Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студентки *Сисоєвої Анастасії Дмитрівни*

академічної групи *125м-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Аналіз вимог до забезпечення безпеки даних при проведенні операцій з платіжними картками*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Войцех С.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Сисоєвій А.Д.*** **академічної групи** ***125м-17-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Аналіз вимог до забезпечення безпеки даних при проведенні операцій з платіжними картками***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.18 № 2025-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***процес забезпечення безпеки даних платіжних карток***

Предмет досліджень ***сервіси безпеки даних індустрії платіжних карток***

Мета ***підвищення рівня захисту даних платіжних карток***

Вихідні дані для проведення роботи ***законодавство України та міжнародні стандарти у сфері інформаційної безпеки та кібербезпеки, наукові публікації вітчизняних та іноземних авторів, офіційні статистичні дані***

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна ***створення рекомендацій для підвищення рівня безпеки при проведенні операцій з платіжними картками***

Практична цінність ***впровадження рекомендацій для підвищення рівня інформаційної безпеки в організаціях, які зберігають, оброблюють та передають дані тримачів платіжних карток***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

результати роботи мають відповідати вимогам чинного законодавства України та методичним рекомендаціям до підготовки та захисту дипломної роботи для студентів галузі знань «Кібербезпека»

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Огляд джерел за темою та напрямом досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-01.12.18
Виконання економічного розділу	02.12.18-09.12.18
Оформлення пояснювальної записки	10.12.18-13.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***полягає у зменшенні збитків від шахрайства з платіжними картками***

Соціальний ефект ***полягає у підвищенні впевненості керівництва та працівників організацій, клієнтів з точки зору рівня захищеності даних при проведенні операцій з платіжними картками***

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ Кагадій Т.С.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Сисоєва А.Д.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка __ с., ___ рис., ___ табл., ___ додатків, ___ джерела.

Об’єкт дослідження: процес забезпечення безпеки даних платіжних карток.

Мета роботи: підвищення рівня захисту даних платіжних карток.

У першому розділі проаналізовані системи електронних платежів, способи шахрайств з платіжними картками, методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції.

У спеціальній частині проаналізовано вимоги стандарту безпеки даних індустрії платіжних карток (PCI DSS) та створені рекомендації для підвищення рівня безпеки при проведенні операцій з платіжними картками.

В економічному розділі наведено економічне обґрунтування доцільності використання розроблених рекомендацій.

Практична цінність роботи полягає у впровадженні рекомендацій для підвищення рівня інформаційної безпеки в організаціях, які зберігають, оброблюють та передають дані тримачів платіжних карток.

Наукова новизна роботи полягає у розробці рекомендацій для підвищення рівня безпеки при проведенні операцій з платіжними картками з урахуванням вимог стандарта PCI DSS.

ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМА ЕЛЕКТРОННИХ ПЛАТЕЖІВ, ЕЛЕКТРОННИЙ ОБМІН ДАНИМИ, ПЕРСОНАЛЬНІ ДАНІ, АНТИ-ФРОД СИСТЕМА, ПРОЦЕСИНГОВИЙ ЦЕНТР, РИЗИКИ БЕЗПЕКИ, СТАНДАРТ PCI DSS.

РЕФЕРАТ

Пояснительная записка: ____ с., ___ рис., ___ табл., __ приложений, __ источников.

Объект исследования: процесс обеспечения безопасности данных платежных карт.

Цель работы: повышение уровня защиты данных платежных карт.

В первом разделе проанализированы системы электронных платежей, способы мошенничества с платежными картами, методы и средства оценки рисков безопасности информации в системах электронной коммерции.

В специальной части проанализирован стандарт безопасности данных индустрии платежных карт (PCI DSS) и на его основе созданы рекомендации для повышения уровня безопасности при проведении операций с платежными картами.

В экономическом разделе приведено экономическое обоснование целесообразности использования разработанных рекомендаций.

Практическая ценность работы состоит во внедрении рекомендаций по повышению уровня информационной безопасности в организациях, которые хранят, обрабатывают и передают данные держателей платежных карт.

Научная новизна работы заключается в разработке рекомендаций по повышению уровня безопасности при проведении операций с платежными картами с учетом требований стандарта PCI DSS.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, СИСТЕМА ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ, ЭЛЕКТРОННЫЙ ОБМЕН ДАННЫМИ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ, АНТИ-ФРОД СИСТЕМА, ПРОЦЕССИНГОВЫЙ ЦЕНТР, РИСКИ БЕЗОПАСНОСТИ, СТАНДАРТ PCI DSS.

ABSTRACT

Explanatory note: ____ p., ___ fig., ___ tab, __ applications, __ sources.

Object of the study: process of the security payment data.

The target of the article : increasing the level of security for payment cards data.

The first section analyzes electronic payment systems, methods of fraud with payment cards, methods and tools of assessing information security risks in electronic commerce systems.

In the special part, the data security standard of the payment card industry (PCI DSS) was analyzed and recommendations were made to increase the level of security by conducting transactions with payment cards on its basis.

The economic section provides the economic feasibility for using the designed recommendations.

The practical value of the work is the implementation of recommendations by increasing the level of information security in organizations which store, process and transmit data of cardholders.

The scientific novelty of the article is to develop recommendations by increasing the level of security by conducting transactions with payment cards, taking into account the requirements of the PCI DSS standard.

INFORMATION SECURITY, ELECTRONIC PAYMENT SYSTEM, ELECTRONIC DATA EXCHANGE, PERSONAL DATA, ANTI-FRAud SYSTEM, PROCESSING CENTER, SAFETY RISKS, PCI DSS STANDARD.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

API – application-programming interface;

EDI – електронний обмін даними;

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;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

СЕК – система електронної комерції;

СЕП – система електронних платежів.

ЗМІСТ

ВСТУП

Актуальність. В наш час усі підприємства пов’язані з процесами зберігання та обробки інформації. Ця інформація може містити конфіденційні дані, розкриття яких завдасть значної шкоди репутації підприємства, його роботоздатності або фінансовому положенню.

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.

Діяльність у сфері захисту персональних даних на території України регламентується Законом України "Про захист персональних даних", Конституцією України, іншими законами та нормативно-правовими актами, а також міжнародними договорами, стандартами.

Метою роботи є створення рекомендацій для підвищення рівня безпеки при проведенні операцій з платіжними картками з урахуванням вимог стандарта PCI DSS.

У роботі були поставлені такі задачі:

- проаналізувати підходи до процедури обробки платіжних карток;
- проаналізувати методи боротьби з шахрайськими операціями;
- проаналізувати вимоги міжнародного стандарту у сфері інформаційної безпеки даних індустрії платіжних карток PCI DSS;

– на основі вимог стандарту PCI DSS розробити рекомендації щодо підвищення рівня безпеки даних тримачів карток для організацій, в інформаційній інфраструктурі яких зберігаються, обробляються або передаються дані платіжних карт;

– обґрунтувати доцільність створених рекомендацій, їх практичну та економічну ефективності.

Об’єктом досліджень є процес забезпечення безпеки даних платіжних карток.

Предметом досліджень є сервіси безпеки даних індустрії платіжних карток.

Наукова новизна роботи полягає у розробці рекомендацій для підвищення рівня безпеки при проведенні операцій з платіжними картками з урахуванням вимог стандарта PCI DSS.

Практична цінність роботи полягає у впровадженні рекомендацій для підвищення рівня інформаційної безпеки в організаціях, які зберігають, оброблюють та передають дані тримачів платіжних карток.

РОЗДІЛ 1
АНАЛІЗ БЕЗПЕКИ ПЛАТІЖНИХ СИСТЕМ

Кібербезпека – це безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам.

Лише з початку 2018 року (12 травня – комп'ютерний вірус WannaCry та 27 червня – PetyA) сталися дві потужні кібератаки, націлені на численні держустанови та відомства, а також приватний сектор. Ці кібернапади підтвердили, що підготовка фахівців із кібербезпеки повинна стати пріоритетом кадрової політики держави та окремих компаній.

Розуміючи сучасний стан та актуальність проблеми забезпечення кібернетичної безпеки, більшість країн світу проводять комплексні заходи щодо забезпечення безпеки в кібернетичному просторі. Ці заходи пов’язані перш за все з розробкою та вдосконаленням нормативно-правової бази, що регулює питання сфери кібербезпеки. Створюються структури, що відповідають за забезпечення кібернетичної безпеки. Спеціальні служби різних країн вивчають методи діяльності хакерських груп, а іноді навіть активно співпрацюють з ними, використовуючи їхні знання та навички при проведенні кібернетичних операцій, пропонуючи їм натомість лояльність та захист.

Україна кожен рік потрапляє в антирейтингові списки щодо піратства, розповсюдження шкідливого програмного забезпечення, DDoS атак та інше. Так, відповідно до дослідження корпорації Майкрософт (Microsoft Corporation), на 86% комп’ютерів в Україні встановлено неліцензійне програмне забезпечення. Використання неліцензійного програмного

забезпечення – це прямий шлях для надання доступу хакерам до ресурсів систем, на яких воно встановлено [1].

Загрози національній безпеці України в кібернетичному просторі призвели до появи Стратегії кібербезпеки України (далі Стратегія), що була введена в дію указом Президента України від 15 березня 2016 року. Метою створення стратегії було забезпечення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства та держави.

Стратегія є важливим кроком на шляху побудови системи кібербезпеки України та являє собою програму дій для державних органів. В стратегічному документі поставлено завдання щодо формування державного реєстру об'єктів критичної інформаційної інфраструктури, а на власників цих об'єктів покладені зобов'язання створити підрозділи атестованих спеціалістів з ІТ-безпеки для оперативного виявлення загроз та реагування на інциденти в інформаційному середовищі.

Відповідальність за кібербезпеку у фінансовій сфері покладено на Національний банк України, що має сформувати власні вимоги до банків та інших суб'єктів фінансового ринку, а приватний бізнес визнається повноправним суб'єктом системи кібербезпеки в Україні [2].

Щодня кожен з нас стикається із необхідністю користування інформаційними системами та технологіями від соціальних мереж, розміщення інформації про свої персональні дані в Інтернеті до користування банківськими рахунками, системами e-commerce та інші.

1.1 Загальна характеристика платіжних систем в Україні

Нині в Україні діють створені Національним банком України Система електронних платежів (СЕП), Національна система масових електронних платежів (НСМЕП) та приватні внутрішньодержавні та міжнародні платіжні системи банків та небанківських установ [3].

Закон України «Про платіжні системи та переказ грошей в Україні» [6] платіжну систему визначає як платіжну організацію, членів платіжної системи та сукупність відносин, що виникають між ними при проведенні переказу коштів.

Також платіжну систему можна представити як систему механізмів, які служать для переказу грошових коштів між суб'єктами господарювання, розрахунку за платіжними зобов'язаннями, що виникають між ними. Платіжна система – це набір платіжних інструментів, банківських процедур і, як правило, міжбанківських систем переказу коштів, поєднання яких забезпечує грошовий обіг разом з інституційними та організаційними правилами та процедурами, що регламентують використання цих інструментів та механізмів [7].

Платіжна система складається з кількох самостійних систем, а саме: системи «клієнт-банк»; внутрішньобанківські платіжні системи; системи міжбанківських розрахунків; системи масових платежів.

Платіжні системи виконують функцію передачі потоку інформації, який містить деталі платежу, і безпосередньо переказу грошових коштів.

Розроблення та впровадження Національним банком України СЕП та НСМЕП дало змогу у стислі строки відмовитись від внутрішньобанківських та міжбанківських розрахунків [3].

Впровадження СЕП підняло банківську індустрію України на якісно новий рівень. СЕП НБУ ефективно виконує покладені на неї функції державної системи міжбанківських розрахунків, оперативно і надійно обслуговує учасників СЕП, гарантуючи високий рівень безпеки та надійність міжбанківського переказу коштів у національній валюті.

На сьогоднішній день, через СЕП здійснюється понад 98% міжбанківських переказів у національній валюті в межах України, тоді як через кореспондентські рахунки, що відкриті банками в інших банках – менше 2% [5].

Отже, основними досягненнями СЕП на сучасному етапі її розвитку є прискорення доставки платежів від відправника до отримувача та обслуговування великої кількості платежів. Окрім того, система забезпечує можливість виконувати міжбанківський переказ у двох режимах: файловому та режимі реального часу.

Основними елементами сучасної платіжної системи є:

- нормативно-правова база, що регулює платіжні відносини, має створювати сприятливі умови для забезпечення потреб нормального функціонування платіжної системи;
- бухгалтерська і технологічна моделі, що є основним операційним механізмом здійснення платежів, який ґрунтується на принципах бухгалтерського обліку і звітності, включає платіжні інструменти та механізми переказу коштів;
- технологічна інфраструктура, що є основою життєздатності платіжної системи. Вона включає, зокрема, програмні та технічні засоби обробки та передачі даних, обслуговуючий персонал;
- захист інформації як сукупність програмно-технічних, нормативно-правових, адміністративно-організаційних засобів [7].

Інформаційна безпека є останнім елементом платіжної системи, а тому для забезпечення її ефективного функціонування потрібно всі елементи розглядати у системній єдності і тісному взаємозв'язку.

Для забезпечення безпеки платіжних операцій всі фінансові установи періодично повинні проходити аудити Національного банку України та незалежний аудит щодо відповідності міжнародним стандартам безпеки, проводити цілодобовий моніторинг фінансових операцій з метою виявлення підозрілих транзакцій за територіальним критерієм, за критеріями суми та типу операції. За вимогами міжнародних платіжних систем фахівці з питань безпеки платіжних операцій повинні проходити регулярне навчання щодо новітніх засобів шахрайства в галузі ПК, а також ознайомлюватись з новітніми методиками боротьби з ним [8].

Оцінка функціонування НПС як карткової платіжної системи залежить від дослідження стану ринку банківських платіжних карток в Україні. Загалом ситуація на цьому сегменті ринку банківських послуг характеризується поступовим зростанням кількості та суми безготівкових операцій з використанням карток, зокрема збільшенням обсягу емітованих платіжних карток та їхніх держателів, розширенням мережі банкоматів і термінального обладнання, використанням різних типів карток.

Згідно з даними НБУ станом на 1 серпня 2017 року в Україні функціонують 89 банків, що є членами платіжних систем (83,3% від загальної кількості банків в Україні) [9]. Також слід зазначити, що за останнє десятиліття обсяг операцій з використанням платіжних карток збільшився в багато разів (рис. 1.1).

Рисунок 1.1 – Обсяг операцій (безготівкових платежів) з використанням платіжних карток комерційними банками України за 2006–2016 роки

Така позитивна динаміка на ринку платіжних карток є результатом реформ НБУ у сфері національної платіжної системи.

Слід зазначити, що подальший розвиток національної системи масових електронних платежів «ПРОСТІР» дасть змогу прискорити здійснення розрахунків та обігу коштів, зменшити документообіг, знизити вірогідність фальсифікації міжбанківських розрахункових документів, посилити контроль

за станом грошової маси в державі, знизити збитки держави та підприємців від низької швидкості виконання розрахунків та використання підроблених платіжних документів, підвищити можливості комерційних банків і Національного банку України контролювати здійснення платежів.

Як свідчить зарубіжний досвід, з метою гарантування безперервного та стабільного функціонування платіжних систем центральні банки розвинутих країн розпочали здійснювати оверсайт платіжних систем.

Згідно з Постановою правління НБУ «Про затвердження оверсайту платіжних систем» [10], яку розробили вітчизняні науковці, оверсайт платіжних систем – це діяльність центрального банку, спрямована на забезпечення безперервного, надійного та ефективного функціонування платіжних систем, яка полягає в оцінюванні діючих платіжних механізмів і тих, що плануються, а також, якщо є така необхідність, ініціюванні змін до них.

Метою оверсайту платіжних систем є надійність та ефективність систем щодо забезпечення ними переказу коштів. Для досягнення зазначеної мети НБУ має встановити вимоги, яким повинні відповідати платіжні системи, та здійснювати оцінку систем щодо цих вимог. Під час оцінювання платіжної системи увага Національного банку України має приділятися таким характеристикам побудови та роботи системи, як:

- здатність системи надавати швидкі, безпечні та економічно вигідні послуги суб’єктам економіки, що має значення для створення сприятливих умов функціонування фінансових ринків та економіки;
- ефективність та надійність схем взаєморозрахунків за виконаними операціями з переказу коштів у платіжній системі;
- дієвість політики управління ризиками, яку проводить платіжна організація платіжної системи тощо [10].

Зазначимо, що здійснення НБУ оверсайту платіжних систем повинно базуватися на таких міжнародних принципах:

1) прозорість – центральний банк має відкрито оприлюднити політику оверсайту та загальні вимоги до платіжних систем;

2) наявність повноважень та можливостей – центральний банк повинен мати дієві повноваження та можливості для здійснення ефективного оверсайту;

3) послідовність – вимоги до платіжних систем мають застосовуватися до всіх платіжних систем, зокрема створених центральним банком;

4) співпраця з іншими державними регуляторами – центральний банк має співпрацювати з іншими державними регуляторами та центральними банками інших країн з метою сприяння безпеці та ефективності платіжних систем [10, 11].

