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

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

Дипломної роботи
магістра
(назва освітньо-кваліфікаційного рівня)

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

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*
(назва освітньої програми)

освітньо-наукова програма *кібербезпека*

на тему: «Створення криптографічного модуля для ACS серверу»

Виконавець: студентка ІІ курсу, групи КБм-21

(підпис)	**Бєлозьорова Олеся Андріївна** (прізвище ім'я по-батькові)

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

Київ 2022

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

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

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

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студентці КБм-21 (група) Бєлозьоровій Олесі Андріївні (прізвище ім'я по-батькові)

Тема дипломної роботи Створення криптографічного модуля для ACS серверу

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

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

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес забезпечення безпеки даних, що обробляються під час проведення платіжних операцій.
Предмет досліджень	Методи та засоби створення умов для безпечної роботи ACS серверу.
Мета	Забезпечення безпеки платіжних даних.
Вихідні дані для проведення роботи	Методи захисту платіжних даних під час проведення електронних платежів.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна Розроблено модель для обміну даними з ACS на основі поєднання стеганографії та візуальної криптографії.

Практична цінність Запропоноване рішення може бути використане при впровадженні протоколу 3D-Secure в інформаційних системах банківського сектору

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Постановка та уточнення завдання	29.10.2021 - 30.10.2021
Формування запропонованого методу	01.11.2021 – 31.01.2022
Реалізація програмного рішення	01.02.2022 – 31.03.2022
Аналіз ефективності запропонованого рішення	01.04.2022 – 05.05.2022
Перевірка роботи на антиплагіат	06.05.2022 – 08.05.2022
Оформлення пояснювальної записки	09.05.2022 – 14.05.2022
Підготовка до захисту роботи	15.05.2022 – 19.05.2022

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Мінімізація ризиків, пов’язаних із аутентифікацією клієнта під час проведення оплати.

Соціальний ефект Підвищення рівня довіри користувачів до електронних платіжних операцій.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____
(підпис) (прізвище, ініціали)

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

РЕФЕРАТ

Пояснювальна записка: 74 с., 26 малюнків, 50 джерел.

Об’єкт дослідження: процес забезпечення безпеки даних, що обробляються під час проведення платіжних операцій.

Мета роботи: забезпечення безпеки платіжних даних.

Методи дослідження: спостереження, системний аналіз, формалізація, синтез, експеримент.

У роботі досліджено механізми безпеки при проведенні платіжних операцій, роботу протоколу 3D-Secure та роль ACS. Проведено аналіз сучасних рішень для ACS, які використовуться в українському та світовому банківському секторі. На основі проведеного аналізу було з’ясовано, що важливими елементом ACS, для якого необхідно впровадити нове рішення, є криптографічний модуль. У роботі запропоновано технологію передачі даних від ACS під час аутентифікації користувача, що базується на поєднанні стеганографії та візуальної криптографії. Для запропонованої технології було розроблено та протестовано програмне рішення.

Наукова новизна дослідження полягає у тому, що вперше було запропоновано метод поєднання стеганографії та візуальної криптографії для використання під час роботи протоколу 3D-Secure.

Напрямки подальших досліджень: дослідження роботи алгоритму у середовищі квантової криптографії; покращення роботи алгоритму; модифікація алгоритму при появі оновлень у протоколі 3D-Secure.

Ключові слова: електронний платіж, 3D-Secure, Access Control Server, аутентифікація, візуальна криптографія. стеганографія.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ACS - Access Control Server

ЕПЗ - Електронний платіжний засіб

3DS - 3D-Secure

CNP - Card Not Present

AVS - Address Verification Service

XML - eXtensible Markup Language

PCI DSS – Payment Card Industry Data Security Standard

ВК – Візуальна криптографія

OWASP - Open Web Application Security Project

API - Application Programming Interface

ЦС – Центр сертифікації

XSS - Cross-Site Scripting

E-banking - Electronic Banking

PAN – Personal Account Number

IP – Internet Protocol

ВСТУП

Актуальність. Протягом останніх років електронна платіжна система продовжує розвиватися все більше і більше через збільшення поширення інтернет-банкінгу та систем електронних покупок. Сучасні технології перетворюються на важливий елемент у фінансовій торгівлі.

Мільйони користувачів по всьому світу регулярно здійснюють різноманітні платежі через Інтернет. За останні два десятиліття електронні платіжні системи викликали величезний інтерес через важливу роль, яку вони відіграють у сучасній електронній комерції. Згідно зі звітом Statista Fintech, у 2020 році загальна сума транзакцій у сегменті цифрових платежів оцінювалась у 3 670 864 мільйона євро, а до 2023 року, за оцінками, зросте до 5 921 831 мільйона євро.

Систематичний огляд літератури показує, що інтерес суспільства до електронних гаманців та онлайн-платежів має позитивну тенденцію та зростає. Окрім цього, було виявлено, що із зростанням використання електронних платежів все більше досліджень зосереджують свою увагу на питаннях безпеки. Результати показують, що для подолання ключових питань безпеки електронні платежі повинні захищати такі властивості інформації як саме доступність, авторизацію, цілісність, невідмовність, аутентифікацію та конфіденційність.

Сьогодні вимоги до забезпечення безпеки електронних платежів, як правило, більш вимогливі, ніж існуючі загальні вимоги до безпеки в Інтернеті. З цього випливає, що постачальники електронних транзакцій та учасники платіжного процесу повинні звертати особливу увагу на свої контролі безпеки.

Метою роботи є забезпечення безпеки онлайн-платежів.

Для досягнення поставленої мети вирішуються такі **задачі:**

- дослідження існуючих технологій та програмних рішень аутентифікації користувача;

- розробка технології, яка може бути застосована в ACS із врахуванням поточних вимог безпеки банківського сектору;

- розробка програмного рішення, яке базується на запропонованій технології;
- перевірка програмного рішення на предмет стійкості до атак, а також виконання міжнародних регламентних документів у сфері інформаційної безпеки фінансового сектору.

Об'єктом дослідження є процес забезпечення безпеки даних, що обробляються під час проведення платіжних операцій.

Предметом дослідження є методи та засоби створення умов для безпечної роботи ACS серверу.

Методи дослідження, які були використані під час підготовки роботи: спостереження, системний аналіз, формалізація, синтез, експеримент.

Новизна одержаних результатів полягає в тому, що під час виконання роботи було розроблено технологію для обміну даними з ACS на основі поєднання стеганографії та візуальної криптографії.

Практична цінність отриманих результатів: запропоноване рішення може бути використане при впровадженні протоколу 3D-Secure в інформаційних системах банківського сектору.

Апробація. Роботу було апробовано на VII міжнародній конференції «Information Technology and Implementation» (IT&I-2021), на V Міжнародній науково-практичній конференції "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS)".

Увагу цієї роботи зосереджено на технології онлайн-платежів, які є елементом електронної платіжної системи. У даній роботі запропоноване рішення для розробки криптографічного модуля для ACS серверу, який є важливою складовою механізму 3DS-аутентифікації в системі онлайн-платежів.

РОЗДІЛ 1
ACCESS CONTROL SERVER ЯК ОБ'ЄКТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Структура систем електронних платежів

Система електронних платежів – це система для проведення грошових транзакцій, які здійснюються між споживачами та роздрібними продавцями з використанням можливостей інформаційно-обчислювальних систем, технології Інтернет та не потребують фізичної присутності власника ЕПЗ.

Існує досить багато систем електронних платежів, які створені в платіжному секторі в усьому світі, більшість джерел їх класифікують як: електронна готівка, електронний гаманець, карткова оплата.

Електронний гаманець – це комплекс програмного забезпечення комп'ютерного банкінгу, яке за допомогою відомостей про особу та її цифрові облікові дані дозволяє фізичній особі здійснювати онлайн-платежі [1].

Онлайн покупки користувачів, зроблені на мобільних пристроях, зростають швидкими темпами у всьому світі. У 2017 році обсяг мобільної роздрібної торгівлі становив понад 156 мільярдів доларів, а у 2018 році він зріс до 207 мільярдів доларів. Очікується, що до 2023 року дохід від мобільної комерції (mCommerce) сягне понад 339 мільярдів доларів [2].

1.2 Завдання безпеки у системах електронних платежів

Враховуючи те, що здійснення покупок в Інтернеті, є дуже зручним для користувачів, а відповідно, важливим для бізнесу, ключовим завданням учасників процесу є забезпечення безпеки для цього процесу. Системи електронних платежів часто стають метою для кіберзлочинців.

На Рис. 1 показано динаміку щодо зростання рівня шахрайста з платіжними картками у Великобританії у період 1998–2016 років [3].

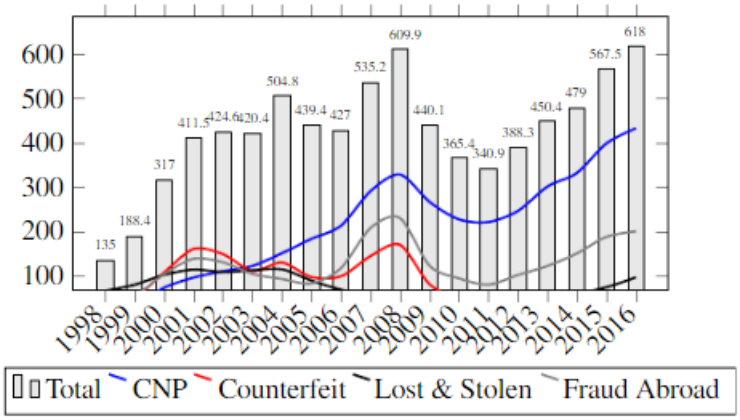


Рисунок 1.1 Рівень шахрайства з використанням платіжних карток у Великій Британії

З рисунка видно, що платіжна галузь ефективна для боротьби із існуючими видами шахрайства з платіжними картками. Однак шахрайство з платежами CNP досягло найвищої позначки, на яку припадає 70% загального шахрайства з картками, спричинивши збитки на суму 432,3 мільйона фунтів стерлінгів виключно за картками, випущеними у Великобританії [4]. Цей факт став поштовхом для інтеграції комплексної системи виявлення шахрайства з потоками протоколів платіжної системи CNP.

Загалом, платіжна система вимагає від ініціатора платежу (клієнта) ввести інформацію про свою платіжну картку на сторінці оформлення замовлення, наданій веб-сайтом продавця. Продавець, або сертифікований платіжний провайдер, збирає інформацію про картку, поєднує її з інформацією про транзакції та пересилає до банку-емітента картки для авторизації. Під час процесу авторизації емітент картки вирішує, схвалити чи відхилити трансакцію. Враховуючи, що дані платіжної картки статичні та надаються кожному онлайн-продавцю, існує значний ризик витоку та використання даних картки в шахрайських трансакціях. Після того, як дані платіжної картки залишають пристрій ініціатора платежу, немає гарантії, що дані картки будуть безпечно оброблятися продавцями.

