові документи обробляються та передаються в межах країни для переказів, документи на транзакції та документи на зняття коштів за допомогою спеціальних способів оплати можуть бути оброблені через національну та міжнародну систему з платіжними системами.

Внутрішня платіжна система сама по собі є платіжною системою, резидентом якої є платіжна організація, яка здійснює свою діяльність та забезпечує переказ коштів лише в межах території України.

І навпаки, міжнародна платіжна система - це платіжна система, в якій платіжна організація може бути як резидентом, так і нерезидентом, функціонує в двох або більше країнах і забезпечує переказ коштів у межах цієї платіжної системи, в тому числі з однієї країни в іншу одну країну.

В нашому світі працює велика кількість платіжних систем, користувачами яких є сотні мільйонів жителів планети. Найбільші міжнародні платіжні системи Visa, MasterCard, American Express, Europay, DinersClub, які цілодобово надають своїм клієнтам широкі послуги практично в будь-якій точці планети та сфері обслуговування.

З економічної точки зору, робота міжнародної платіжної системи полягає у використанні сукупності інструментів та методів, що застосовуються в господарстві для переказу грошей, здійснення розрахунків та врегулювання боргових зобов'язань між учасниками економічного обігу, а також наявності інфраструктури, що забезпечує реалізацію завдань.

Структура платіжної системи може складатися з елементів, котрі тісно пов'язані одне з одним і не можуть розглядатись у відриві один від одного.

Серед таких можна виділити:

- платник - утримувач картки;
- емітент - банк платника (або інша фінансова чи нефінансова установа), що здійснює випуск карток;
- одержувач - підприємство торгівлі або сфери послуг, що має в наявності пристрої для обслуговування карток встановленого типу;
- еквайр - банк, що обслуговує одержувача;
- платіжна асоціація - організатор-власник технологічного стандарту розрахунків, що координує діяльність карткової платіжної системи, забезпечує процесинг платежів за платіжними картками даного стандарту, видає дозвіл на випуск чи обслуговування платіжних карток банками-учасниками;

- центральна процесингова компанія;
- розрахункові банки.

Для ефективної роботи системи необхідна підвищена відповідальність та організація всіх її елементів. Оскільки при невиконанні своїх функцій однією із сторін платіжної системи інша сторона неспроможна змінити перебіг подій.

Серед організаційних засад, щодо функціонування банківських установ на ринку платіжних інструментів полягають у забезпеченні ефективної роботи системи карткових розрахунків. У процесі обігу між учасниками платіжної системи виникають фінансові відносини, які пов'язані з переказом коштів, видачою кредитів, купівлею товарів, взаєморозрахунками [69].

Головною причиною створення оптимального механізму просування банківських карток на ринок є, передусім, його ретельне та всебічне вивчення, яке дозволяє не тільки визначити структуру попиту, але й встановити, який тип картки буде необхідний для даної конкретної особи чи організації.

Завдяки цьому користувач оцінює кожну особливість та переваги послуг, а в кінцевому підсумку обирає найбільш раціональний варіант, виходячи із запропонованих варіантів та власних можливостей.

Спільні дії міжнародних платіжних систем та комерційних банків на ринку карткових платіжних інструментів полягають у розробці платіжних функцій банківських платіжних карток, обґрунтуванні територіального розширення мережі їх використання, визначенні механізму просування карткових продуктів серед споживачів.

Загалом платіжні системи та комерційні банки, намагаючись отримати прибуток, здійснюють комплекс заходів, кінцевою метою яких є збільшення обсягів продажу. Натомість не завжди виділяють необхідні ресурси та фінанси для впровадження необхідних систем безпеки.

Проаналізувавши функціонування міжнародних платіжних систем в діяльності банківських установ України можна сказати, що карткові платіжні системи, які функціонують у банківській сфері України, можна розбити на міжнародні, тобто ті що працюють в 2 та більше країнах та внутрішньо-державні.

Серед міжнародних систем можна особливо виділити MasterCard та Visa, серед систем котрі не є власністю банківських установ слід виділити: American Express, Diners Club, JCB. Окремо можна виділити такі системи як Золота корона та UnionCard.

Щодо внутрішньо-державні та локальних систем котрі впроваджені вітчизняними банками можна виділити МТ-Картта, УкрКарт та інші. Окремо можна виділити Національна система масових електронних платежів (НСМЕП).