Через законодавчо визначену відповідальність за стійкість національної валюти НБУ належить центральна роль у використанні грошей як ефективного засобу платежу. НБУ може сприяти підвищенню ефективності і надійності платіжної системи на основі таких повноважень, які приведені у табл 1.1.

Таблиця 1.1 – Повноваження НБУ щодо підвищення ефективності платіжної системи

№	Повноваження НБУ щодо підвищення ефективності платіжної системи	Конкретні дії з боку регулятора
1	2	3
1	НБУ, як оператор, може надавати і розвивати платіжні і кредитні послуги	Емітувати готівкові гроші як безпосередній платіжний документ і депозитні вимоги як розрахунковий актив для міжбанківських платежів.
		Виступати в ролі власника системно-важливих клірингових і розрахункових систем, їх оператора або

		брати участь в управлінні ними.
		Керувати розрахунковими рахунками і надавати розрахунковий кредит (як протягом дня, так і наприкінці дня) для учасників системи.

Продовження таблиці 1.1

1	2	3
2	Як каталізатор	Ініціювати, координувати проводити дослідження і консультації щодо дизайну, функціонування СЕП, а також розробляти відповідну політику.
		Розробляти відповідні законопроекти щодо розвитку СЕП.
3	Як орган нагляду	Здійснювати моніторинг діючих і проектних платіжних систем, оцінювати їх відповідність принципам надійності й ефективності.
		Проводити консультації, розробляти рекомендації; за необхідності стимулювати зміни дизайну і функціонування платіжної системи; розробляти свої керівні принципи щодо нагляду за СЕП.
4	НБУ, як користувач, може брати участь в клірингових і розрахункових системах	Для використання систем, власниками і операторами яких є зовнішні сторони, для здійснення і отримання платежів від свого імені або від імені свої клієнтів (таких як держава та її органи).
		Для використання систем розрахунку по цінних паперах і депозитарних систем для реалізації своїх операцій.
		Для використання кореспондентських банківських послуг інших центральних банків і фінансових установ.

Таким чином, дії НБУ щодо розвитку національної платіжної системи є невід'ємною складовою його діяльності у сфері реалізації монетарної політики, яка має спрямовуватися на виконання таких завдань:

- визначення пріоритетів і планування розвитку платіжної системи;
- виділення ресурсів для моніторингу стану СЕП, проведення аналізу і досліджень;
- розробка комунікаційної стратегії для підвищення координації дій у сфері розвитку СЕП з іншими зацікавленими сторонами;
- підвищення кваліфікації експертів, які займаються проблемами розвитку національної платіжної системи тощо.

На рисунку 1.2 відображено системний підхід до формування безпеки платіжної системи України. Кожен комерційний банк, що є учасником платіжної системи, повинен використовувати сучасні платіжні інструменти та механізми переказу коштів, новітні програмні та технічні засоби обробки та передачі даних, чітко дотримуватись вимог вітчизняного законодавства та НБУ.

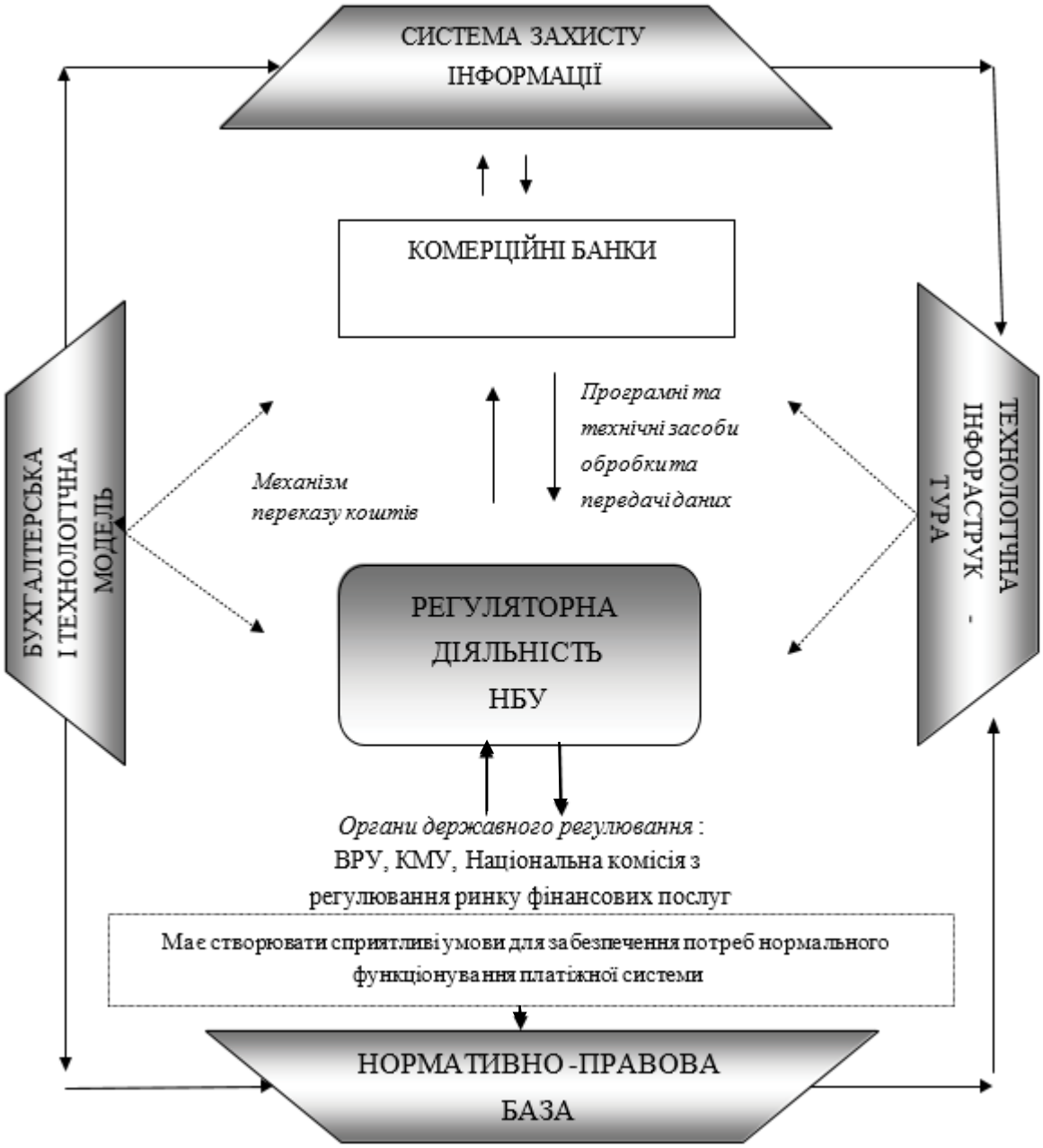

Рисунок 1.2 – Системний підхід до формування безпеки платіжної системи України

У кожній фінансовій установі має бути підрозділ, що займається забезпеченням безпеки платіжних операцій, фінансовим моніторингом та реагуванням на спроби порушення безпеки платіжних карток, а також тісно взаємодіє з аналогічними підрозділами інших фінансових установ в Україні, представниками міжнародних платіжних систем [8].

1.2 Безпека платіжних систем

Інформаційна безпека (стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення) означає можливість протистояти спробам нанесення збитків власникам або користувачам платіжної системи при різних навмисних або ненавмисних впливах на неї. Система захисту інформації повинна забезпечувати безперервний захист інформації щодо переказу коштів на всіх етапах її формування, обробки, передачі та зберігання. Електронні документи, що містять інформацію, яка належить до банківської таємниці або є конфіденційною, повинні бути зашифрованими під час передавання їх за допомогою телекомунікаційних каналів зв'язку [12].

Захист інформації – сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та осіб, які користуються інформацією. Об'єктом захисту є інформація, що обробляється в автоматизованій системі, права власників автоматизованої системи, права користувача [13].

Безпеку платіжних систем можна розглядати як таку, що складається із зовнішньої та внутрішньої.

Зовнішня безпека включає:

- захист від втрати або модифікації системою інформації при стихійних лихах (пожежах, землетрусах та ін.);
- захист системи від проникнення зловмисників ззовні з метою викрадення, отримання доступу до інформації або виведення системи з ладу.

Мета внутрішньої безпеки – забезпечення надійної та коректної роботи, цілісності інформації і компонентів (ресурсів) системи. Це передбачає створення надійних і зручних механізмів регламентування діяльності всіх

користувачів та обслуговуючого персоналу, підтримання дисципліни доступу до ресурсів системи.

Можна виділити два підходи до гарантування безпеки інформаційних систем: фрагментарний та комплексний.

Фрагментарний підхід орієнтується на протидію чітко визначеним загрозам при певних умовах використання системи. Головною позитивною рисою такого підходу є міцний захист щодо конкретної загрози, але основний недолік – локальність дії та відсутність єдиного захищеного середовища для обробки інформації. Тому такий підхід неприйнятний для захисту платіжних систем.

Для створення захисту платіжних систем треба використовувати комплексний підхід, а саме: створення захищеного середовища для обробки платіжної та службової інформації в системі, яке об'єднує різноманітні (правові, організаційні, програмно-технічні) засоби для протидії будь-яким загрозам.

Варто звернути увагу на те, що суб'єктами відносин, пов'язаних з обробкою інформації в автоматизованій системі, є:

- власники інформації чи уповноважені ними особи;
- власники автоматизованої системи чи уповноважені ними особи;
- користувачі інформації;
- користувачі автоматизованої системи.

Створення надійної системи захисту можна розділити на чотири основних етапи:

1) аналіз можливих загроз;

2) розробка (планування) системи захисту;

3) реалізація системи захисту;

4) супроводження системи захисту під час експлуатації платіжної системи [12].

Аналіз можливих загроз – це вибір із усієї безлічі можливих впливів на систему лише таких, які реально можуть виникати і наносити значні збитки.

Усі загрози можна розподілити за їх характеристиками на такі класи:

1. За цілями реалізації загрози:

- порушення конфіденційності інформації;
- порушення цілісності (повна або часткова компрометація інформації; дезінформація; несанкціоноване знищення або модифікація інформації чи програмного забезпечення);
- порушення (часткове або повне) працездатності системи.

2. За принципом впливу на систему:

- за допомогою доступу до об'єктів системи (файлів, даних, каналів зв'язку);
- за допомогою прихованих каналів (у тому числі через роботу з пам'яттю).

3. За характером впливу на систему:

- активний вплив – виконання користувачами деяких дій поза межами своїх обов'язків, які порушують систему захисту та змінюють стан системи;
- пасивний вплив – спостереження побічних ефектів роботи системи та їх аналіз, які не змінюють стан системи, але дають можливість отримання конфіденційної інформації.

4. За причинами появи помилок у системі захисту:

- некоректність системи захисту, що призведе до дій, які можна розглядати як несанкціоновані, але система захисту не розрахована на їх припинення або недопущення;
- помилки адміністрування системи;
- помилки в алгоритмах програм, зв'язках між ними тощо, які виникають на етапі проектування;
- помилки реалізації алгоритмів, тобто помилки програмування, які виникають на етапі реалізації або тестування програмного забезпечення.

5. За способом впливу на об'єкт атаки:

- безпосередній вплив на об'єкт атаки (в тому числі за допомогою використання привілеїв);
- вплив на систему привілеїв (у тому числі захоплення привілеїв) і доступ до системи, який система вважатиме санкціонованим;
- опосередкований вплив через інших користувачів.

6. За способом впливу на систему:

- під час роботи в інтерактивному режимі;
- під час роботи у пакетному режимі.

7. За об'єктом атаки:

- на систему загалом;
- на об'єкти системи з порушенням конфіденційності, цілісності або функціонування об'єктів системи (дані, програми, устаткування системи, канали передачі даних);
- на суб'єкти системи (процеси, користувачів);
- на канали передачі даних, причому як на пакети даних, що передаються, так і на самі канали передачі даних.

8. За засобами атаки, що використовуються:

- за допомогою штатного програмного забезпечення;
- за допомогою спеціально розробленого програмного забезпечення.

9. За станом об'єкта атаки:

- під час зберігання об'єкта (на диску, в оперативній пам'яті тощо) у пасивному стані;
- під час передачі;
- під час обробки, тобто об'єктом атаки є сам процес користувача або системи [12].

Найбільш розповсюдженою загрозою для безпеки є несанкціонований доступ (НСД), тобто отримання користувачем доступу до об'єкта, на який він не має дозволу. Для реалізації НСД використовуються два способи:

подолання системи захисту або спостереження за процесами та аналіз інформації.

Незаконне використання привілеїв – теж загроза безпеці, яка досить часто трапляється.

Інша загроза безпеки має назву "маскарад", тобто виконання будь-яких дій одним користувачем від імені іншого користувача, якому ці дії дозволені. Досить небехпечною загрозою є вірусні атаки будь-якого типу.

На етапі розробки (планування) система захисту формується у вигляді єдиної сукупності заходів різного плану для протидії можливим загрозам. Вони включають:

- правові заходи: закони, укази та інші нормативні документи, які регламентують правила роботи з платіжною інформацією, що обробляється, накопичується та зберігається в системі, та відповідальність за порушення цих правил;
- морально-етичні заходи: норми поведінки учасників розрахунків та обслуговуючого персоналу;
- адміністративні заходи: заходи організаційного характеру, які регламентують процес функціонування системи обробки платіжної інформації, використання її ресурсів, діяльність персоналу тощо;
- фізичні заходи захисту, які включають охорону приміщень, техніки та персоналу платіжної системи;
- технічні (апаратно-програмні та програмні) засоби захисту, які самостійно або в комплексі з іншими засобами забезпечують функції захисту: ідентифікацію й автентифікацію користувачів, розподіл доступу, реєстрацію основних подій роботи системи, криптографічні функції та ін.

На етапі реалізації системи захисту виготовляються, обладнуються, встановлюються та настроюються засоби захисту, які були заплановані на попередньому етапі.

Важливо знати, що захист інформації забезпечується суб'єктами переказу коштів шляхом обов'язкового впровадження та використання відповідної системи захисту, що складається з:

– законодавчих актів України та інших нормативно-правових актів, а також внутрішніх нормативних актів суб'єктів переказу, що регулюють порядок доступу та роботи з відповідною інформацією, а також відповідальність за порушення цих правил;

– заходів охорони приміщень, технічного обладнання відповідної платіжної системи та персоналу суб'єкта переказу;

– технологічних та програмно-апаратних засобів криптографічного захисту інформації, що обробляється в платіжній системі.

Система захисту інформації повинна забезпечувати:

1) цілісність інформації, що передається в платіжній системі, та компонентів платіжної системи;

2) конфіденційність інформації під час її обробки, передавання та зберігання в платіжній системі;

3) неможливість відмови ініціатора від факту передавання та отримувачем від факту прийняття документа на переказ, документа за операціями із застосуванням засобів ідентифікації, документа на відкликання.

4) забезпечення постійного та безперешкодного доступу до компонентів платіжної системи особам, які мають на це право або повноваження, визначені законодавством України, а також встановлені договором.

Необхідно акцентувати увагу на тому, що розробка заходів охорони, технологічних та програмсно-апаратних засобів криптографічного захисту здійснюється платіжною організацією відповідної платіжної системи, її членами або іншою установою на їх замовлення [12].

1.3 Системи електронних платежів в Інтернет

XXI вік ознаменувався розвитком електронної комерції. Обороти в цій сфері щорічно ростуть, росте і кількість фінансових організацій, що надають підтримку проведенню транзакцій в Інтернет. Зокрема, дуже популярні в світі системи електронних платежів. Фактично вони стали стандартом де-факто оплати в електронних магазинах, біржах, аукціонах, тоталізаторах і т.п. В Україні в основному поширені зарубіжні системи, такі, як російська дебетова система WebMoney, американська система PayPal і інші. Серед вітчизняних до недавнього часу успішно використовувалися споживачами лише банківські СЕП (Приват-24, Дельта Он-лайн і інші). Проте в останні три роки дуже активно стала розвиватись міжбанківська система доставки і оплати рахунків Portmone.com [14].

Причини активного розвитку: співпраця з банками, розробка програм для підключення нових партнерів, проведення ефективних рекламних акцій. В даний час клієнти Portmone.com можуть оплачувати рахунки 488 компаній. Друга причина – закономірний розвиток Уанет і експоненціальне зростання числа українців, що мають постійний доступ в Інтернет, відповідно числа клієнтів СЕП. Особливий внесок в це зробили мобільні оператори, надаючи послугу широкосмугового Інтернету.

Portmone.com сертифікована на відповідність вимогам стандарту PCI DSS (Payment Card Industry Data Security Standard), перша в Україні.

Аналогічний Portmone сервіс в Україні – платіжний сервіс ukrpays.com.

Слід також звернути увагу, що емітентом платіжних карток в Україні можуть бути тільки ті кредитні організації, які мають відповідний дозвіл НБУ. Особливе місце серед емітентів платіжних карток посідають банки, об'єднані в так звані платіжні асоціації. До міжнародних платіжних систем на основі пластикових карток прийнято відносити такі системи, що представлені на українському ринку:

- Europay/MasterCard;
- VISA;

- Dinners Club;

- American Express.

