Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет прикладних інформаційних технологій та електроінженерії
(назва факультету)
Кафедра комп'ютерно-інтегрованих технологій
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: Розробка комп'ютерно-інтегрованої системи для реалізації безпечних електронних платежів

Виконав: студент 4 курсу, групи КТ-41
Спеціальність *151*
"Автоматизазія та комп'ютерно-інтегровані технології"
(шифр і назва спеціальності)

(підпис) Блавіцький А.М. (прізвище та ініціали)

Керівник (підпис) Микитишин А.Г. (прізвище та ініціали)

Нормоконтроль (підпис) Чихіра І.В. (прізвище та ініціали)

Рецензент (підпис) Трембач Р.Б. (прізвище та ініціали)

Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)

Кафедра комп'ютерно-інтегрованих технологій
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Микитишин А.Г
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавра
(назва освітнього ступеня)

за спеціальністю 151 "Автоматизазія та комп'ютерно-інтегровані технології"
(шифр і назва спеціальності)

студенту Блавіцькому Андрію Михайловичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка комп'ютерно-інтегрованої системи для реалізації безпечних електронних платежів

Керівник роботи Микитишин Андрій Григорович, к.т.н., доцент, зав.каф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 7 » лютого 2023 року № 4/7-131

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи науково-технічна література

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналітична частина 1.1. Міжнародна організація зі стандартизації 1.2. Europay Mastercard Visa Consortium 1.3. Рада зі стандартів безпеки індустрії платіжних карток 1.4. Взаємодія EMVCo та PCI SSC 2. Проєктна частина 2.1. Структура платіжної картки 2.2. Платіжні канали 3.Спеціальна частина 3.1. Специфікації EMV 3.1.1. Контактна та безконтактна специфікація EMV 3.1.2. Методи аутентифікації 3.2. Стандарти PCI 3.2.1 Стандарт безпеки платіжних карток PCI-DSS 3.2.2. Шифрування PCI Point-to-Point Encryption 4.Безпека життєдіяльності, основи хорони праці. Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Гурик Олег Ярославович, к.т.н., доцент, доцент кафедри МТ		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.01.2023	*Виконано*
2.	Підбір джерел по темі дослідження	04.01.2023-30.01.2023	*Виконано*
3.	Переклад та опрацювання джерел по темі дослідження	31.01.2023-06.02.2023	*Виконано*
4.	Виконання дослідження щодо розробки комп'ютерно-	12.06.2023-	*Виконано*
	інтегрованої системи для реалізації безпечних платежів	13.06.2023	
5.	Оформлення розділу «Аналітична частина»	14.02.2023-	Виконано
		06.03.2023	
6	Оформлення розділу «Проєктна частина»	07.03.2023-	*Виконано*
		03.04.2023	
7.	Виконання завдання до підрозділу «Безпека	04.04.2023-	*Виконано*
	життєдіяльності»	17.04.2023	
8.	Виконання завдання до підрозділу «Основи хорони	18.04.2023-	*Виконано*
	праці»	01.05.2023	
9.	Оформлення кваліфікаційної роботи	02.05.2023-15.05.2023	*Виконано*
10.	Нормоконтроль	16.05.2023-22.05.2023	*Виконано*
11.	Перевірка на плагіат		*Виконано*
12.	Попередній захист кваліфікаційної роботи		*Виконано*
13.	Захист кваліфікаційної роботи		

Студент _____ Блавіцький А.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Микитишин А.Г.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

У даній кваліфікаційній роботі бакалавра здійснено аналіз науково-технічних публікацій по темі дослідження та здійснено компіляцію інформації про технології та стандарти платіжних карток, яка була зібрана та співставлена з різних офіційних документів.

Проведено детальний аналіз структурних елементів платіжної картки, який дозволив виділити десять елементів, які, за винятком двох, реалізують функцію захисту платіжної картки.

Вивчення життєвого циклу платіжної картки дозволило виявити щонайменше п'ять суб'єктів, які відіграють певну роль у платіжному процесі.

Детально описано механізми безпеки, які забезпечують технології та стандарти.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

LUK – ключ обмеженого використання;

MAC – код автентифікації повідомлення;

NFC – зв'язок ближньої дії;

nSCD – незахищений криптографічний пристрій;

P2PE – шифрування “точка-точка”;

PA-DSS – стандарт безпеки даних платіжних додатків;

PIN – персональний ідентифікаційний номер;

POI – точка взаємодії або картковий платіжний термінал;

PSP – провайдер платіжних рішень;

PTS – безпека PIN-транзакцій;

RReq – запит результатів;

SDA – статична автентифікація даних;

SUK – одноразовий ключ;

TLS – безпека транспортного рівня.

ЗМІСТ

ВСТУП

Сьогодні застарілі та недосконалі інформаційні технології все ще використовуються в операціях з платіжними картками. Для вирішення цієї ситуації важливо проаналізувати та оцінити розвиток безпеки електронних платіжних засобів, щоб зрозуміти, як покращилася безпека даних, що використовуються в платіжних операціях, з появою нових технологій.

Перш за все, важливо надати короткий вступ до індустрії платіжних карток, починаючи з поняття платіжних карток. Платіжні картки - це пластикові або металеві картки, які дозволяють держателю картки здійснювати платежі у торговельному закладі. Ця форма оплати відома як електронні платежі, і такі картки зараз широко використовуються в усьому світі і конкурують з готівковими платежами. Через їх широке розповсюдження в усьому світі злочинці постійно здійснюють атаки на платежі, які здійснюються за допомогою карток.

Ці атаки, у разі успіху, впливають на різних суб'єктів, що беруть участь у карткових платежах, включаючи, наприклад, власника картки, торговця та банк-емітент. Для власника картки злочинець, використовуючи зібрані в результаті атаки конфіденційні дані про рахунок, може здійснити вид шахрайства, який називається крадіжкою особистих даних, що має такі наслідки для власника картки, як, наприклад, зменшення загального залишку на рахунку до нуля, велика сума боргу та погіршення кредитного рейтингу.

Для продавця купівля злочинцем товару або послуги з використанням викраденої інформації платіжної картки призводить до ініційованого власником картки - повернення грошей власнику картки, в результаті чого торговець втрачає товар або послугу, продані шахраєві.

Для банку-емітента зловмисник може зняти гроші в банкоматі з використанням викраденої або клонованої платіжної картки, що призводить до відшкодування банком суми знятих грошей тримачу картки. Як наслідок, організації та фізичні особи, задіяні в індустрії платіжних карток, зазнають

значних збитків. Для протидії шахрайству основними брендами в індустрії платіжних карток було створено дві важливі організації, які встановлюють стандарти та технічні специфікації. Це Рада зі стандартів безпеки індустрії платіжних карток (Payment Card Industry Security Standards Council) та Консорціум Europay Mastercard Visa (Europay Mastercard Visa Consortium). Ці стандарти і технології відіграють вирішальну роль, вони забезпечують безпеку і правила захисту для всіх учасників процесу здійснення платіжних операцій.

Наразі існує багато джерел інформації, технічних документів та стандартів, які пояснюють різні елементи, процедури та вимоги щодо захисту даних, які використовуються в карткових платіжних операціях. Оскільки ці дані надходять з багатьох джерел, може бути складно зрозуміти, як технології та стандарти, задіяні в індустрії платіжних карток, забезпечують безпеку протягом життєвого циклу платіжної операції з використанням платіжної картки. Також може бути складно знайти кількісні показники для оцінки різних технологій та інструментів, які продавець може використовувати для дотримання стандартів безпеки даних в індустрії платіжних карток.

Після отримання картини поточного платежу важливо зрозуміти різні ролі, які кожна організація, залучена в цю галузь, повинна відігравати для забезпечення безпеки транзакцій. Ці установи визначають концепції, стандарти і технології, які при спільному використанні, безсумнівно, впливають на безпеку всього процесу.

Ще одним важливим моментом є розуміння структури платіжних карток. Це дуже важливо, тому що це вносить ясність щодо кількості елементів, якими володіє платіжна картка, а також цілей, які ці елементи виконують. Хоча не всі з цих елементів мають позитивний вплив на загальний життєвий цикл платіжної операції з використанням платіжної картки, ті елементи, вплив яких є негативним, все ж таки присутні, і вкрай важливо зрозуміти причини цього.

Для подальшого розуміння процесу здійснення платіжних операцій з використанням платіжних карток необхідно розуміти його життєвий цикл та

різні інституції, що беруть у ньому участь. Знання учасників та їхніх обов'язків допомагає отримати більш детальне уявлення про процес. Крім того, краще розуміння каналів, що використовуються для карткових платежів, і процесів, що в них відбуваються, дає чіткіше розуміння потоку карткових платежів.

Як зазначалося вище, існують різні інформаційні та комунікаційні технології та стандарти, які зазвичай використовуються для карткових платежів. Важливо розуміти ІКТ, задіяні в платіжному процесі, а також процедури, механізми безпеки та вимоги, які ці технології використовують для захисту платіжних каналів.

Стандарти є додатковим заходом безпеки, окрім технологій, що використовуються. Вкрай важливо дізнатися, від кого вимагається дотримання різних типів стандартів, цілі цих стандартів і різні інструменти, що використовуються для їх дотримання. Таким чином, стає зрозумілішим обсяг і відповідальність різних установ у забезпеченні безпеки при здійсненні платіжних операцій з використанням платіжних карток.

Нарешті, після збору та аналізу всієї попередньої інформації, важливо оцінити задіяні ІКТ в платіжному процесі. Оцінка забезпечує розуміння сильних і слабких сторін безпеки карткових платежів і дає відповіді на два конкретних питання.

Мета роботи описати та порівняти технології, які забезпечують безпеку даних, що використовуються в карткових платіжних операціях для різних платіжних каналів.

Завдання дослідження:

- провести порівняння і компіляцію інформації про технології та стандарти платіжних карток
- здійснити аналіз структурних елементів платіжної картки
- вивчити життєвого циклу платіжної картки.
- описати механізми безпеки та які технології та стандарти забезпечують ці механізми

Об’єкт дослідження – платіжна карта

1. Аналітична частина

1.1. Міжнародна організація зі стандартизації (ISO)

Перш ніж згадувати організації, що відповідають за електронні платежі, необхідно відзначити Міжнародну організацію зі стандартизації.

ISO визначає різні набори стандартів; два з них представляють особливий інтерес: ISO 24760 з безпеки та конфіденційності інформаційних технологій [5] та ISO 27000 з систем управління інформаційною безпекою [6]. Ці стандарти визначають наступні поняття, які є важливими для розуміння цього документу.

- Ідентифікація: Процес розпізнавання суб'єкта в певній предметній області як відмінного від інших суб'єктів.
- Автентифікація (автентифікація): Надання впевненості в тому, що заявлена характеристика особи є правильною.
- Авторизація: Процес надання привілеїв із зрозумілим рівнем довіри, встановленим заявленою ідентифікацією.

Вимоги та процедури для технологій і стандартів, що розглядаються в цій роботі, розроблені на основі вищезазначених ключових понять.

1.2. Europay Mastercard Visa Consortium (EMVCo)

EMVCo є професійною організацією, яка об'єднує всесвітньо визнані стандарти з метою сприяння розвитку інфраструктури для отримання послідовного, інтероперабельного та безпечного платіжного процесу. Крім того, EMVCo взаємодіє з Near Field Communication Forum, GlobalPlatform, Global Systems for Mobile Communications Association, PCI SSC, Французькою асоціацією безконтактних мобільних послуг, Азіатсько-Тихоокеанською асоціацією смарт-карт, Advance Card Technology Canada, Європейським інститутом телекомунікаційних стандартів, Європейською платіжною радою,

Fast Identity Online Alliance, Secure Technology Alliance, Платіжним форумом США та Консорціумом Всесвітньої павутини для отримання та обміну думками щодо сфер, які становлять спільний інтерес [7].

EMVCo класифікувала країни за регіонами для отримання статистики розгортання та прийняття чіпів Europay Mastercard Visa (EMV). ,

Специфікації EMVCo наведені нижче [7]:

- Специфікація контактного EMV
- Специфікація безконтактного EMV
- Специфікація мобільного EMV
- Специфікація токенізації платежів EMV
- Специфікація QR-коду EMV
- Специфікація EMV Secure Remote Commerce
- Специфікація EMV 2-го покоління
- Специфікація EMV Three Domain Secure (3DS)

1.3. Рада зі стандартів безпеки індустрії платіжних карток (PCI SSC)

PCI SSC - це глобальний форум, який очолює глобальні зусилля між організаціями, що зберігають, обробляють або передають конфіденційні дані держателів карток, з метою забезпечення безпеки даних.

Для правильного впровадження стандартів PCI SSC Рада надає такі інструменти, як оцінка та перевірка кваліфікації, навчання та освіта, програми сертифікації продукції та анкети самооцінки (SAQ) [9].

PCI SSC визначає наступний набір стандартів [10]:

- Стандарт безпеки даних індустрії платіжних карток (PCI) (DSS)
- Стандарт безпечного програмного забезпечення PCI
- Стандарт життєвого циклу безпечного програмного забезпечення PCI
- Стандарт безпеки даних платіжних додатків PCI (PA-DSS)
- Стандарт шифрування між точками (P2PE) PCI
- Стандарт PCI PIN Transaction Security (PTS) Апаратний модуль безпеки (HSM)

- Стандарт PCI PTS
- Стандарт PCI PTS Point of Interaction (POI)
- Стандарт логічної безпеки виробництва та надання карток PCI
- Стандарт фізичної безпеки виробництва та надання карток PCI

Стандарт базової безпеки PCI 3DS

- Стандарт PCI 3DS Software Development Kit (SDK)
- Стандарт безпеки персональних ідентифікаційних номерів (PIN) PCI
- Стандарт безпеки PIN-коду на основі програмного забезпечення PCI для комерційних готових виробів (COTS)
- Стандарт безпеки програмного введення PIN-коду на основі тестування COTS
- Стандарт безпеки постачальників послуг токенів PCI (TSP)

1.4. Взаємодія EMVCo та PCI SSC

EMVCo та PCI SSC співпрацюють з метою підвищення безпеки даних та зниження рівня шахрайства. Для досягнення цих цілей EMVCo за допомогою свого чіпа EMV зберігає конфіденційні дані держателя картки в зашифрованому вигляді, тоді як стандарти PCI визначають процедури, що забезпечують безпеку даних протягом усього процесу транзакції, як це детально описано в [11].