Це також доводить статистика атак на такі сервіси як Ticketmaster і British Airways, під час яких були скомпрометовані дані мільйонів карток користувачів. У такій системі ускладнюється перевірка ініціатора платежу як дійсного власника

картки. Отже, платіжна система CNP сама по собі заснована на статичній інформації картки і, як така, за своєю суттю незахищена.

Таким чином, автор роботи доходить до висновку, що система забезпечення електронних платежів повинна підтримувати властивості, наведені нижче [5].

Авторизація

Електронний платіж має бути доступним лише для авторизованих клієнтів, і, крім того, дані, що обробляються в процесі проведення платежу, мають охоплювати лише авторизовані теми. Система повинна мати критерії для визначення того, що, використовуючи вхідний набір даних, задана транзакція може бути схвалена. Залучені активи мають бути в змозі підтвердити, що кожен, хто бере участь у транзакції, має право на здійснення відповідних операцій.

Конфіденційність

Конфіденційність надзвичайно важлива у сфері електронної комерції через можливість того, що хакери можуть отримати конфіденційні дані користувачів. У системах електронних платежів користувачі повинні отримувати доступ до керування електронними рахунками тільки після проходження системи верифікації. Інформація, введена клієнтом, не повинна бути легкодоступною для інших клієнтів систем електронного банкінгу.

Конфіденційність – це гарантія того, що інформація надається виключно уповноваженим особам або компаніям. Тільки авторизовані одержувачі повинні мати можливість отримати зашифроване повідомлення, щоб інші не могли переглянути його вміст та здійснювати керування перебігом транзакцій. Він повинен захищати конфіденційну інформацію від будь-якої неавторизованої особи, процесу чи пристрою.

Цілісність

Щоб запобігти несправності або фізичної шкоди, мережа електронних платежів потребує точних даних. Цілісність повинна учасникам процесу для того, щоб переконатись у тому, що інформація, яка обробляється, є достатньо точною для потреб процесу. Інформація має бути повною та автентичною, щоб переконатися, що не будуть скомпрометовані під час виконання транзакції або, можливо, процесі

передачі. Цілісність даних збереже конфіденційність усіх складових електронної транзакції. Інформація та пристрої не були змінені та пошкоджені зовнішніми сторонами. Зазвичай підтверджуються дійсні облікові дані користувача.

Надійність та ефективність

Оскільки технології електронних платежів трансформуються, виникає потреба змінюватися та розвиватися. У конкурентних ситуаціях стійкість до виходу на ринок має вирішальне значення для вимірювання успіху системи. Заходи безпеки для електронних платіжних рішень повинні бути перевірені під наглядом функції моніторингу небезпеки, щоб забезпечити їхню надійність та ефективність. Зростання фінтех відбувається високими темпами в банківському секторі усього світу. Щоб залишатися доступними для своїх користувачів, банки розвивають інтернет-банкінг з метою досягнення більшої продуктивності, а також ефективності. Ефективність є важливою характеристикою системи електронних платежів. Забезпечуючи високу ефективність у здійсненні транзакцій, споживачі, частіше за все, починають частіше використовувати послуги електронних гаманців у повсякденному житті. Ефективність можна істотно підвищити за рахунок зменшення трансакційних витрат за рахунок пошуку оптимальної технології проведення платежу із залученням мінімальної кількості учасників платіжного процесу.

Зручність підтримки операції

Застосунок, на базі якого здійснюється операція, повинен підтримувати механізм, що здійснювати електронний Інтернет-платіж, а продавець повинен максимально спростити шлях увімкнення механізму користувачем, наприклад, використовувати плагін, який підтримується більшістю наявних браузерів. Додаток не суперечить іншим мобільним системам або неплатіжним функціям.

Системи електронних платежів не можуть бути успішні без відповідної залученості користувачів. Для підтримки зв’язку між пристроями користувача та мобільними платіжними системами необхідна бездротова мережа 2G/3G/4G/5G або мережа Wi-Fi, відповідно, дуже важливо, щоб мережа, за допомогою якої відбувається обмін даними між пристроєм користувача та банківськими мережами,

була достатньо захищена, оскільки інциденти безпеки Інтернет-банкінгу зашкодять довірі до банку.

Окрім цього, важливо, щоб у емітента була можливість збирати та приймати до уваги достатню кількість про транзакцію та користувацьку активність. Це дає можливість передбачити, запобігти або швидко відреагувати на інцидент безпеки та можливі протиправні дії щодо власника картки. З цього випливає, що учасники процесу повинні підтримувати функції передачі деталізованої інформації про перебіг операції: версія браузера клієнта, пристрій, деталі операції, країна продавця, назва продукту, що оплачується тощо.

На Рис. 1.2 наведено схему взаємодії учасників процесу у відповідності із тим, за які властивості безпеки вони відповідають.

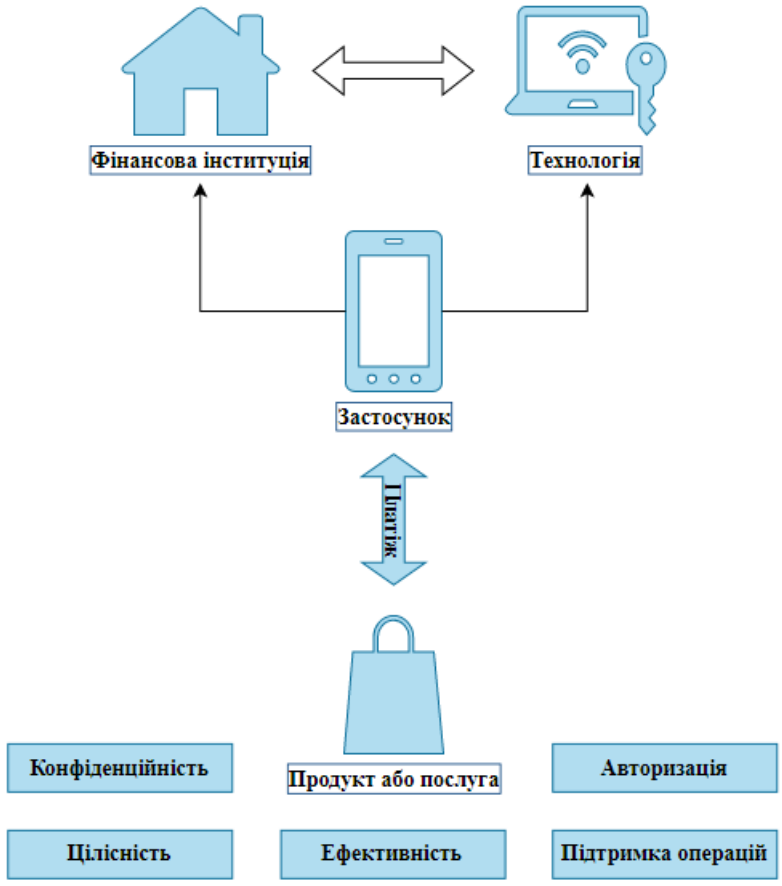


Рисунок 1.2. Учасники процесу електронної операції

1.3 Огляд наявних механізмів верифікації користувачів у системах електронних платежів

Address Verification Service

Система AVS [6] дозволяє емітенту картки порівнювати дані адреси, що надаються продавцем разом із деталями транзакції, із даними користувача, які емітент знає про нього. На основі того, наскільки надана інформація відповідає дійсності, учасники процесу можуть приймати рішення щодо того, чи продовжувати конкретну операцію. Таким чином, емітент приймає рішення про авторизацію на основі даних, включно з результатом перевірки AVS, а продавець може попередити шахрайство, якщо результат перевірки буде повністю негативним.

Результат перевірки AVS може бути одним із параметрів, які приймаються до уваги під час побудови скоринг системи та формування аналітики, але не може виступати самостійним інструментом захисту від шахрайства.

Токенізація картки

Принцип токенізації полягає у тому, що дані картки, разом із будь-якими даними, які сервіс токенізації вважатиме важливими, за допомогою перетворень замінюються на токен, після чого для ініціювання транзакції використовується саме токен [7]. Токен виступає вказівником для емітента картки, де зберігаються дані картки, при цьому сам не несе цінності, тому що може працювати тільки для заданих учасників процесу. Таким чином, якщо зловмисник отримає доступ до токену, але не отримає доступ до системи продавця, він не матиме можливості для проведення маніпуляцій із карткою користувача.

Аналітика поведінки

Під час проведення фінансових операцій, всі учасники процесу повинні забезпечувати на своєму боці якісну аналітику відносно користувацької активності. За допомогою наявної інформації емітент, еквайер та продавець можуть формувати тенденції поведінки того чи іншого користувача для того, щоб швидко та однозначно ідентифікувати аномальні відхилення від звичної поведінки та

попереджати шахрайство із карткою. До параметрів, які приймаються до уваги, входять [8]:

- кількість, частота та середня сума фінансових операцій;
- сфера діяльності продавця, що визначається за допомогою параметра MCC – Merchant Service Code;
- якість та повнота інформації, що передається про користувача, в тому числі пошта, адреса, ім’я користувача;
- відповідність країни перебування користувача та країни його IP адреси.

3D-Secure

3-D Secure - це протокол на основі XML, який створює додатковий механізм верифікації користувача під час створення онлайн-платежів з використанням платіжної картки [9].

Протокол був запропонований Visa у грудні 2001 року як «Virefied by Visa», а також імплементований Mastercard як «SecureCode». У 3-D Secure протоколі кожен банк-емітент повинен підтримувати Сервер контролю доступу (ACS) для підтримки аутентифікації власників картки.

3D-Secure 2 (3DS2) - це новий протокол автентифікації для онлайн-платежів карткою, призначений для вдосконалення 3D Secure 1 (3DS1) шляхом вирішення проблемних ситуацій старого протоколу та забезпечення набагато більш плавної та інтегрованої взаємодії з користувачем. У проткоолі другої версії розроблено механізми верифікації користувача без необхідності проходити двохфакторну верифікацію за допомогою одноразового паролю [11].