На теперішньому етапу розвитку ринку платіжних карток в Україні властивий ряд характеристик. Серед них виділяють:

- активна участь у міжнародних карткових платіжних системах;
- вдосконалення нормативно-правової бази з метою підвищення ефективності функціонування ринку карткових платіжних інструментів в Україні спрощення його взаємодії з міжнародними платіжними системами;
- розвиток вітчизняних платіжних систем, що потребує ретельного визначення правил і процедур обігу вітчизняних платіжних карток; зростання обсягів платежів по пластикових картках;
- зростання об’єму емітованих карток;
- зростання значення еквайрінгу.

Платіжні системи можна охарактеризувати наявністю великої ймовірності ризику, котрий пояснюється обсягом та розміром виконуваних у цих системах операцій. Зменшити імовірність виникнення ризиків платіжних систем можливо з використанням методу котрій буде об’єднувати:

- удосконалення законодавства стосовно відповідальності кредитора за своєчасне погашення власних зобов’язань;
- збільшити забезпечення майбутніх зобов’язань зі збільшенням обсягів платежів;
- покращити регулювання та нагляд за діяльністю учасників розрахунків;
- застосовувати економіко-математичні методи в процесі прогнозування фінансового стану учасників та імовірності виникнення ризиків платіжних систем.

В сучасних умовах компанії дуже швидко змінюють традиційні форми безготівкових розрахунків і опановують оплату через інтернет-браузери. Саме це зумовлює появу та розвиток електронних платіжних систем, котрі базуються на новій формі грошей - електронні гроші.

Електронні гроші - це різновид кредитних грошей, які являють собою одиниці виміру вартості, що зберігаються на відповідному електронному пристрої, приймаються як засіб платежу на користь емітента та інших юридичних та фізичних осіб і є грошовими зобов'язаннями емітента.

Задля широкого поширення електронних грошей в Україні, необхідною умовою є врегулювання законодавчих норм щодо безготівкових розрахунків, створення контролюючих органів, котрі будуть попереджувати порушення у сфері такого грошового обігу.

Наразі є велика необхідність у впорядкуванні діяльності платіжних систем, використанні електронних платіжних засобів, посиленні контролю за функціонуванням платіжних систем і захист інтересів їх користувачів.

Помилки в роботі платіжних систем зазвичай призводять до непоправних обставин в фінансових сферах, які обслуговують такі системи. Саме наразі головна тема сьогодення – це питання про забезпечення та всебічний захист для продуктивного та правомірного функціонування, розвинення банківської роботи та розрахунків в платіжних системах, зокрема їх робота в всесвітній Інтернет-мережі.

Консолідованість та сукупність методів, які мають бути спрямовані на рішення проблем, які забезпечують надійність індивідуальних та персональних даних платіжної картки, які мають результативно працювати тільки при поєднанні удосконалення та розвитку організаційних, новітніх технічних та правових аспектів.

Коли ми детально вивчимо професійні джерела, то прийдемо висновку, що нажаль сьогодні в Україні більше уваги надається лише в більшій мірі технічній складовій. Менше організаційній. І наразі майже відсутня тема юридичного аспекту. Зокрема, юридичні гарантії та чистота алгоритмів при розрахунках, які використовує платіжна система, зокрема будь-яка, є підтвердженням безумовної гарантії при розрахунках для учасників системи. Але також надає можливість таким учасникам зробити цілком самостійне та виважене рішення- якою ж системою при

здійсненні розрахунків все ж таки користуватися, які б наслідки, в тому числі й юридичні не мали такі розрахунки в такій системі.

Ці фактори мають продуктивно здійснювати вплив на результативність праці в економічному секторі країни. Саме ці головні продуктивні риси правової сторони питань спричинені тим, що зокрема правове питання є головна діюча сила у фінансових відносинах учасників ринку.

Обов’язково, коли спеціалісти створюють або мають намір створити таку систему надійних даних таких систем платіжних карток, дуже чітко треба розуміти особливості , тип роботи , класифікацію системи, особливу увагу треба приділити самій організації як для розрахунків, так і для платіжних інструментів, які будуть використані використовують для проведення фінансових операцій.