Крім міжнародних платіжних систем в Україні впроваджується й національна платіжна система. Істотних технологічних розходжень між українськими і міжнародними платіжними системами немає, однак масштаби діяльності міжнародних компаній суттєво відрізняються від українських.

В Україні нині функціонує Національна системи масових електронних платежів, яка є внутрішньодержавною банківською багатоемітентною платіжною системою масових електронних платежів. Вона використовує інформаційні технології, що забезпечують формування, обробку, передавання та зберігання документів, зокрема персональні дані, за операціями із застосуванням платіжних карток і формування відповідних документів на переказування коштів в електронній формі.

До складу НСМЕП входять:

- платіжна організація, тобто юридична особа, яка є власником або одержала право на використання знака для товарів і послуг НСМЕП;
- члени НСМЕП, якими є емітенти та еквайри;
- учасники НСМЕП.
- учасниками НСМЕП є:

а) розрахунковий банк, яким може бути уповноважений Платіжною організацією банк-резидент або НБУ;

б) Головний процесинговий центр (ГПЦ) - юридична особа, що здійснює процесинг та виконує функції клірингової установи НСМЕП;

в) регіональний процесинговий центр (УПЦ) - юридична особа, що здійснює процесинг та виконує кліринг для окремої групи членів НСМЕП;

г) процесинговий центр банківського рівня (БПЦ) - юридична особа, що здійснює процесінг та виконує інформаційне обслуговування емітента та/або еквайра;

д) технічний екваєр – юридична особа, яка здійснює технічний еквайринг, тобто діяльність щодо технологічного, інформаційного обслуговування торговців та/або еквайрів за операціями, здійсненими із застосуванням карток;

є) торговці – торгова чи сервісна компанія, що приєдналася до платіжної системи з метою надати можливість своїм клієнтам здійснювати оплату платіжною карткою;

ж) держателі платіжних карток.

НСМЕП розрахована на роботу в режимі офлайн, тобто без реального зв'язку з емітентом та еквайром (під час здійснення таких операцій використовується залишок коштів відповідного платіжного додатка платіжної картки, а авторизація операції проводиться терміналом, на якому виконується ця операція з використанням модуля безпеки термінала) [15].

1.4 Безготівкові операції з платіжними картками

У межах України еквайринг здійснюється виключно юридичними особами-резидентами, що уклали договір із платіжною організацією відповідної платіжної системи. Договір між еквайром і торговцем дає можливість торговцеві приймати до оплати платіжні картки відповідної платіжної системи з дотриманням її правил і виконувати інші операції, які передбачені договором.

Для забезпечення приймання платіжних карток з метою безготівкової оплати товарів (послуг) та видавання готівки торговці можуть за погодженням з еквайром самостійно придбати платіжні термінали, імпринтери та інше обладнання, яке потрібне для обслуговування платіжних карток. Порядок використання цього обладнання визначається правилами відповідної платіжної системи та договорами, які укладені торговцями з еквайрами.

Послідовність здійснення операцій купівлі товару з використанням платіжних карток на підприємстві торгівлі можна розглянути на схемі, відображеній на рис.1.3

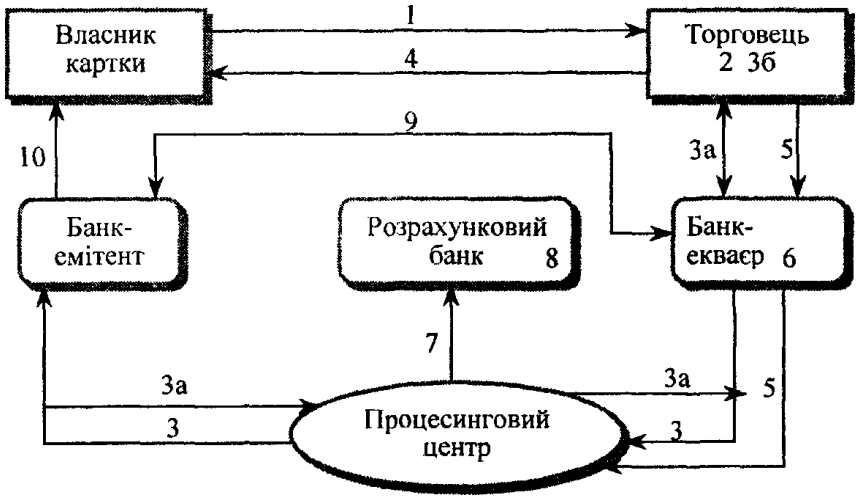

Рисунок 1.3 – Схема проходження грошових коштів із рахунку власника платіжної картки до підприємства торгівлі

Бажаючи здійснити купівлю або отримати послугу, власник картки надає її торговцеві (1). Торговець (2) перевіряє картку візуально, а потім проводить авторизацію – голосову по телефону або електронну через POS-термінал (3а). Отримавши дозвіл, торговець оформляє чек (3б), переносячи на нього дані з картки. Власник картки підписує всі примірники чека (при авторизації через POS-термінал підпис не потрібен, оскільки його роль виконує ПІН-код). Примірник чека і товар передаються покупцеві (4). Наприкінці кожного робочого дня торговець надає в банк-еквайєр примірники чеків, котрі слугують документальним підтвердженням транзакції. Дані за транзакціями передаються у процесинговий центр (5). Банк-еквайєр перевіряє документи і кредитує рахунок торговця на відповідну суму (6). Процесинговий центр обробляє інформацію і передає її у розрахунковий банк, в якому банки-учасники відкрили кореспондентські рахунки (7). Розрахунковий банк проводить взаємозалік між банками-учасниками (5). Банки, які не мають кореспондентських рахунків у

розрахунковому банку, здійснюють розрахунки самостійно. Банк-емітент щомісяця сповіщає власника картки про стан його карткового рахунка (10). Банки-емітенти знімають комісійну платню з рахунків власників карток за послуги при здійсненні операцій.

1.5 Еволюція та види банківських платіжних карток і їх призначення

Пластикова карта може використовуватися для платежів, у тому числі через Інтернет.

Утримувача карти часто називають «власником» (таке використання зустрічається навіть в документах банків), насправді власником карти є банк-емітент (це положення закріплюється відповідними пунктами договору на обслуговування банківських карт) [16].

Система безготівкового розрахунку створена в США за часів «торгового буму» (1940-1950-і роки). Вона замінила чекові книжки. В процесі свого розвитку відбувалася технічна модернізація карт. Спершу це був просто шматочок картону, потім він став працювати за принципом перфокарти, на початку 1970-х була розроблена магнітна смуга, а в кінці 1990-х в кредитні карти сталі інтегруватися чипи [17].

Всі види карток спочатку свого існування дозволяли одержувати практично необмежені кредити від банків. Зазвичай це було зв'язано з тим, що, карта Diners Club автоматично позначала дуже багату людину. Цим стали користуватися шахраї, які брали в кредит гроші, а потім ховалися з ними.

Види карт (за технологією виробництва):

- з магнітною смугою;
- мікропроцесорні карти (смарт-карти);
- безконтактні мікропроцесорні карти;
- карти оптичної пам'яті (лазерні карти);
- карти з вбудованим тачскрином (інновація Visa 2012 року).

Банківська карта може випускатися банком як локальна (що належить локальній платіжній системі, як правило в межах однієї держави, наприклад, в Україні НМСЕП, або Visa / Mastercard, але призначені тільки для місцевих платежів) і міжнародна (в рамках платіжної системи, об'єднуючої безліч банків-учасників по всьому світу).

Найпопулярніші платіжні системи – Visa (Visa Electron, Visa Classic, Visa Gold, Visa Platinum) і MasterCard (Cirrus, Maestro, MasterCard Mass, MasterCard Gold, MasterCard Platinum).

Найпопулярніші в світі – карти Visa Classic і Mastercard Standart. Вони є як дебетові, так і кредитові, а також дозволяють розраховуватися через Інтернет [18].

Розрахункові (дебетові) карти.

Розрахункова карта призначена для здійснення операцій її утримувачем в межах залишку грошових коштів клієнта, що знаходяться на його банківському рахунку з урахуванням встановлених лімітів.

Відсутність необхідності ретельної перевірки особи і вивчення кредитної історії власника карти спрощує процес оформлення і знижує вартість їх обслуговування. На залишок коштів на рахунку іноді нараховуються відсотки, як на звичайному банківському внеску.

Кредитні карти.

Кредитна карта призначена для здійснення її утримувачем операцій, розрахунки по яких здійснюються за рахунок грошових коштів, наданих кредитною організацією-емітентом клієнту в межах встановленого ліміту відповідно до умов кредитного договору. Банк встановлює ліміт виходячи з платоспроможності клієнта. На залишок коштів на рахунку також нараховуються відсотки, але вони, як правило, на порядок нижче комісії при овердрафті.

Передплачені карти.

Передплачена карта призначена для здійснення її утримувачем операцій, розрахунки по яких здійснюються кредитною організацією-

емітентом від свого імені, і засвідчує право вимоги утримувача передплаченої карти до кредитної організації-емітенту по оплаті товарів (робіт, послуг, результатів інтелектуальної діяльності) або видачі наявних грошових коштів.

Prepaid card – заздалегідь оплачувана картка:

- термін відноситься до цілого ряду класу дебетових карток (з магнітною смугою, мікросхемою пам'яті, з мікропроцесором), що використовуються для розрахунків за товари або послуги в межах заздалегідь сплаченої суми;
- загальними ознаками заздалегідь оплачуваних карток є: завантажена на картки «цінність», негайне дебетування «цінності» на картці у момент оплати товарів або послуг;
- невелика величина «цінності»;
- підрозділяються на два великі типи залежно від характеру завантаженої на них «цінності»: картки-електронні гаманці, електронні гроші і картки, в яких завантажуються «одиниці» послуги (наприклад, число поїздок на суспільному транспорті, число хвилин в телефонних картках, число «балів» в картках лояльності і т. п.);
- емітентами заздалегідь оплачуваних карток можуть бути як банки і кредитно-фінансові установи (це відноситься, головним чином до карток-електронних гаманців) так і небанківські організації (торгові, телекомунікаційні, транспортні компанії);
- заздалегідь сплачені картки можуть не бути ідентифікаційними (наприклад, телефонні картки, картки для оплати проїзду в суспільному транспорті).

Подарункова картка – передплачена карта, що дає її власнику право на отримання товарів або послуг на суму вказану на карті, зазвичай використовується як подарунок замість грошового подарунка. Але треба розуміти, що з юридичної точки зору ця карта належить утримувачу, що оформляє карту і та особа, якій передана карта, буде просто користуватися чужим рахунком без юридичних на те підстав. Оскільки власник рахунку не

виписував йому довіреності, не оформляв додаткову карту і ніяк юридично не закріпив повноваження на використання свого рахунку, а просто передав карту. Так що це карти не передплачені, а звичайні дебетові карти без вказівки прізвища і імені на карті.

Віртуальні карти.

Багато банків випускають віртуальні карти. Вони є дебетовими і зовні схожі на звичайні, але не мають чипа або магнітної смуги, і розплачуватися з їх допомогою можна виключно через Інтернет. Фактично, така карта є просто шматком пластика з номером, ім'ям власника і іншими даними. Власники таких карт не можуть отримати з них наявні грошові кошти, за винятком випадку закриття карти в банку. В цьому випадку власнику повертається залишок коштів на рахунку за вирахуванням комісій по закриттю, якщо такі передбачені договором.

Складність застосування.

Хоча банки-емітенти прагнуть спростити інтерфейс банкоматів, для багатьох людей, особливо немолодих, виникають помітні складнощі в отриманні готівки, а іноді навіть і при розрахунках.

Безпека.

При розрахунках через Інтернет і отриманні готівки через банкомати і оплати товарів існує ненульова вірогідність стати жертвою шахрайства з використанням технічних засобів. Частковим виходом з цієї ситуації є використання мікропроцесорних карт.

1.6 Аналіз способів шахрайства з платіжними картками

Поява електронної комерції викликала серйозні проблеми безпеки, а отже оператори платежів, виробники електронних карт, а також власники карток продовжують шукати ефективні засоби боротьби з загрозою шахрайства в Інтернеті. Злочинність з кредитною карткою відбувається кількома способами:

– Скіммінг – несанкціонована установка пристроїв на банкомат з метою отримання даних з магнітної смуги платіжної картки (встановлюється зчитувач на картрідер) та ПІН-коду до неї (за допомогою відеокамери або накладної клавіатури). Щоб уберегтися від шахраїв, надавайте перевагу банкоматам, які знаходяться на території, що охороняється. Також звертайте увагу на зовнішній вигляд картридера і клавіатури, спробуйте підколупнути їх пальцем, як правило, пристрої шахраїв легко зсуваються з місця. Для зняття готівки краще використовувати картку з чіпом, дані з чіпа набагато складніше підробити, і шахраї не витрачають на це час [19].

– Cash trapping (захоплення грошей) – відносно новий вид шахрайства, який швидко поширюється. Його суть полягає в наступному: шахрай встановлює спеціальну планку на щілину для видачі грошей, тим самим перешкоджаючи їх видачі. Внутрішня сторона даної планки змазана клеєм або ж на неї нанесений двосторонній скотч для приклеювання виданих купюр. Зовнішня сторона планки імітує колір і метал банкомату, щоб держатель картки нічого не запідозрив. Власник картки, здійснюючи операцію зі зняття готівки з банкомату, не отримує її, думаючи, що це технічний збій, і відходить від банкомату. Далі до банкомата підходить шахрай, знімає планку і, діставши гроші, приклеєні до неї, знову встановлює на місце [20].

– Підроблення карток (найбільш поширений вид шахрайства при оплаті в магазинах – банальне переписування реквізитів картки (номер картки, термін дії, CVV-2- card verification value 2) для подальшого проведення шахрайських операцій в мережі Інтернет).

– Шахрайство з викраденими або загубленими картками. Для запобігання випадків шахрайського використання вкрадених або загублених платіжних карток, слід зберігати окремо від картки ПІН-код (пароль), а також негайно інформувати банк про випадок втрати / крадіжки картки для подальшого її блокування. Ефективним методом контролю коштів на картці є підключення

послуги СМС-інформування по кожній операції і послуги 3D Secure для безпечних інтернет-платежів.

– Напад хакерів на магазин для доступа до бази даних клієнтів.

– Клієнти добровільно подають інформацію про картку (невідомі особи створили фальшиві онлайнові магазини, які використовують спроектований процес імітації. Іншим способом є відправлення шахрайського електронного листа з проханням особистістю оновити реєстраційну інформацію та дані кредитної картки для використання веб-служби);

– Більшість користувачів Internet користуються зручною автоматичною функцією – запам'ятовування даних, включаючи інформацію про кредитну картку, яка використовується для заповнення веб-форм і зберігає її. У наступний раз, коли потрібно заповнити подібну форму, вона підставляє всі дані автоматично. Якщо хтось отримує віддалений або фізичний доступ до комп'ютера, інформація про кредитну картку власника може бути викрадена.

– Соціальна інженерія. На сьогоднішній день шахраї дуже активно використовують такий простий спосіб отримання даних по картці, як прямий дзвінок клієнту. Даний метод особливо популярний при купівлі або продажу лотів на онлайн-аукціонах. Шахраї, представляючись співробітниками банку, правоохоронних органів, органів опіки, НБУ або навіть СБУ, входять до держателя картки в довіру або використовують психологічний тиск, і в результаті випитують реквізити картки і персональні дані. Причини того можуть бути абсолютно різними, наприклад, можуть сказати, що створюється єдиний реєстр всіх банківських карт, що є підозра, що операції по картці пов'язані з шахрайством, або картка потрапила в список карток на анулювання. Шахраї також можуть змусити людину провести операцію з переказу коштів зі своєї картки на їхній рахунок, розповідаючи, що це необхідно для верифікації її картки і зняття всіх підозр [21,22].

Під час придбання товару дані про оплату передаються між комп'ютером клієнтів та магазином постачальника через Інтернет. Це викликає занепокоєння щодо інтернет-безпеки кредитних карток та крадіжки

особистих даних. Оплату слід проводити тільки на тих веб-сайтах, які також захищені від зовнішніх загроз. Сторінка для оплати повинна мати захищене з'єднання, тобто адреса повинна починатися з https. Ніколи не потрібно розраховуватися карткою на підозрілих сайтах і не вводити дані карти, якщо сайт обіцяє грошовий приз. Це ще один виверт шахраїв. Найкраще завести для інтернет платежів окрему картку і встановити на неї мінімальний ліміт на проведення операцій.

Суттєво зросла кількість незаконних дій/сумнівних операцій, що проводилися через Інтернет. Такий тренд фахівці Нацбанку пояснюють зміною фокусу уваги шахраїв з технологічних методів шахрайства на людський фактор, що потребує від усіх учасників платіжного ринку реалізації заходів з підвищення фінансової грамотності держателів платіжних карток. При цьому оплата в торговельній мережі стає одним з найбільш безпечних способів використання платіжних карток (порівняно зі збитками, понесеними держателями та банками через банкомати та Інтернет).