У 2017 році EMVCo та PCI SSC розпочали безпосередню співпрацю для підтримки запуску 3DS версії 2.0. Роль EMVCo полягала в наданні специфікації EMV 3DS 2.0, тоді як мета PCI SSC полягала в забезпеченні вимог безпеки, процедур тестування, навчання асесорів та шаблонів звітності для вирішення специфікації 3DS 2.0 [12].

2. Проєктна частина

2.1. Структура платіжної картки

Платіжні картки мають вбудовані в пластик або метал різні елементи. Кожен з цих елементів відіграє певну роль у процесі здійснення платіжної операції, і їх можна побачити на рисунку 2.1 [13]:

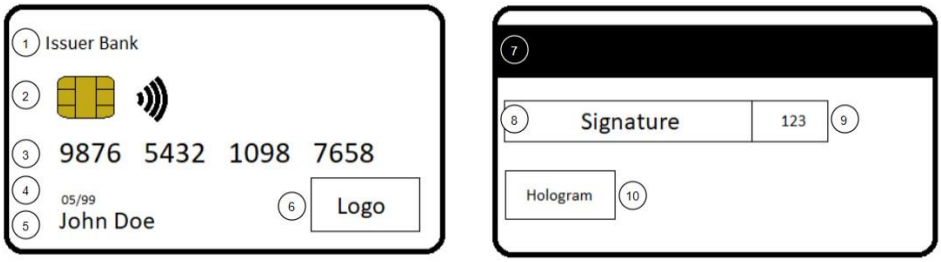

Рисунок. 2.1 – Структура платіжних карток

1. Назва банку-емітента
2. EMV-чіп
3. Номер основного рахунку (PAN)
4. Термін дії
5. Ім'я власника картки
6. Логотип карткової мережі
7. Магнітна смуга (MS)
8. Підпис держателя картки
9. Контрольний номер картки (CVV)
10. Захисна голограма

2.1.1. Банк-емітент

Банки-емітенти - це фінансові установи, які пропонують платіжні картки, надають кредитні ліміти кваліфікованим споживачам [14] та забезпечують фінансову підтримку продавцям за операціями, здійсненими за допомогою емітованих платіжних карток.

Для кредитних карток банк-емітент бере на себе зобов'язання щодо спроможності власників карток сплачувати свій борг при використанні кредитних карток. Для дебетових карток банк-емітент використовує залишок коштів на рахунку держателя для оплати покупок, здійснених за допомогою дебетових карток

2.1.2. EMV-чіп

Специфікації EMV Contact та Contactless відносяться до форми зв'язку між картою інтегральної схеми (ICC) та пристроєм POI, що виконує пристрій. Для EMV Contact, ICC і POI повинні вступати в фізичний контакт [15], в той час як в EMV Contactless, ICC і POI використовують зв'язок ближнього поля.

Структура платіжної картки (NFC) і повинні знаходитися на достатній відстані [16] (див. рис. 2.2).

Чіп EMV підвищує безпеку в сценаріях "картка-присутність" (CP) завдяки наступним функціям, які зменшують шахрайство з підробленими, втраченими та викраденими картками [17]:

-Аутентифікація чіпової картки: Виконується POI для того, щоб відрізнити справжні картки від підроблених або викрадених.

-Параметри управління ризиками: Емітент визначає умови, за яких здійснювати операції в режимі офлайн або онлайн.

-Цілісність транзакції: Це результат цифрового підпису платіжних даних.

-Надійні методи верифікації власника картки: Допомагають захиститися від шахрайства з втраченими та викраденими картками.

Чіп використовує різні криптографічні функції для зберігання конфіденційних даних власника картки [18].

Рисунок 2.2 – Контактний та безконтактний зв'язок між ICC та POI

Згідно зі звітом EMVCo за 2018 рік, половина платіжних карток, випущених у світі, є платіжними картками на основі EMV-чіпа [19].

2.1.3. Основний номер рахунку (PAN)

PAN ідентифікує платіжну картку та використовується банком-емітентом для визначення походження або призначення транзакції. Структура PAN є наступною [20]:

-Перші шість цифр ідентифікують карткову мережу. Ці цифри відомі як ідентифікаційний номер емітента (IIN) або ідентифікаційний номер банку, і містять в якості першої цифри ідентифікатор основної галузі. MII ідентифікує галузь, до якої належить емітент платіжної картки.

Остання цифра - контрольна цифра, яка використовується для перевірки правильності передачі ПІН під час здійснення платіжної операції з використанням картки.

Аналіз та оцінка розвитку безпеки електронних платіжних засобів

-Цифри між IIN та контрольною цифрою ідентифікують рахунок власника картки.

Для визначення контрольної цифри використовується алгоритм Луна [21]. На рисунку 2.3 показано його процедуру з подальшим поясненням.

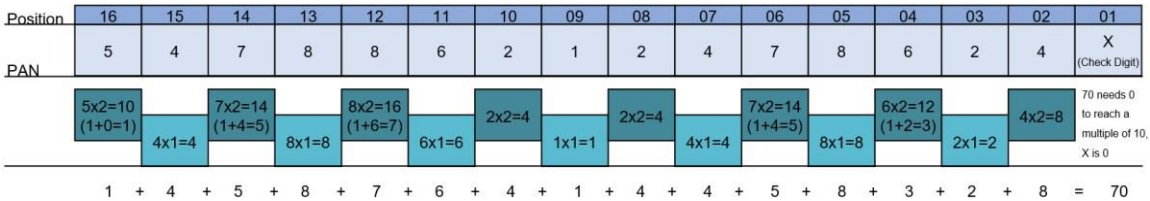

Рисунок 2.3 – Процес роботи алгоритму Луна

1. Пронумеруйте кожну цифру справа наліво.

2. Для парних позицій помножте на 2, а для непарних - на 1.

Якщо в результаті множення вийшло двозначне число, складіть цифри разом.

3. Складіть всі результати, отримані з кроку 2, разом.

4. Контрольна цифра - це різниця між результатом з кроку 3 та найближчим кратним 10.

ПІН-код - це конфіденційна інформація, що зберігається на платіжній картці. Для його захисту PCI DSS визначив максимальну кількість цифр, які можуть відображатися на дисплеї, щоб не скомпрометувати держателя картки.

2.1.4. Термін дії, ім'я тримача та мережа карток

Дата закінчення терміну дії дозволяє емітентам своєчасно замінювати картки та оновлювати технологію своїх EMV-чіпів. Він також використовується для запобігання шахрайству в платіжному каналі CNP, оскільки без дати закінчення терміну дії PAN не може бути використаний [22].

Ім'я держателя картки - це особа, уповноважена банком-емітентом використовувати платіжну картку. Користуватися платіжною карткою можуть лише уповноважені фізичні особи, а на платіжному каналі CP торговець зобов'язаний запитати документ, що посвідчує особу, перед початком процесу здійснення операції з платіжною карткою [23] під час використання МПС платіжної картки.

Логотип карткової мережі використовується для ідентифікації мережі платіжної картки. Ці карткові мережі виступають в якості підтримки для таких установ, як еквайри та емітенти з їх відповідними клієнтами. Ці установи є впізнаваними брендами, які відповідають за забезпечення правильної обробки транзакцій, встановлення керівних принципів та кваліфікаційних вимог для своїх установ-членів, а також виступають посередниками у вирішенні спорів між сторонами, що беруть участь у процесі транзакції [24].

2.1.5. Магнітна смуга (МС)

МС містить конфіденційну інформацію про власника картки, яка зберігається в магнітних полях смуги у вигляді відкритого тексту. Ця смуга є пасивним елементом, який все ще використовується для забезпечення сумісності із застарілими моделями POI, і активується при проведенні через POI . Див. рисунок 2.4.

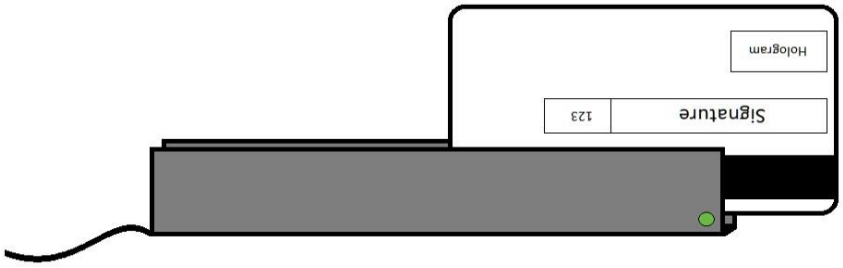

Рисунок 2.4 – Картка MS та зчитувальний пристрій

Ця смуга містить три інформаційні доріжки. Перша та друга доріжки містять PAN-код та ім'я держателя картки, дату закінчення терміну дії картки та код країни, а третя доріжка зберігає додаткову інформацію. Кожна доріжка також включає в себе поздовжню перевірку надмірності (LRC), яка використовується для контролю помилок під час передачі даних з цієї доріжки.

Зловмисники можуть націлюватися на магнітні стрічки та клонувати їх, оскільки вони містять статичну інформацію, їх легко виготовити та закодувати. Клонування вимагає стороннього електронного пристрою для сканування картки перед вставленням в POI. Такий пристрій записує збережену інформацію з МПС, потім переносить дані на нову картку або переписує їх на викрадену картку.

Європейський центральний банк у своєму резюме за 2018 рік вказує на зменшення шахрайства з боку POS-систем та банкоматів завдяки високому рівню впровадження EMV-чіпів у POI, використанню гео-блокування та посиленню заходів безпеки.

2.1.6. Підпис тримача картки

Ця функція наразі не використовується торговцями. Ідея цієї функції полягала в тому, щоб звірити підпис на платіжній картці з посвідченням особи або водійським посвідченням для підтвердження особи власника картки. З появою більш надійних механізмів верифікації підпис держателя став застарілим заходом безпеки для платіжних карток. Як наслідок, з квітня 2018 року підпис держателя картки більше не вимагається та не використовується платіжними системами American Express, Discover, Mastercard та Visa.

2.1.7. Контрольний номер картки (CVV)

CVV - це три- або чотиризначний код безпеки, який використовується банком-емітентом для перевірки платіжної картки. CVV розвивався та вдосконалювався з плином часу. Його перша версія, CVV1, була закодована в MC картки. Друга версія, CVV2, використовується в сценаріях CNP. Для генерації CVV2 банк-емітент використовує секретні ключі шифрування для шифрування PAN та терміну дії картки.

2.1.8. Захисна голограма

Голограми на платіжних картках є ще одним механізмом захисту, який забезпечує більш безпечну обробку платежів у торговельно-сервісній точці. Працівник торгового терміналу перевіряє наявність захисної голограми. Якщо вона є, то це підтверджує, що пред'явлена картка є дійсною платіжною карткою. Якщо ж вона відсутня, то це свідчить про те, що пред'явлена картка може бути підробленою.

Основне призначення захисних голограм - унеможливити підробку або, принаймні, ускладнити її. Голограми не можна відсканувати або скопіювати на ксероксі, вони мають приховані зображення або текст, розміщені в них для забезпечення негайної автентифікації та перевірки. Захисні голограми мають багато функцій, включаючи приховані зображення, що зчитуються лазером, кінетичні зображення, мікротексти, нанотексти, приховані зображення, гільйошні візерунки (див. рис. 2.5).

Рисунок 2.5 – Приклад захисної голограми

-Приховані зображення, що зчитуються лазером: Генеруються матричними принтерами і перевіряються лазером.

-Кінетичні зображення: Зміна кута спостереження дає ілюзію руху.

-Мікротексти: Текст, вбудований в голограми розміром від 50 до 150 мікрометрів.

-Нанотексти: Текст, вбудований в голограми, перевірений за допомогою мікроскопа, і з розміром менше 50 мікрометрів.

Структура платіжної картки 13

-Приховані зображення: Тонкі лінії та контури з'являються при розгляді під певним кутом.

-Гільйошні візерунки: Набір складних геометричних візерунків, які намальовані з високою роздільною здатністю і відрізняються за кольором на кожній лінії.

2.2. Платіжні канали

Платіжні канали - це форми, в яких торговець приймає платежі від клієнта. Існує два типи платіжних каналів: CP та CNP.

2.2.1. Життєвий цикл платежу

Для більш повного розуміння теми, що розглядається в цій дипломній роботі, необхідно розглянути життєвий цикл платіжного процесу та суб'єктів, що беруть у ньому участь (див. рис. 2.6).

Рисунок 2.6 – Життєвий цикл платіжного процесу

Нижче наведено визначення різних залучених суб'єктів:

-Держатель картки: Держатель картки - це особа, якій банк-емітент видає платіжну картку; іншими словами, це власник платіжної картки.

-Торговець: Торговець - це будь-яка особа, яка прийняла платіжну картку як форму оплати за свої товари або послуги.

-Провайдер платіжних рішень (PSP): Також відомий як платіжна мережа, PSP є організацією, відповідальною за зв'язок торговця з різними банками-еквайрами та картковими мережами.

Банк-емітент: Банк-емітент - це фінансова установа, яка випускає платіжні картки та пропонує інші послуги своїм споживачам .

Банк-еквайр: Банк-еквайр - це фінансова установа, яка за дорученням торговця обробляє платежі, здійснені за допомогою платіжних карток.

Необхідно визначити елементи, які використовуються для обробки платіжних операцій:

-ICC: Пластикова картка з вбудованою мікросхемою, що використовується для контролю доступу до ресурсу або послуги.