Лише враховуючи та розуміючи ці важливі моменти є можливість продуктивно створити модель можливих загроз та обрати найбільш ефективні методи захисту, які повинні бути невід’ємною частиною інтернет-браузеру або банківської системи в цілому та здійснюватися на усіх етапах створення та обробки платежів [70].

Основою методу захисту даних платіжних карток є необхідність впровадження та неухильного дотримання таких заходів безпеки:

- шифрування інформації на картці під час передачі по каналах зв'язку;
- контролювати дотримання правил безпеки та зберігання інформації банками або процесинговими центрами;
- забезпечення фізичної та технічної безпеки процесу виготовлення картки;
- обмежити та розмежувати рівні доступу співробітників до інформації про картки банківської системи;
- створити спеціальну структуру для аналізу ризиків і безпеки карткових проектів;
- обробляти транзакції та забезпечувати процес авторизації.

Вирішення зазначених завдань в процесі вдосконалення існуючих методів захисту дозволить прискорити платежі, мінімізувати ризики їх проведення, оптимізувати рух коштів банків на кореспондентських рахунках, зберегти кошти клієнтів, збільшити рівень довіри до інтернет платежів, що згодом вплине на значне збільшення прибутку компаній задіяних у цих банківських операціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Федорченко В. Н., Гензерский І. В., Шевякова Н. Ю. Аналіз загроз для мобільних пристроїв та способів їх захисту. Харківський національний економічний університет. Системи обробки інформації. 2011. Вип. 7. С.68.

2. Про інформацію: Закон України від 05.07.94 №31 - [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

3. Концепція інформаційної безпеки України від 30.09.15 - [Електронний ресурс] - Режим доступу: https://www.osce.org/files/f/documents/0/2/175056.pdf

4. Політика інформаційної безпеки. Інструкція АТ "Айбокс Банк" № 324 від 04.02.2019. - [Електронний ресурс] - Режим доступу: http://www.iboxbank.online/doc.php?id=677

5. Мукоіда Р. В. Законодавство України у сфері боротьби з кіберзлочинністю. 2016. С.35

6. Пфо О. М.. Основні поняття і класифікація кіберзлочинності. 2016. С.33

7. Погорецький М. А. Кіберзлочини: до визначення поняття. Вісник прокуратури. 2012. Вип. 8. С. 89-96.

8. Заходи виявлення злочинів у сфері інтелектуальної власності, пов’язаних з розповсюдженням контрафактної аудіовізуальної продукції та комп’ютерного програмного забезпечення - [Електронний ресурс] - Режим доступу: http://journals.uran.ua/index.php/2415-3818/article/view/87276/82868

9. Замкова Т. В. Проблеми захисту інформації у сучасних інформаційних системах - [Електронний ресурс] - Режим доступу: http://www.rae.ru/snt/?section=content&op=show_article&article_id=3893

10. Бобришов О. О. Один з аспектів боротьби з кібертероризмом у всесвітній павутині. Кіровоград. 2016. С. 23

11. Концепція інформаційної безпеки України від 30.09.15 - [Електронний ресурс] - Режим доступу: https://www.osce.org/files/f/documents/0/2/175056.pdf

12. Резолюція про злочинне використанням інформаційних технологій від 2002 - [Електронний ресурс] - Режим доступу: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/60/PDF/N1545760.pdf

13. Кривогін М. С. Міжнародно-правові аспекти боротьби з кібернетичними злочинами. Чіта, 2017. С. 77-79

14. Про ратифікацію Угоди про співпрацю держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерних технологій - [Електронний ресурс] - Режим доступу: https://cutt.ly/cy3axQT

15. Про державну таємницю: Закон України від 21.01.94 №16 [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/3855

16. Конвенція про кіберзлочинність - [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575

17. Дорошенко І.І. Впровадження розрахунків у євро міжнародні платіжні системи. Вісник НБУ № 6. 2011. С. 59-60

18. Padmavathi .G, , Sujithra. M. Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism. International Journal of Computer Applications, №.14, 2012. P. 24

19. Троянські коні (Trojan Horse) - [Електронний ресурс] - Режим доступу: https://sites.google.com/site/zagrozu/project-updates/logicnibombi

20. Люк (trapdoor) - [Електронний ресурс] - Режим доступу: http://ito.vspu.net/ENK/2011-2012/inf_bezpeka_2010/rob_stud/Backo2/Preview/page-6.html

21. Результати безготівкових розрахунків [Електронний ресурс] - Режим доступу: https://retailers.ua/news/partneryi/11539-nbu-ukraintsyi-vse-chasche-oplachivayut-pokupki-v-internete-i-vse-reje-snimayut-nalichnyie-itogi-beznalichnyih-raschetov-2020-goda-v-infografike

22. Золотогоров В. Г. Економіка. 2003. С. 720

23. Савін К. Платіжні картки як сучасний інструмент банківського маркетингу. 2010. С. 40-46.