Традиційно найбільша кількість шахрайських випадків припадає на великі міста України (з населенням понад один мільйон осіб) та найбільші області – до 97%.

НБУ нагадує, що користувачі платіжних карток мають бути обачними та не розголошувати особисту інформацію та реквізити платіжних карток (термін її дії, код CVC2/CVV2, ПІН-код до картки), а також логін/пароль для входу до веб-банкінгу, одноразові паролі для проведення додаткової автентифікації платежів або входу до веб-банкінгу (представники банків ніколи не запитують цю інформацію).

Задля упередження шахрайських дій Нацбанк також рекомендує користуватись послугами sms-інформування та застосовувати ліміти на проведення операцій з використанням платіжних карток.

Тим часом міжбанківська Асоціація членів платіжних систем ЕМА констатує, що кіберзлочинці подвоїли суму крадіжок із банківських рахунків

українців. Протягом 2017 року кіберзлочинці викрали з банківських рахунків українців загалом 670 млн грн.

1.7 Аналіз методів та засобів оцінювання ризиків безпеки інформації в системах електронної комерції

Під інформаційною безпекою системи електронної комерції (СЕК) розуміють захищеність інформації та інфраструктури, яка її підтримує, від випадкових або навмисних впливів природного чи штучного характеру, здатних нанести збитки власникам або користувачам інформації. Будь-яке порушення безпеки інформації в електронній комерції може бути розглянуте в термінах загроз, уразливості та атак [23].

Серед основних вимог до проведення комерційних операцій – конфіденційність, цілісність, аутентифікація, авторизація, гарантії та збереження таємниці [24-27]. Перші чотири вимоги забезпечуються технічними та програмними засобами, але виконання останніх двох – досягнення гарантій і збереження таємниці – однаково залежить як від програмно-технічних засобів та відповідальності окремих осіб і організацій, так і від дотримання законів, що захищають споживача від можливого шахрайства. У світі багато уваги приділяється фізичній безпеці, а у світі електронної комерції треба піклуватися про засоби захисту даних, комунікацій і транзакцій. Маючи справу з мережевими системами Internet та Intranet, необхідно пам’ятати про існування декількох можливих загроз:

- дані навмисно перехоплюються, читаються чи змінюються;
- користувачі навмисно ідентифікують себе неправильно;
- користувач одержує несанкціонований доступ з однієї мережі до іншої.

Вказані загрози реалізуються через такі вразливості:

1. Уразливості сервісів TCP/IP – ряд сервісів TCP/IP є небезпечними і можуть бути скомпрометовані зловмисниками. Особливо вразливі сервіси,

що використовуються в локальних обчислювальних мережах для поліпшення управління мережею;

2. Легкість спостереження за каналами та перехоплення інформації – більшість трафіку Інтернет не зашифровано. Електронна пошта, паролі та файли, що передаються, можуть бути перехоплені при використанні легкодоступних програм. Потім зловмисники можуть використати паролі для проникнення в системи електронної комерції;

3. Відсутність політики – багато мереж можуть бути сконфігуровані через незнання так, що даватимуть можливість доступу до них з Інтернету, не враховуючи можливих зловживань. Значна кількість мереж допускає використання більшої кількості сервісів TCP/IP, ніж це потрібно для діяльності їх організації. Адміністратори таких мереж не намагаються обмежити доступ до інформації з комп'ютерів. Це може допомогти зловмисникам проникнути до мережі;

4. Складність конфігурування – ресурси управління доступом до мереж у хостах часто є складними в налаштуванні та контролі за ними. Неправильно сконфігуровані засоби часто призводять до неавторизованого доступу;

5. Помилки при конфігуруванні хоста або ресурсів управління доступом, які або погано встановлені, або настільки складні, що важко адмініструються;

6. Роль та важливість адміністрування системи, які часто не враховуються під час опису посадових обов'язків співробітників (більшість адміністраторів наймаються на неповний робочий день та є низькокваліфікованими);

7. Слабка аутентифікація;

8. Можливість легкого спостереження за даними, що передаються;

9. Можливість легкого маскування під інших;

10. Недоліки служб локально обчислювальних мереж та взаємної довіри хостів один до одного;

11. Складність конфігурування і заходів захисту;

12. Слабкий захист на рівні хостів.

У забезпеченні інформаційної безпеки в електронній комерції зацікавленими є три різні категорії суб'єктів: державні організації, комерційні структури та окремі громадяни.

1.8 Основні складові забезпечення безпеки систем електронної комерції

Електронна пошта є дешевим засобом взаємодії з клієнтами, діловими партнерами і з її використанням пов'язаний ряд проблем з безпекою:

- адреси електронної пошти в Інтернет легко підробити;
- електронні листи можуть бути просто модифіковані. Стандартний SMTP-лист не містить ресурсів перевірки їх цілісності;
- електронну пошту можуть прочитати на кожній проміжній робочій станції;
- немає гарантій доставки електронного листа. Хоч деякі поштові системи надають можливість отримати повідомлення про доставку, часто такі повідомлення означають лише те, що поштовий сервер одержувача (а не обов'язково сам користувач) отримав повідомлення.

Електронний обмін даними (EDI). Найпростіша форма – це обмін інформацією між двома бізнес-суб'єктами (торговими партнерами) у стандартизованому форматі. Базовою одиницею обміну є набір транзакцій, який загалом відповідає стандартному бізнес-документу, такому як платіжне доручення або накладна на товар. За допомогою стандартів, основу яких становлять X.9 і UN/EDIFACT, ділове співтовариство розробило групу стандартних наборів транзакцій [28].

Кожний набір транзакцій складається з великої кількості елементів даних, необхідних для даного бізнес-документа, кожний з яких має свій формат і місце серед інших елементів даних. Компанії почали використовувати EDI, щоб зменшити час і витрати на контакти з постачальниками. Так, в автомобільній промисловості великі компанії

вимагали від постачальників використати EDI для всіх транзакцій, що дозволило зберегти безліч паперу, значно прискорило процес постачання і зменшило зусилля на підтримку актуальності баз даних. Зазвичай для виконання EDI-транзакцій використовувалися приватні глобальні мережі, які були дешевшими, ніж виділені лінії, однак надавали сервіс надійної і безпечної доставки.

Internet забезпечує можливості взаємодії, необхідні для EDI, за низькими цінами. Але він не забезпечує сервісів безпеки (цілісності, конфіденційності, контролю учасників взаємодії), необхідних для EDI. Транзакції EDI вразливі до модифікації, компрометації або знищення при пересиланні через Internet.

Інформаційні транзакції – основний і дорогий елемент комерції. Інформація в комерції може мати декілька форм [28]:

- статичні дані, такі як історична інформація, карти і т.д.;
- корпоративна інформація, така як телефонні номери, адреси, структура організації тощо;
- інформація про продукцію або послуги;
- платна інформація, така як новини, періодичні видання, доступ до баз даних і т.д.

Використання Internet для надання таких сервісів значно дешевше, ніж використання факсу, телефону або звичайної пошти. Потенційні клієнти можуть шукати й одержувати інформацію в потрібному їм темпі, і це не вимагатиме додаткових витрат на службу технічного супроводу [28].

Зазвичай такі інформаційні сервіси використовують WWW як базовий механізм для надання інформації. Цілісність і доступність інформації, що надається, – головні проблеми забезпечення безпеки, що вимагають застосування засобів безпеки і створення політики безпеки [29].

Фінансові транзакції. Комп’ютери і мережі давно використовуються для обробки фінансових транзакцій. Переказ грошей з рахунку на рахунок в електронному вигляді використовується для транзакцій банк – банк, а

банкомати – для операцій клієнт – банк. Авторизація покупця за допомогою кредитних карток виконується по телефонних лініях і мережах передавання даних [26, 27]. Для підтримки безпеки ці транзакції виконуються через приватні мережі або шифруються. Використання приватних глобальних мереж (як і для EDI) обмежувало можливості взаємодії [28]. І тільки Internet надав дешеву можливість здійснювати фінансові транзакції.

Застосування Internet для виконання всіх типів транзакцій дає змогу замінити використання готівки, чеків, кредитних карток їх електронними еквівалентами. Основними визначеннями, що стосуються всіх класів безпеки електронної комерції, є експозиція, вразливість, атака, загроза, управління.

Експозицією називається форма можливої втрати або збитку для СЕК. Наприклад, експозиціями вважається неавторизований доступ до даних або протидія авторизованому використанню СЕК.

Уразливість – це деяка слабкість системи безпеки, яка може стати причиною нанесення пошкоджень СЕК.

Атакою називається дія деякого суб'єкта СЕК (користувача, програми, процесу і т.д.), що використовує вразливість комп'ютерної системи електронної комерції для досягнення цілей, які виходять за межі авторизації даного суб'єкта в комп'ютерній системі. Тобто, якщо, наприклад, користувач не має права на читання деяких даних, що зберігаються в системі електронної комерції, а йому цікаво їх знати і тому він виконує ряд відомих йому нестандартних маніпуляцій, що забезпечують доступ до цих даних (у разі відсутності або недостатньо надійної роботи засобів безпеки) або завершилися невдачею (у разі надійної роботи засобів безпеки), то цей користувач здійснює щодо СЕК атаку.

Загрозою для СЕК є умови, що створюють потенційну можливість нанесення СЕК збитку.

Управлінням у термінології безпеки називається захисний механізм (дія, пристрій, процедура, технологія тощо), що зменшує вразливість СЕК. Збиток СЕК – поняття також досить широке. Збитком уважається не тільки

явне пошкодження будь-якого з компонентів СЕК, але і приведення СЕК в непрацездатний стан (наприклад, знеструмлення приміщення, в якому знаходяться апаратні засоби), різні витоки інформації (наприклад, незаконне копіювання програм, одержання конфіденційних даних), зміна деяких фізичних та логічних характеристик системи (наприклад, неавторизоване додавання записів до системних файлів і т.д.) Визначення можливого збитку СЕК – справа надто складна і залежить від багатьох умов. Наприклад, від того, чи визнається юридично в даній країні так звана інтелектуальна власність або загальновідомий Copyright, чи розглядаються судами позови з відшкодування морального збитку, понесеного деякою особою або організацією внаслідок розголошування третьою стороною конфіденційної інформації і т.д.

Проблеми безпеки систем, що стосуються електронної комерції, можна умовно поділити на такі групи:

- Проблеми забезпечення фізичної СЕК. До них належить захист систем від пожежі, затоплення, інших стихійних лих, збоїв живлення, крадіжки, пошкодження і т.д.
- Проблеми забезпечення логічної безпеки СЕК. До них належить захист систем від неавторизованого доступу, від навмисних і ненавмисних помилок у діях людей і програм, які можуть призвести до збитку тощо.
- Проблеми забезпечення соціальної безпеки компонентів СЕК. До них належать: розроблення законодавства, яке регулює застосування СЕК і визначає порядок розслідування та покарання за порушення їх безпеки; принципи і правила такої організації обслуговування користувачів у СЕК, яка зменшувала б ризик порушення безпеки систем і т.д.
- Проблеми забезпечення етичної безпеки СЕК. У забезпечення безпеки СЕК чималу роль відіграють питання формування в користувачів певної дисципліни, а також формування конкретних етичних норм, обов’язкових для виконання всіма, хто працює з комп’ютерами. Наприклад, нещодавно експерти Національного наукового фонду США зробили спробу створити

своєрідний “кодекс поведінки” фахівця у сфері ІС, зокрема систем електронної комерції. Вказувалося, що неетичними потрібно вважати будь-які навмисні або ненавмисні дії, які:

1) порушують нормальну роботу комп’ютерних систем;

2) викликають додаткові витрати ресурсів (машинного часу, лінії передачі тощо);

3) руйнують цілісність інформації, що зберігається й обробляється в комп’ютерних системах;

4) порушують інтереси легальних користувачів;

5) викликають незаплановані витрати ресурсів на ведення додаткового контролю, відновлення працездатності систем, видалення наслідків порушення безпеки систем та ін.

Як випливає з визначення ІС, зокрема систем електронної комерції, основними її компонентами є апаратні засоби, математичне (зокрема програмне) забезпечення і дані (інформація).

Теоретично існує лише чотири типи загроз для цих компонент [30]:

- переривання – при перериванні компонент системи втрачається (наприклад, через викрадення), стає недоступним (наприклад, через блокування – фізичного або логічного) або втрачає працездатність;
- перехоплення – деяка третя неавторизована сторона отримує доступ до компонента. Прикладами перехоплення є незаконне копіювання програм і даних, неавторизоване читання даних з ліній зв’язку комп’ютерної мережі тощо;
- модифікація – деяка третя неавторизована сторона не тільки отримує доступ до компонента, але і маніпулює ним. Наприклад, модифікаціями є неавторизована зміна даних у базах даних або взагалі у файлах комп’ютерної системи; зміна алгоритмів програм, що використовуються з метою виконання деякої додаткової незаконної обробки. Іноді модифікації виявляються досить швидко (якщо не відразу), але більш тонкі з них можуть залишатися невиявленими тривалий час;

– підроблення – порушник може додати деякий фальшивий процес до системи для виконання потрібних йому, але не врахованих системою дій або підроблені записи у файли системи чи інших користувачів. Наприклад, знаючи формат запису в файлі, на основі якого у вашій організації нараховується зарплата, можна занести в цей файл підробний запис.

На етапі проектування або вибору систем електронної комерції необхідно сформулювати вимоги до забезпечення режиму інформаційної безпеки при реалізації функцій і задач систем електронної комерції, а також розробити концепцію політики ІБ. При цьому після складання списку функцій і задач систем електронної комерції треба визначити вимоги до забезпечення режиму ІБ при їх реалізації. Ці вимоги формуються в термінах:

– доступність;

– цілісність;

– конфіденційність.

Розробка концепції політики ІБ починається після вибору варіанта концепції систем електронної комерції, що створюється/вибирається і проводиться на основі аналізу таких груп чинників:

– правові і договірні вимоги;

– вимоги до забезпечення режиму ІБ за функціями і задачами системи електронної комерції;

– загрози (класи ризиків), яких зазнають інформаційні ресурси.

Унаслідок аналізу формулюються загальні положення ІБ, що стосуються систем електронної комерції загалом:

– цілі і пріоритети, які переслідує організація у сфері ІБ;

– загальні напрями в досягненні цих цілей;

– аспекти програми ІБ, які повинні вирішуватися на рівні всієї організації;

– посадові особи та їх обов’язки щодо реалізації програми ІБ.

Потім розробляється політика ІБ, яка передбачає такі етапи:

– аналіз ризиків;

- визначення вимог до засобів захисту;
- вибір основних рішень щодо забезпечення режиму ІБ;
- розроблення планів забезпечення безперебійної роботи організації;
- документальне оформлення політики ІБ.

Аналіз ризиків передбачає вивчення та систематизацію загроз ІБ, визначення вимог до засобів забезпечення ІБ [29] і здійснюється такими етапами:

- вибір елементів системи електронної комерції та інформаційних ресурсів, для яких проводитиметься аналіз;
- розроблення методології оцінки ризику;
- аналіз загроз, визначення слабких місць у захисті;
- аналіз і оцінка ризиків [26, 31].

Розроблення методології оцінки ризику. На цьому етапі повинні бути отримані оцінки граничнодопустимого та існуючого ризику здійснення загрози протягом певного часу. В ідеалі для кожної із загроз одержується значення ймовірності її здійснення протягом певного часу. Це допомагає співвіднести оцінку можливого збитку з витратами на захист. На практиці для більшості загроз неможливо отримати достовірні дані про ймовірність реалізації загрози і доводиться обмежуватись якісними оцінками. У розроблення методології оцінки ризику можуть бути використані методи системного аналізу.

Аналіз загроз, визначення слабких місць в системі захисту. Формується детальний список загроз, складається матриця загроз/елементів систем електронної комерції або інформаційних ресурсів. Кожному елементу матриці відповідає опис можливого впливу загрози на відповідний елемент системи або інформаційний ресурс. У процесі складання матриці уточнюється список загроз і виділених елементів.

Аналіз і оцінка ризиків. Цей етап передбачає такі кроки:

- оцінку збитку, пов’язану з реалізацією загроз. Оцінюється збиток, який може нанести діяльності організації реалізація загроз безпеки з урахуванням

можливих наслідків порушення конфіденційності, цілісності і доступності інформації;

– оцінку витрат на заходи, пов’язані із захистом і залишкового ризику. Попередньо оцінюються прямі витрати за кожним заходом без урахування витрат на заходи, що мають комплексний характер;

– аналіз співвідношення – вартість/ефективність. Витрати на систему захисту інформації необхідно співвіднести з цінністю інформації, що захищається, й інших інформаційних ресурсів, що зазнають ризику, а також із збитком, який може бути нанесений організації через реалізацію загроз.

За результатами аналізу уточнюються допустимі залишкові ризики і витрати щодо заходів, пов’язаних із захистом інформації, і потім робляться висновки про допустимі рівні залишкового ризику і доцільність застосування конкретних варіантів захисту. За результатами проведеної роботи складається документ, що містить:

– переліки загроз ІБ,

– оцінки ризиків і рекомендації щодо зниження ймовірності їх виникнення і захисні заходи, необхідні для нейтралізування загроз.