-POI: Апаратний компонент, який дозволяє здійснювати покупки за допомогою платіжних карток.

-POS: Місце, де клієнт ініціалізує платіж карткою.

Іншим терміном, який часто використовується в цьому документі, є ПІН-код, який є ідентифікаційним номером, присвоєним емітентом держателю картки, і який використовується для аутентифікації держателя картки перед здійсненням транзакції в каналі МПС.

2.2.2. Присутня картка (CP)

Транзакція CP відбувається, коли держатель картки фізично присутній у торговельному підприємстві. Цей тип платіжного каналу використовує технології MS або EMV-чіп для запуску платіжного процесу. У каналі CP EMV використовує різні методи верифікації держателя картки.

На рисунку 2.7представлено загальний вигляд каналу CP.

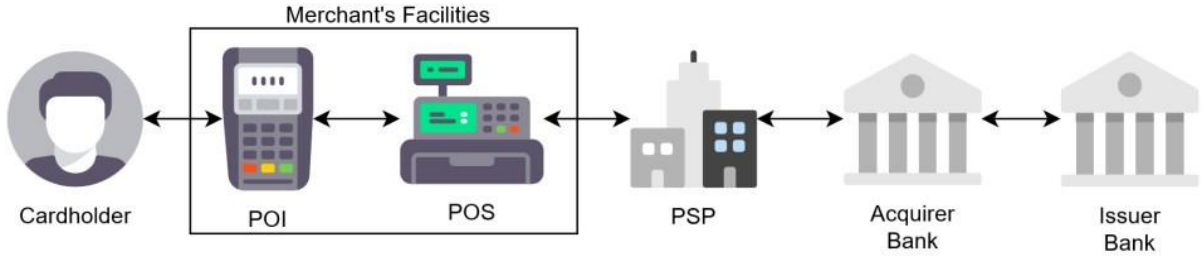

Рисунок 2.7 – Канал пред'явлення картки

2.2.3. Відсутність картки (Card-Not-Present, CNP)

Операція CNP відбувається, коли держатель картки фізично не присутній у торгово-сервісному підприємстві. CNP-транзакція може бути

здійснена через додаток або веб-сайт торговця або за допомогою поштового замовлення та замовлення по телефону (MOTO). Схема цього каналу представлена на рис. 2.8.

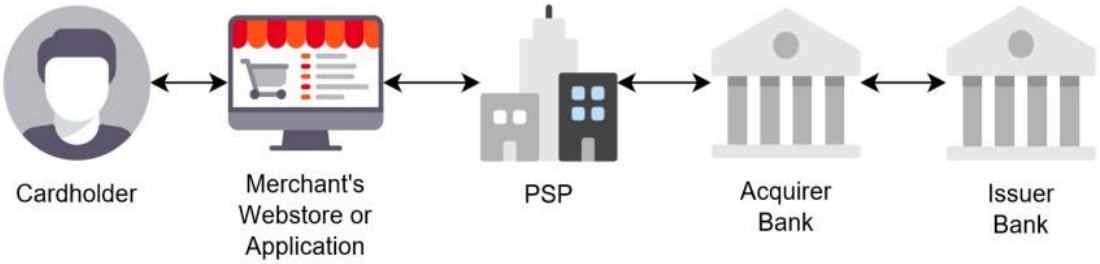

Рисунок 2.8 – Канал відсутності картки

Ці типи платіжних каналів є більш вразливими до шахрайства через фізичну відсутність держателя картки під час здійснення транзакції та складність чіткої аутентифікації законного держателя картки.

3 Спеціальна частина

Як показано на Рисунку 3.1, EMVCo та PCI SSC визначили різні специфікації та стандарти для забезпечення безпеки процесу платіжних операцій

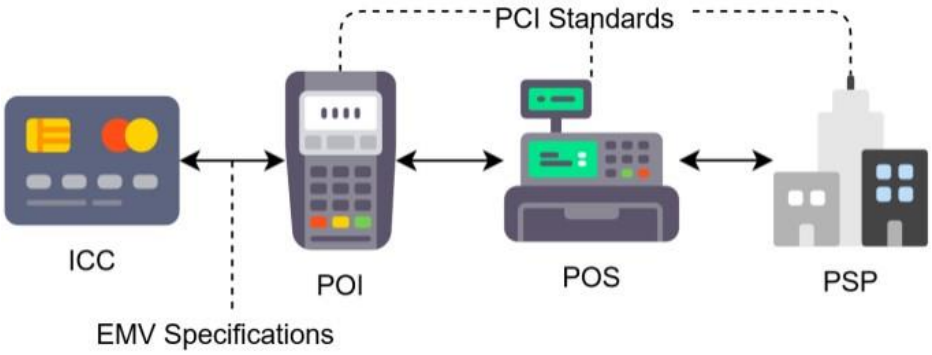

Рисунок 3.1 – Сфера застосування стандартів у процесі здійснення операцій

3.1. Специфікації EMV

Як зазначалося раніше, специфікації EMVCo спрямовані на досягнення інтероперабельності шляхом визначення вимог та забезпечення безпечних платежів. З цією метою в цьому розділі розглядаються наступні специфікації EMV:

-специфікації контактної та безконтактної EMV - специфікація EMV 3DS версії 2.0

-специфікація токенізації платежів EMV

3.1.1 Контактна та безконтактна специфікація EMV

Основною метою є забезпечення безпеки платіжних транзакцій в каналі CP, ініціалізованих контактною або безконтактною взаємодією між МПС та POI. У безконтактній специфікації платіжні бренди визначають свою процедуру, в той час як в контактній специфікації EMV визначила процес, показаний на рисунку 3.2

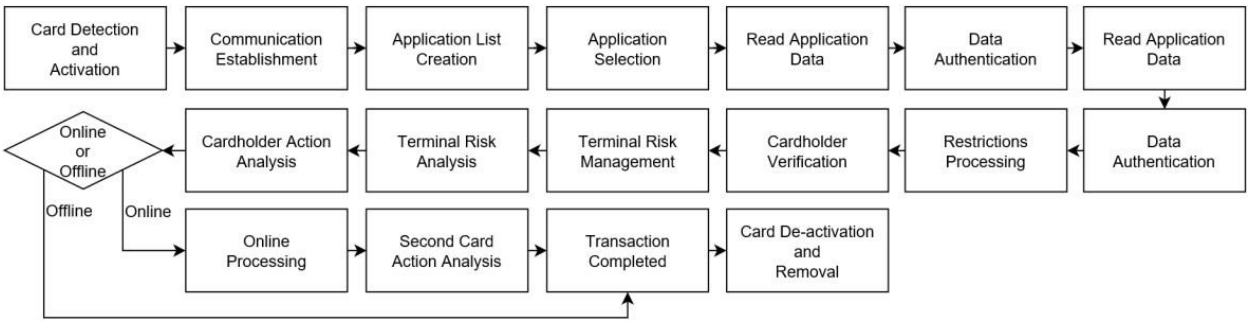

Рисунок 3.2 – Процес контактної транзакції EMV

Крім того, чіп EMV вводить код автентифікації повідомлення (MAC), щоб банки-емітенти могли перевірити цілісність та автентичність переданих повідомлень.

Для забезпечення автентичності платіжної картки EMV-чіп виконує автентифікацію даних, як показано на рисунку 4.2, яка досягається одним із таких способів:

-статична автентифікація даних (SDA)

-динамічна автентифікація даних (DDA)

-комбінованої динамічної автентифікації даних (CDA)

3.1.2 Методи аутентифікації

Для забезпечення автентичності платіжної картки EMV-чіп виконує автентифікацію даних, як показано на рисунку 3.2, яка досягається одним із таких способів:

-статична автентифікація даних (SDA)

-динамічна автентифікація даних (DDA)

-комбінованої динамічної автентифікації даних (CDA)

SDA не залежить від фактичної транзакції, що робить її вразливою до атак повторного відтворення, які відбуваються, коли передані дані зловмисно затримуються або повторно передаються. Процедура SDA показана на рисунку 3.3 з подальшим поясненням.

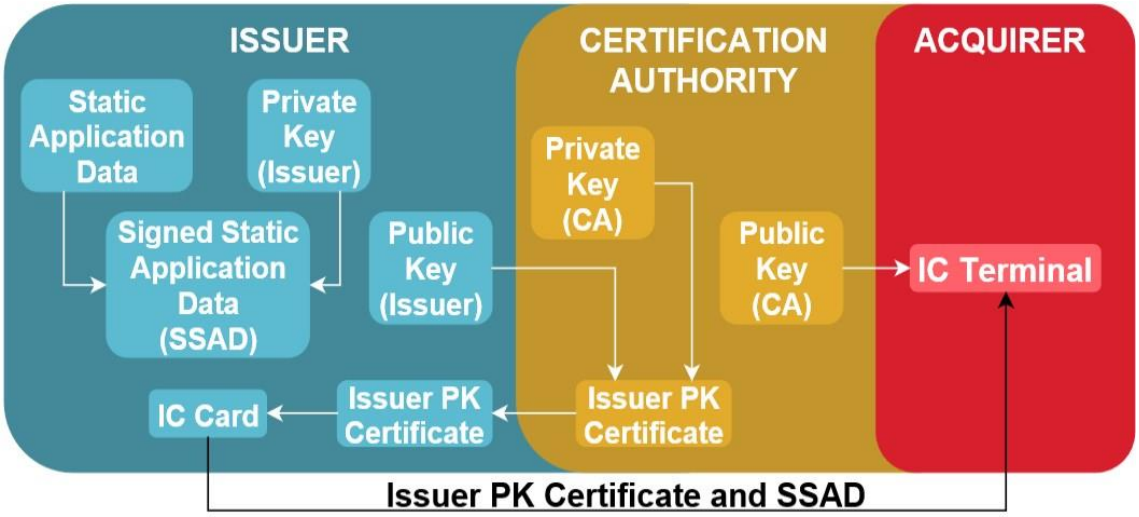

Рисунок 3.3 – Процедура статичної автентифікації даних

Видача МТП:

1. Емітент генерує пару ключів, потім зберігає закритий ключ в ICC та надсилає відкритий ключ у складі запиту на підписання сертифіката (CSR) до центру сертифікації ключів (ЦСК).

2. ЦСК підписує та надсилає назад отриманий CSR, створюючи сертифікат для емітента. Потім емітент зберігає сертифікат в ICC.

Процес оплати:

1. МТП підписує збережені статичні дані програми за допомогою закритого ключа емітента. Це створює підписані статичні дані додатку (SSAD), які ICC передає разом з сертифікатом емітента до POI.

2. POI перевіряє підпис ЦСК на сертифікаті емітента за допомогою відкритого ключа ЦСК.

3. Нарешті, POI перевіряє отриманий SSAD за допомогою відкритого ключа емітента, витягнутого з сертифіката емітента

На відміну від SDA, DDA запобігає атакам повторного відтворення, хоча і є чутливою до атак "людина посередині" (MITM), спрямованих на зв'язок між ЦСК та POI. Процедура його роботи показана на рисунку 3.4 з подальшим поясненням.

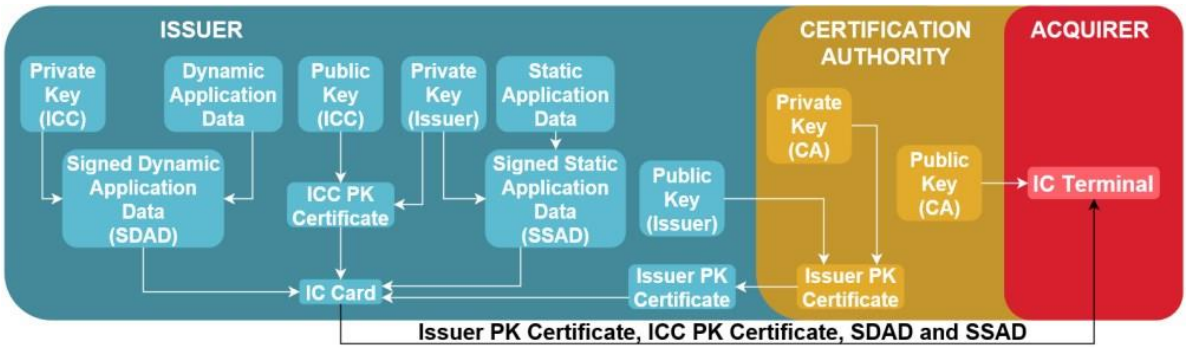

Рисунок 3.4 – Процедура динамічної автентифікації даних

Видача МТП:

1. Емітент генерує пару ключів, потім зберігає закритий ключ у МЦСК, а відкритий ключ надсилає у складі ЦСК до АЦСК.

2. Засвідчувальний центр підписує та надсилає назад отримані CSR, створюючи сертифікат для емітента. Потім емітент зберігає сертифікат в ICC.

3. Емітент генерує пару ключів для ICC, потім зберігає приватний ключ в ICC та формує CSR з відкритим ключем.

4. Емітент підписує CSR, створюючи сертифікат, а потім зберігає сертифікат в ICC.

Процес оплати:

1. МТП формує файл SSAD.

2. МТП підписує динамічні дані додатку (SDAD), використовуючи свій приватний ключ. Ці динамічні дані додатку є випадковим числом, яке генерується терміналом для кожної нової EMV-транзакції.

3. Під час комунікації з POI ICC надсилає сертифікати емітента та ICC, SSAD та SDAD.

4. POI перевіряє сертифікат емітента за допомогою відкритого ключа ЦСК.

5. POI перевіряє SSAD за допомогою відкритого ключа емітента, витягнутого з сертифіката емітента.

6. POI перевіряє сертифікат ICC за допомогою відкритого ключа емітента, витягнутого з сертифіката емітента.

7. Нарешті, POI звіряє SDAD з відкритим ключем ICC, витягнутим із сертифіката ICC.

Динамічні дані складаються з даних, що генеруються або зберігаються в ICC, та динамічного номера. Цей динамічний номер є змінним у часі параметром, що генерується ICC.