24. Коробова Г. Г. Банківська справа. 2006.С 766.

25. Захист інформації від комп'ютерних вірусів - [Електронний ресурс] - Режим доступу: http://www.kgau.ru/istiki/umk/ismar/c_5_6.html

26. Безпека смартфона: рекомендації щодо забезпечення захисту телефона - [Електронний ресурс] - Режим доступу: https://eset.ua/ua/blog/view/24/bezopasnost-smartfona-rekomendatsii-po-obespecheniyu-zashchity-telefona - 2016

27. Колдовський М.В., Ващенко О.М. Ризики використання банківських платіжних карток. Вісник Української академії банківської справи. 2010. С. 45-49.

28. Платоненко А. В. Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту. Вісник Сучасний захист інформації. Вип.1. 2017. С. 128-131

29. Актуальні кібервразливості 2019 - [Електронний ресурс] - Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/

30. The new faces of privacy - [Електронний ресурс] - Режим доступу: https://www.tandfonline.com/doi/abs/10.1080/01972243.1993.9960141

31. Пиріг С.О. Аналіз карткового ринку України: перспективи розвитку. Економічний форум № 3. 2013.

32. 3D Secure - [Електронний ресурс] - Режим доступу: https://www.piraeusbank.ua/ua/3D_Secure.html

33. Безпечні інтернет-платежі 3D Secure - [Електронний ресурс] - Режим доступу: https://kramar-eko.com.ua/politika-oplati-ta-povernennya-koshtiv/

34. Офіційний Інтернет-сайт представництва VISA в Україні. 2014 [Електронний ресурс] - Режим доступу: http://visa.com.ua/ua/uk.ua/merchants/acceptingvisa/identifyingcards.sht

35. Іванов А.Н. Банківські послуги: зарубіжний досвід. 2002. С. 175.

36. Рекомендації Національного інституту стандартів і технологій. Керівництво з безпеки Bluetooth - [Електронний ресурс] - Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-121r1.pdf

37. Платіжні системи для інтернет магазину: як обрати [Електронний ресурс] - Режим доступу : https://brander.ua/blog/platizhni-sistemi-dlya-internet-magazinu-yak-obrati

38. Найкращі платіжні системи в Інтернеті - [Електронний ресурс] - Режим доступу: http://www.profi-forex.org/internet/poiskovye-sistemy/jandeks/entry1008203696.html

39. Навчальні матеріали онлайн. Банківська платіжна картка [Електронний ресурс] - Режим доступу: http://pidruchniki.com/18060203/finansi/bankivska_platizhna_kartka

40. Положення НБУ “Про порядок емісії платіжних карток і здійснення операцій з їх застосуванням”. 27.08.2001 [Електронний ресурс] - Режим доступу: http://www.rada.gov.ua

41. Політика інформаційної безпеки. Інструкція АТ "Айбокс Банк" № 324 від 04.02.2019. - [Електронний ресурс] - Режим доступу: http://www.iboxbank.online/doc.php?id=677

42. Постанова Правління Національного банку України “Положення про електронні гроші в Україні”. 01.11.2010. [Електронний ресурс] - Режим доступу: http://www.rada.gov.ua

43. Навчальні матеріали онлайн. Розвиток платіжної системи України. [Електронний ресурс] - Режим доступу: http://osvita.ua/vnz/reports/bank/20768/

44. Капошко А.В. Електронні гроші. [Електронний ресурс] - Режим доступу: http://udau.edu.ua/ library.php.

45. Крупка М. І., Андрущак Є. М., Пайтра Н. Г. Банківські операції. Львів: Видавничий центр ЛНУ ім. Івана Франка . 2009. С. 248.

46. Інформаційний банківський сайт [Електронний ресурс] - Режим доступу : http://www.uabanker.net.

47. Страхарчук А.Я., Страхарчук В. П. Інформаційні системи і технології в банках. 2010. С.515.