Початковий протокол 3D Secure, створений у співавторстві Visa і Arcot (тепер CA Technologies) [12], забезпечив безпечні покупки в Інтернеті, забезпечуючи зв’язок «трьох доменів» між емітентом, продавцем і власником картки та полегшував діалог автентифікації між власником картки та емітентом. Тоді головною метою було покращити безпеку онлайн-покупок і 3D Secure. З часом відмова від транзакцій став проблемою, яка дала зрозуміти, що створення кращого досвіду користувачів для покупок в Інтернеті стає необхідним для бізнесу. Лідери галузі, як-от CA Technologies, розробили рішення, які зосереджені на покращенні

платежів власником картки для транзакцій 3D Secure шляхом оцінки ризику транзакції, щоб допомогти визначити, чи була вона ініційована законним власником картки. Якщо транзакція мала низький ризик, аутентифікацію можна було б обійти, що допомогло зменшити кількість відмов від транзакції.

Одним з головних моментів, що відрізняють нову технологію, є те, що 3DS 2.0 надає додаткові дані, які розширять здатність рішень аутентифікації на основі ризиків для ідентифікації власника картки та поведінки пристрою. Фундаментальна передумова 3DS 2.0 подібна до нашої реалізації 3DS 1.0 з CA Risk Analytics — використовувати додаткові елементи даних аутентифікації, які доступні під час транзакції, щоб як продавець, так і емітент могли зробити більш інформований і точний рішення про завершення чи відмову в транзакції за відсутності картки. Доступні дані включають інформацію, пов’язану з транзакцією, а також деталі про пристрій, який використовується для транзакції. CA Risk Analytics також використовуватиме ці додаткові дані в 3DS 2.0, щоб покращити весь процес прийняття рішень.

У таблиці 1.1 наведено порівняльну таблицю наведено дані щодо використання додаткових механізмів верифікації у різних країнах [14].

Таблиця 1.1.

Додаткові механізми верифікації

Регіон	**Домінуюча інституція**	**Вимоги**
Австралія	Visa	Усі кредитні, дебетові та передплачені картки з можливістю перезавантаження мають бути зареєстровані в Verified by Visa (VbV). Продавець повинен підтримувати VbV, якщо обсяг трансакцій, які визнані шахрайськими, електронної комерції Visa становить 25 000 доларів США або вище і перевищує 0,25% загального обсягу

Регіон	**Домінуюча інституція**	**Вимоги**
		трансакцій електронної комерції продавця. Якщо продавець перевищує поріг шахрайства, він повинен запровадити VbV протягом 120 днів після виявлення відповідних інцидентів. Будь-який покупець повинен мати змогу перевірити, що продавець використовує VbV, якщо вони продавець перевищив поріг шахрайства у будь-якому кварталі.
Бразилія	Visa	Емітенти повинні переконатися, що всі дебетові рахунки та ідентифікатори банку (BIN) беруть участь у VbV.
Канада	Visa/Mastercard	Емітенти повинні переконатися, що всі корпоративні та особисті дебетові BIN беруть участь у 3DS.
Китай	Visa	Програми VbV емітентів повинні використовувати динамічну аутентифікацію.
Європа	Visa/Mastercard	Друга Директива про платіжні послуги (PSD2) зобов’язує впроваджувати надійну автентифікацію клієнтів (SCA) для електронних транзакцій. Постачальники платіжних послуг, до яких входять банки, постачальники електронних грошей та платіжні установи, повинні застосовувати SCA до всіх електронних платежів, ініційованих платником (наприклад, карткові платежі та кредитні

Регіон	**Домінуюча інституція**	**Вимоги**
		перекази), якщо платіж не кваліфікується як низикоризиковий і не потрапляє під перелік винятків.
Індія	Головний банк	Двофакторна аутентифікація вимагається для всіх трансакцій з карткою на суму понад 2000 рупій. Порогове значення було введено у 2018 році, щоб полегшити процес оплати для користувачів та задовольнити потреби компаній електронної комерції, компаній з онлайн-бронювання квитків і додатків для виклику таксі.
Японія	Japan Online Game Association	Усі члени асоціації повинні впроваджувати 3DS.
Нова Зеландія	Visa	Усі кредитні, дебетові та передоплачені картки Visa мають бути зареєстровані у VbV. Віртуальні рахунки, пов’язані з комерційними картками Visa, виключені з цієї вимоги. Продавець повинен підтримувати VbV, якщо обсяг шахрайських трансакцій електронної комерції Visa становить 25 000 доларів США або вище і перевищує 0,25% загального обсягу трансакцій електронної комерції продавця або якщо обсяг шахрайських транзакцій електронної комерції продавця перевищує 05 000

Регіон	Домінуюча інституція	Вимоги
		доларів США або більше 050 доларів США або 205% від загального обсягу трансакцій електронної комерції продавця.

1.4 Опис протоколу 3D-Secure

Під час проведення верифікації, у роботі протоколу 3DS залучені 3 сторони-учасники процесу («Три домени»), що наведені нижче [15].

Домен покупця – транзакція та 3DS перевірка транзакції ініціюються з домену банку, що проводить обмін між учасниками процесу (еквайера);

Домен взаємодії – середовище, за допомогою якого відбувається обмін даними між доменом покупця та доменом емітента. Зазвичай цю функцію виконують міжнародні платіжні системи.

Домен емітента – процес авторизації платежу та приняття рішення щодо необхідності додаткової перевірки відбувається на стороні банка-емітента.

На рисунку 1.2 наведено схему взаємодії учасників 3DS-процесу. На схемі вказано функції конкретних компонентів процесу, при цьому схема фактичної реалізації системи може відрязнятись. Так, наприклад, клієнт 3DS може взаємодіяти безпосередньо із сервером 3DS або або 3DS Server і 3DS Requestor можуть бути функціонально об’єднані [16].

Рисунок 1.2 Схема взаємодії 3DS

Процес починається з того, що ініціатор платежу заповнює дані своєї платіжної картки на сторінці оформлення замовлення, наданій веб-сайтом продавця. Коли натискається кнопка «Оплатити», веб-сервер продавця, на якому розміщено плагін 3DS 2.0, генерує унікальний ідентифікатор транзакції та з'єднує сеанс ініціатора платежу з емітентом картки. Емітент картки підключається до веб-браузера ініціатора платежу (WB) і надсилає пристрою JavaScript (dfp.js), запрограмований для отримання даних про браузер і операційну систему. JavaScript в основному включає такі методи [17]:

- deviceprint browser(): Цей метод отримує інформацію про ініціатора платежу (WB) та операційну систему, включаючи: назву браузера, основну та додаткову версію, підтримувані мови, встановлені мови, назву операційної системи, версію операційної системи та платформу операційної системи (Win32 або Win64);

- deviceprint display(): Цей метод фіксує детальну інформацію про екран, включаючи глибину кольору, ширину екрана, висоту, доступну висоту, глибину буфера та глибину пікселів;

- deviceprint software(): записує (WB'S) плагіни та їх типи. Метод також має логіку для вилучення налаштувань відстеження та реклами браузера, як це передбачено DoNot-Track і Useofadblock;

- deviceprint java(): використовується для перевірки, чи підтримує браузер ініціатора платежу Java чи ні.

- cookies(): використовується для перевірки, чи ввімкнено файли cookie користувачем WB.

Інформація, зібрана за допомогою вищевказаних методів, об'єднується в один рядок і кодується у звичайний текст base-64 (як визначено специфікаціями протоколу 3DS 2.0) перед відправкою як елемент форми до емітента картки. Часто емітент картки використовує IP-адресу як індикатор для визначення місцезнаходження машини ініціатора платежу. На наступному етапі продавець формує запит на аутентифікацію (AReq), який пересилається відповідному емітенту картки.

Сервер контролю доступу – Access Control Server (ACS) керує повідомленнями із запитом/відповіддю на аутентифікацію 3DS 2.0. AReq містить дані картки, надані ініціатором платежу, інформацію про обліковий запис продавця та іншу інформацію, пов'язану з транзакціями. Емітент картки збирає інформацію про транзакції від продавця та відомостей WB, наданих скриптами відбитків пальців пристрою, і виконує оцінку ризику шахрайства (FRA) для даної трансакції. На основі результатів FRA емітент картки вирішує, чи кинути виклик ініціатору платежу одноразовими кодами доступу, чи автентифікувати ініціатора платежу без додавання додаткового кроку для ініціатора платежу. Для трансакції, показаної на 2, емітент картки вирішує оскаржити аутентифікацію. У випадку, якщо емітент має сумніви щодо верифікації кінцевого користувача, він через повідомлення Authentication Response (ARes) відповідає продавцю, вказуючи, що для подальшої обробки транзакції необхідний додатковий крок перевірки. У випадку frictionless аутентифікація емітент одразу надасть відповідь про успішну аутентифікацію.

Продавець ініціює повідомлення Challenge Request(CReq) і надсилає його емітенту картки. Видавець надсилає інтерфейс користувача виклику (UI) до WB

ініціатора платежу. Інтерфейс користувача — це платформа взаємодії, де емітент картки може взаємодіяти з ініціатором платежу, щоб отримати відповідь на виклик. У цей момент емітент картки запропонує запит або OTP на зареєстрованому пристрої ініціатора платежу (наприклад, мобільному телефоні). Ініціатор платежу вводить OTP на інтерфейсі 3DS2.0, і після успішної аутентифікації емітент визначає ініціатора платежу як відповідного власника картки та форматує повідомлення із запитом на результати (RReq) із криптографічним хешем, яке пересилається продавцю.

RReq і хеш пізніше використовуються мережею авторизації для перевірки цілісності повідомлень аутентифікації. Щоб підтвердити отримання RReq, продавець готує відповідь на результати (RRes) і пересилає її емітенту. Нарешті, емітент форматує повідомлення відповіді на виклик (CRes) і передає його назад до продавця. CRes вказує на завершення оскаржуваної аутентифікації. Слід зазначити, що повідомлення CReq і CRes застосовні лише до транзакції 3DS2.0, у якій потребується додатковий крок перевірки. На Рисунку 1.3 зображено схему інформаційних потоків 3DS2.