Комбінована динамічна автентифікація даних. На додаток до кроків DDA, ICC використовує другий динамічний підпис, який містить рішення ICC про поточну транзакцію, яку POI повинен перевірити, таким чином запобігаючи MITM-атакам.

Крім того, CDA має опцію шифрування PIN-коду, яка використовує додаткову пару ключів, пов'язану виключно з шифруванням PIN-коду. POI використовує відкритий ключ для шифрування PIN-коду, тоді як ICC використовує закритий ключ для перевірки PIN-коду.

Методи верифікації держателя картки (CVM). Чіп EMV використовує декілька CVM, як показано на Рисунку 4.2 розділу 4.1.1, для перевірки особи держателя картки:

-Офлайн-обробка ПІН-коду -Онлайн-обробка ПІН-коду -Обробка підпису -Комбіновані CVM

-метод верифікації держателя картки за допомогою споживчого пристрою (CD-CVM)

Офлайн обробка ПІН-коду. Офлайн обробка ПІН-коду використовується тільки у випадку, якщо не працює онлайн обробка ПІН-коду. Процедура пояснюється нижче та зображена на рисунку 3.5:

1. Держатель картки вводить PIN-код у POI.

2. POI передає PIN-код до ICC у відкритому або зашифрованому вигляді.

3. МЦК порівнює отриманий ПІН-код зі своїм ПІН-кодом, що зберігається в пам'яті.

4. ICC надсилає POI відповідь "так" або "ні" в залежності від результату порівняння.

5. ТСЦ показує держателю картки результати перевірки ПІН-коду.

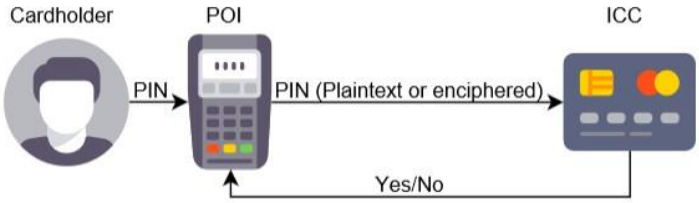

Рисунок 3.5 – Процедура отримання PIN-коду в режимі офлайн

Обробка ПІН-коду в режимі онлайн. Процедура введення ПІН-коду в режимі онлайн пояснюється нижче та зображена на рисунку 3.6:

1. Держатель картки вводить PIN-код у POI.

2. POI надсилає PSP PIN-код разом з PAN-кодом та іншими конфіденційними даними.

3. ПСП передає отриману інформацію банку-еквайру.

4. Банк-еквайр перевіряє ІІН для передачі отриманої інформації відповідному банку-емітенту.

5. Банк-емітент отримує передану інформацію та перевіряє ПІН.

6. Емітент надсилає назад до POI відповідь "так" або "ні" в залежності від результатів перевірки. Результати перевірки ПІН проходять через банк-еквайр та ПТКС.

7. Точка обслуговування показує держателю картки результати перевірки ПІН-коду.

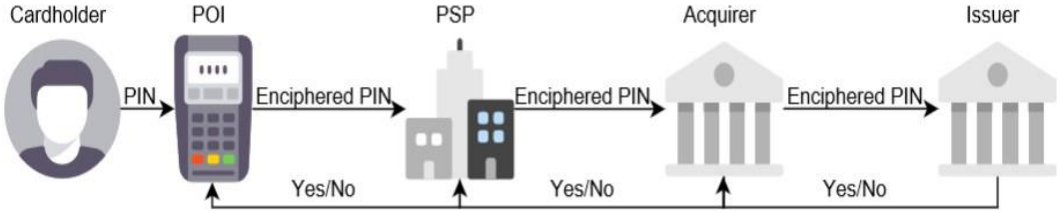

Рисунок 3.6 – Процедура введення PIN-коду онлайн

Обробка підпису та комбіновані БПК. POI виконує обробку підпису, яка завершує процес верифікації держателя картки. У комбінованих CVM має бути успішно завершено декілька CVM.

CVM для споживчих пристроїв. Цей тип CVM використовується для мобільних платежів, і його основним завданням є перевірка особи, яка пред'являє споживчий пристрій (CD). Для цього в даному методі використовуються аутентифікатори платформи та додатки, що покладаються на неї.

-Платформні аутентифікатори: Механізми, що надаються базовим пристроєм, які використовуються споживачем для розблокування пристрою за допомогою, наприклад, кодів, паролів, розпізнавання обличчя або відбитків пальців.

-Додатки, що покладаються: Програми для пристроїв, які потребують інформації про автентифікацію споживача.

Існує три рівні оцінки, що використовуються в рішеннях CD-CVM:

-Рівень пристрою: Захоплює дані аутентифікації за допомогою аутентифікаторів платформи і відправляє ці дані в додаток, що покладається.

-Рівень операційної системи: Реалізує механізми аутентифікації за допомогою інтерфейсів прикладного програмування.

-Рівень додатків: Покладається на функції безпеки, що надаються пристроєм та мобільним додатком.

3.1.3. EMV Three Domain Secure 2.0 (3DS 2.0)

EMVCo спроектувала, розробила та стандартизувала 3DS (див. розділ 1.4) для каналу CNP на заміну CVV2, який вважався незахищеним методом автентифікації

Версія 2.0 EMV 3DS була розроблена для вирішення проблем EMV 3DS 1.0, які включали відсутність підтримки додатків, відмінних від веб-

браузерів, складний процес оплати та вразливість до фішингу та MITM-атак.

Ця специфікація включає три домени: домен еквайра, домен інтероперабельності та домен емітента. Домен еквайра збирає інформацію про власників карток. Потім домен інтероперабельності передає інформацію між доменом еквайра та доменом емітента. Нарешті, домен емітента виконує верифікацію та аутентифікацію власника картки.

EMV 3DS 2.0 визначає три випадки ініціалізації аутентифікації:

-На основі додатку: CD використовує додаток-запитувач 3DS, інтегрований з 3DS SDK, щоб ініціювати транзакцію.

-На основі браузера: Компакт-диск за допомогою браузера отримує доступ до веб-сайту для ініціалізації транзакції.

3DS-запитувач: Запитувач 3DS ініціалізує підтвердження інформації про рахунок та автентифікацію держателя картки.

Для забезпечення безпеки платежів існують наступні вимоги.

Для зв'язків між елементами 3DS вимогами є методи взаємної автентифікації та протокол безпеки зв'язку транспортного рівня.

Для функцій безпеки каналу автентифікації на основі додатків вимогами є автентифікація додатка-запитувача 3DS, шифрування даних 3DS SDK та метод Діффі-Хеллмана, який є методом безпечного обміну криптографічними ключами по ненадійному каналу.

Потоки автентифікації. Існує два типи потоків автентифікації, що використовуються в 3DS 2.0 - без тертя та з викликом, як показано на рисунках 3.7 та 3.8. Різні типи повідомлень, що використовуються цими двома потоками автентифікації,.

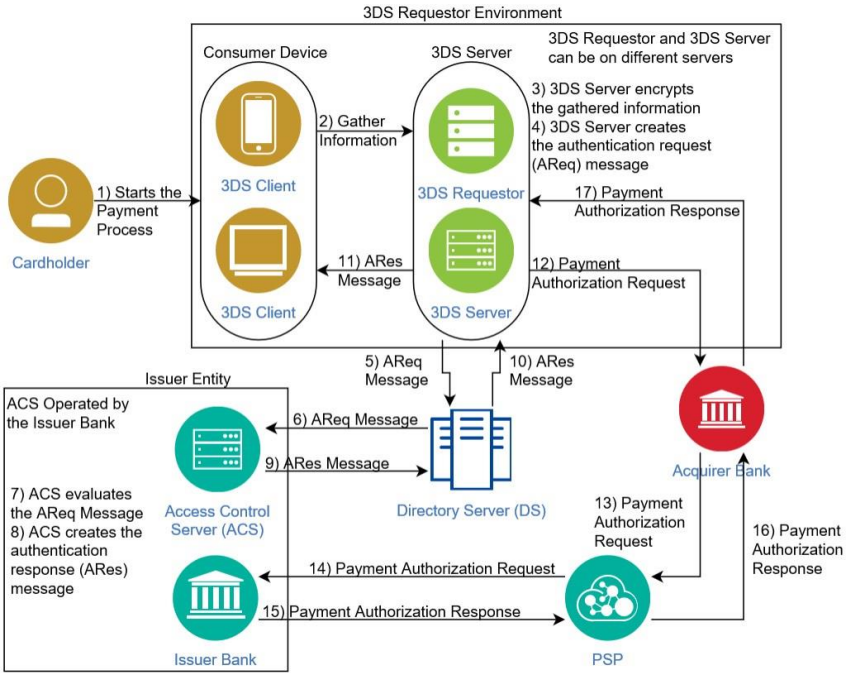

Рисунок 3.7 – Потік безконтактної автентифікації

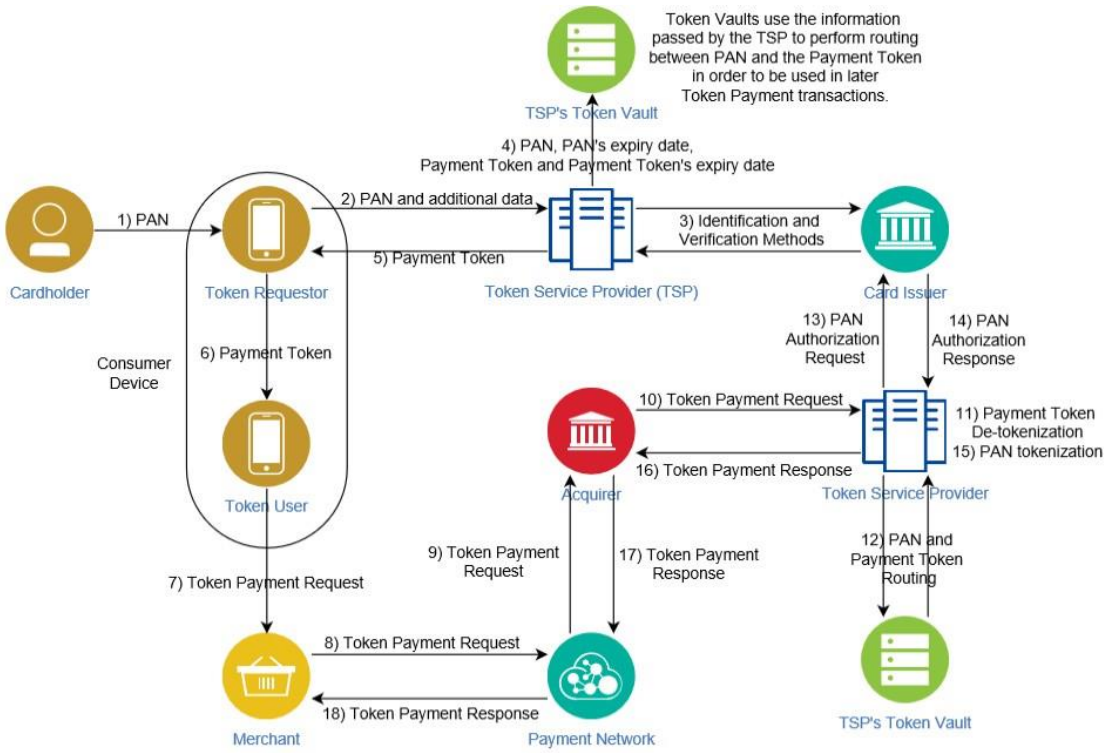

Рисунок 3.8 – Потік виклику автентифікації

3.1.4.Токенізація платежів EMV

Специфікація токенізації платежів EMV використовується в каналах CP та CNP. Ця специфікація спрямована на зменшення ризиків та шахрайства. Процедуру її виконання можна побачити на рисунку 3.9. Кожен згенерований токен є специфічним для комбінації PAN держателя картки, запитувача токену та початково визначеного середовища. Таким чином, PAN держателя картки може мати декілька токенів, пов'язаних з ним. Для дотримання регуляторних вимог та аналізу ризиків кожен токен може бути пов'язаний з ПІН-кодом за допомогою посилання на платіжний рахунок.

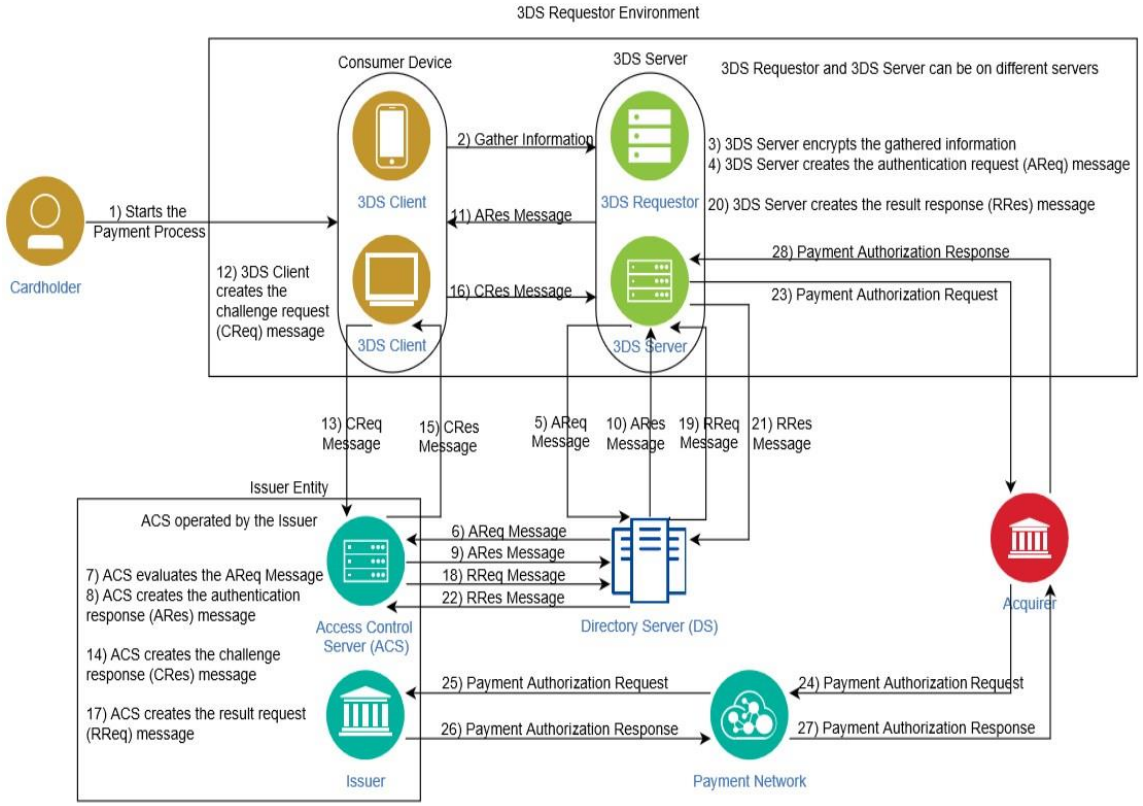

Рисунок 3.9 – Процедура токенізації

3.1.5 Методи ідентифікації та верифікації (ID&V)

Методи ідентифікації та верифікації використовуються для аутентифікації держателя картки перед випуском платіжного токена.