48. Кравець В. М. Інтернет комерція в Україні. Вісник НБУ. 2011. С. 9-12.

49. Системи електронних платежів - [Електронний ресурс] - Режим доступу: https://bankchart.com.ua/e_banking/statti/sistemi_elektronnih_platezhiv

50. Ільницька Н. Аналіз світового ринку електронних грошей .Вісник НБУ № 4. 2010. С. 31-36.

51. Алексеєнко М.Д., Ярова А.В. Електронні гроші: сутність і види. 2012. С. 9-14.

52. Положення НБУ “Про діяльність в Україні внутрішньодержавних і міжнародних платіжних систем. 25.09.2007. [Електронний ресурс] - Режим доступу: http://www.rada.gov.ua

53. Кравець В. М. Організація контролю за операціями з банківськими платіжними картками. Вісник НБУ. С. 39-40.

54. Слабченко К.К. Сходинками до наукових вершин тези наукових робіт : Біла Церква, 2019. С. 23

55. Львівський державний університет внутрішніх справ. Теорія та практика протидії злочинності у сучасних умовах. 2020. Львів. С. 30-35

56. Організація і функціонування систем міжбанківських розрахунків в Україні - [Електронний ресурс] - Режим доступу: https://ronl.org/referaty/bank/267611/

57. Міжбанківські розрахунки в Україні- [Електронний ресурс] - Режим доступу: https://zavantag.com/docs/index-18320044-3.html?page=6

58. Карпов В.А., Кучеренко В.Р. Маркетинг: прогнозування кон`юнктури ринку. 2001. С. 215.

59. Маріупольський державний університет. Збірник матеріалів наукового круглого столу «Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку» : Маріуполь, 2018. С. 23

60. Здійснення міжбанківських розрахунків через систему електронних платежів- [Електронний ресурс] - Режим доступу: https://studopedia.com.ua/1_333585_zdiysnennya-mizhbankivskih-rozrahunkiv-cherez-sistemu-elektronnih-platezhiv.html

61. Beyond Black Friday Threat Report - [Електронний ресурс] - Режим доступу: https://securelist.com/beyond-black-friday-threat-report/83238/

62. ПАТ «Банк Форвард». Інформаційний матеріал про технологію 3D Secure. 2018. С. 1-4

63. Електронна комерція - [Електронний ресурс] - Режим доступу: https://www.vuzlib.su/banki/4.htm

64. Операції з платіжними картками слід здійснювати по-новому - [Електронний ресурс] - Режим доступу: https://news.dtkt.ua/finance/bank-system/74808

65. Посилюються захист прав держателів платіжних карток та вимоги до еквайрів - [Електронний ресурс] - Режим доступу: https://buhgalter911.com/uk/news/news-1063684.html

66. Перспективи розвитку сучасних інформаційних систем і технологій - [Електронний ресурс] - Режим доступу: https://kazedu.com/referat/168545/9

67. Порівняльна характеристика платіжних інструментів - [Електронний ресурс] - Режим доступу: https://cwetochki.ru/ref-kontrolnaia-rabota-porivnialna-kharakteristika-platizhnikh-instrumentiv.html?page=3

68. Аналіз платіжних систем, що використовуються в мережі Інтернет - [Електронний ресурс] - Режим доступу: http://www.0qm.ru/bankovskoe-birzhevoe-delo-i-straxovanie/porivnyalna-xarakteristika-platizhnix-instrumentiv.html

69. Електронні платіжні системи - [Електронний ресурс] - Режим доступу: https://bit.ly/3w3x9kO

70. Розвиток електронної комерції в Україні в умовах глобалізації - [Електронний ресурс] - Режим доступу: https://dodiplom.ru/ready/17483

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Тези наукових доповідей:

1. Організація безпечної роботи при використанні електронної пошти/Міжнародна науково-практична конференція «прикладні системи та технології в інформаційному суспільствіої пошти/ В.В. Луценко/» (AISTIS) 2020 / С.110-113

2. How to protect your card on the internet/ В.В. Луценко, С.В.Толюпа / ITI 2021 December

3. Захист даних платіжних карток при проведенні банківських операцій через інтернет-браузер/ Сергій Толюпа, Владислав Луценко/ V Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)” 14 - 15 КВІТНЯ 2022, КИЇВ, Україна