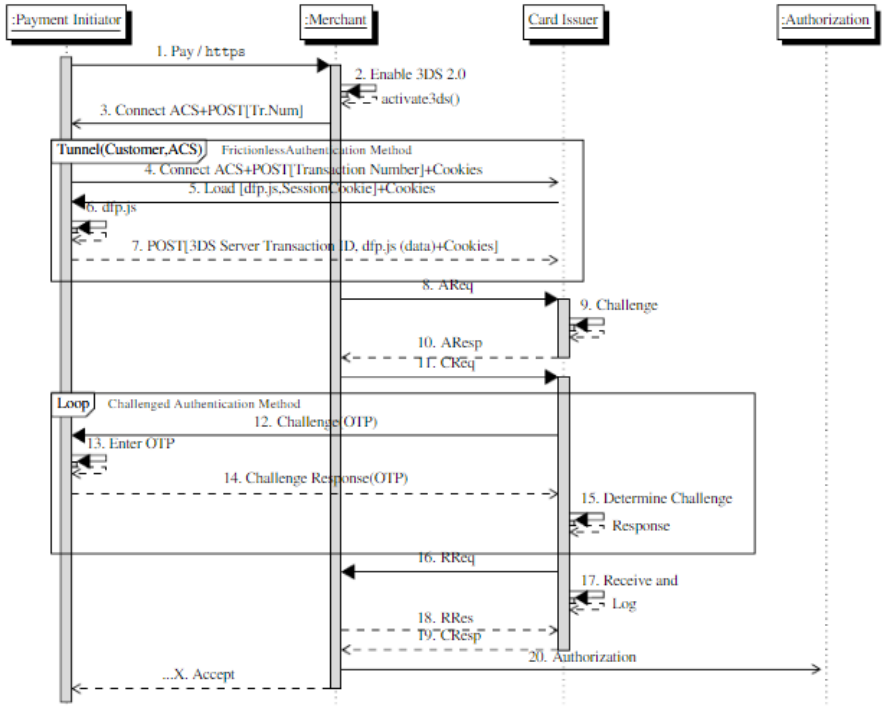


Рисунок 1.3. Схема інформаційних потоків 3DS2

Елементи даних 3DS можна розділити на чотири основні категорії [18]:

1. Дані пристрою – включає конкретну інформацію про пристрій для кожного каналу, наприклад, нативну програму для iOS або рідну програму для Android та деталі браузера. Ці поля обов'язкові для заповнення для визначення середовища, у якому проходить платіж.

2. Дані сторінки транзакцій та оформлення замовлення – містить необхідну (а іноді й умовно необхідну) інформацію, зібрану в процесі оформлення покупки споживачем із елементами продавця та транзакції.

3. Дані аутентифікації – складається з двох категорій необов'язкових елементів даних, обидва пов'язані з аутентифікацією, які продавець може надати емітенту для додаткової інформації.

- Аутентифікація продавця включає дані про будь-яку автентифікацію, не пов'язану з 3DS, яка може бути використана споживачем для отримання доступу до веб-сайту продавця, облікового запису або даних картки в файлі.

- Попередня аутентифікація користувача включає елементи даних, зібрані з попередньої транзакції з тим самим споживачем і PAN, де 3DS було застосовано та проведено з іншою транзакцією.

4. Дані продавця – складається з двох категорій необов'язкових елементів даних, пов'язаних із ризиками споживача та інформацією про обліковий запис, яку продавець може надати емітенту для додаткової інформації.

- Інформація про ризики продавця включає дані, які тільки продавець зможе перевірити на основі поточних деталей замовлення і які використовуються для аналізу ризиків на рівні продавця.

- Інформація про обліковий запис власника картки включає дані, характерні для облікового запису споживача на веб-сайті або в додатку продавця; це пов'язано з історією або деталями їхнього облікового запису.

Завдяки 3DS продавці також мають можливість надавати емітенту додаткову інформацію на основі інформації продавця про аутентифікацію споживача та дані облікового запису. Ці дані можуть допомогти емітентам визначити ризик транзакції. Регулярне отримання цієї інформації може підвищити впевненість емітента в

аутентифікації транзакцій і забезпечити безперебійний досвід для користувача (порівняно з вимогою виклику).

Емітенти також мають доступ до моделей купівлі власника картки за PAN/рахунком і до різноманітних даних, до яких не має доступу користувач. Ці дані можуть включати:

- інші продавці, у яких власник картки здійснює операції;
- канали та моделі купівлі власника картки;
- взаємодія з програмою для мобільного банкінгу, включаючи доступ до аутентифікації;
- середні витрати власника картки;
- будь-яке повідомлення про шахрайство з боку платіжних систем;
- швидкість транзакцій;
- діяльність за іншими картками в портфелі емітента;
- інформація про геолокацію.

Продавці мають унікальну можливість бачити діяльність споживача безпосередньо з ними, що може бути корисно для аутентифікації. Ці дані можуть включати:

- збережені картки на торговому рахунку споживача, незалежно від емітента;
- аутентифікація на веб-сайті/додатку продавця;
- історія пароля та облікового запису;
- використана адреса електронної пошти;
- частота замовлень споживачів у продавця;
- спосіб доставки та терміни доставки;
- взаємодія споживача з їхнім веб-сайтом/додатком;
- сума та підрахунок подарункової картки в межах замовлення;
- будь-яка шахрайська діяльність або підозра у веденні такої.

Отримуючи специфічні для продавця дані та будь-які попередні дані аутентифікації (не 3DS), емітенти можуть побачити детальну інформацію про діяльність власника картки, яку вони ніколи раніше не бачили. Ці додаткові дані

можуть допомогти емітенту впевнено підтвердити трансакцію, оскільки продавець має додаткову видимість цього споживача і впевнений, що транзакція дійсна.

Ці різні категорії даних надають продавцям потужний інструмент. Впроваджуючи 3DS, продавці можуть впливати на моделювання ризиків шляхом обміну цими елементами даних, що може призвести до безперешкодних транзакцій, зміщення відповідальності за шахрайство при застосуванні аутентифікації та прийнятних рішень щодо авторизації емітента.

Головними функціональними системами є компоненти, наведені нижче.

ACS – постачальник технологічних рішень, який дозволяє емітентам і процесорам розгортати програму 3DS для власників своїх карток. Ця служба може бути локальною або розміщеною, і отримує повідомлення про автентифікацію, пропонуючи наступні дії у процесі та відповідь. Перед використанням у виробництві ACS може бути сертифікований, PCI та кожною мережею, яку вона підтримує, для кожної версії 3DS.

3DS Server (3DSS) – раніше відомий як плагін для продавців (MPI), цей постачальник технологічних рішень підтримує еквайєрів і продавців програм 3DS з платіжних мереж. Перед використанням у виробництві 3DSS може бути сертифікований EMVCo, PCI та кожною мережею, яку він підтримує, для кожної версії EMV 3DS. 3DSS забезпечує функціональний інтерфейс між потоками середовища запитувача 3DS і сервером каталогів (DS). Функції, виконувані сервером 3DS, включають [19]:

- збір необхідних елементів даних для повідомлень 3DS.
- автентифікація DS.
- перевірка DS, 3DS SDK та 3DS Requestor.
- забезпечення захисту вмісту повідомлення.

3DS SDK (Набори для розробки програмного забезпечення) – постачальник технологічних рішень або платформа, яка надає продавцям можливість розгортати аутентифікацію в середовищі нативного мобільного додатка. Перед використанням у виробництві пакет SDK 3DS може бути сертифікований EMVCo, PCI та кожною мережею, яку він підтримує, для кожної версії EMV 3DS.

Сервер каталогів (DS) - сервер, який керує маршрутизацією запиту аутентифікації до належного ACS. DS також може бути «замінним» для аутентифікації, коли ACS має простої або якщо емітенти ще не підключені до EMV 3DS. DS також підтримує повідомлення PReq/PRes, інформуючи 3DSS про активацію BIN емітента. DS веде списки діапазонів карток, для яких може бути доступна автентифікація, і координує зв'язок між 3DSS та ACS, щоб визначити, чи доступна автентифікація для певного номера картки та типу пристрою. Функції:

- автентифікація сервера 3DS та ACS.
- маршрутизація повідомлень між сервером 3DS та ACS.
- перевірка сервера 3DS, пакета SDK 3DS та запитувача 3DS.
- визначення конкретних програмних правил (наприклад, логотипи, значення часу очікування тощо).
- вбудовані сервери 3DS та ACS.
- ведення версій ACS та URL-адрес методу 3DS.

1.5 Функції та вимоги до серверу контролю доступу

1.5.1. Функції серверу контролю доступу

ACS містить правила аутентифікації та контролюється емітентом. Функції ACS включають [20]:

- перевірку того, чи придатний номер картки для аутентифікації 3-D Secure;
- перевірку того, чи придатний тип пристрою користувача для автентифікації 3-D Secure;
- аутентифікація власника картки або підтвердження інформації облікового запису.

Хоча ці функції можуть належати до однієї логічної системи ACS, різні реалізації можуть розділяти обробку за функціями або іншими характеристиками (наприклад, діапазон номерів картки) між кількома фізичними серверами.

1.5.2. Функціональні вимоги до серверу контролю доступу

Робота ACS поділяється на три етапи, наведені нижче [21].

Етап верифікації клієнта є одним із важливих етапів безпеки Ebanking, оскільки багато шахрайств, пов’язаних з E-banking, трапляються через неідентифікованих зловмисників. Цей етап гарантує, що оригінальний власник є користувачем і запитує послуги електронного банкінгу. Це реалізовано за допомогою MAC-адреси банківського ключа, інформації відбитків пальців конкретного користувача, особистого імені користувача та одноразового пароля. Початковий запит на операцію E-banking надсилається з MAC-адресою електронного банківського ключа конкретного користувача. Подальші операції виконуються тільки за умови правильної MAC-адреси. Далі відбиток пальця користувача перевіряється на підтвердження. Якщо результат позитивний, система запропонує ім’я користувача. У випадку, якщо ім’я користувача коректне, йому надається доступ до одноразового SMS або Push-повідомлення для підтвердження.

Етап перевірки сервера гарантує, що клієнт отримує доступ до оригінального сайту електронного банкінгу. Це реалізується шляхом перевірки відбитка пальця з боку клієнта. Відбитки пальців дійсних користувачів зберігаються в базі даних банківського сервера. Ця інформація відбитків пальців надсилається на дійсний запит клієнта. Додаток електронного банківського ключа дозволяє подальший процес електронного банкінгу, лише якщо інформація відбитків пальців збігається одна з одною. Ця перевірка відбитків пальців підтверджує оригінальність обох сторін одночасно (тобто лише оригінальний банківський сайт зможе надіслати відбиток пальця оригінального клієнта).

Етап захищеної передачі даних гарантує, що операції з обслуговуванням електронного банкінгу здійснюються безпечно між клієнтом і сервером. Це реалізовано з використанням тимчасових ключів сеансу для шифрування та дешифрування інформації про транзакції. Ключі сеансу видаються в кінці процесів перевірки клієнта і сервера. Сесійний ключ шифрується відкритим ключем клієнта та закритим ключем сервера E-banking і видається клієнту. Сеансовий ключ

шифрується за допомогою приватного ключа сервера E-banking, щоб гарантувати, що ключ сесії видається оригінальним сайтом Ebanking, і зашифрований за допомогою відкритого ключа клієнта, щоб гарантувати, що ключ сеансу розшифровується тільки оригінальним клієнтом. Термін дії ключів сеансу закінчується, якщо жодна транзакція не записана протягом 10 хвилин після ініціації, або якщо користувач запитує припинення сеансу.