Для кращого розуміння методів верифікації держателя картки, передбачених специфікацією платіжних токенів EMV, важливо визначити

термін "фактор аутентифікації". Фактор автентифікації - це процедура або частина інформації, що використовується для перевірки автентичності особи. Такими факторами автентифікації є щось-ви-знаєте, щось-ви-є або щось-ви-маєте.

-Щось, ким ти є: Цей фактор автентифікації спрямований на автентифікацію притаманних особі рис, що може бути досягнуто за допомогою, наприклад, біометричних даних, малюнка райдужної оболонки ока або відбитків пальців.

-Щось, що ви знаєте: Цей фактор автентифікації спрямований на автентифікацію відомої особі інформації, яка може бути, наприклад, паролем або ім'ям користувача.

Токенізація використовує різні методи верифікації держателя картки. Ця специфікація також використовує 3DS 2.0.

-Ризик-орієнтована неінтерактивна автентифікація держателя картки: Виконує ризик-орієнтовану оцінку з використанням даних, що зберігаються та надаються запитувачем токенів.

-Автентифікація, що підтверджується емітентом картки: Емітент картки запевняє, що затверджений ним метод аутентифікації є достатнім.

-перевірка рахунку емітента картки: Емітент здійснює перевірку рахунку.

-Однофакторна автентифікація: Використовується лише фактор автентифікації "щось ти знаєш" або "щось ти маєш".

-Двофакторна аутентифікація: Використовує два з трьох типів аутентифікації, а саме: "щось ти знаєш", "щось ти є" або "щось ти маєш".

3.1.6 Варіанти використання

Сервіси Google Pay та Apple Pay використовують токенізацію для більш безпечного проведення платежів.

У випадку з Google Pay, на компакт-диску держателя картки закріплений токен, на якому зберігається ключ шифрування. Цей ключ

шифрування розшифровує ключі обмеженого використання (LUK) та одноразові ключі (SUK). Нарешті, TSP використовує LUKs та SUKs для зв'язування токену з PAN власника картки та для перевірки токену.

Поряд з токенізацією, для Google Pay також використовується емуляція хост-картки (HCE). HCE - це технологія, що використовується для емуляції платіжної картки, яка може взаємодіяти з POI через NFC-чіп. Оскільки хост-пристрій не є безпечним, HCE використовує різні платіжні дані для кожної транзакції та криптограми транзакцій.

Для Apple Pay на компакт-диску власника картки призначається токен, а захищений елемент компакт-диска зберігає цей токен біля мікросхеми NFC. Потім токен, ключ токена, сума транзакції та інша необхідна інформація використовуються для генерації динамічної криптограми після кожної транзакції. Нарешті, TSP використовує токен для перевірки токена всередині динамічної криптограми.

3.2. Стандарти PCI

Як зазначалося, стандарти PCI встановлюють вимоги до захисту даних у процесі здійснення платіжних операцій з використанням платіжних карток. На рис. 3.10 показані стандарти PCI SSC, на які посилається цей документ, та сфера їх застосування.

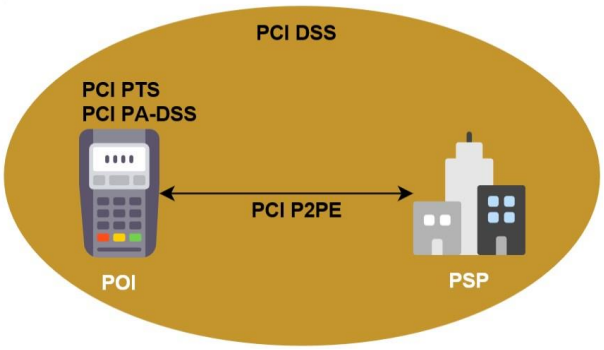

Рисунок 3.10 – Сфера застосування стандартів PCI

3.2.1 Стандарт безпеки платіжних карток PCI-DSS (PCI-DSS)

PCI DSS визначає вимоги до всіх суб'єктів, які обробляють, передають або зберігають дані про держателів карток, включаючи торговців. Ці вимоги були розроблені для захисту даних облікових записів та сприяння глобальному прийняттю заходів безпеки даних.

Для торговців платіжні бренди визначили чотири рівні відповідності (див. Таблицю 3.1). Ці рівні залежать від кількості операцій на рік, які бізнес обробляє за допомогою платіжних карток. Ці рівні відповідності визначають методи перевірки, яким має відповідати підприємство, щоб залишатися відповідним.

- Підприємства 1-го рівня: Проходять щорічний внутрішній аудит акредитованим аудитором PCI. Крім того, раз на квартал вони повинні проходити зовнішнє сканування вразливостей мережі (ENVS), яке виконується затвердженим постачальником послуг зі сканування (ASV).
- Суб'єкти 2-го, 3-го та 4-го рівнів: Щорічне проходження відповідного SAQ. Крім того, від компанії може знадобитися, щоб ENVS виконував ASV.

Таблиця 3.1 – Рівні відповідності підприємства вимогам стандарту PCI DSS

Рівні відповідності стандарту PCI DSS	
Рівень 1	Понад 6 млн транзакцій на рік
Рівень 2	Від 1 млн. до 6 млн. транзакцій на рік
Рівень 3	Від 20 тис. до 1 млн транзакцій на рік
Рівень 4	Менше 20 тис. транзакцій на рік

PCI DSS поділяє дані облікового запису на дані держателя картки та конфіденційні дані автентифікації (див. табл. 3.2). Дані держателя картки можуть зберігатися в пристроях, за винятком PAN-коду, який повинен зберігатися в нечитабельному вигляді, в той час як конфіденційні дані рахунків не можуть зберігатися в пристроях.

Таблиця 3.2 – Категоризація даних облікових записів PCI DSS

		Елемент даних	Зберігання дозволено
Дані рахунку	Дані держателя картки	PAN	Так (не читається)
		Ім'я власника картки	Так
		Код послуги	Так
		Термін придатності	Так
	Конфіденційні дані	Повна інформація	Ні
		CVV2	Ні
		PIN	Ні

Цей стандарт визначає, що якщо PAN повинен відображатися, то він повинен бути замаскований, за винятком випадків, коли у торговця є особлива потреба показувати повний PAN. Маскування означає приховування частини цифр PAN під час його відображення або друку. PCI DSS визначає перші шість та останні чотири цифри як максимальні цифри PAN, які не потрібно маскувати.

У випадку зберігання PAN, стандарт визначає, що торговець повинен виконати одну з наступних процедур:

-Одностороннє хешування: використовується одностороння математична функція, яка використовує PAN в якості вхідних даних і виробляє вихідні дані фіксованої довжини, які називаються дайджестом повідомлення. Цей дайджест повідомлення є незворотнім.

-Усічення: Видаляє частину PAN назавжди.

-Токенізація індексу: Заміна PAN на непередбачуване значення з використанням індексу в якості вхідних даних.

-Шифрування: Перетворення PAN в нерозбірливу форму, яка вимагає певного ключа для відновлення PAN. Цей метод вимагає об'єднання процесів і процедур управління ключами.

Загалом, PCI DSS визначає шість цілей, які досягаються шляхом виконання вимог стандарту.

1. Побудова та підтримка безпечної мережі та систем 2. Захист даних про держателів карток

3. Підтримувати програму управління вразливостями 4. Впроваджувати суворі заходи контролю доступу

5. Регулярно контролювати та тестувати мережі 6. Підтримувати політику інформаційної безпеки

Анкети самооцінки (SAQ). Опитувальники самооцінки - це інструменти самооцінки, які торгові підприємства використовують для підтвердження відповідності вимогам ДСБО PCI-DSS. PCI SSC визначає декілька видів SAQ, які перераховані в Таблиці 3.3. Для отримання додаткової інформації зверніться до Додатку С.

Таблиця 3.3 – Типи САК за каналами платежів

SAQs for PCI DSS compliance	
CP	**CNP**
P2PE	A
	A-EP (e-commerce)
D	D (e-commerce)
B	B (MOTO)
B-IP	B-IP (MOTO)
C-VT	C-VT (MOTO)
C	C (MOTO)

3.2.2. Шифрування PCI Point-to-Point Encryption (PCI P2PE)

PCI P2PE - це набір вимог безпеки для постачальників рішень шифрування для перевірки їх роботи та забезпечення захисту конфіденційних даних автентифікації та даних держателя картки шляхом їх шифрування перед передачею в каналі CP.

Середовище та типи дешифрування. PCI P2PE визначає різні середовища: середовище шифрування, середовище дешифрування, засоби введення ключа та середовище даних держателя картки. Ці середовища визначаються наступним чином.

-Середовище шифрування: Це середовище знаходиться на стороні торговця і містить схвалені PCI пристрої POI, що використовуються для прийняття та шифрування даних облікового запису.

-Середовище дешифрування: Це середовище знаходиться у постачальника рішень P2PE. Воно містить HSM, що використовується для дешифрування зашифрованих даних облікового запису, надісланих середовищем шифрування.

-Засоби введення ключів: Це середовище знаходиться або у постачальника компонентів, або у постачальника рішень P2PE. Ці засоби введення ключів вводять ключі як у пристрої POI, схвалені PCI, для виконання шифрування, так і в HSM постачальника рішень P2PE для виконання дешифрування.

-Середовище даних про держателів карток: Це середовище включає людей, процеси та технології, які обробляють дані держателів карток та конфіденційні дані

Крім того, PCI P2PE виконує два типи дешифрування: апаратне дешифрування та гібридне дешифрування.

-Апаратне дешифрування: HSM виконують дешифрування даних облікового запису. -Гібридне дешифрування: Дешифрування даних рахунку виконується

HSM та хост-системою з незахищеним криптографічним пристроєм (nSCD).

Типи доменів. PCI P2PE застосовується до декількох доменів, як показано в Таблиці 3.4. Ці домени складають регіони, в яких необхідно застосовувати та перевіряти безпеку.

Таблиця 3.4 – Домени та обов'язки PCI

PCI P2PE Домени	
Ім'я Домену	Підсумок
Пристрій та програма для шифрування керування	Охоплює використання безпечних пристроїв POI, схвалених PCI, додатків P2PE та програмного забезпечення для несплати P2PE. Вимоги цього домену включають огляд, встановлення та налаштування
Безпека додатків	Цей домен включає в себе безпечні платіжні додатки з доступом до відкритих текстових даних облікового запису, які встановлюються тільки на пристроях POI, схвалених PCI.
Управління рішенням P2PE	Цей домен включає постачальників різних пристроїв, продуктів і середовищ, які складаються з рішення P2PE, а також постачальників інструкцій з експлуатації P2PE.
Рішення мерчант-менеджера	Мерчанти керують рішенням P2PE, в якому обов'язки та функції середовища шифрування та дешифрування розділені.
Середовище розшифрування	Це середовище охоплює безпечне управління HSM та хост-системами nSCD, що беруть участь у розшифровці зашифрованих даних рахунків

На рисунку 3.11 показано процедуру, якої дотримується PCI P2PE.

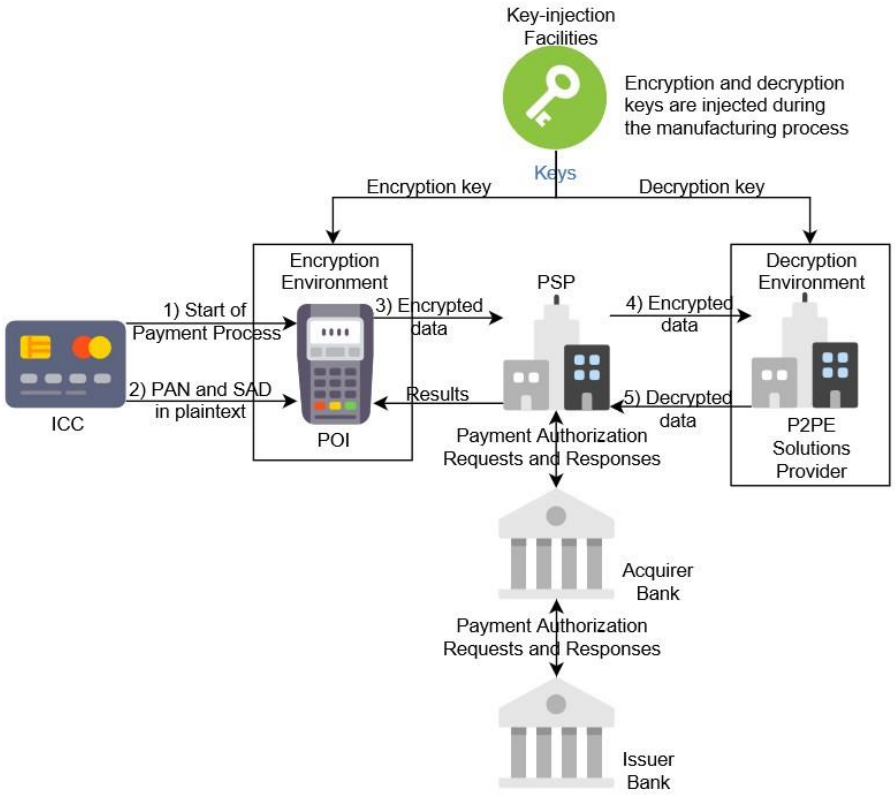

Рисунок 3.11 – Процедура PCI P2PE

Важливо зазначити, що незалежно від того, чи здійснює торговець P2PE самостійно, чи залучає стороннього постачальника послуг, процедура залишається однаковою.