1.9 Висновки до першого розділу. Постановка задачі

У першому розділі досліджено теоретичні матеріали у сфері платіжної системи України.

Проведено аналіз системи електронних платежів, способів шахрайства з платіжними картками, методів та засобів оцінювання ризиків безпеки інформації в системах електронної комерції.

Проведено аналіз основних складових безпеки систем електронної комерції.

Для підвіщення рівня безпеки даних платіжних карток необхідно особливу увагу приділити забезпеченню інформаційній безпеці організацій, що обробляють, зберігають чи передають карткові дані.

У дипломній роботі поставлені такі задачі:

- проаналізувати підходи для процедури обробки платіжних карток;
- проаналізувати методи боротьби з шахрайськими операціями;
- проаналізувати вимоги міжнародного стандарту у сфері інформаційної безпеки даних індустрії платіжних карток PCI DSS;
- на основі вимог стандарту PCI DSS розробити рекомендації щодо забезпечення безпеки даних тримачів карток для організацій, в інформаційній інфраструктурі яких зберігаються, обробляються або передаються дані платіжних карт;
- обґрунтувати доцільність створених рекомендацій, їх практичну та економічну ефективності.

2 РОЗДІЛ
БЕЗПЕКА ДАНИХ ПЛАТІЖНИХ КАРТОК

Тенденція зростання збитків із використанням платіжних карток стала однією з головних причин для того, щоб міжнародні платіжні системи об'єднали свої зусилля і прийняли додаткові заходи для захисту клієнтів. З цією метою в 2004 році був розроблений єдиний набір вимог до безпеки даних - Payment Card Industry Data Security Standard, що об'єднав в собі вимоги ряду програм з безпеки таких платіжних систем як Visa, MasterCard, American Express, Discover Card і JCB. Згодом, у вересні 2006 року, для розвитку і просування стандарту PCI DSS, була створена спеціальна Рада з безпеки - PCI Security Standards Council. Основними функції Ради з безпеки є розробка та публікація стандартів PCI і всієї супутньої документації, визначення вимог до компаній, які планують отримати сертифікацію для проведення аудитів за PCI DSS («QSA») і сканувань («ASV»), здійснення безпосередньо самої сертифікації, проведення навчальних тренінгів для майбутніх QSA-аудиторів, а також здійснюють контроль якості проведених аудиторами робіт. У свою чергу міжнародні платіжні системи приймають звітність за результатами аудитів і оцінюють роботу QSA. Всі організації, які зберігають, обробляють або передають інформацію та уповноважені платіжними системами VISA, MasterCard, American Express, Discover і JCB мають відповідати стандарту безпеки PCI DSS. До них відносяться банки, постачальники платіжних послуг, інтернет-магазини і традиційні торговельні підприємства. Відповідність не є одноразовою вимогою. Торговельні підприємства повинні підтверджувати свій статус відповідності один раз на

рік, але передбачається, що підтримка відповідності буде проводитися щоденно.

2.1 Загальні відомості про стандарт PCI DSS

Стандарт PCI DSS [32] – це стандарт безпеки даних індустрії банківських платіжних карток, розроблений Радою зі стандартів безпеки індустрії платіжних карток (Payment Card Industry Security Standards Council, PCI SSC), заснованою міжнародними платіжними системами Visa, MasterCard, American Express, JCB і Discover. Стандарт складається з переліку вимог як з технічного, так і з організаційного боку, маючи на увазі комплексний підхід з високим ступенем вимогливості до забезпечення безпеки даних платіжних карт (ДПК).

Стандарт визначає вимоги до організацій в інформаційній інфраструктурі яких зберігаються, обробляються або передаються дані платіжних карт, а також до організацій, які можуть впливати на рівень безпеки цих даних. Мета стандарту – забезпечити безпеку використання платіжних карт. З середини 2012 року всі організації, залучені в процес зберігання, обробки і передачі ДПК, повинні відповідати вимогам PCI DSS. На прикладі структурної схеми (рис 2.1) можна визначити необхідність відповідності вимогам стандарту PCI DSS.

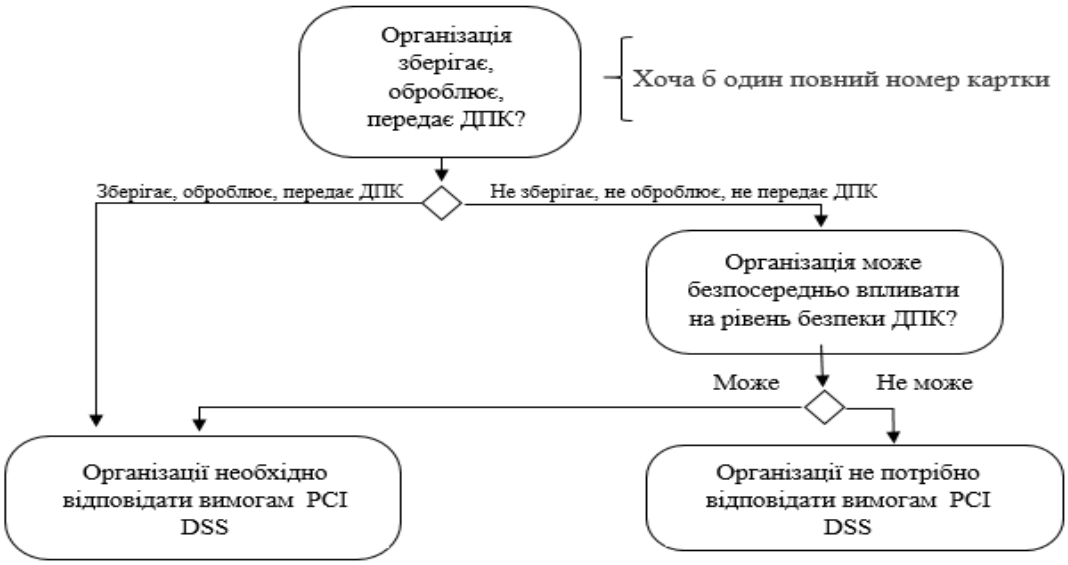

Рисунок 2.1 – Схема визначення необхідності відповідності стандарту PCI DSS

Організація, яка має відповідати стандарту PCI DSS, повинна виконати всі вимоги, представлені у таблиці 2.1 [33].

Таблиця 2.1 - Вимоги стандарту PCI DSS

Ціль	Вимоги
Створення і підтримка безпечної мережі	1. Розробка і забезпечення підтримки конфігурацій міжмережевих екранів для захисту даних тримача карти
	2. Використання системних паролів та інших параметрів безпеки, встановлених виробником забороняється.
Захист даних тримача	3. Забезпечення безпеки даних тримачів карт, що зберігають карти
	4. Шифрування даних тримачів карт при передачі їх через відкриті і загальнодоступні мережі
Підтримка програми управління вразливостями	5. Використання і регулярне оновлювання антивірусного програмного забезпечення
	6. Розробка і підтримка безпечних систем і додатків
Впровадження посилених засобів	7. Обмеження доступу до даних тримачів

управління доступом	карт лише службовою необхідністю
	8. Призначення унікального ідентифікатора кожній особі, що має доступ до комп'ютерної мережі
	9. Обмеження фізичного доступу до даних тримача карти
Регулярний моніторинг і тестування мережевої	10. Відстеження і контролювання будь-якого доступу до мережевих ресурсів і даних тримачів карт
	11. Регулярна перевірка систем і процесів забезпечення безпеки
Підтримка Політики інформаційної безпеки	12. Підтримка Політики, що визначає правила інформаційної безпеки для співробітників і партнерів

2.2 Аналіз способів підтвердження відповідності стандарту PCI DSS

Способи підтвердження відповідності вимогам стандарту PCI DSS, полягають в проведенні зовнішнього аудиту (QSA), внутрішнього аудиту (ISA) або самооцінки (SAQ) організації. Особливості кожного з них наведено в таблиці 2.2.

Таблиця 2.2 - Способи підтвердження відповідності стандарту PCI DSS

Зовнішній аудит QSA (Qualified Security Assessor)	Внутрішній аудит ISA (Internal Security Assessor)	Самооцінка SAQ (Self Assessment Questionnaire)
Виконується зовнішньоїю аудиторською організацією QSA, сертифікованої Радою PCI SSC.	Виконується внутрішнім аудитором, який пройшов навчання і сертифікований за програмою Ради PCI SSC. Може бути проведений тільки в разі, якщо перший раз відповідність була підтверджена QSA-	Виконується самостійно - шляхом заповнення листа самооцінки.

	аудитом.	
В результаті перевірки QSA-аудитори збирають свідчення виконання вимог стандарту і зберігають їх протягом трьох років.	В результаті перевірки ISA-аудитори, як і при зовнішньому аудиті, збирають свідчення виконання вимог стандарту і зберігають їх протягом трьох років.	Збір свідчень виконання вимог стандарту не потрібен.
За результатами проведеного аудиту готується звіт про відповідність - ROC (Report on Compliance).	Самостійно заповнюється лист самооцінки SAQ.	

Вибір типу аудиту залежить від типу організації і кількості транзакцій, що оброблюються в рік. Випадковим вибором не можна керуватися, оскільки існують задокументовані правила, що регулюють, який спосіб підтвердження відповідності стандарту буде використовувати організація. Всі ці вимоги встановлюються міжнародними платіжними системами, найбільш популярними з них в Україні є Visa і MasterCard [35; 36].

2.3 Класифікація організацій за рівнями стандарту PCI DSS

Виділяють два типи організацій: торгово-сервісні підприємства (мерчанти) і постачальники послуг.

Торгово-сервісне підприємство (ТСП) – це організація, яка бере платіжні картки до оплати за товари і послуги (магазини, ресторани, інтернет-магазини, автозаправні станції та інше).

Постачальник послуг – організація, що надає послуги в індустрії платіжних карт, пов'язані з обробкою платіжних транзакцій (дата-центри, хостинг-провайдери, платіжні шлюзи, міжнародні платіжні системи і т. д.).

Мерчанти і постачальники послуг, за класифікацією Visa и MasterCard, в залежності від кількості оброблюваних на рік транзакцій, можуть бути віднесені до чотирьох рівнів, а саме:

Рівень 1 (Level 1) – ТСП, які оброблюють більш ніж 6 млн транзакцій на рік.

Вимоги до сертифікації:

- щорічний аудит, що здійснюється QSA-аудитором на об'єкті організації;
- щоквартальне ASV-сканування (Approved Scanning Vendor – автоматизована перевірка всіх точок підключення інформаційної інфраструктури до мережі Інтернет з метою виявлення вразливостей. Відповідно до вимог стандарту PCI DSS).

Рівень 2 (Level 2) – ТСП, які оброблюють від 1 до 6 млн транзакцій на рік.

Вимоги до сертифікації:

- щорічна самооцінка відповідності із заповненням опитувального листа (SAQ);
- щоквартальне ASV-сканування

Рівень 3 (Level 3) – ТСП, які оброблюють від 20 000 до 1 млн транзакцій на рік із використанням засобів електронної комерції.

Вимоги до сертифікації:

- щорічна самооцінка відповідності із заповненням опитувального листа (SAQ);
- щоквартальне ASV-сканування

Рівень 4 (Level 4) – ТСП, які оброблюють до 20 000 транзакцій на рік з використанням засобів електронної комерції.

Вимоги до сертифікації:

- рекомендована щорічна самооцінка відповідності із заповненням опитувального листа;
- рекомендовано щоквартальне ASV-сканування

– вимоги визначаються банком-еквайром.

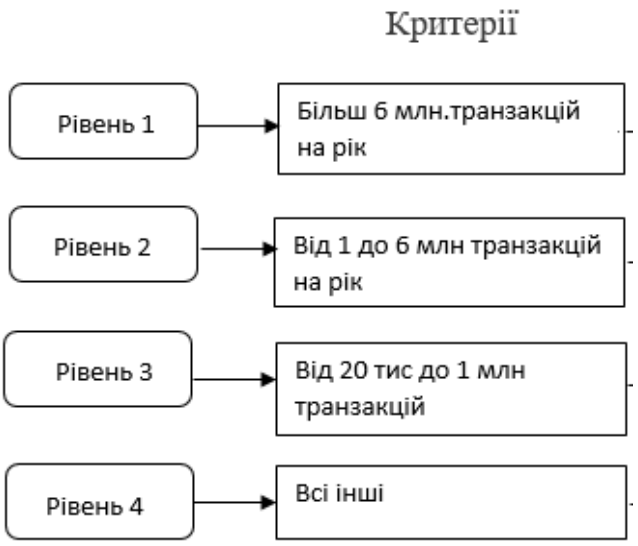

Рисунок 2.2 – Класифікація рівнів та вимоги для підтвердження відповідності стандарту PCI DSS

Наприклад, компанія WayForPay, що оброблює більш ніж 6 млн транзакцій на рік, за класифікацією (рис 2.2) Visa и MasterCard відноситься до Рівню 1. Тому для підтвердження відповідності PCI DSS необхідно проводити щорічний аудит, що здійснюється QSA-аудитором на об'єкті організації та щоквартальне ASV-сканування.

2.4 Боротьба з шахрайськими операціями

Сертифікація PCI DSS дозволяє працювати з банками безпосередньо через платіжні інтерфейси банку і самого інтернет-підприємства. Це дозволяє виключити перехід покупця на сайт третьої сторони. Крім того, побудова власної платіжної системи дозволяє працювати безпосередньо відразу з декількома банками, «балансуючи» між ними, і побудувати систему «каскадного» проведення платежів. При «каскадному» проведенні платежу, його авторизація здійснюється послідовно в декількох банках і процесингових центрах, що дозволяє значно знизити відсоток відхилених

транзакцій. Але самостійна робота з банками дає компанії не тільки перевага в адаптації платіжної системи «під себе». Вона зобов'язує компанію взяти на себе боротьбу з шахрайськими операціями при обробці даних банківських карт на своєму сайті. Іншими словами, компанії необхідно побудувати власну систему моніторингу та боротьби з шахрайськими операціями (анти-фрод).

2.4.1 Анти-фрод система

Анти-фрод – це система моніторингу та запобігання шахрайських операцій, яка в режимі реального часу перевіряє кожен платіж, проганяючи його через десятки, а інколи і сотні фільтрів. Механізми антіфрода працюють таким чином, щоб простежити, чи немає в платежі чогось «незвичайного».

Фільтри-валідатори. Наприклад – валідатор реквізитів банківської карти. На етапі введення даних, на платіжній формі, номер карти перевіряється системою за алгоритмом «Луна»(визначення контрольної цифри номера пластикової картки в відповідності до стандарту ISO/IEC 7812) [34] – так система може зрозуміти, що покупець не здійснив помилку, і введений на платіжній формі номер карти є коректним.

Географічні фільтри. Наприклад – по країнам IP-адрес. Статистика показує, що в деяких країнах Африки високий рівень скіммінгу, і як результат платежі, що здійснюються з цих країн, з високою часткою ймовірності виявляться шахрайськими.

Фільтри-стоплисти. Наприклад – стоплист банківських карт. Якщо система отримує дані картки, по якій вже проходили платежі з поміткою «Фрод», або власник карти заявив в банк-емітент про компрометацію її даних, така картка потрапляє в стоп-лист - система «знає», що по ній не можна пропускати транзакції, так як вони виявляться шахрайськими.

Фільтри відповідності (збігу) параметрів. Наприклад – відповідність країни IP-адреси платника і країни емітента банківської карти. Якщо платіж

здійснюється не з тієї країни, де була випущена картка, а власник картки не попередив банк заздалегідь про свої подорожі, є ймовірність того, що реквізити картки були викрадені і використовуються зловмисниками.

Фільтри лімітів авторизації. Наприклад – ліміт суми однієї транзакції, кількості спроб авторизації з однієї IP-адреси або з однієї банківської карти. Для захисту платника і інших учасників процесу онлайн-оплати існують обмеження за кількістю і сумою платежів, що здійснюються протягом дня або іншого періоду. Для деяких типів бізнесу особливо великий платіж, якби опинився шахрайським, при поверненні може значно знизити прибуток.

Всього система може включати в себе сотні різних фільтрів, і чим більше сфера бізнесу схильна до шахрайських дій, тим більше фільтрів включається і тим краще кожен з них налаштовується під конкретний інтернет-магазин або онлайн-сервіс.

Механізми анти-фрода працюють таким чином, щоб простежити, чи немає в платежі чогось «незвичайного».

Завдання системи – перевірити кожну транзакцію (рис 2.3), знайти в ній «підозрілі» моменти (розбіжність банку-емітента з країною оплати або проживання платника і т.д.) і винести рішення: відхилити платіж або прийняти його. Система анти-фрода складається з декількох компонентів: це автоматичний моніторинг транзакцій, що включає в себе безліч параметрів фільтрів, механізми аутентифікації власника картки і валідації карти, а також моніторинг транзакцій в «ручному» режимі для крайніх випадків.