1.5.3. Вимоги до заходів безпеки для серверу контролю доступу

Кожна система, яка виконує функції ACS, повинна постійно проходити процедуру аудиту за міжнародним стандартом PCI 3DS [22].

Ризики для середовища 3DS слід оцінювати щонайменше раз на рік та при значних змінах. Оцінка ризику має визначити активи, загрози, ймовірність та потенційні наслідки. До уваги ризиків слід віднести внутрішні та зовнішні атаки, наприклад, для кіберзлочинів, шахрайства або крадіжки, збої внутрішнього контролю та шкідливе програмне забезпечення. Ризикам слід розставити пріоритети та виділити ресурси для впровадження засобів контролю, які знижують ймовірність та/або потенційний вплив реалізації загрози.

Якщо підозрілий трафік не блокується автоматично, має бути створено сповіщення, яке активно відстежується та негайно досліджується.

Якщо підозрілий трафік автоматично блокується, запис трафіку також має бути створений та досліджений, щоб визначити, чи потрібні дії для запобігання подальшій атаці.

Якщо програмне забезпечення розробляється організацією 3DS, або програмне забезпечення на замовлення або спеціально розроблене третьою стороною для об’єкта 3DS, у процесі розробки програмного забезпечення слід використовувати методи безпечного кодування для усунення поширених уразливостей, застосовних до певної технології. Підприємство має залишатися в курсі тенденцій щодо вразливості та оновлювати свої методи безпечного кодування та навчання розробників, якщо це необхідно для подолання нових загроз.

Приклади поточних найкращих практик включають OWASP, SANS CWE Top 25 та CERT Secure Coding [23].

Розробники програм повинні бути належним чином навчені для виявлення та вирішення проблем, пов’язаних із поширеними вразливими місцями кодування. Наявність персоналу, компетентного у практиці безпечних методів розробки програмного забезпечення, мінімізує кількість вразливостей безпеки, випадково запроваджених через погані методи кодування. Навчання для розробників може проводитися вдома або третіми сторонами і має відповідати використаній технології.

Загальні методи тестування безпеки програмного забезпечення включають моделювання загроз, огляди коду, нечіткове тестування та тестування на проникнення. Тестування безпеки програмного забезпечення має проводити хтось інший, ніж розробник коду, щоб забезпечити незалежну, об’єктивну перевірку. Автоматизовані інструменти або процеси також можуть використовуватися замість ручних оглядів, але майте на увазі, що автоматизованому інструменту може бути важко або навіть неможливо визначити деякі помилки кодування або інші проблеми безпеки.

Суб’єкти 3DS часто передають розробку та підтримку залучених сервісі на аутсорсинг або покладаються на стороннього постачальника послуг для певних зі своїх функцій. Поширені приклади включають розміщення програм, керування мережевими пристроями або базами даних, а також підтримку фізичної безпеки. Крім того, суб’єкт 3DS може делегувати аспекти процесу транзакцій 3DS, наприклад, аналіз трансакцій 3DS на основі оцінки ризик, третій стороні. Якщо стороння служба може вплинути на функціональність 3DS або безпеку роботи протоколу, для цієї служби повинні впроваджуватись і підтримуватись відповідність міжнародним сертифікаціям, які покладаються на всіх учасників платіжного процесу.

Критичні кроки в цьому процесі включають розуміння того, на які функції та компоненти системи 3DS може вплинути постачальник послуг, а також визначення

вимог PCI 3DS, які є відповідальністю постачальника(ів) послуг, а які є відповідальністю об’єкта 3DS.

Відповідно, якщо сторона, у керуванні якої знаходиться сервер керування доступом, передала деякі або всі функції постачальнику, такий постачальник повинен відповідати всім нормам безпеки PCI 3DS.

Очікується, що до ACS будуть застосовані процеси для управління ризиками, пов’язаними із сторонніми постачальниками, зокрема:

- проведення належної перевірки перед залученням;
- чітке визначення відповідальності за безпеку;
- періодична перевірка того, що узгоджені обов'язки виконуються;
- письмова угода, яка гарантує, що обидві сторони розуміють і визнають свої обов'язки щодо безпеки.

Хоча остаточну відповідальність за безпеку даних 3DE і 3DS несе суб’єкт 3DS, від постачальників послуг може знадобитися продемонструвати відповідність застосовним вимогам PCI 3DS на основі наданої послуги. Постачальник послуг може зробити це одним із способів:

(a) проходження оцінки PCI 3DS та надання доказів своїм клієнтам 3DS, щоб продемонструвати його відповідність застосовним вимогам PCI 3DS; або

(b) для кожної з оцінок клієнтів-об’єктів 3DS, надання необхідних доказів для демонстрації відповідності застосовним вимогам PCI 3DS.

Докази, надані постачальниками послуг, мають бути достатніми для підтвердження того, що обсяг оцінки постачальника послуг 3DS охоплює послуги, застосовні до об’єкта 3DS, і що відповідні вимоги PCI 3DS були вивчені та визначені як діючі. Конкретний тип наданих доказів буде залежати від того, як здійснюється управління оцінками. Наприклад, якщо постачальник послуг проходить власну оцінку PCI 3DS, сертифікат відповідності 3DS постачальника послуг та/або відповідні розділи звіту про відповідність 3DS постачальника послуг (відредагований для захисту будь-якої конфіденційної інформації) можуть надати деякі або всі інформації. Якщо постачальник послуг не має 3DS AOC або звіту про

відповідність, надані докази повинні охоплювати конкретні вимоги, які оцінюються, і відповідати методам перевірки, описаним для кожної вимоги.

Єдиний дозволений трафік має здійснюватися для транзакцій 3DS або для підтримки функції 3DS, або для підтримки компонента системи 3DS — наприклад, для цілей безпеки чи керування. Системи в рамках 3DE повинні бути обмежені тими, які необхідні для виконання або підтримки функцій 3DS.

Слід ідентифікувати всі типи інтерфейсів, включаючи фізичні, логічні та віртуальні.

Приклади типів файлів, які потребують захисту, включають файли базової конфігурації, дані збірки системи, образи системи та процедури збірки. Засоби керування повинні захищати як цілісність, так і конфіденційність таких даних, щоб зловмисник не міг змінити безпечну конфігурацію компонента системи 3DS, встановити власну конфігурацію або використати інформацію для виявлення пробілів у безпеці, які вони потім можуть використати.

Усі функції, які явно не потрібні для роботи системи, слід вимкнути або заблокувати; і конфігурації повинні бути розроблені таким чином, щоб запобігти поширеним сценаріям атак додатків, таким як XSS, Clickjacking та атаки ін'єкції. Програми мають бути налаштовані так, щоб обмежувати вміст і функціональність із зовнішніх джерел лише тим, що необхідно для бізнес-цілей. Якщо функціональність або вміст із надійних зовнішніх джерел, наприклад, веб-сайтів третіх сторін, необхідні для бізнес-цілей, тоді ці джерела та методи, за допомогою яких їм дозволено надавати такий вміст (наприклад, як iframe, прямі повідомлення тощо) мають бути явно авторизовані, а всі інші джерела та методи заблоковані.

1.6 Дослідження рішень для ACS у банківському секторі України

Ключове питання для більшості емітентів полягає в тому, які позитивні зміни у продуктивності роботи вони можуть отримати із впровадженням рішень, які відповідають сучасним нормам безпеки, але практика впровадження технології показує, зо найкращий рівень ефективності досягається тоді, коли всі учасники

процесу можуть обмінюватися і обробляти велику кількість даних про користувача і транзакцію. Відповідно, сучасне рішення для серверу контролю доступу повинно включати в себе широкий спектр інструментів для обробки інформації та прийняття рішень на основі побудованих скорингових моделей.

Taslink

Taslink – процесинговий центр, на базі якого працюють такі банки як Універсал банк (включаючи продукт Monobank), Таскомбанк, А-Банк, ProCreditBank та інші.

У якості рішення для ACS використовується продукт TranzWare e-Commerce ACS 3.1, розроблений компанією Compass Plus [13].

Продукт офіційно входить до складу сертифікованих партнерських програм Verified by Visa, Mastercard SecureCode, American Express SafeKey, JCB J/Secure, UPI SecurePay та SecurePlus, а також MirAccept.

Підтримує роботу з мобільними платіжними сервісами Apple Pay, Samsung Pay та Google Pay та надає незалежність від існуючих хостових рішень.

Розробники гарантують легкість інтеграції за мінімального впливу на наявні системи. Є серверним програмним забезпеченням, відповідно, може бути модульно встановлений на сервер, який виконуватиме відповідні функції. Окрім цього, програмний комплекс дає можливість гнучкого використання: впровадження у самому банку чи аутсорсинг.

Проте головним недоліком продукту є те, що він розроблений російською технологічною компанією. Таким чином, за допомогою оплати послуг з оновлення та підтримки відповідного програмного забезпечення, власники ACS фінансуватимуть країну агресор. У зворотньому випадку, компанія приймає ризик того, що з часом наявне програмне забезпечення потрібно буде самостійно модифікувати, щоб підтримувати його в актуальному стані відповідно до сучасних вимог, які часто змінюються.

Приватбанк

Приватбанк має власне технологічне рішення для ACS та проводить верифікацію користувача, перевівши його на сторінку власного ACS серверу. При

цьому небезпечним для користувача є те, що технологічне рішення банку не входить до переліку сертифікованих постачальників послуг [10]. Це означає, що система не проходить процедури зовнішнього аудиту відповідно до міжнародних норм, а відповідно користувачі та учасники процесу не можуть бути впевнені у тому, чи достатні механізми контролю застосовуються у банку, в тому числі під час верифікації клієнтів.

Ощадбанк

Банк використовує програмне рішення WAY4 ACS v.1.0.

Першим недоліком є те, що при наявності більш нових версій продукту банк використовує першу версію, у якій можуть бути збережені проблеми, що не були виявлені при первинному релізі. Окрім цього, оновлення програмних продуктів дає можливість впроваджувати більш якісний сервіс та підходи на основі власного досвіду роботи продукту.