3.2.3.Стандарт безпеки даних платіжних додатків PCI (PCI PA-DSS)

PCI PA-DSS - це набір вимог безпеки, призначених для готових додатків. Цей стандарт накладається на постачальників програмного забезпечення для платіжних додатків з метою мінімізації витоку конфіденційних даних з платіжного додатку під час процесу транзакції. Хоча цей стандарт походить від PCI DSS, той факт, що суб'єкт господарювання використовує додаток PCI PA-DSS, не означає повну відповідність стандарту PCI DSS.

PCI PA-DSS визначає шість основних цілей щодо захисту даних держателів карток, які використовуються в платіжному додатку. Деякі з цих цілей є спільними з PCI DSS.

3.2.4.Безпека транзакцій за допомогою PCI PIN-коду (PCI PTS)

PCI PTS охоплює PCI PTS HSM та PCI PTS POI. Ці стандарти є набором вимог безпеки, керівних принципів та процедур тестування, які виробники та постачальники повинні виконувати, щоб задовольнити потреби індустрії фінансових платежів шляхом забезпечення безпеки HSM та POI на всіх етапах від виробництва до початкового місця розгортання. Узгоджені цілі цих стандартів полягають у наступному:

-Забезпечити безпеку пристроїв на фізичному та логічному рівнях для захисту та гарантування безпеки конфіденційних даних та криптографічних ключів.

Кожен з цих стандартів переслідує різні цілі. Наприклад, PCI PTS HSM націлений на безпечне поводження з криптографічними ключами для безпечного виконання віддаленого адміністрування. PCI PTS POI націлений на

інтеграцію POI в POS-термінал, конфігурацію і обслуговування пристрою, а також вимоги, необхідні для безпечного зчитування і обміну даними.

Коли торговець прагне забезпечити відповідність стандарту PCI DSS, однією з вимог є те, що POI, які використовуються торговцем, повинні бути сумісними з PCI PTS POI. На відміну від цього, HSM можуть бути підтверджені або PCI PTS HSM, або федеральним стандартом обробки інформації 140-2.

3.2.5. PCI Three Domain Secure (PCI 3DS)

Стандарт PCI 3DS 1.0 визначає вимоги, засоби контролю та заходи безпеки, необхідні для захисту середовищ 3DS. Цей стандарт діє як настанова з безпеки, і рішення про необхідність його застосування приймається картковими платіжними брендами.

PCI SSC співпрацювала над публікацією стандартів безпеки PCI 3DS Core Security та PCI 3DS SDK Security Standards. Ці стандарти стосуються різних компонентів, які беруть участь у специфікації EMV 3DS 2.0.

Стандарт безпеки PCI 3DS Core Security Standard розглядає всі вимоги безпеки, методи та процеси, необхідні організації для забезпечення захисту та безпеки сервера 3DS, сервера каталогів 3DS (DS) та сервера управління доступом 3DS (ACS).

Стандарт безпеки PCI 3DS SDK охоплює конкретні елементи даних 3DS, які відіграють певну роль у процесі транзакцій 3DS 2.0, та визначає тип захисту, якого потребує кожен з цих елементів, що може бути спрямований на забезпечення конфіденційності, цілісності або обох.

4. Безпека життєдіяльності, основи охорони праці

4.1. Вимоги і норми охорони праці приміщень де використовується комп’ютерна техніка

Охорона праці – це система законодавчих актів, соціально-економічних, організаційних, технічних, гігієнічних і лікувально-профілактичних заходів та засобів, що забезпечують безпеку, збереження здоров'я і працездатності людини в процесі праці. Техніка безпеки являє собою систему засобів і методів, що запобігають або знижують до безпечного рівня вплив небезпечних факторів. Виробнича санітарія покликана усунути або знизити до безпечного рівня вплив шкідливих факторів.

Повністю безпечних та нешкідливих виробничих процесів не існує. Завдання охорони праці звести до мінімуму ймовірність ураження або захворювання працюючого з одночасним забезпеченням комфорту при максимальній продуктивності праці.

З точки зору ступеня потенційної небезпеки для здоров'я і життя людини фактори поділяються на небезпечні та шкідливі.

Небезпечним виробничим фактором є такий фактор виробничого процесу, вплив якого на працюючого приводить до травми або різкого погіршення здоров'я.

Шкідливі виробничі фактори це несприятливі фактори трудового процесу або умов навколишнього середовища, які можуть зробити шкідливий вплив на здоров'я і працездатність людини. Тривала дія на людину шкідливого виробничого фактора призводить до захворювання.

Негативні фактори трудового процесу призводять до зниження працездатності та погіршення якості продукції, що випускається. Тривалий вплив несприятливих умов праці може призвести до порушення здоров'я працюючого, розвитку професійного захворювання або інвалідності.

Завданням охорони праці є гарантування безпечних і здорових умов праці та підтримання працездатності робітників. Безпечними умовами праці вважаються такі умови, при яких вплив на працюючих шкідливих та небезпечних виробничих факторів виключено або рівні їх впливу не перевищують встановлені нормативи.

Обов'язки забезпечення санітарно-побутових умов праці повинні брати на себе керівники структурних підрозділів.

Площа приміщення, в якому буде розташовано персональний комп'ютер, має підпадати під норми, які визначають згідно з чинними нормативними документами з розрахунку на одне робоче місце, обладнане ПК:

- площа має бути не менше 6 кв;
- об'єм не менше 20 куб.м;
- відстань від вікна до робочого місця не менше 1 м;
- відстань між бічними поверхнями комп'ютерів не менше 1.5 м;
- відстань між тильною поверхнею одного комп'ютера і екраном іншого – не менше 2.5 м;
- прохід між рядами не менше 1 кв.м.

Також існують вимоги до організації приміщення: заземлені конструкції, що знаходяться в приміщеннях (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном тощо), мають бути надійно захищені діелектричними щитками або сітками для запобігання випадкового дотику. В робочих приміщеннях повинні бути медичні аптечки першої допомоги та система автоматичної пожежної сигналізації з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з розрахунку 2 шт. на кожні 20 кв.м площі приміщення. Засоби пожежогасіння повинні бути вільними для швидкого доступу.

Робоче місце працівника повинно забезпечувати оптимальну сидячу позу з такими характеристиками: ступні ніг – на підлозі або на підставці для ніг; стегна – в горизонтальній площині; передпліччя – вертикально; лікті – під

кутом 70-90 град. до вертикальної площини; зап'ястя зігнуті під кутом не більше 20 град. відносно горизонтальної площини, нахил голови – 15-20 град. відносно вертикальної площини. Якщо користування ПК є основним видом діяльності, то ПК і його периферійні пристрої (принтер, сканер тощо) розміщується на основному робочому столі з лівого боку. Висота робочої поверхні столу для ПК має бути в межах 680-800 мм., а ширина – забезпечувати можливість виконання операцій в зоні досяжності моторного поля. Він повинен мати простір для ніг висотою не менше 600 мм., шириною не менше 500 мм., глибиною на рівні колін не менше 450 мм., на рівні витягнутої ноги – не менше 650 мм.

Робоче крісло користувача ПК повинно мати такі елементи: сидіння, спинку стаціонарні або знімні підлокітники.

Конструкція стільця повинна забезпечувати:

– ширину і глибину поверхні сидіння не менше 400 мм;

– поверхню сидіння з заокругленим переднім краєм;

– регулювання висоти поверхні сидіння в межах 400-550 мм і кутом нахилу вперед до 15 градусів і назад до 5 градусів;

– висоту спинки стільця 300 ± 20 мм, ширину – не менше 380 мм, радіус кривизни горизонтальної площини 400 мм;

– кут нахилу спинки у вертикальній площині в межах 0 ± 30 градусів;

– врегулювання відстані спинки від переднього краю сидіння в межах 260-400 мм;

– стаціонарні або знімні підлокітники довжиною не менше 250 мм і шириною 50-70 мм;

– регулювання підлокітників по висоті над сидінням у межах 230 ± 30 мм і відстанню між підлокітниками в межах 350-500 мм;

– поверхню сидіння, спинки та підлокітників має бути напівм'якої, з нековзним неелектрізующімся, повітронепроникним покриттям, що легко очищується від забруднення.

Монітор та клавіатура мають розташовуватися на такій оптимальній відстані від очей користувача, але не повинні бути не ближче ніж 600 мм, з урахуванням розміру алфавітно-цифрових знаків та символів.

Відображення блискоту на робочих поверхнях обмежується за рахунок правильного вибору світильника і розташування робочих місць по відношенню до природного джерела світла. Яскравість відблисків на екрані монітора не повинна перевищувати 40 кд/м^2. Показник осліпленості для джерел загального штучного освітлення у приміщеннях повинен бути не більше 20, показник дискомфорту в адміністративно-громадських приміщеннях не більше 40. Співвідношення яскравості між робочими поверхнями і поверхнями стін і обладнання повинно бути 10:1.

Хибна організація робочого місця сприяє загальній і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, скривленню хребта й розвитку остеохондрозу та інших захворювань.

Продуктивність праці сильно залежить від умов праці, таких як освітлення, повітря, простору, шум та шкідливих речовин. Ці параметри, окремо і в комбінації, впливають на організм людини.

Відповідно до витрат на енергію людського тіла, дослідницька робота належить до категорії 1а (легка), оскільки це відбувається сидячи, та не вимагає систематичної фізичної активності або підйому та перенесення важких речей (витрати на енергію при виконанні роботи – до 120 Ккал/год).

Обладнання для робочих місць повинно забезпечувати необхідні умови освітлення приміщень та робочих місць, ергономічні характеристики основних елементів робочого місця, а також враховувати шкідливі чинники (шум, вібрація, пил, озон, оксиди азоту, аероіонізація, електромагнітні, ультрафіолетові, інфрачервоне та рентгенівське випромінювання, електростатичне поле між екраном та оператором).

Вимоги до відео терміналів відповідно до «Правил захисту праці при роботі з ПК» наведені в таблиці 4.1.

Таблиця 4.1 – Вимоги до відео терміналів

Найменування параметру	Значення параметру
1 Яскравість знаку (фону), кд/ кв.м.	35-120
2 Зовнішня освітленість екрану, лк	100-250
3 Нерівномірність яскравості у робочій області екрану , не більш	1,7:1
4 Відхилення форми робочої зони екрана від прямокутника: - по горизонталі та по вертикалі, не більш - по діагоналі, не більш	 2% 4%
5 Розмір мінімального елемента зображення (пікселя) для монохромних зображень, мм.	0,3
6 Співвідношення ширини екрану до висоти для великих букв	0,7-0,9іі

З метою забезпечення нормальних умов роботи санітарні норми ДСаНПіН 3.3.2-007-98 встановлюють на одному робочому місці об'єм виробничого приміщення не менше 20 куб.м., площа – не менше 6 кв.м.

Мікроклімат виробничого середовища – це комбінація температури, відносної вологості та швидкості повітря. Великий вплив на мікроклімат має джерела тепла в приміщеннях (обладнання, прилади освітлювальне, робочий персонал). Роботу на організм людини та обладнання також сильно впливає відносна вологість повітря. При відносній вологості 75-80% знижується опір ізоляції, змінюються робочі характеристики елементів ПК.

Відповідно до ГОСТ 12.1.005-88 найкращий мікроклімат категорії 1а наведено в таблиці 4.2.

Таблиця 4.2 – Оптимальні параметри мікроклімату

Категорія важкості робіт по енерговитратам	Період року	Температура, С°	Відносна вологість, %	Швидкість руху повітря,м/с
Легка -І а	Хо	22-24	40-	0,1
	Те	23-25	40-	0,1

В даний час як організаційні методи, так і технічні засоби використовуються для забезпечення комфортних умов. Серед організаційних заходів є раціональна організація проведення роботи та організація

правильного чергування роботи і відпочинку. Технічні засоби включають в себе вентиляцію, кондиціювання повітря та опалення.

Освітленість – освітлення поверхні, що створюється світловим потоком, який падає на поверхню. Одиницею вимірювання освітленості є люкс. На відміну від освітленості, вираз кількості світла відображеного поверхнею, називається яскравістю. Освітленість прямо пропорційна силі світла джерела світла. При віддаленні його від освітлюваної поверхні, її освітленість зменшується обернено пропорційно до квадрата відстані.

Робота оператора ПК багато в чому залежить від освітлення. Освітлення приміщень поділяється на штучні та природні. Природне світло забезпечується через бічні отвори, орієнтовані переважно на північ. Стан освітлення виробничих, сервісних і допоміжних приміщень регулюється державними будівельними нормами ДБН 79-92.

Ця робота проводилася з природним і штучним освітленням. Відповідно до ДБН 79-92 аналізуються комфортні умови для довгострокової зорової роботи, таблиця 4.3.