Рисунок 2.3 – Алгоритм перевірка транзакцій на підозрілість

На стадії побудови і налагодження анти-фрод системи багато часу займає збір та аналіз даних про операції з банківськми картками. Мета збору даних - виявлення характерних ознак шахрайських операцій. В процесі збору статистики компанії доведеться зіткнутися з великим об'ємом «charge-back» операцій. Побудова власної анти-фрод системи логічно та фінансово обґрунтована для компаній з великим оборотом платежів з банківськими картками. Для таких компаній гнучкість і повний контроль над системою фільтрації платежів є критично важливими. У таких компаній є можливість виділити ресурси на розробку і постійний розвиток технологій та інструментів власного "мініпроцесингового центру". Варто відзначити, що для моніторингу ризиків кращий постачальник послуг – процесинговий центр (ПЦ). Завдяки різноманітності та значній кількості клієнтів, ПЦ має велику історією моніторингу і фільтрації. Навіть, якщо компанія займається

побудовою власної анти-фрод системи, вона може віддавати на обробку в ПЦ транзакції, що викликають сумніви у внутрішніх фахівців з ризиків.

Плюси і мінуси системи "анти-фрод". Самий головний недолік: неможливість довести сам факт фроду. Через недостатню доказову базу, відсутність необхідних технічних деталей. Наприклад, «дружній фрод», про який не раз писали банківські портали. Шахрайська схема приблизно така:

1) Держатель картки здійснює покупку в інтернет-магазині.

2) Власник картки звертається в банк-емітент з проханням повернути кошти на його рахунок щодо причини ненадання послуги або недоставлення товару (провести чарджбек).

Якщо магазин не може довести недобросовісність претензій власника картки, банк зобов'язаний списати цю суму з рахунку маркету і повернути її на рахунок невдалого клієнта. В результаті страждають інтернет-магазини.

При наявності недобросовісних клієнтів завідомо неправдиві дані можуть вказуватися з метою несплати або клієнти можуть ініціювати повернення коштів після отримання товару або фактичного надання послуги.

Щодо власних співробітників, то вони в корисливих цілях можуть використовувати персональні відомості роботодавця.

Хакери і кіберзлочинці можуть незаконно отримати доступ до особистої базі даних магазину.

Навіть найдосконаліша антифрод-система сьогодні не зможе ефективно протистояти і людському фактору. Навіть у випадку наявної змови між співробітниками банку і працівниками магазину неможливо успішно цьому протистояти.

Крім того, використання подібних систем веде до "витрат виробництва". Якщо захисне ПО стане часто відхиляти платежі і перекази клієнтів банку через те, що вони виглядають «підозрілими», то організація буде втрачати держателів своїх карток, незадоволених обмеженнями в розпорядженні власними фінансами. Якщо систему фрод-моніторингу

запровадять віртуальні магазини, то в наявності будуть проблеми з захистом даних користувачів - як особистих, так і платіжних карток.

Крім того, необхідно пройти сертифікацію на відповідність вимогам PCI DSS, а також врахувати українські закони про захист персональної інформації.

Антифрод-системи - це спеціальне програмне забезпечення (ПЗ), здатне протистояти кібератакам, хакерам і іншого роду шахрайства в банківських платіжних системах. Найдосконалішими на сьогодні інтелектуальні системи, здатні до самонавчання під час роботи.

До суттєвих недоліків фрод-моніторинг поки що можна віднести: ймовірність помилкового блокування платежів і переказів та неможливість ефективного протистояння людському фактору.

2.5 Аналіз підходів до обробки платіжних карт

Для прийняття виваженого рішення про вибір способу обробки даних банківських карт, необхідно оцінювати всі складові процесу від подачі документів до підтримки кардхолдерів (держатель картки). Для того щоб прийняти рішення було простіше, було проведено порівняння двох основних підходів (табл. 2.3) з приймання та обробки даних банківських карт: якщо введення даних здійснюється на сторонньому сайті і якщо дані вводять на сайті підприємства з подальшою авторизацією платежу в банку.

Таблиця 2.3 - Підходи для обробки платіжних карт

Параметри	Введення даних банківської карти здійснюється на сайті підприємства з подальшою авторизацією платежів (наприклад, в банку)	Введення даних банківської карти здійснюється на сторонньому сайті (наприклад, на захищеній платіжній сторінці ПЦ)

1	2	3
PCI DSS	Проходження сертифікації на відповідність обов'язково.	Проходження сертифікації не обов'язково.
Підключення	Для прийому платежів необхідно самостійно підключитися до банка. Рішення банку залежить, в тому числі, від обороту компанії.	Для підключення необхідно передати пакет документів особистого менеджера, який буде взаємодіяти з банком і займатися підготовкою договору.
Комісія	Комісія (за обробку платежів) становить від 2% (суми транзакції) і залежить від обсягу обороту і сфери діяльності компанії. % комісії, отриманий клієнтом від банку, часто дорівнює відсотку, що надається ПЦ. Це пов'язано з "оптовими" умовами роботи для ПЦ і високим рівнем надійності моніторингу транзакцій, в якому зацікавлений банк.	Комісія, що стягується ПЦ за обробку платежів і комплекс додаткових послуг, становить від 2,5% від суми транзакції і залежить від обсягу обороту і сфери діяльності компанії.
Бухгалтерія	Взаємодією з банком з питань бухгалтерської звітності і проведенням платежів компанія займається самостійно. Для складання	Біллінгова система ПЦ надає клієнтам можливість виробляти online-облік здійснених транзакцій.

Прожовження таблиці 2.3

1	2	3
	звітів потрібно активна робота з банком і побудова власної білінгової системи.	Можливість самостійно вивантажувати бухгалтерські документи (акт, деталізована виписка системи PayOnline,

		рахунок) в інтерфейсі особистого кабінету.
Підтримка платників	Для надання кваліфікованої підтримки платників необхідно організувати власний Call-центр або купувати послуги стороннього. Якщо у Вас вже є Call-центр, необхідно провести додаткову навчання фахівців для роботи з держателями карток, потрібна побудова інфраструктури Call-центру: софт, телефонія.	Підтримка власників карток, які роблять платежі в Вашому інтернет-магазині, здійснюється фахівцями Call-центру ПЦ.
Моніторинг транзакцій	Моніторинг транзакцій повинен здійснюватися штатними кваліфікованими фахівцями підприємства e-commerce, що обробляє дані банківських карт.	Моніторинг транзакцій, з тому числі програмний, здійснюється фахівцями департаменту ризиків ПЦ.
Сервер	Потрібні вкладення в серверну частину, необхідні для проходження сертифікації і забезпечення достатнього рівня безпеки. Сума залежить від рівня сертифіката і передбачуваної інфраструктури.	Не обов'язково здобувати додаткові витрати на розвиток серверної частини, так як обробка транзакцій відбувається на захищених серверах ПЦ.

Прожовження таблиці 2.3

1	2	3
Розробка	Для організації самостійного прийому платежів необхідна розробка або купівля	Для підключення до ПЦ потрібно одноразове залучення розробника для

	білінгової системи, в тому числі сервісів безпечної передачі даних в банк, безпечних форм прийому платежів, додаткових інтерфейсів. (потрібна постійна робота фахівця високої кваліфікації вартістю не менше 35 000 грн. / міс.)	впровадження платіжної форми на сайт компанії. При необхідності брендування платіжна форма розробляється фахівцями ПЦ.
Прийом платежів на сайті (без переходу на сторонній ресурс)	Ви обробляєте дані банківських карт на сайті без переходу на сторонній ресурс.	Можлива реалізація прийому платежів без прямого переходу на сайт ПЦ з використанням технології IFrame.

2.6 Аналіз вимог стандарту PCI DSS

Стандарт PCI DSS представляє собою перелік вимог (табл. 2.1) по відношенню до систем керування безпекою, мережевої інфраструктури, політик, процедур, розробки програмного забезпечення та інших заходів захисту даних власників банківських карт. Вимоги стандарту призначені в першу чергу для виконання фінансовими організаціями та постачальниками послуг, які зберігають, передають чи обробляють дані власників карт.

Для розробки і забезпечення підтримки конфігурацій міжмережевих екранів для захисту даних тримача карти необхідно здійснити наступні дії:

- розробити стандарти конфігурації міжмережевих екранів;
- створити конфігурацію міжмережевих екранів, яка забороняє будь-які з'єднання між елементами середовища даних тримачів карт та мережами, до яких немає довіри (“untrusted network”);
- заборонити прямий відкритий доступу між Інтернетом та будь-яким системним компонентом середовища даних тримачів карт;

– установити персональні програмні міжмережеві екрани на всіх мобільних або службових комп’ютерах співробітників, що мають доступ в Інтернет і використовуються для доступа до локальної мережі організаціїю.

Для заборони використання системних паролів та інших параметрів безпеки, встановлених виробником, необхідно виконати наступні дії:

– завжди слід міняти встановлені, за умовчанням, виробником налаштування перед установкою системи в мережеву інфраструктуру, видаляти непотрібні для роботи облікові записи$

– розроблити стандарти конфігурації для всіх системних компонентів;

– шифрувати канал віддаленого адміністративного доступу до системи, для цього необхідно використовувати такі технології, як SSH, VPN або SSL/TLS для орієнтованих для веб-сервера систем адміністрування і інших способів віддаленого адміністративного доступу;

Для забезпечення безпеки даних тримачів карт, що зберігають карти, необхідно виконати наступні дії:

– зберігання даних тримачів карт має бути обмежене лише необхідним мінімумом даних, має бути розроблена політика зберігання і обробки даних, кількість даних і терміни їх зберігання мають бути обмежені лише параметрами, необхідними для виконання вимог бізнесу, законодавства і інших регулюючих вимог, ці параметри мають бути відображені в політиці зберігання даних;

– забороняється зберігати критичні аутентифікаційні дані після авторизації (навіть у зашифрованому вигляді);

– необхідно маскувати Primary Account Number (PAN – це спеціальна комбінація цифр, яка представлена на банківській картці довгим номером, що знаходиться на її лицьовій стороні) при його відображенні (максимально можлива кількість знаків PAN для відображення - перші 6 і останні 4 знаки). Ця вимога не відноситься до співробітників і інших сторін, для роботи яких необхідно бачити повний PAN, також ця вимога не замінює собою інші

строгіші вимоги до відображення даних тримача карти (наприклад, на чеках POS-терміналів);

– з усіх даних тримача карти, як мінімум, PAN має бути представлений в нечитаному вигляді у всіх місцях зберігання, для цього слід використовувати будьякий з наступних методів:

а) стійка однонаправлена хеш-функція;

б) укорочення (truncation);

в) використання механізмів One-Time-Pad («одноразові блокноти») і використання і зберігання посилань на дані замість самих даних (index tokens);

г) стійкі криптографічні алгоритми, спільно з процесами і процедурами управління ключами. З усієї інформації тримача карти, як мінімум, PAN має бути перетворений в нечитаний вигляд. Якщо, з якихось причи, компанія не може шифрувати дані тримача карти, то компенсуючі заходи відображають у Додатку В: «Компенсуючі заходи для шифрування даних, що зберігаються»;

– забезпечити захист ключів шифрування даних тримача карти від їх компрометації або неправильного використання;

– документувати всі процеси і процедури управління ключами шифрування даних тримача карти;

Для шифрування даних тримачів карт при передачі їх через відкриті і загальнодоступні мережі необхідно виконати наступні дії:

– під час передачі даних через загальнодоступні мережі слід використовувати стійкі криптографічні алгоритми і такі протоколи: SSL/TLS і IPSEC. Прикладами загальнодоступних мереж, на які поширюються вимоги PCI DSS, є Інтернет, IEEE 802.11x, IEEE 802.16x, GSM, GPRS;

– не пересилати незашифрований PAN електронною поштою.

Для використання і регулярного оновлювання антивірусного програмного забезпечення необхідно виконати наступні дії:

– антивірусне програмне забезпечення має бути розгорнуте на всіх системах схильних до дії вірусів (особливо робочих станціях і серверах);

– антивірусні механізми мають бути актуальними, постійно включеними і повинні вести журнали протоколювання подій.

Для розробки і підтримки безпечних систем і додатків необхідно виконати наступні дії:

– встановити найсвіжіші оновлення безпеки, випущені виробником, на всі системні компоненти і програмне забезпечення. Оновлення безпеки мають бути встановлені протягом місяця з моменту їх випуску виробником.

– запровадити процес визначення знов виявлених вразливостей безпеки (наприклад, підписка на безкоштовну розсилку повідомлень про нові вразливості), стандарти конфігурації системних компонентів повинні оновлюватися для обліку знов виявлених вразливостей;

– розробляти додатки відповідно до накопиченого в даній галузі досвіду, з врахуванням вимог інформаційної безпеки протягом всього циклу розробки;

– розробляти та впроваджувати процедури управління змінами;

– розробка веб-додатків повинна проходить відповідно до керівництва з безпечного програмування, програмний код додатків має бути досліджений на наявність потенційних вразливостей до відомих атак;

– забезпечити захист веб-орієнтованих застосувань від відомих атак одним з наступних методів:

а) перевіркою програмного коду в ручному або автоматичному режиму на наявність вразливостей щонайменше раз на рік або після будь-яких змін, користуючись відповідними програмними засобами;

б) встановити міжмережевий екран прикладного рівня перед веб-орієнтованими додатками.

Для обмеження доступу до даних тримачів карт лише службовою необхідністю необхідно виконати наступні дії:

– дозволити доступ до компонентів системи і даних тримача карт тільки тим співробітникам, яким такий доступ необхідний відповідно до їх посадових обов'язків;

– встановити механізм розмежування доступу, заснований на чиннику – «знає тільки те, що необхідно» та «заборонено все, що явно недозволено» для систем, розрахованих на багато користувачів.

Для призначення унікального ідентифікатора кожній особі, що має доступ до комп'ютерної мережі, необхідно виконати наступні дії:

– призначити унікальне ім'я облікового запису кожному користувачеві для доступу до компонентів системи і даних тримача карти;

– застосовувати хоч би один з наступних методів для аутентифікації всіх користувачів (крім ідентифікатора):

а) парольне слово або парольна фраза;

б) двохфакторна аутентифікація (наприклад, апаратні електронні ключі, смарт карти, біометричні системи, відкриті ключі);

– реалізувати механізм двохфакторної аутентифікації при віддаленому доступу співробітників, адміністраторів і третіх осіб до комп'ютерної мережі.;

– зберігати і передавати всі паролі лише в зашифрованому вигляді;

– встановити контроль над виконанням процедур аутентифікації і управління паролями облікових записів співробітників і адміністраторів.

Для обмеження фізичного доступу до даних тримача карти необхідно виконати наступні дії:

– використовувати засоби контролю доступу в приміщення, аби обмежити і відстежувати фізичний доступ до систем, які зберігають, обробляють або передають дані тримача карти;

– впровадити процедури, що дозволяють легко розрізняти співробітників і відвідувачів, особливо в приміщеннях, де можливий доступ до даних тримача карти;

– ввести процедуру допуску відвідувачів на об'єкт;

– вести журнал обліку відвідувачів і використовувати його для аналізу відвідин, цей журнал слід зберігати не менше трьох місяців, якщо інший термін не визначено законодавством;

– зберігати носії з резервними копіями даних в безпечних місцях, бажано поза об'єктом, таких як запасний центр обробки даних, або використовувати послуги компаній, що забезпечують безпечне зберігання, переглядати місце збереження не рідше одного разу на рік;

– забезпечити фізичну безпеку всіх паперових і електронних засобів (включаючи комп'ютери, електронні носії інформації, мережеве устаткування, лінії телекомунікацій, паперові звіти, чеки і факсимільні повідомлення), що містять дані тримача карти;

– забезпечити строгий контроль над переміщенням носіїв інформації, що містять дані тримача карти;

– впровадити процедуру дозволу керівництвом винесення за межі території, що охороняється, носіїв, що містять дані тримача карти;

– забезпечити строгий контроль за зберіганням і доступом до носіїв, що містять дані тримача карти;

– знищувати носії, що містять дані тримача карти, зберігання яких більш не потрібно згідно виконання бізнес-завдань або вимог законодавства.

Для відстеження і контролювання будь-якого доступу до мережевих ресурсів і даних тримачів карт необхідно виконати наступні дії:

– розробити процес розподілу доступу до компонентів системи (особливо доступу з адміністративними повноваженнями) між персоналом.

– для кожного системного компонента має бути включений механізм протоколювання подій (будь-які дії, здійснені з використанням адміністративних повноважень; будь-який доступ до записів про події в системі; спроби невдалого логічного доступу; використання механізмів ідентифікації і аутентифікації; ініціалізація журналів протоколювання подій; створення і видалення об'єктів системного рівня);

– ваписувати параметри(ідентифікатор користувача, тип події, дата та час, джерело події, вдала чи невдала подія, ідентифікатор або назва даних, системного компонента або ресурсу, на які вплинула подія) для кожної події кожного системного компонента;

– синхронізувати усі критичні системні годинники;

– захистити від змін журнали протоколювання подій;

– переглядати журнали протоколювання подій не рідше одного разу на день, аналізувати журнали систем виявлення вторгнень (IDS) і серверів що здійснюють аутентифікацію, авторизацію і аудит (наприклад, RADIUS), для забезпечення відповідності вимозі можуть бути використані засоби збору і аналізу журналів протоколювання подій, а також засобу сповіщення;

– зберігати не менше одного року журнали протоколювання подій, вони повинні бути в оперативному доступі не менше трьох місяців.