Другим недоліком, є те, що версії продукту до 1.2 мають виявлені вразливості [11]:

- /way4acs/enroll в OpenWay WAY4 ACS до 1.2.278-2693 дозволяє неавтентифікованим зловмисникам використовувати відмінності відповідей, щоб дізнатися, чи зберігається в системі певний номер платіжної картки.

- OpenWay WAY4 ACS до 1.2.278-2693 дозволяє XSS через параметр дії /way4acs/enroll.

Ukrainian Processing Center

Український процесинговий центр – процесинг, чиї технологічні рішення використовують такі банки як Райфайзен Банк Аваль, Ідея банк, Форвард Банк, Credit Agricole, Правекс Банк та інші. Компанія використовує рішення ActiveAccess 9, розроблене провайдером GPayments.

Програмний модуль підтримує велику кількість функцій, необхідних для ефективної роботи, серед яких: ризик-аналіз, безперервна аутентифікація для користувача.

Недолік є в тому, що API [15], за допомогою якого відбувається взаємодія із сервером, не захищений від атак, які використовуються відносно учасників 3DS процесу:

- Blind XSS – всі параметри та заголовки обміну даними потрапляють в системи моніторинку;

- у випадку challenge flow із браузером клієнта відбувається обмін повідомленнями, які містять в собі конфіденційну інформацію про беребіг транзакції: ідентифікатори 3DS сесії, тип повідомлення, версія повідомлення.

1.7 Висновки до розділу 1

Роль кібербезпеки в індустрії цифрових платежів є надзвичайно важливою для електронної комерції. Пандемія COVID-19 прискорила технологічну взаємозалежність електронної комерції та споживачів: одні використовують технологію для швидкої, легкої та безпечної покупки, а також для зниження ризику зараження, а інші використовують її для адаптації до поточних потреб ринку.

Як результат, кількість кібератак на електронну комерцію зросла в усьому світі: у Сполучених Штатах вони зросли в чотири рази (The Hill), в Іспанії фішингові шахрайства зросли на 70% (La Vanguardia), понад 80% організацій у Франції мали справу з успішною кібератакою (Comparitech), а 50% компаній у Великобританії постраждали від кібератак (ICEX) [25].

Ризик і проблеми кібербезпеки ставлять під сумнів заходи, вжиті електронною комерцією. Зіткнувшись із цими проблемами, сектор потребує стратегічного плану, заснованого на методах сек’юритизації платежів, таких як токенізація карток та протокол 3D Secure, які ми обговоримо в цій публікації. Шахрайство в електронній комерції стає все більш поширеним видом кіберзлочинів. Враховуючи це, система потребує ефективних та надійних методів аутентифікації, яким є 3D-Secure при належному налаштуванні правил та дотримань всіх вимог безпеки.

РОЗДІЛ 2
РОЗРОБКА КРИПТОГРАФІЧНОГО МОДУЛЯ ДЛЯ ACS СЕРВЕРУ

2.1 Постановка завдань для програмного рішення

Як було зазначено у попередньому розділі, програмне рішення для серверу контролю доступу повинно створювати умови для безпечної передачі даних під час процесу аутентифікації клієнта.

Від програмного модулю очікується забезпечення властивостей, важливих для перебігу транзакції:

- безпосередньо можливість авторизувати користувача;
- забезпечення конфіденційної передачі даних;
- забезпечення цілісності інформації, яка обробляється;
- надійність та ефективність технології;
- підтримка програмного модулю більшістю інформаційних систем.

2.2 Вибір методологічної основи

У якості рішення для впровадження пропонується схема, під час якої секретне повідомлення для двохетапної перевірки при Challenge flow 3DS2 формується та передається з використанням поєднання стеганографії та візуальної криптографії.

Стеганографія

Технологія стеганографії [26] – це технологія приховування одного повідомлення під іншим повідомленням, за допомогою якого дуже важко розрізнити приховане повідомлення. Перевага такого типу повідомлень полягає в тому, що воно не буде видимим. Стеганографія дозволяє використовувати кілька форматів, щоб приховати дані за допомогою стеганографії. Аудіо, відео, текст і зображення є одними з популярних форматів.

Якщо взяти для прикладу текстову стеганографію, є кілька способів приховати повідомлення. Змінюючи порядок слів і рядків, можна приховати повідомлення, додаючи або видаляючи кількість слів, кількість літер або голосних, ми також можемо приховати повідомлення. Стеганографія тексту широко використовується через свою перевагу перед іншими форматами. Використовуючи текст як формат, необхідний обсяг пам’яті набагато менший у порівнянні з іншими формами, а спосіб спілкування також простий.

Стеганографія зображень набула більшої популярності в пресі в останні роки, у порівнянні з іншими видами стеганографії, можливо, через потік електронної інформації про зображення, доступної з появою цифрових камер і високошвидкісного Інтернет-розповсюдження. Стеганографія зображення часто передбачає приховування інформації в природному «шумі» в зображенні і є гарною ілюстрацією для таких методів.

Більшість видів інформації містять якийсь шум. Шум можна описати як небажане спотворення інформації всередині сигналу. У аудіосигналі концепція шуму очевидна. Однак для зображень шум зазвичай відноситься до недоліків, властивих процесу відтворення аналогового зображення як цифрового. Наприклад, значення кольорів у палітрі для цифрового зображення не тільки не будуть точними кольорами реального зображення, а розподіл цих кольорів також буде недосконалим.

Стеганографія, як правило, використовується при повідомленні таємної інформації та коли потрібна повна свобода передачі даних Безпека зв'язку дуже важлива як у відкритому, так і в контрольованому середовищі. Приватні комунікації, які неможливо захистити за допомогою криптографії, можна захистити за допомогою стеганографії. Однак Конклін запропонував використовувати стеганографію з іншими механізмами безпеки для забезпечення багатошарової безпеки, оскільки зловмисник, який досягає успіху на одному рівні, все одно повинен обійти інші рівні, щоб бути повністю успішним [27]. Комунікації у військовій та розвідувальній сферах повинні відбуватись без перешкод; навіть за допомогою шифрування вмісту виявлення сигналу може призвести до атаки на

відправника на сучасному полі бою. Такі сигнали можна приховати за допомогою стеганографії. За допомогою стеганографії також можна зберігати інформацію, яка не призначена для обміну з кимось. Інша конфіденційна інформація, така як банківська інформація, також може бути прихована в обкладинці та збережена на приватному комп'ютері.

Для забезпечення безпеки даних були розгорнуті різні стеганографічні алгоритми. Слід зазначити, що не всі стеганографічні системи працюють із секретними ключами; однак безпеку стеганографічних систем можна підвищити, застосовуючи принцип Керкгофа. Принцип передбачає, що навіть якщо зловмисник знає проект і реалізацію стеганографічної системи, він повинен мати секретний ключ для успішної атаки на систему. Тому, можливо, було б розумно включити секретні ключі (публічні чи приватні) під час впровадження стеганографічних систем.

Стеганографія забезпечує виконання інформаційної безпеки шляхом вбудовування інформації в іншу інформацію; таким чином, реалізує властивість конфіденційності. Таку приховану інформацію можна розкрити лише за допомогою стеганографічного ключа. Однак техніка та спосіб, які використовуються для приховування інформації, також можуть служити доказом особи. Техніка вбудовування інформації може стати загальною таємницею, якщо її зробити неправильно, може бути способом ідентифікації та аутентифікації. Вбудована інформація не може бути піддана перевірці цілісності, оскільки інформація могла бути змінена навмисно чи ненавмисно, а зміни, внесені до витягнутої інформації, можуть не спостерігатися.

Візуальна криптографія

Візуальна криптографія (VC) [28] — це метод шифрування, коли секретне зображення поділяється на достатню кількість акцій на основі банківських схем, а потім укладання цієї достатньої кількості акцій допоможе розкрити секретне зображення. Це метод, який використовується для захисту секретів на основі зображень.

Цей метод також не вимагає жодного обчислювального процесу для розшифрування зображення. Припустимо, що наше секретне зображення буде розділене на дві частини. Оригінальне зображення буде відновлено лише шляхом накладання цих двох часток. Жодна інформація не може бути відновлена за допомогою будь-якого окремого ресурсу. Ці спільні файли будуть надруковані на прозорих плівках. Під час дешифрування ці дві спільні ресурси будуть складені, і секретне зображення буде передбачатися нашим неозброєним оком без будь-якого складного процесу обчислень.

Візуальна криптографія може працювати на основі ключа та без нього.

Візуальна криптографія без ключа знову була більш перспективним підходом. Її запровадили Джая і Сардана, ця схема передбачає поділ зображення на кілька часток [29]. Тут розглядається кольорове зображення, спільні ресурси, згенеровані цим методом, не містять інформації про оригінальне секретне зображення, і для отримання секретного зображення потрібні всі спільні ресурси. Запропонована методика реалізована за допомогою алгоритму Seiving-Division-Shuffling, запропонованого в цій роботі, і включає три кроки. На першому етапі отримання секретного зображення розбивається на основні кольори. На другому етапі розділення ці розділені зображення випадковим чином діляться. На третьому кроці Перемішування ці розділені частки потім перемішуються кожна всередині себе, щоб отримати остаточні випадкові частки.

Візуальна криптографія на основі ключів заснована на концепції візуальної криптографії без ключа, де ключі не задіяні, це вигідно з точки зору того, що не потрібно генерувати ключі та керувати ними, це просто, не задіяно складність підходів на основі ключів [30].

На основі цього підходу була представлена схема, спрямована на забезпечення захисту ключів і секретного обміну зображеннями. Математичні розрахунки були використані для створення зображення, яке виступало в якості ключового зображення. Цей ключ генерується із секретного зображення та деяких вибраних захисних зображень (p). Щоб відновити секретне кольорове зображення,

використовуються зображення ключа та зображення q, де q<p. Це називається (p,q) пороговою схемою.

Поєднання стеганографії та криптографії

Було відзначено, що стеганографія та криптографія окремо недостатні для повної безпеки інформації [31].

Таблиця 2.1

Порівняльна таблиця криптографії та стеганографії

Критерій/метод	**Стеганографія**	**Криптографія**
Визначається як	Відкрите повідомлення	Приховане повідомлення
Завдання	Підтримка секретності повідомлення, секретність комунації	Сбереження вмісту секретного повідомлення, захист даних
Канал	Будь-який цифровий формат	Орієнтована на текст
Вхідні файли	Мінімум два	Один
Використання ключа	Опціональне	Обов'язкове
Забезпечення властивостей	Аунтентифікація, конфіденційність, ідентифікація	Конфіденційність, ідентифікація, цілісність даних, аутентифікація
Тип атаки	Стеганоаналіз (аналіз файлу на предмет того, чи є він стеганографічним файлом)	Криптоаналіз
Атака	Відбувається, коли зловмисник може визначити, що стеганографія використовувалась відносно файлу	Відбувається, коли зловмисник може прочитати секретне повідомлення.