Таблиця 4.3 – Характеристика промислового освітлення

Показник	**Значення**
Мінімальний розмір об'єкта розрізнення , мм	0,3 - 0,5
Фон	Світлий
Контраст об'єкта розрізнення із фоном	Середній
Розряд зорової роботи	III
III, % при бічному освітленні	2
IV, % при бічному освітленні	1,35
Освітленість Е, Лк, при загальному освітленні	500
Тип ламп	Газорозрядні

Згідно ДБН II природне освітлення нормується коефіцієнтом природного освітлення, який залежить від поясу світового клімату. Місто Тернопіль знаходиться у IV поясі світового клімату.

На робочому місці, що досліджується, джерелом шуму є ЕОМ та зовнішній кондиціонер (постійний). Допустимий рівень постійного звуку при програмуванні на ЕОМ – 50 дБ. Оскільки основні механічні частини кондиціонера знаходяться зовні приміщення, шумовий тиск, що він створює, є мінімальний, та не перевищує фоновий. ПК, а саме кулери та блоки живлення, при роботі створюють мінімальний шумовий тиск. Інших джерел шуму у приміщенні немає. Отже, рівень звуку, який створюється джерелом шуму, повністю відповідає нормам.

У кімнаті комп'ютерного приміщення причиною шуму є прилади та обладнання (комп'ютери, принтери тощо). Рівень звуку в приміщенні, де працюють працівники, не повинен перевищувати 50 дБ.

Основні методи захисту від шуму та вібрації:

- зменшення шуму та вібрації у джерелі;
- зменшення шуму та вібрації шляхом розподілу;
- застосування індивідуальних засобів захисту;
- організаційно-профілактичні методи захисту.

Шум – один з більш розповсюджених несприятливих фізичних причин навколишнього середовища, які купують принципове соціально-гігієнічне значення, у зв'язку з урбанізацією, також механізацією і автоматизацією технологічних дій, майбутнім розвитком дизелебудування, реактивної авіації, транспорту. Наприклад, при запуску реактивних двигунів літаків рівень шуму коливається від 120 до 140 дБ. при клепанні й рубання листової сталі – від 118 до 130 дБ., роботі деревообробних верстатів від 100 до 120 дБ., ткацьких верстатів – до 105 дБ.; побутового шум, пов'язаний з життєдіяльністю людей, складає 45-60 дБ.

Вібрація – механічні коливання механізмів, машин або відповідно до ДСТУ ГОСТ 12.1.012:2008 вібрацію класифікують наступним чином.

За способом передачі на людину вібрацію поділяють на загальну, що передається через опорні поверхні на тіло сидить або стоїть людини, та локальну, що передається через руки людини.

По напрямку розрізняють вібрацію, що діє вздовж осей ортогональної системи координат для загальної вібрації, що діє вздовж всієї ортогональної системи координат для локальної вібрації.

За джерела виникнення вібрацію поділяють на транспортну (при русі машин), транспортно-технологічну (при поєднанні руху з технологічним процесом, при розкиданні добрив, косовиці або обмолоті самохідним комбайном і т. д.) і технологічну (при роботі стаціонарних машин).

У комп'ютерному приміщення використовується електрична енергія (трифазна мережа з напругою 220 В. і частотою 50 Гц.).

Конструктивні заходи безпеки спрямовані на запобігання доступу оператора до поточних провідних частин. Для цього всі ручні перемикачі встановлюються в закриті корпуси, всі елементи, що несуть струм, розташовані в захисних коробках або покриті шаром ізоляції що виключає можливість торкатися їх. Ступінь захисту обладнання відповідає IP44 (де 4 це захист від проникнення твердих тіл більше 1мм, 4 це захист від бризок) відповідно ПУЕ-87.

Перший клас захисту від ураження електричним струмом обслуговуючим персоналом, оскільки комп'ютер має робочу ізоляцію та заземлюючі елементи.

Схематичні проектні заходи електричної безпеки гарантують безпеку людини, торкаючись металевих частин електричного апарату у випадку випадкового розбиття ізоляції та появи електричного потенціалу на них.

Оскільки напруга менше 1000 В., однак, більше 42 В., занулення використовується для захисту від ураження електричним струмом.

Вимоги до електромережі а також запобіжні засоби для уникнення травм від контакту з струмопровідними елементами електроустаткування :

– величина напруги мережі не більше за 380В. та 220В. (міжфазна лінійна і фазна відповідно);

– всі струмопровідними елементи (в першу чергу електричні дроти) вкриті ізоляційними матеріалами;

– в джерелі безперебійного живлення персонального комп’ютера використовується механічне захисне блокування, що забезпечує вимикання напруги при його відкриванні;

– електромережа в приміщенні розведена в спеціальних каналах стін і підлоги.

Пожежна безпека – стан об'єкта, при якому з регламентованою ймовірністю відкидається можливість виникнення та розвиток пожежі, і впливу на людей її небезпечних факторів, а також забезпечується захист матеріальних цінностей.

На підприємствах існує два види пожежної охорони: професійна і воєнізована. Воєнізована охорона створюється на об'єктах з підвищеною небезпекою. Крім того, на підприємствах для посилення пожежної охорони організовуються добровільні пожежні дружини і команди, добровільні пожежні товариства і пожежно-технічні комісії з числа робітників та службовців. При Міністерстві внутрішніх справ існує управління пожежної охорони (УПО) і його органи на місцях.

З огляду на можливість виникнення пожежі слід з’ясувати, які речовини і матеріали можуть горіти. У приміщенні, що розглядається, можуть горіти вироби з дерева, пластмас, тканини і паперу. Тому приміщення, що аналізується, відноситься, відповідно до нормативної документації, до зони П-IIа і до категорії пожежної небезпеки В.

Ймовірними причинами виникнення пожару можуть бути несправність електрообладнання (кабелів, розеток), короткі замикання внаслідок виходу з ладу чи експлуатації несправного електроустаткування (периферійних пристроїв), порушення правил протипожежної безпеки тощо.

Комплекс заходів для попередження пожеж:

– обов’язковий інструктаж персоналу з питань охорони праці,

– зокрема, правила пожежної безпеки у приміщеннях з ЕОМ;

– заборона використання відкритого вогню у приміщенні;

– наявність системи автоматичної пожежної сигналізації з димовими пожежними оповіщувачами;

– ступінь вогнестійкості будівлі, у якій розташовано приміщення - II;

– наявність шляхів евакуації при виникненні пожежі;

– розміщення схеми евакуації людей при пожежі і ознайомлення з нею персоналу.

Для гасіння пожежі кожна кімната повинна бути обладнана ручними вуглекислотними вогнегасниками ВВК-1,4. У загальному коридорі встановлені пінні вогнегасники ВВП. На сходах присутній спеціальний щит пожежного гідранта з відповідним рукавом. Розглянуте приміщення обладнане датчиками централізованої системи пожежної сигналізації. Призначена відповідальна особа, що відповідає за дотримання персоналом вимог пожежної безпеки. Розроблено план евакуації персоналу і найбільш коштовного устаткування

4.2. Структура цивільного захисту міста Тернопіль

Цивільний захист це система організаційних, інженерно-технічних, санітарно-гігієнічних, протиепідемічних та інших заходів, які здійснюються центральними і місцевими органами виконавчої влади, органами місцевого самоврядування, підпорядкованими їм силами і засобами, підприємствами, установами та організаціями незалежно від форми власності, добровільними рятувальними формуваннями, що забезпечують виконання цих заходів з метою запобігання та ліквідації надзвичайних ситуацій, які загрожують життю та здоров'ю людей, завдають матеріальних збитків у мирний час.

Цивільний захист здійснюється з метою реалізації державної політики, спрямованої на забезпечення безпеки та захисту населення і територій, матеріальних і культурних цінностей та довкілля від негативних наслідків надзвичайних ситуацій у мирний час та в особливий період подолання наслідків надзвичайних ситуацій, у тому числі наслідків надзвичайних

ситуацій на територіях іноземних держав відповідно до міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Цивільний захист здійснюється на принципах гарантування державою громадянам конституційного права на захист життя, здоров'я та їх майна, а юридичним особам – права на безпечне функціонування добровільності при залученні людей до здійснення заходів у сфері цивільного захисту, пов'язаних з ризиком для життя і здоров'я:

- комплексного підходу до вирішення завдань цивільного захисту;
- створення системи раціональної превентивної безпеки з метою максимально можливого, економічно обґрунтованого зменшення ймовірності виникнення надзвичайних ситуацій і мінімізації їх наслідків;
- територіальності та функціональності єдиної системи цивільного захисту;
- мінімізації заподіяння шкоди довкіллю;
- гласності, вільного доступу населення до інформації у сфері цивільного захисту відповідно до законодавства.

Відділ організації заходів цивільного захисту (далі – Відділ) Управління ДСНС України у Тернопільській області (далі –Управління) є структурним підрозділом Управління, що забезпечує реалізацію державної політики у сфері цивільного захисту, захисту населення і територій від надзвичайних ситуацій, підпорядкований начальнику Управління та заступнику начальника Управління з організації запобігання надзвичайним ситуаціям та заходів цивільного захисту.

Основні завдання відділу:

- реалізує в межах повноважень державну політику у сфері організації заходів цивільного захисту, захисту населення і територій від надзвичайних ситуацій, інженерного, радіаційного, хімічного захисту та оперативної підготовки, запобігання, реагування і ліквідації наслідків надзвичайних ситуацій (далі – НС) у мирний час та особливий період, а також

впровадження вимог інженерно-технічних заходів цивільного захисту (далі – інженерно-технічні заходи) у містобудівній і проектній документації;

- участь у розробленні, координації впровадження та контроль за реалізацією заходів на території області щодо інженерного, радіаційного та хімічного захисту населення і територій від наслідків НС, евакуації населення із зон ураження у мирний час та особливий період;
- розробляє нормативно-правові документи на особливий період, щодо інженерного, радіаційного та хімічного захисту населення і територій, організації евакуації населення, укриття у захисних спорудах;
- здійснює планування інженерних, радіаційних, хімічних та евакуаційних заходів цивільного захисту, прогнозування можливої техногенно-екологічної, інженерної, радіаційної, хімічної обстановки на території області при повсякденній діяльності та внаслідок стихійних лих, аварій, катастроф у мирний час і особливий період;
- бере участь, у межах компетенції, в перевірках місцевих органів виконавчої влади, підприємств, установ і організацій щодо інженерного, радіаційного та хімічного захисту населення і територій, організації евакуації населення, а також готовності органів управління та сил територіальної підсистеми єдиної державної системи цивільного захисту Тернопільської області до дій у разі виникнення НС;
- організовує, в межах повноважень, виконання заходів з ліквідації наслідків НС, проведення пошуково-рятувальних робіт, а також виконання невідкладних робіт у мирний час та особливий період при загрозі або виникненні НС.

Функції Відділу:

- реалізує, у межах повноважень, державну політику у сфері організації заходів цивільного захисту;
- приймає участь у визначенні основних напрямків діяльності та розвитку Тернопільської територіальної підсистеми єдиної державної системи цивільного захисту (далі – ТП ЄДСЦЗ), організовує, у межах повноважень,

виконання вимог законодавства, інших нормативно-правових актів у цій сфері та здійснює контроль за їх реалізацією;

- здійснює управління, координацію та організаційно-методичне керівництво, у межах наданих йому повноважень, діяльністю структурних підрозділів Управління з питань інженерного, радіаційного та хімічного захисту населення і територій, організації евакуації населення, укриття у захисних спорудах;
- бере участь, в межах компетенції, у визначенні стану та оцінки готовності органів управління та сил цивільного захисту ланок ТП ЄДСЦЗ до дій на випадок виникнення НС;
- бере участь, за запитами уповноважених органів, у проведенні планових і раптових перевірок органів управління райдержадміністрацій, міських (міст обласного значення) рад, підприємств, установ, організацій незалежно від форм їх власності та підпорядкування у частині впровадження і дотримання ними нормативно-правових актів з питань інженерного, радіаційного, хімічного та медико-біологічного захисту населення і територій від НС, планування евакуаційних заходів;
- бере участь у розробленні проектів програм щодо запобігання надзвичайним ситуаціям та розвитку ТП ЄДСЦЗ;
- розробляє план цивільного захисту Управління на особливий період та, у межах наданих повноважень, координує планування заходів цивільного захисту місцевими органами виконавчої влади;
- приймає участь у розроблені проектів рішень обласної державної адміністрації щодо організації та забезпечення роботи органів влади в особливий період та у разі введення в державі надзвичайного стану;
- вносить начальнику Управління пропозиції щодо підвищення ефективності захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру, удосконалення заходів цивільного захисту на території Тернопільської області, в місцевих органах виконавчої

влади та органах місцевого самоврядування, на підприємствах, в установах та організаціях незалежно від форми власності;

- здійснює разом з місцевими органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами, організаціями прогнозування ймовірності виникнення надзвичайних ситуацій, вносить пропозиції щодо показників ризику та здійснює районування території щодо ризику виникнення надзвичайних ситуацій;
- приймає участь у підготовці органів управління та сил функціональних і територіальної підсистеми ЄДСЦЗ, їх складових та проведення командно-штабних навчань з органами управління та силами цивільного захисту;
- здійснює в межах повноважень контроль за готовністю сил і засобів ТП ЄДСЦЗ до пропуску паводків і льодоходів, накопичення матеріальних засобів для запобігання та ліквідації наслідків паводків та повені;
- веде облік населених пунктів і територій, що потрапляють до зон паводків, повені, зсувних процесів.

Заходи державної політики щодо інженерного захисту населення та територій, впровадження вимог інженерно-технічних заходів цивільного захисту (далі – інженерно-технічні заходи) у містобудівній і проектній документації, зокрема:

- надає, в межах повноважень, на запити замовників вихідні дані та вимоги, необхідні для розроблення та проектування інженерно-технічних заходів; бере участь у проведенні експертизи містобудівної документації та проектів будівництва техногенно-небезпечних об’єктів у частині дотримання вимог інженерно-технічних заходів ЦЗ (ЦО);
- бере участь, у межах наданих повноважень, у діяльності місцевих архітектурно-містобудівних рад з питань реалізації інженерно-технічних заходів; бере участь, за запитами уповноважених органів, у розроблені цих

заходів, проведенні їх експертизи та здійсненні контролю за їх реалізацією та впровадженням;

- готує пропозиції щодо віднесення населених пунктів та об'єктів національної економіки до груп (категорій) із цивільного захисту;
- надає консультативну допомогу стосовно розроблення та реалізації інженерно-технічних заходів у проектній документації та містобудівній документації.