Для регулярна перевірки систем і процесів забезпечення безпеки необхідно виконати наступні дії:

– аналізувати бездротові мережі з метою ідентифікації всіх використовуваних пристроїв не рідше за один раз в квартал або встановити бездротову IDS/IPS, яка буде ідентифікувати всі пристрої у використанні;

– проводити зовнішнє і внутрішнє сканування мережі на наявність вразливостей не рідше одного разу у квартал, а також після внесення значимих змін (наприклад, установки нових системних компонентів, зміни топології мережі, зміни правил міжмережевих екранів, оновлення системних компонентів);

– проводити тест на проникнення не рідше одного разу в рік, а також після будь-якої значимої зміни або оновлення інфраструктури і додатків (наприклад, оновлення операційної системи, додавання підмережі, установки веб-серверу);

– використовувати системи виявлення вторгнень на рівні вузла і на рівні мережі, а також системи попередження вторгнень для контролю всього мережевого трафіку і сповіщення персоналу про підозрілі дії.

– використовувати додатки контролю цілісності файлів для сповіщення персоналу про несанкціоновані зміни критичних системних файлів і файлів даних. Перевірка цілісності критичних файлів повинна проводитися не рідше одного разу на тиждень.

Для підтримки Політики , що визначає правила інформаційної безпеки для співробітників і партнерів, необхідне виконання наступних дій:

– розробити, опублікувати і поширити підтримувана в актуальному стані політики безпеки;

– розробити щоденні процедури безпеки, що відповідають вимогам діючого стандарту (наприклад, процедури управління обліковими записами користувачів, процедури аналізу журналів протоколювання подій);

– розробити правила експлуатації для критичних пристроїв та технологій, з якими безпосередньо працюють співробітники (таких як модеми і бездротові мережі), аби визначити коректний порядок використання цих пристроїв співробітниками;

– Політика і процедури безпеки повинні однозначно визначати обов'язки всіх співробітників і партнерів, що відносяться до інформаційної безпеки.

– призначити обов’язки певному співробітникові або групі співробітників в області управління інформаційною безпекою (розробка, документування і поширення політики і процедур безпеки; моніторинг, аналіз і доведення до відповідного персоналу інформації про події, що мають відношення до безпеки даних; розробка, документування і поширення процедур реагування на інциденти і повідомлення про них, аби гарантувати швидку і ефективну обробку всіх ситуацій; адміністрування облікових записів користувачів, включаючи їх додавання, видалення і зміну; моніторинг і контроль будь-якого доступу до даних);

– впровадити офіційну програму підвищення обізнаності персоналу про питання безпеки, аби донести до них важливість забезпечення безпеки даних тримача карти;

– перевіряти кандидатів при прийомі на роботу для мінімізації ризиків внутрішніх атак;

– створити і запровадити політику і процедури керування постачальників послуг, коли дані тримача карти стають доступні постачальникові послуг;

– впровадити план реагування на інциденти. Компанія має бути готова негайно відреагувати на порушення в роботі системи.

Аналізуючи основні вимоги стандарту PCI DSS зроблено такі висновки:

1) Міжмережевий екран аналізує весь мережевий трафік і блокує з'єднання, які не задовольняють визначеним критеріям безпеки. Всі системи повинні бути захищені від несанкціонованого доступу з мережі Інтернет, будь то підключення система електронної торгівлі, доступ працівників до Інтернету через браузери, доступ працівників до електронної пошти, виділені підключення зі сторонніми організаціями, підключення по бездротових мережах або іншими способами. Міжмережеві екрани - найважливіші механізми забезпечення безпеки будь-якої комп'ютерної мережі.

2) Зловмисники (зовнішні і внутрішні) при здійсненні атаки на систему часто намагаються використовувати встановлені виробником, за умовчанням, паролі і інші параметри. Ці паролі добре відомі в певних співтовариствах, і їх легко отримати з відкритих джерел інформації.

3) Шифрування - критичний компонент захисту даних тримачів карт. Якщо шахрай обійде елементи заходів безпеки і отримає доступ до зашифрованих даних, не знаючи ключа шифрування, то ці дані залишаться для нього невідомими. Інші способи захисту даних, що зберігаються, повинні розглядатися як засоби зменшення ризиків. Методи мінімізації ризиків включають:

– заборону зберігання даних тримачів карт, окрім випадків крайньої необхідності;

– зберігання укороченого PAN, якщо не потрібне зберігання повного PAN;

– уникнення пересилки PAN по електронній пошті в відкритому вигляді.

4) Критична інформація повинна передаватися лише в зашифрованому вигляді через загальнодоступні мережі, де її легко перехопити, змінити або перенаправити.

5) Більшість вірусів («черв'яків», «троянів») проникають в мережу через прикладні програми, включаючи електронну пошту співробітників, через мобільні комп’ютери, змінні носії даних і таке інше. Антивірусне програмне забезпечення має бути встановлене на всіх системах, які схильні до дії вірусів, аби захистити їх від шкідливих кодів.

6) Зловмисники використовують вразливості безпеки для здобуття привілейованого доступу до системи. Більшість з таких вразливостей закриваються шляхом установки оновлень безпеки, що випускаються виробником. На всі системи мають бути встановлені найсвіжіші відповідні оновлення програмного забезпечення для захисту від використання вразливостей внутрішніми і зовнішніми зловмисниками, а також вірусами. Відповідними є ті оновлення, які протестовано на сумісність з поточною конфігурацією безпеки. В разі самостійної розробки додатків вдасться уникнути безлічі вразливостей, якщо використовувати стандартні процеси розробки систем і прийоми безпечного написання програмного коду.

7) Доступ до критичних даних має бути лише в авторизованих співробітників.

8) Призначення унікального ідентифікатора кожній персоні, що має доступ до комп'ютерної системи, дозволяє гарантувати, що дії з критичними даними і системами виконуються відомими і авторизованими користувачами і можуть бути відстежені.

9) Фізичний доступ до систем, що містять дані тримача карти, надає можливість отримати контроль над пристроями і даними, а також вкрасти пристрій або документ, і має бути відповідним чином обмежений.

10) Наявність механізмів протоколювання подій і можливості відстежувати дії користувачів необхідно для попередження, виявлення та

мінімізації наслідків компрометації даних. Ці механізми дозволяють проведення розслідування і аналіз інцидентів. Визначення причин інцидентів ускладнено при відсутності журналів протоколювання подій в системі.

11) Вразливості безперервно виявляються зломщиками і дослідниками, а також з'являються разом з новим програмним забезпеченням. Необхідно періодично, а також при внесенні змін, перевіряти системи, процеси і програмне забезпечення, аби переконатися, що їх захищеність підтримується на належному рівні.

12) Політика безпеки задає тон безпеки у всій компанії і інформує співробітників про те, що від них вимагається. Всі співробітники мають бути обізнані про критичні дані і свої обов'язки щодо їх захисту. Цільовою аудиторією цих вимог є: персонал - постійний, частково зайнятий, тимчасовий; партнери, консультанти, ті, що постійно перебувають у компанії.

Таким чином, якщо компанії необхідно пройти сертифікацію на відповідність PCI DSS і самостійно обробляти дані банківських карт на сайті, до неї застосовуються всі вимоги стандарту PCI DSS. Вони охоплюють безпеку на рівні мереж, обладнання, додатків, баз даних, фізичних сховищ, документування та управління процесами. Побудова анти-фрод системи і білінгової системи – завдання непросте і тривале в реалізації, також виконується компанією самостійно. Для компаній, які працюють тільки з платіжним шлюзом і не приймають на своєму даних банківських карт клієнтів, відносяться тільки вимоги департаменту ризиків платіжного шлюзу (ПШ). Вони стосуються сайта підприємства e-commerce, коректності контенту і цінових пропозицій, організаційної форми компанії.

2.7 Рекомендації для підвищення рівня захисту даних платіжних карток

В результаті проведеного в роботі аналізу вимог стандарту PCI DSS, практичного досвіду, набутого під час проходження технологічної та переддипломної практик в організації, яка займається обробкою платежів на міжнародному рівні, працює з тисячами мерчантів, стало зрозумілим, що для забезпечення подальшого підвищення рівня безпеки даних даних тримачів карт необхідно постійно вдосконалювати систему захисту, враховуючи при цьому вимоги стандарту PCI DSS.

Кожен день у світі виникають нові загрози, методи проникнення у систему. У звязку з цим, опрацювавши теоретичні матеріали на тему забезпечення безпеки даних платіжних карт, спираючись на інформацію, отриману під час консультацій з фахівцями з безпеки та розробниками ПО процесингових оргвнізацій, в дипломній роботі розроблено рекомендації щодо підвищення рівня безпеки в організаціях, інформаційна інфраструктура яких передбачає зберігання, обробку або передачу даних платіжних карт.

Рекомендації:

1) Зберігати критичні карткові дані виключно в зашифрованому вигляді.

2) Зберігати карткові дані в окремому незалежному сховищі (СУБД), доступ до якого обмежений тільки тим внутрішнім сервісам платіжної системи, яким необхідно мати можливість зберігати або отримувати повні карткові дані.

3) Окремо зберігати критичні та загальні дані. Такий поділ дає можливість проведення аналітики і співвіднесення нових транзакцій з історичними даними без необхідності дешифрування та доступу до повного набору інформації до даних картки. Наприклад:

- загальні дані – замаскований частковий PAN або хеші від повного PAN, або його частин (останні 6-8 знаків), expiration date, card holder name;
- критичні дані – повний PAN та його зв'язок з відповідною публічною частиною.

4) Використовувати токенізацію для card holder data. Тобто привласнювати штучний унікальний ідентифікатор картковим даним, який

сам по собі не містить ніяких даних про карту але дозволяє оперувати ними, як для розуміння кореляції між різними транзакціями в системі, так і для оперування картами в рамках API між сервісами в системі або за рамками системи. Не потрібно для цих цілей використовувати будь-які монотонні послідовності або хеш від картки, тому що це, у випадку часткового витоку даних з системи, дає додаткові можливості для зіставлення при розшифровці карткових даних.

5) CVV2 / CVC зберігати в системі можна лише в рамках платіжної сесії. Наприклад : тримати їх виключно в оперативній пам'яті, в рамках процесів/потоків, що оброблюють певну платіжну транзакцію. Зберігати їх в будь-якому персистентному сховищі будь-то СУБД або навіть система черг/повідомлень (messaging queue) з персистентним зберіганням повідомлень не рекомендується, навіть у разі можливого регулярного очищення цих даних.

6) Не записувати карткові дані в логи. Системно моніторити логи на відсутність запису в них карткових даних. Використовувати централізоване логування, щоб уникнути наявності неврахованих логів, налаштувати автоматичну аналітику записів в логах з повідомленнями на випадок аномалій.

7) Виділяти весь функціонал щодо шифрування-дешифрування карткових даних в окремий сервіс, ізольований від решти процессингової платформи. Кожна операція цього сервісу повинна записуватися в окремий аудит-лог. Доступ до цього сервісу повинен бути максимально обмежений, як аутентифікацією та авторизацією сервісів, які з ним взаємодіють, так і на рівні мережі.

8) Ключі для шифрування / дешифрування не зберігати в конфігураційних файлах, які знаходяться на файловій системі сервера, або в СУБД, а в спеціалізованих сховищах секретів з окремою авторизацією і логування, наприклад Hashicorp Vault. Як варіант зберігати ключі

розподіленно, наприклад: частина ключа в базі, а інша частина в сховищі секретів.

9) Необхідно періодично змінювати ключі шифрування, при цьому всі збережені карткові дані необхідно перешифровувати.

10) Зберігати карткові дані необхідно тільки на обгрунтований бізнесом час. Наприклад: на період життя підписки або на максимальний період повернення платежу по картці. При цьому для отримання аналітики за історичними даними достатньо залишати який-небудь хеш від карти з прив'язкою до транзакції.

11) Обмежити зовнішній доступ в мережу для сервісів, у яких немає необхідності робити мережеві запити поза білого списку адрес.

12) Приділяти особливу увагу до доставки додатків на production. Code review, звірка контрольних зібраних артефактів додатків і т.д.

13) Перевіряти логи та метрики додатків, наприклад: збільшення кількості потоків на один запит в сервісі вже може бути показником впровадженого стороннього коду в додаток.

2.8 Висновки до другого розділу

У другому розділі дипломної роботи проаналізовані підходи для процедури обробки платіжних карток, методи боротьби з шахрайськими операціями. Проаналізовані вимоги міжнародного стандарту у сфері інформаційної безпеки даних індустрії платіжних карток PCI DSS та на основі аналізу вимог стандарту PCI DSS розроблені рекомендації щодо забезпечення безпеки даних тримачів карток для організацій, в інформаційній інфраструктурі яких зберігаються, обробляються або передаються дані платіжних карт.

РОЗДІЛ 3
ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ ВИКОРИСТАННЯ РЕКОМЕНДАЦІЙ

3.1 Вступ

Метою данного розділу є обґрунтування економічної доцільності застосування рекомендацій для підвищення рівня безпеки організацій в інформаційній інфраструктурі яких зберігаються, обробляються або передаються дані платіжних карт.

Для визначення ефективності необхідно розрахувати:

1) капітальні витрати на розробку, впровадження та підтримку рекомендацій;

2) трудомісткість витрати на розробку, впровадження та підтримку рекомендацій;

3) річні експлуатаційні витрати на впровадження та підтримку рекомендацій;

4) показники економічної ефективності застосування рекомендацій в організації.

3.2 Розрахунок фіксованих (капітальних) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на створення та впровадження рекомендацій Кпз є одноразовими та складаються з витрат на заробітну плату виконавцям Ззп і вартості витрат машинного часу, що необхідний для опрацювання всіх рекомендацій на ПК Змч:

$$K_{пз} = (З_{пр} + З_{мч)} \cdot N, \text{ грн} \qquad (3.1)$$

$З_{пр}$ – заробітна плата виконавця за годину, грн./год.;

$З_{мч}$ – вартість витрат машинного часу за годину, грн./год

N – Кількість фахівців.

Заробітна плата працівника враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{ЗП} = t \cdot З_{ПР}, \text{ грн}, \qquad (3.2)$$

де t – загальна тривалість створення керівництва, годин;

Розрахуємо час, який буде витрачено на створення рекомендацій:

$$t = t_{тз} + t_{â} + t_{сеп} + t_{мз} + t_{бс} + t_{фс} + t_{ст} + t_{оп}, \text{ годин}, \qquad (3.3)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку рекомендацій;

$t_{â}$ – тривалість вивчення технічного завдання;

$t_{сеп}$ – тривалість аналізу систем електронних платежів;

$t_{мз}$ – тривалість аналізу методів та засобів оцінювання ризиків безпеки інформації в системах електронної комерції;

$t_{\text{бс}}$ – тривалість аналізу основних складових безпеки систем електронної комерції;

$t_{\text{фс}}$ – тривалість аналізу анти-фрод систем;

$t_{\text{ст}}$ – тривалість аналізу стандарту PCI DSS;

$t_{\text{оп}}$ – тривалість опрацювання рекомендацій;

У таблиці 3.1 представлена трудомісткість процесів.

Таблиця 3.1 - Трудомісткість процесів

Назва процесу	Трудомісткість, год.
Складання технічного завдання на розробку рекомендацій	24
Вивчення технічного завдання	8
Аналіз систем електронних платежів	40
Аналіз методів та засобів оцінювання ризиків безпеки інформації в системах електронної комерції	40
Аналіз основних складових безпеки систем електронної комерції	56
Аналіз анти-фрод систем	48
Аналіз стандарту PCI DSS	120
Опрацювання рекомендацій	56

t = 24 + 8 + 40 + 40 + 56+48+120 + 56=392 години.