Результат	Стеганографічний файл	Шифртекст

Враховуючи сказане вище, більш надійного і міцного механізму можна досягти комбінуванням обидвох технік. Поєднання цих стратегій може забезпечити покращену безпеку секретної інформації та відповідатиме вимогам безпеки та надійності для передачі важливої інформації через відкриті канали.

Використання стеганографії в комбінованій візуальній криптографії є надійною моделлю і додає багато проблем для ідентифікації таких прихованих і зашифрованих даних.

По суті, можна було б мати секретне зображення з конфіденційними даними, які можна було б розділити на різні зашифровані спільні ресурси. Нарешті, коли такі зашифровані спільні ресурси повторно збираються або розшифровуються, щоб переробити справжнє зображення, можна отримати відкрите зображення, яке все ж складається з конфіденційних даних. Такі типи алгоритмів не можуть зберігатися без належних характеристик у процедурі візуальної криптографії. Підставою для цього є те, що якщо метод перебудови або навіть метод кодування змінює дані, що існують у зображенні, то система відповідно змінить зашифровану інформацію, що зробить систему можливим для вилучення зашифрованих даних із відкритого зображення.

2.3 Опис запропонованої схеми роботи

Запропоноване рішення дозволить надавати мінімальну інформацію про перебіг аутентифікації продавцю, оскільки весь процес буде зосереджений на ACS сервері. Таким чином можна успішно приховати важливу інформацію щодо банківських реквізитів та особистої інформації. Для цього запроваджується CA, тобто центральний сертифікований орган, і він буде об’єднаний із сервером контролю доступу. Його застосування буде базуватись на об’єднанні стеганографії та візуальної криптогрфії. При використанні такої схеми роботи лише інформація, яка буде доступна продавцю, буде у формі номера рахунку, пов’язаної з дебетовою

або кредитною карткою. Ця інформація буде авторизована та підтверджена лише клієнтом. Використовуючи запропонований метод, кінцевий користувач банку за допомогою методу стеганографії згенерує пароль аутентифікації, який буде приховано всередині тексту обкладинки.

Інформація для автентифікації кінцевих користувачів, тобто номер його рахунку, розміщена над текстом обкладинки в оригінальному вигляді. Таким чином робиться знімок обох текстів. Тепер одна частка знімка зберігається в кінцевого користувача, а інша спільна доступна центральному сертифікованому центру. Тепер, коли користувач буде переходити до процесу аутентифікації ви завершите покупки та виберете потрібний продукт у кошику, кінцевий користувач буде спрямований на портал CA.

Після цього ЦС порівняє свій власний спільний ресурс із спільним ресурсом кінцевих користувачів і отримає вихідне зображення. Тепер CA перешле номер торгового рахунку з обкладинним текстом до банку, де з тексту буде відновлено пароль аутентифікації кінцевих користувачів. Як тільки банк отримає реквізити від ЦС, він спробує узгодити реквізити з доступними реквізитами в банках. Після того, як банк підтвердить, що дані збігаються, він переведе кошти з облікового запису кінцевого користувача на обліковий запис продавця. Як тільки продавець отримає платежі, він надасть кінцевому користувачеві квитанцію.

На Рисунку 2.1 зображено схему взаємодії учасників процесу.

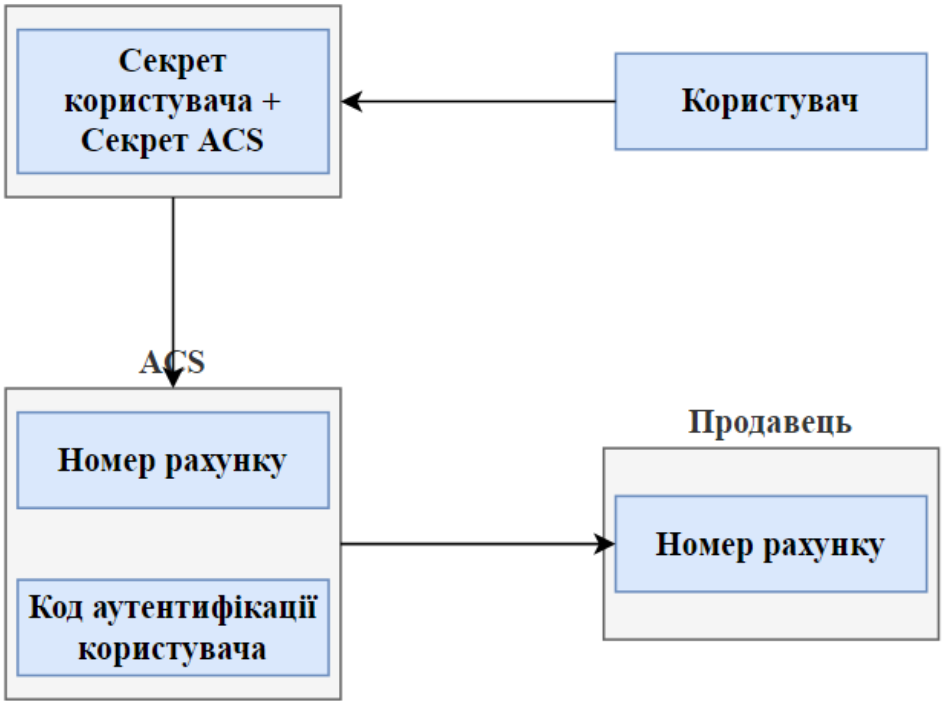


Рисунок 2.1 Схема взаємодії учасників процесу

Вхідне зображення приймається у якості ключа для вхідного повідомлення у форматі простого тексту. Після імплементації секретного повідомлення в LSB (найменший значущий біт), вхідне зображення деформуються за допомогою технології візуальної криптографії, для того, щоб зберегти їхні статистичні значення.

Таким чином, власник системи, може вибрати цільову інформацію у вигляді простого тексту для вбудовування в секретне повідомлення у якості вхідного зображення. Результати роботи візуальної криптографії дозволять значенню пікселів стеганографічного зображення зберігати свсвої статистичні характеристики [33]. Стеганографія LSB не складна для обчислення, відовідно, може бути імплементована у більшість сучасних інформаційних систем, окрім цього відрізняється високою здатність того, щоб бути вбудованою в іншу інформаційну систему, в якій секретна двійкова послідовність використовується для заміни найменш значущих бітів основного середовища.

Цей алгоритм також дозволятиме захищати дані від роботи зловмисників.

У чистому стенографічному фреймворку техніка побудови повідомлення невідома третім сторонам, а отже реалізує безпечну передачу інформації між двома учасниками [34].

Стеганографічна частина працює за алгоритмом:

1. Зчитується вхідне зображення

2. Зчитується вхідне текстове повідомлення

3. Відбувається аутентифікація на основі пароля

4. Викликається метод Switch

5. Викликається алгоритм BattleSteg. Цей алгоритм виконує «BsttleShip Steganography» [37]. Спочатку він фільтрує зображення, а потім використовує найвищі значення фільтра як "кораблі". Потім алгоритм випадковим чином «стріляє» по зображенню, і коли він знаходить «корабель», він об’єднує його навколо цього удару в надії «потопити» «корабель». Внаслідок цього повідомлення випадковим чином приховується, але часто ховається в «найкращих» частинах, де можна сховатися завдяки «кораблям». Це безпечно, оскільки для отримання повідомлення все-таки потрібен пароль. Метод є ефективним, оскільки він приховує більшість інформації в найкращих областях.

6. Вихід із методу

7. Викликається метод BlindHide [38]. Він приховує дані «всліпу», тому що він просто починає роботу у верхньому лівому куті зображення і проходить через зображення (а потім вниз – у рядках сканування) піксель за пікселем. По ходу він змінює найменші значущі біти кольорів пікселів, щоб відповідати повідомленню. Для декодування процесу зчитуються найменші значущі біти, які починаються зверху ліворуч.

8. Вихід із методу

9. Викликається метод FilterFirst [39]. Цей алгоритм фільтрує зображення за допомогою одного з вбудованих фільтрів, а потім спочатку ховається в найвищих значеннях фільтра. По суті, це одна із версій методу BlindHide, оскільки для отримання повідомлення не потрібен пароль. Оскільки змінюються пікселі, нам потрібно бути обережними з фільтруванням зображення, оскільки ми не хочемо

використовувати інформацію для фільтрації, яка може змінитися. Якщо ми це зробимо, то може бути важко (якщо взагалі неможливо) отримати повідомлення знову. Таким чином, цей алгоритм фільтрує найбільш значущі біти і залишає найменші біти для зміни. Це менш помітно на зображенні, оскільки використання фільтра гарантує, що ми ховаємося в тих частинах зображення, які є найменш помітними.

10. Вихід із методу

11. Виклик методу HideSeek [40]. Цей алгоритм випадковим чином розподіляє повідомлення по зображенню. Він названий на честь інструмента стеганографії Windows 95, який використовує подібну техніку. Для створення випадкого початкового значення використовується пароль, після чого це початкове знаення використовується щоб вибрати першу позицію для приховування. Він продовжує генерувати випадковим чином позиції, поки не закінчить приховувати повідомлення. Це більш грамотно щодо того, як він приховується, тому що зловмисник повинен спробувати кожну комбінацію пікселів у кожному порядку, щоб спробувати «зламати» алгоритм, якщо пароль невідомий. Це все ще не найкращий метод, тому що він не розглядає пікселі, в яких він ховається – може бути корисніше визначити ділянки зображення, де краще сховатися.