Заходи державної політики щодо створення, утримання та реконструкції фонду захисних споруд цивільного захисту (далі – захисні споруди), а саме:

- організовує та здійснює ведення електронного обліку захисних споруд, що знаходяться на території області;
- розглядає та погоджує документи щодо обґрунтування виключення з обліку захисних споруд цивільного захисту (цивільної оборони);
- організовує спільно із місцевими органами виконавчої влади періодичну інвентаризацію фонду захисних споруд та здійснює контроль за її проведенням;
- вносить пропозиції з питань будівництва та реконструкції захисних споруд та їх пристосування для використання у господарських, культурних і побутових потребах;
- бере участь у прийнятті в експлуатацію закінчених будівництвом захисних споруд;
- бере участь, у межах своїх повноважень, у розгляді питань будівництва та реконструкції захисних споруд та їх пристосування для використання у господарських, культурних та побутових потребах.

Аналізує інформацію про виникнення надзвичайних ситуацій та попередньо визначає, в межах своєї компетенції, рівень надзвичайних ситуацій.

Забезпечує реалізацію державної політики у сфері радіаційного, хімічного та медико-біологічного захисту, зокрема: готує пропозиції

керівництву управління щодо координації та контролю місцевих органів виконавчої влади, підприємств, установ та організацій з питань радіаційного та хімічного захисту населення у разі виникнення радіаційних аварій та надзвичайних ситуацій, пов'язаних із виливом (викидом) небезпечних хімічних речовин; здійснює координацію місцевих органів виконавчої влади, підприємств, установ та організацій з питань виявлення та оцінки радіаційної і хімічної обстановки, організації та здійснення дозиметричного і хімічного контролю, розроблення та впровадження типових режимів радіаційного захисту, забезпечення і використання засобів індивідуального захисту, приладів радіаційної та хімічної розвідки, дозиметричного і хімічного контролю, проведення санітарної обробки населення та спеціальної обробки одягу, майна і транспорту у разі виникнення надзвичайних ситуацій.

В розділі розглянуто;

- структуру цивільного захисту міста Тернопіль,
- вимоги і норми охорони праці приміщень де використовується комп’ютерна техніка.

ВИСНОВОК

В результаті виконання кваліфікаційної роботи бакалавра отримано наступні результати:

- здійснено компіляцію інформації про технології та стандарти платіжних карток, яка була зібрана та співставлена з різних офіційних документів
- аналіз структурних елементів платіжної картки дозволив виділити десять елементів, які, за винятком двох, реалізують функцію захисту платіжної картки.
- вивчення життєвого циклу платіжної картки дозволило виявити щонайменше п'ять суб'єктів, які відіграють певну роль у платіжному процесі.
- описано механізми безпеки, які забезпечують технології та стандарти

Перелік посилань

1. Методичні рекомендації з виконання, оформлення та захисту кваліфікаційних робіт магістрів спеціальності 151 – «Автоматизація та комп’ютерно-інтегровані технології» / ТНТУ ім. І. Пулюя; уклад. А.Г. Микитишин, М.М. Митник. – Тернопіль: ТНТУ, 2020. – 80 с.
2. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп’ютерні мережі. Книга 1. [навчальний посібник] (Лист МОНУ №1/11-8052 від 28.05.12р.) - Львів, «Магнолія 2006», 2013. – 256 с.
3. “The History of PCI Compliance,” WEXInc. [Online]. Available: https://bit.ly/33zObqu [Accessed Jun. 12, 2022]
4. “PCI DSS history, everything you need to know,” WorldPay from FIS. [Online]. Available: https://bit.ly/2ZZpxx8 [Accessed Jun. 12, 2012022]
5. “ENVCo the Basics,” EMVCo. [Online]. Available: https://bit.ly/2MkFcUF [Accessed Jun. 12, 2022]
6. “About Us,” PCI Security Standard Council. [Online]. Available: https://bit.ly/2gaBJoR [Accessed Jun. 12, 2022]
7. "ISO/IEC 24760-1:2019: IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts," ISO. [Online]. Available: https://bit.ly/2XSUW2y [Accessed Jun. 12, 2022]
8. "ISO/IEC 27000:2018: Information technology – Security techniques – Information security management systems – Overview and vocabulary," ISO. [Online]. Available: https://bit.ly/2XSenZb [Accessed Jun. 12, 2022]
9. “EMVCo: Operating Principles,” EMVCo. [Online]. https://bit.ly/2WI9CWx [Accessed Jun. 12, 2022]
10. “Worldwide EMV Chip Card Deployment and Adoption,” EMVCo. [Online]. Available: https://bit.ly/2Xili1L [Accessed Jun. 12, 2022]
11. "PCI Security," PCI Security Standards Council. [Online]. Available: https://bit.ly/1Wgodxc [Accessed Jun. 13, 2022]

12. “PCI Security Standards Overview,” PCI Security Standards Council. [Online]. Available: https://bit.ly/2XbkCuS [Accessed Jun. 13, 2022]
13. “Increasing Security and Reducing Fraud with EMV Chip and PCI Standards,” PCI Security Standards Council. [Online]. Available: https://bit.ly/1hjFA2i [Accessed Jun. 13, 2022]
14. “EMVCo and PCI SSC Combine Expertise on 3-D Secure 2.0,” PCI Security Standards Council. [Online]. Available: https://bit.ly/2ReiVHs [Accessed Jun. 13, 2022]
15. “First Data: Credit Card Fraud Protection – User Guide,” First Data. [Online]. Available: https://bit.ly/31gX5XJ [Accessed Jun. 14, 2022]
16. “What is a Credit Card Issuer?,” The Balance. [Online]. Available: https://bit.ly/2wX6NBm [Accessed Jun. 14, 2022
17. “Contact EMV,” EMVCo. [Online]. Available: https://bit.ly/2ZsFuuX [Accessed Jun. 17, 2022]
18. Contactless EMV," EMVCo. [Online]. Available: https://bit.ly/2Y8YJNa [Accessed Jun. 17, 2022]
19. A Guide to EMV Chip Technology,” EMVCo. [Online]. Available: https://bit.ly/2tJLnGI [Accessed Jun. 17, 2022]
20. Henk C. A. van Tilborg (2005), “Encyclopedia of Cryptography and Security,” Springer, New York
21. “EMVCo Reports Over Half of Cards Issued Globally are EMV-enabled,” EMVCo. [Online]. Available: https://bit.ly/2vuxsI2 [Accessed Jun. 17, 2022]
22. What Is A Credit Card Number? The Meaning of Each Digit,” WalletHub. [Online]. Available: https://bit.ly/2ZuUoBy [Accessed Jun. 19, 2022]
23. Credit Cards,” DataGenetics. [Online]. Available: https://bit.ly/2WGJnzD [Accessed Jun. 19, 2022]
24. “Why Do Credit Cards Expire?,” CreditCardsCanada. [Online]. Available: https://bit.ly/2WZQlQA [Accessed Jun. 20, 2022]

ДОДАТКИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

X НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

7–8 грудня 2022 року

ТЕРНОПІЛЬ
2022

УДК 001
М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Сергій Лупенко– докт. техн. наук, професор.

Співголови: Павло Марущак– докт. техн. наук, професор, проректор з наукової роботи.
Ігор Баран– канд. техн. наук, доцент, декан факультету ФІС.

Науковий секретар: Галина Семенишин– старший викладач.

Члени: докт. фіз.-мат. наук, професор Василь Кривень; докт. техн. наук, професор Ярослав Литвиненко; докт. техн. наук, професор Микола Карпінський; докт. фіз.-мат. наук, професор Михайло Петрик; канд. техн. наук, доцент Галина Осухівська; канд. пед. наук, доцент Жанна Баб'як; канд. техн. наук, доцент Наталія Загородна.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Юрій Скоренький– канд. фіз.-мат. наук, доцент, завідувач кафедри фізики

Члени: канд. техн. наук, доцент Вячеслав Никитюк; канд. техн. наук, доцент Дмитро Михалик; канд. техн. наук, асистент Марія Стадник; асистент Наталія Шаблій; ст. викладач Ліліана Джиджора.

М34 Матеріали X науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 7–8 грудня 2022 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2022. –162 с.

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,
тел. (0352) 52-41-33, факс (0352) 254983.
E-mail: conffis2022@gmail.com

Редагування, оформлення та верстка: Галина Семенишин

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання;
- Інформаційні системи та технології;
- Комп'ютерні системи та мережі;
- Програмна інженерія та моделювання складних розподілених систем;
- Новітні фізико-технічні та освітні технології.

В збірнику надруковано тези доповідейIX науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 7–8 грудня 2022 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології; комп'ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

© Тернопільський національний технічний університет імені Івана Пулюя, …… 2022

УДК 004.6
А. Блавіцький, С. Мацюк, С. Криськова
(Тернопільський національний технічний університет імені Івана Пулюя)

ОЦІНКА РОЗВИТКУ БЕЗПЕКИ ОПЛАТИ ПЛАТІЖНИМИ КАРТКАМИ

UDC 004.6
A. Blavitskyi, S. Matsiuk, S. Kryskova

ASSESSMENT OF THE SECURITY DEVELOPMENT OF PAYMENT CARDS

Навіть сьогодні в операціях з платіжними картками все ще використовуються застарілі технології. Щоб вирішити цю ситуацію, важливо проаналізувати та оцінити розвиток безпеки в методах електронних платежів, щоб зрозуміти, як захист даних, що використовуються в платіжних транзакціях, покращився з появою нових технологій.

Аналіз структурних елементів платіжної картки виявив десять елементів. Кожен із цих елементів, крім двох, реалізує функцію захисту платіжної картки. Першим винятком є магнітна смуга, яка є застарілою та незахищеною технологією для каналу наявної картки, яка все ще використовується, щоб зробити платіжну картку зворотною сумісністю із застарілими POI.

Другим винятком є CVV2, який є механізмом безпеки для каналу відсутності картки, який лише підтверджує володіння платіжною карткою.

Вивчення життєвого циклу платежу карткою виявило щонайменше п’ять суб’єктів, які відіграють певну роль у платіжному процесі. Для процесу оплати карткою доступні два платіжні канали: канал наявності картки та канал відсутності картки. Ці канали вказують на присутність або відсутність власника картки на об’єктах продавця, коли ініціюється оплата карткою.

Було розглянуто три технології EMVCo: чіп EMV, EMV 3DS 2.0 і токенізація платежів EMV. Кожна з цих технологій реалізує кілька функцій безпеки, включаючи автентифікацію даних, методи перевірки власника картки, потоки автентифікації, а також методи перевірки та ідентифікації. Ці функції безпеки є важливими, оскільки їх наявність, відсутність або поєднання впливає на загальну безпеку технології.

Дослідження стосувалося чотирьох стандартів PCI SSC: PCI DSS, PCI PTS, PCI PA-DSS і PCI P2PE. Головною метою цих стандартів є захист конфіденційних даних власника картки.

В майбутньому важливо продовжити детальне вивчення нових механізмів безпеки, які впроваджуються для інноваційних та альтернативних методів електронних платежів. Крім того, постійні дослідження та інновації в механізмах автентифікації покращать безпеку платежів карткою для обох платіжних каналів. Зазначимо, що постійна еволюція злочинних атак на електронні платежі з метою отримання незаконної вигоди повинна супроводжуватися та протистояти розробка нових технологій та заходів безпеки.

Література

1. «Payment Card Industry 3-D Secure (PIC 3DS) – Security Requirements and Assessment Procedures for EMV 3-D Secure SDK,» PCI Security Standard Council. [Online]. URL: https: //bit.ly/2xPLm5R (Accessed: Nov. 10, 2022).

УДК 004.6
А. Блавіцький, С. Мацюк, С. Криськова
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЖИТТЄВИЙ ЦИКЛ ПЛАТЕЖУ

UDC 004.6
A. Blavitskyi, S. Matsiuk, S. Kryskova

PAYMENT LIFE CYCLE

Щоб отримати більш повне розуміння здійснення платежів, важливо розглянути життєвий цикл платіжного процесу та суб'єкти, які задіяні (див. рис. 1).

Рисунок 1. Життєвий цикл платіжного процесу

Нижче перераховано задіяні суб'єкти:

- Власник картки: Власник картки – особа, якій банк-емітент видає платіжну картку; іншими словами, це власник платіжної картки.
- Продавець: продавець – це будь-яка організація, яка прийняла платіжну картку як форму оплати своїх товарів або послуг.
- Постачальник платіжних рішень (PSP): також відомий як платіжна мережа, PSP є організацією, яка відповідає за зв'язок продавця з різними банками-еквайерами та мережами карток.
- Банк-емітент: Банк-емітент – це фінансова установа, яка випускає платіжні картки та пропонує інші послуги своїм споживачам.
- Банк-еквайр: банк-еквайр – це фінансова установа, яка на підтримку торговця опрацьовує платежі, здійснені за допомогою платіжних карток.

Важливо визначити елементи, які використовуються для обробки платіжних операцій:

- ICC: пластикова картка з вбудованою схемою, яка використовується для контролю доступу до ресурсу чи послуги.
- POI: Апаратний компонент, що дозволяє здійснювати покупки платіжними картками.
- POS: Місце, де клієнт ініціалізує платіж карткою.

Іншим терміном, який часто використовується, є PIN-код, який є ідентифікаційним номером, призначеним емітентом власнику картки та який використовується для автентифікації власника картки перед транзакцією в каналі CP.