$З_{\text{пр}}$– середньогодинна заробітна плата фахівця з нарахуваннями, грн/годину.

$$З_{\text{пр}} = \frac{З_{\text{м}}}{t_m} = \frac{15000}{160} = 93{,}75, \text{ грн/год,} \qquad (3.4)$$

де $З_м$– середня заробітна плата фахівця з інформаційної безпеки – 15 000 грн. t_m – робочій час на місяць -160 год.

$$З_{зп} = 392 \cdot 93{,}75 = 36\ 750, \text{ грн}$$

Вартість машинного часу для впровадження рекомендацій визначається за формулою:

$$З_{мч} = (t_{опр} \cdot C_{мч} + t_д), \text{ грн,} \quad (3.5)$$

де $t_{опр}$ – трудомісткість налогодження всіх необхідних операцій на ПК, годин (80 год);

$t_д$ – трудомісткість підготовки документації на Пк, годин (40 год);

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot C_e + \frac{Ф_{зал} \cdot H_a}{F_p} + \frac{K_{лпз} \cdot H_{апз}}{F_p}, \quad (3.6)$$

де P – встановлена потужність ПК, 0.5 кВт;

C_e – тариф на електричну енергію, 1.68 грн/кВт·година;

$Ф_{зал}$– залишкова вартість ПК на початок року, 2700 грн.;

H_a – річна норма амортизації на ПК, 0.1 частки одиниці;

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

F_p – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920 год).

$$С_{мч} = 0{,}5 \cdot 1{,}68 + \frac{2700 * 0{,}1}{1920} = 0{,}98, \text{ грн/год}$$

$$З_{мч} = 80 \cdot 0,98 + 40 = 118,4 \quad \text{грн.}$$

Таким чином, капітальні (фіксовані) витрати на створення та впровадження рекомендацій складають:

$$К_{пз} = (118,4 + 36\,750) \cdot 3 = 110\,370, \text{ грн} \qquad (3.7)$$

3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Витрати на підтримку методики (щороку):

$$С_1 = (З_м \cdot N) \cdot m = (15\,000 \cdot 3) \cdot 12 = 540\,000, \text{ грн.} \qquad (3.8)$$

де m - кількість місяців на рік

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_а + С_з + С_{ел} + С_{тос}, \text{ грн,} \qquad (3.9)$$

де $С_а$ - Річний фонд амортизаційних відрахувань (Са) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ):

$$С_а = \frac{К_{пз}}{2} = \frac{110\,370}{2} = 55\,185, \text{ грн,} \qquad (3.10)$$

$С_з$ - Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ,складає:

$$С_з = (З_м + \mathbf{22}\%) \cdot N \cdot m = (15\,000 + 3\,300) \cdot 3 \cdot 12 = 658\,800 \text{ грн}, \quad (3.11)$$

До річного фонду заробітної плати додається єдиний внесок (22%) на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок, збір якого здійснюється відповідно до класів професійного ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності.

Розмір єдиного внеску на загальнообов'язкове державне соціальне страхування визначається на підставі встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати

$С_е$ - Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн}, \quad (3.12)$$

де Р – встановлена потужність апаратури інформаційної безпеки, 0.5 кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (за 40-годинного робочого тижня $F_р$ = 1920 год);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин, 1.68 грн/кВт·година.

$$С_{ел} = 0{,}5 \cdot 1920 \cdot 1{,}68 = 1\,612{,}8 \text{ грн}.$$

$С_{тос}$ - Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки складає 1,5% від вартості капітальних витрат (1 655,55 грн).

Отже, річні поточні (експлуатаційні) витрати складають:

$$C = 55\,185 + 540\,000 + 1\,612{,}8 + 1\,655{,}55 = 589\,453{,}35 \text{ грн.}$$

3.4 Оцінка можливого збитку від атаки

Розрахунок можливого збитку (U) від атаки проведено на прикладі організації Рівня 1(оброблюють більш ніж 6 млн транзакцій на рік):

$$U = n \cdot S, \text{ грн,} \qquad (3.13)$$

де n – кількість транзакцій, що оброблюються в рік (6,5 млн);

S – середня сума за транзакцією (900 грн).

$$U = 6\,500\,000 \cdot 900 = 5\,850\,000\,000 \text{ грн,}$$

Малоймовірно, що під атаку одразу потраплять усі транзакції, тому визначемо відсоткове співвідношення:

Якщо під атаку потрапляють

0,1% - 5 850 000 грн;

0,2% -11 700 000 грн;

0,3% -17 550 000 грн;

0,4% - 23 400 000 грн;

0,5% - 29 250 000 грн;

1% - 58 500 000 грн;

10% -585 000 000 грн.

3.5 Загальний ефект від впровадження рекомендацій

Загальний ефект від впровадження рекомендацій визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = U \cdot R - C, \qquad (3.14)$$

де U – загальний збиток від атаки на систему, грн;

R – очікувана імовірність атаки на систему, (0,4 найбільш ймовірній відсоток);

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E = 5\,850\,000\,000 \cdot 0{,}4 - 589\,453{,}35 = 22\,810\,546{,}65 \text{ грн}$$

3.6 Економічне обґрунтування

Оцінка економічної ефективності впровадження рекомендацій для організацій Рівня 1, здійснюється на основі визначення та аналізу наступних показників:

а) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

б) термін окупності капітальних інвестицій То.

Ключовою перевагою показника ТСО є те, що він дозволяє зробити висновки про доцільність реалізації проекту в області інформаційної безпеки на підставі оцінки одних тільки витрат.

У цьому випадку необхідно порівняти сукупну вартість володіння, розраховану для двох варіантів проектного рішення щодо створення або удосконалення системи інформаційної безпеки, і вибрати варіант із найменшою з них.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \qquad (3.15)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки , тис. грн;

К –капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

$$\text{ROSI} = \frac{22\ 810\ 546{,}65}{110\ 370} = 207.$$

Нормативне значення коефіцієнта повернення інвестицій визначається з наступних міркувань.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань), то в якості $Е_н$ варто приймати бажану норму прибутковості альтернативних варіантів вкладення коштів К (наприклад, у цінні папери, інші проекти, на депозитний рахунок у банку, тощо) з урахуванням інфляції. Визначити бажане значення коефіцієнта ефективності можна також виходячи з прийнятної для підприємства індивідуальної норми прибутковості, якак б, принаймні, не знижувала ринкову вартість фірми.

При цьому проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$\text{ROSI} > (\text{Nдеп} - \text{Nінф})/100), \qquad (3.16)$$

де Nдеп – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, 18%;

Nінф – річний рівень інфляції, 13,7%.

$$207 > (18\text{-}13{,}7)/100$$

$$207 > 0{,}043$$

Для вибраного варіанта визначається розрахунковий строк окупності капітальних інвестицій T_o.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = 0.0048 \text{ років} \approx 2 \text{ дні}.$$

3.7 Висновки до економічного розділу

В результаті розрахунку витрат на впровадження рекомендацій для підвищення рівня інформаційної безпеки в організаціях, які зберігають, оброблюють та передають дані тримачів платіжних карток було визначено, що розмір капітальних витрат складатиме 110 370 грн, а щорічні експлуатаційних витрати 589 453 грн.

Коефіцієнт повернення інвестицій ROSI показав, що 207 грн додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження рекомендацій.

Загальний ефект від впровадження рекомендацій визначається з урахуванням ризиків порушення інформаційної безпеки і становить 22 810 546,65 грн

Було доведено, що застосування рекомендацій в організації Рівня 1 зменшить можливий рівень збитків у розмірі до 5 850 000 000 грн на рік та окупиться лише за 2 дні.

ВИСНОВКИ

У дипломній роботі розроблені рекомендації щодо забезпечення безпеки даних тримачів карток для організацій, в інформаційній інфраструктурі яких зберігаються, обробляються або передаються дані платіжних карт.

В ході виконання поставлених у дипломній роботі задач були отримані наступні наукові та практичні результати:

– шляхом аналізу систем електронних платежів, способів шахрайства з платіжними картками, методів та засобів оцінювання ризиків безпеки інформації в системах електронної комерції, основних складових безпеки систем електронної комерції, підходів для процедури обробки платіжних карток, проаналізувавши методи боротьби з шахрайськими операціями, проаналізувавши вимоги міжнародного стандарту у сфері інформаційної безпеки даних індустрії платіжних карток PCI DSS та на основі вимог стандарту PCI DSS створені рекомендації щодо забезпечення безпеки даних тримачів карток для організацій, в інформаційній інфраструктурі яких зберігаються, обробляються або передаються дані платіжних карт;

– було обґрунтовано економічну доцільність створених рекомендацій шляхом розрахунку витрат на розробку та впровадження рекомендацій для підвищення рівня безпеки платіжних карток на прикладі організації Рівня 1 та було доведено, що їх застосування збереже від збитків у розмірі до 5 850 000 000 грн на рік та окупиться лише за 2 дні.

ПЕРЕЛІК ПОСИЛАНЬ

1. Укрінформ. Гібридна війна. [Електронний ресурс]. – Режим доступу: https://studopedia.com.ua/1_172503_osoblivosti-vikoristannya-bankivskih-kartok-virtualni-kartki.html.https://www.ukrinform.ua/rubric-polytics/2107122-gibridna-vijna-rosii-proti-ukraini-uroki-ta-visnovki.html.
2. Про Стратегію національної безпеки України : указ Президента України від 12.02.2007 р. № 105/2007 (із змінами від 8.06.2012 р. № 389/2012) [Електронний ресурс]. – Режим доступу: http:// zakon4.rada.gov.ua/laws/show/105/2007.
3. Кравець В. Розвиток платіжних систем в Україні та новітні форми розрахунків // Вісник НБУ. – жовтень, 2011. – с. 45-47
4. Закон України «Про платіжні системи і переказ коштів в Україні» [Елект-ронний ресурс] : Режим доступу : http://zakon2.rada.gov.ua/laws/show/2346-14
5. Н. О. Коваль, М. В. Борщ Особливості функціонування платіжних систем України на сучасному етапі їх розвитку [Електронний ресурс]: Режим доступу : http://www.economy.nayka.com.ua/?op=1&z=1441
6. Платіжна система України та стратегія її розвитку [Електронний ресурс]: Режим доступу : http://www.bestreferat.ru/referat-216752.html
7. Платіжні системи : [навч. пос.] / [О. Вовчак, Г. Шпаргало, Т. Андрейків]. – К. : Знання, 2008. – 341 с

8. Забезпечення безпеки даних карткових платіжних систем при проведенні платіжних операцій / Г. Іщук, А. Пелешенко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – № 2. – С. 106–111. – [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/Nzundiz_2014_2_20.

9. Платіжна система України [Електронний ресурс]. – Режим доступу : http://www.bank.gov.ua.

10. Про затвердження Положення про нагляд (оверсайт) платіжних систем та систем розрахунків в Україні : Постанова правління НБУ [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2346-14.

11. Про платіжні системи та переказ коштів в Україні : Закон України від 5 квітня 2001 року із змінами та доповненнями [Електронний ресурс]. – Режим доступу : http://zakon.rada. gov.ua/cgi-bin/laws/main.cgi?nreg=2346-14.

12. Заходи захисту інформаційної безпеки платіжних систем [Електронний ресурс]. – Режим доступу : https://pidruchniki.com/10810806/

13. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

14. Студопедія. Ваша школа [Електронний ресурс]. – Режим доступу: https://studopedia.com.ua/1_172509_virtualni-karti.html.

15. Операції банку з пластиковими картками школа [Електронний ресурс]. – Режим доступу: https://pidruchniki.com/1615032252650/

16. Особливості використання банківських карток [Електронний ресурс]. – Режим доступу: https://studopedia.com.ua/1_172503_osoblivosti-vikoristannya-bankivskih-kartok-virtualni-kartki.html.

17. Еволюція платіжних карт [Електронний ресурс]. – Режим доступу: https://evris.law/uk/fintech_platizhni_systemy.

18. Авакова Ю. М. Платіжні картки. Бізнес-енциклопедія / Ю. М. Авакова, Л. В. Бистров, А. С. Воронін [та ін.]. – Москва, «Маркет ДС». - 2008. 760 с. - ISBN 5-7958-0237-4.

19. Скіммінг. Загрози сьогодення [Електронний ресурс]. – Режим доступу: https://zillya.ua/ckiming-zagrozi-sogodennya.

20. Банкоматне шахрайство: Cash Trapping [Електронний ресурс]. – Режим доступу: https://investtalk.ru/kak-ne-stat-obmanuty-m/bankomatnoe-moshennichestvo-cash-trapping.

21. Соціальна інженерія // Сучасна західна соціологія: Словник. М., 2015.

22. Резник Ю.М. Соціальна інженерія: предметна область і межі застосування // Соціологічні дослідження, 1994, № 2.

23. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції Ó Берко А.Ю., Висоцька В.А., Рішняк І.В., 2008

24. Галіцин В.К., Левченко Ф.А. Багатокористувальницькі обчислювальні системи та мережі. – К.: КНЕУ, 1997.

25. Джерк Н. Разработка приложений для электронной коммерции. – СПб.: Питер, 2001.

26. Берко А.Ю., Висоцька В.А., Чирун Л.В. Алгоритми опрацювання інформаційних ресурсів в системах електронної комерції // Вісн. Нац. ун-ту “Львівська політехніка”. – 2004. – № 519. – С.10–20.

27. Берко А.Ю., Висоцька В.А. Проектування навігаційного графу web-сторінок бази даних систем електронної комерції // Вісн. Нац. ун-ту “Львівська політехніка”. – 2004. – № 521. – С.48–57.

28. Эймор Дэниел, Электронный бизнес. Эволюция и/или революция. – М.: Вильямс, 1999.

29. Верес О.М., Катренко А.В., Рішняк І.В., Чаплига В.М. Управління ризиками в проектній діяльності // Вісн. Нац. ун-ту “Львівська політехніка”. – 2003. – №489. – С.38–49.

30. Катренко А.В. Ситемний аналіз об’єктів та процесів комп’ютерізації. – Львів: “Новий світ – 2000”, 2003. –С. 286 – 322.

31. Катренко А.В. Системні аспекти розвитку архітектури підприємства // Вісн. Нац. ун-ту “Львівська політехніка”. – 2002. – №464. – С. 123–131.

32. Стандарт безопасности данных индустрии платежных карт [Електронний ресурс]. – Режим доступу: https://ru.pcisecuritystandards.org/_onelink_/pcisecurity/en2ru/minisite/en/docs/PCI_DSS_v3_2_RU-RU_Final.pdf

33. Авакова Ю. М. Проверка на соответствие стандарту [Електронний ресурс]. – Режим доступу: https://habr.com/company/payonline/blog/303330/

34. Стандарт ISO/IEC 7812 [Електронний ресурс]. – Режим доступу: http://files.stroyinf.ru/Data/604/60483.pdf

35. Правила и тарифы платежной системы VISA[Електронний ресурс]. – Режим доступу: https://www.visa.com.ru/visa-everywhere/about-visa/legislation.html

36. Правила и тарифы платежной системы MasterCard [Електронний ресурс]. – Режим доступу: https://www.mastercard.ru/ru-ru/about-mastercard/what-we-do/rules-fees.html

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	37	
6	А4	2 Розділ	27	
7	А4	3 Розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	4	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	2	

13	А4	Додаток Г	1	
14	А4	Додаток Ґ	1	

ДОДАТОК Б. Перелік файлів на електронному носії

1. Дипломний проект Сисоєва А.Д. 125м–17–1.docx – Пояснювальна записка.
2. Сисоєва А.Д.pttx – Презентація.

ДОДАТОК В. Терміни та визначення

Cardholder data – дані тримача картки.

CVV2 (англ. Card Verification Value 2) – тризначний код перевірки дійсності картки платіжної системи Visa. Інші платіжні системи мають схожі технології, наприклад, аналогічний код для карток MasterCard носить назву Card Validation Code 2 (CVC2). Наноситься на смузі для підпису держателя після номера картки або після останніх 4 цифр номера картки способом індент-друку. Використовується як захисний елемент при проведенні транзакцій в середовищі CNP (card not present).

Еквaєр – це банк або інша фінансова установа, що надає послуги еквайрингу, тобто, здійснює розрахунки з підприємствами, які приймають оплату від держателів платіжних карток за товари чи послуги або видають їм готівку.

Емітент – це банк, що випускає у обіг (емітує) грошові знаки або цінні папери і платіжно-розрахункові документи (банківські картки, чекові книжки).

Інформаційна безпека – це це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення.

Інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Конфіденці́йна інформація — це інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Доступ до такої інформації та її поширення можливі лише за згодою її власників (тобто тих, кого ця інформація безпосередньо стосується) та на тих умовах, які вони вкажуть. Відповідно до Ст. 21 ЗУ "Про інформацію" конфіденційна інформація разом із службовою та таємною інформацією належить до інформації з обмеженим доступом.

Мерчант – назва для широкої категорії фінансових послуг, призначених для використання у бізнесі.

Платіжна картка (payment card) – електронний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для ініціювання переказу коштів з рахунка платника або з відповідного рахунка банку з метою оплати вартості товарів і послуг, перерахування коштів зі своїх рахунків на рахунки інших осіб, отримання коштів у готівковій формі в касах банків через банківські автомати, а також здійснення інших операцій, передбачених відповідним договором.

Платіжна система — платіжна організація, члени платіжної системи та сукупність відносин, що виникають між ними при проведенні переказу

коштів. Проведення переказу коштів є обов'язковою функцією, що має виконувати платіжна система.

Процесинговий центр – це уповноважений платіжною системою спеціалізований обчислювальний центр, який забезпечує інформаційну та технологічну взаємодію між учасниками розрахунків. Процесинговий центр містить дані про членів платіжної системи, забезпечує обробку запитів на авторизацію, обробку протоколів транзакцій, які фіксують дані про зроблені за допомогою карток платежі і видачу готівки.

Токенізація – це технологія, що дозволяє убезпечити електронні платежі за допомогою системи шифрування даних, дозволяє здійснювати платежі не розголошуючи дані карти/рахунку користувача. Інформація про карту (номер карти/cvv-код і ін.) замінюється унікальними цифровими ідентифікаторами – токенами.

Транзакція – це будь-яка операція з використанням банківського рахунку.

ДОДАТОК Г. Відгук керівника економічного розділу

Керівник : _____ к.е.н., доц. Пілова Д.П.
(підпис)