12. Вихід із методу

13. Перетворення зображення на двійкове значення

14. Вставлення повідомлення у вхідне зображення базуючись на відсотковому значенні

15. Генерація випадкового повідомлення

16. Застосування рівномірно розподілених псевдовипадкових чисел

17. msg = randi([0 round(255*perc/100)],size(I));

18. I=I+msg;

19. Розподілення зображення на блоки 8*8

20. Застосування не позитивної обгортки F-

21. Генерація випадкових з0 та 1

22. Заміна LSB відповідно до обгортки

23. Застосування не негативної обгортки F+
24. Генерація випадкових -1 та 0
25. Заміна LSB відповідно до обгортки
26. Обчислення кореляції
27. Ініціалізація максимальної хромосоми
28. Заміна другого нижчого біту випадковим значенням протягом декількох разів
29. PSNR=snr(Chrom-CN)
30. fitness = alpha*(e1+e2)+PSNR
31. Якщо fitness>maxfitness, тоді maxfitness=0 ініціюється
32. maxfitness=fitness
33. Chrommax=Cp (CP – кореляція для не позитивної обгортки);
34. crossover = crossover+1;
35. Кінець алгоритму
36. Заміна хромосоми новою

Алгоритм розміщення виглядає наступним чином:

1. Для i = 1…,l(c) виконується метод
2. $s_i \leftarrow c_i$
3. Кінець методу
4. Генерація рандомної послідовності k_i з використанням основи k
5. $n \leftarrow k_i$
6. Для i = 1…,l(m) виконується метод
7. $s_n \leftarrow c_n \leftrightarrow m_i$
8. $n \leftarrow n + k_i$
9. Кінець методу

Алгоритм вилучення повідомлення виглядає наступним чином:

1. Генерація рандомної послідовності k_i з використанням основи k
2. $n \leftarrow k_i$
3. Для i = 1…,l(m) виконується метод

4. $m_i \leftarrow LSB(c_n)$

5. $n \leftarrow n + k_i$

6. Кінець методу

Частина з візуальною криптографією працює наступним чином: на вхід приймається стеганографічне повідомлення, а на виході формуються два секретні повідомлення.

1. Зчитується стеганографічне повідомлення

2. Стеганографічне повідомлення розбивається на 3 шари, які називаються split-1, split-2, split-3. Ці файли містять в собі приховану інформацію. Для того, щоб отримати інформацію із цих файлів, якість передачі даних повинна бути достатньо якісною для того, щоб цілісність даних не була порушена.

3. Знову формуються повторно зібране зображення та вихідні дані.

Запропонована схема заснована на стандартній технології візуальної криптографії, а також на передачі секретного повідомлення форматі зображення. Застосована техніка використовує виділення псевдовипадкового числа, а також обмін пікселями. Однією з контрастних частин цієї реалізації є те, що під час дешифрування стего-зображення буде морфологічно таким же порівняно з зображенням обкладинки щодо форми та розміру, що запобігає ефекту розширення пікселя. Реалізація алгоритму дає кращий результат з незначною часткою, коли стего-зображення зазвичай мають світлоконтрастний. Також можна побачити, що алгоритм дає набагато темніші частки як у сірому, так і в кольоровому виведенні.

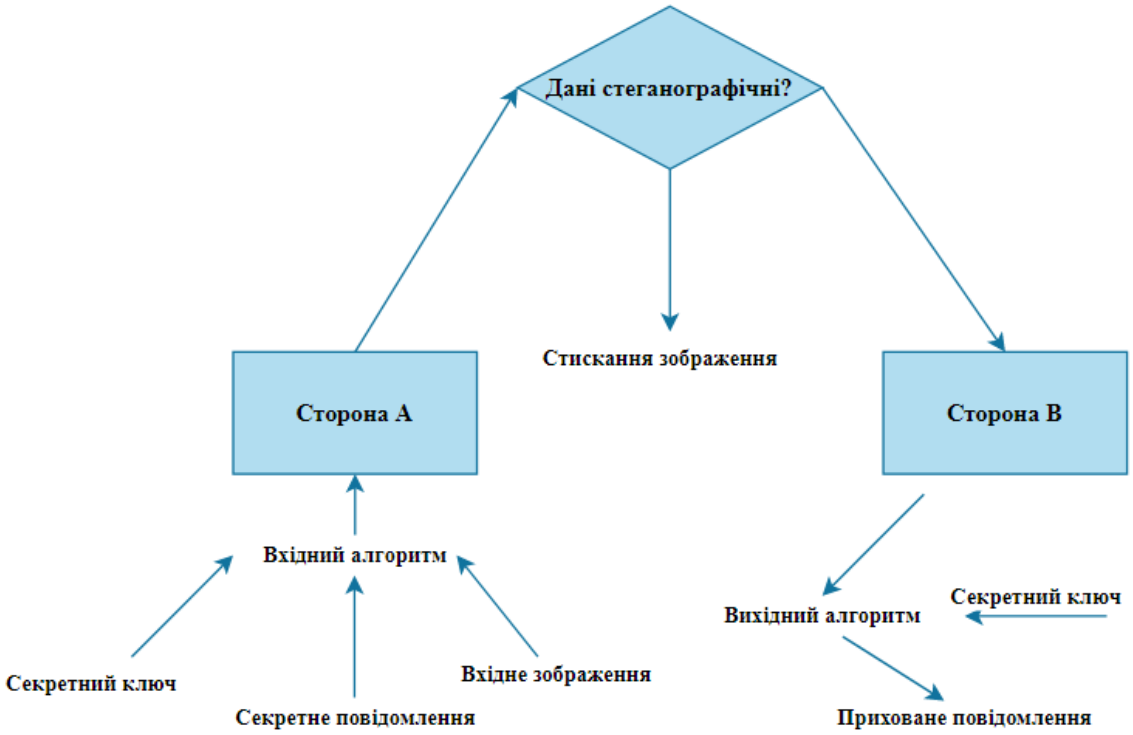


Рисунок 2.2 Схема кодування та декодування повідомлень

КРОК 1:

Підбайти для байт-байтової заміни під час процесу пересилання. Відповідний крок заміни, який використовується під час дешифрування, називається Inv SubByte.

Цей крок складається з використання таблиці пошуку 16 на 16, щоб знайти замінний байт для заданого байта в масиві вхідних станів.

Записи в таблиці пошуку створюються за допомогою ідей мультиплікативних обернених і бітового скремблювання, щоб знищити кореляції на бітовому рівні всередині кожного байта.

КРОК 2:

Викликається метод Shift Rows для зсуву рядків масиву станів під час прямого процесу. Відповідні стовпці змішуються та відбувається зсув стовпців.

Один раунд шифрування показаний ліворуч, а один раунд дешифрування – праворуч. Безпека комп'ютера та мережі під час дешифрування позначається InvShiftRows для Inverse ShiftRow.

КРОК 3:

Викликається метод Mix Columns для змішування байтів у кожному стовпці окремо під час процесу пересилання. Відповідне перетворення під час дешифрування позначається InvMixColumns і означає інверсне перетворення стовпця змішання. Мета полягає в тому, щоб додатково захистити зображення за допомогою 128-бітного вхідного блоку.

Крок зсуву рядків разом із кроком змішування стовпців змушує кожен біт шифрованого тексту залежати від кожного біта відкритого тексту після 10 раундів обробки. У DES один біт відкритого тексту вплинув приблизно на 31 біт зашифрованого тексту. Але тепер ми хочемо, щоб кожен біт відкритого тексту впливав на кожну позицію біта блоку шифрованого тексту розміром 128 біт.

КРОК 4:

Додається раундовий ключ для додавання до результату\виходу попереднього кроку під час процесу. Виконується відповідний крок під час дешифрування.

2.4 Реалізація програмного рішення

Для створення програмного рішення використано мову Python, тому що її функції дозволяють використовувати для написання криптографічних програмних продуктів.

Python є однією з найпопулярніших мов програмування у світі [35]. Це мова загального призначення, що означає, що вона використовується для широкого кола завдань, включаючи криптографію. Він також зручний для початківців, тому це чудове місце для початку, якщо ви новачок у програмуванні.

Python є відкритим вихідним кодом, що означає, що його безкоштовне використання, і він має велику та активну спільноту. Він також має широкий вибір бібліотек і фреймворків, що означає, що у вашому розпорядженні є безліч ресурсів.

Python також є популярною мовою для криптографії. Одна з його бібліотек називається «криптографія» і має безпечні примітиви. Примітив — це найменший, найпростіший тип даних.

Одним із популярних безпекових примітивів є реалізація Fernet, яка підтримує криптографію «секретного ключа» [36]. Цей тип шифрування використовує один і той же ключ для шифрування та дешифрування інформації.

Структура програми складається із:

- головного компоненту, який викликає інші процеси;
- модулю, який здійснює стеганографічні перетворення;
- модулю, який здійснює криптографічні перетворення;
- зображень, які використовуються для формування секрету.

Головний компонент відповідає за запуск користувацького інтерфейсу, імпорт та зберігання файлів та виклик інших служб.

```
  GNU nano 5.9
import os
import sys
cwd = os.getcwd()
print("My directory is")
print(cwd)

sys.path.insert(0, './src')

import streamlit as st

from PIL import Image
from src.lsb_stegno import lsb_encode, lsb_decode
from src.n_share import generate_shares, compress_shares

menu = st.sidebar.radio('Options', ['Docs', 'Encode', 'Decode'])

if menu == 'Docs':
    st.title('Documentation')
    with open('README.md', 'r') as f:
        docs = f.read()
    st.markdown(docs, unsafe_allow_html=True)

elif menu == 'Encode':
    st.title('Encoding')

    # Image
    img = st.file_uploader('Upload image file', type=['jpg', 'png', 'jpeg'])
    if img is not None:
        img = Image.open(img)
        try:
            img.save('images/img.jpg')
        except:
            img.save('images/img.png')
        st.image(img, caption='Selected image to use for data encoding',
                 use_column_width=True)

    # Data
    txt = st.text_input('Message to hide')

    # Encode message
    if st.button('Encode data and Generate shares'):

        # Checks
        if len(txt) == 0:
            st.warning('No data to hide')
        elif img is None:
            st.warning('No image file selected')
```

Рисунок 2.2 Код основного компоненту

Окрім цього, головний компонент відповідає за експортування проміжних результатів роботи сервісу.

```
        # Generate splits
        else:
            generate_shares(lsb_encode(txt))
            try:
                os.remove('images/img.jpg')
            except FileNotFoundError:
                os.remove('images/img.png')
            st.success('Data encoded, Shares generated in folder [images]')

elif menu == 'Decode':
    st.title('Decoding')

    # Share 1
    img1 = st.file_uploader('Upload Share 1', type=['png'])
    if img1 is not None:
        img1 = Image.open(img1)
        img1.save('images/share1.png')
        st.image(img1, caption='Share 1', use_column_width=True)

    # Share 2
    img2 = st.file_uploader('Upload Share 2', type=['png'])
    if img2 is not None:
        img2 = Image.open(img2)
        img2.save('images/share2.png')
        st.image(img2, caption='Share 2', use_column_width=True)

    # Decode message
    if st.button('Compress shares and Decode message'):

        # Check
        if img1 is None or img2 is None:
            st.warning('Upload both shares')

        # Compress shares
        else:
            compress_shares()
            os.remove('images/share1.png')
            os.remove('images/share2.png')
            st.success('Decoded message: ' + lsb_decode('images/compress.png'))
```

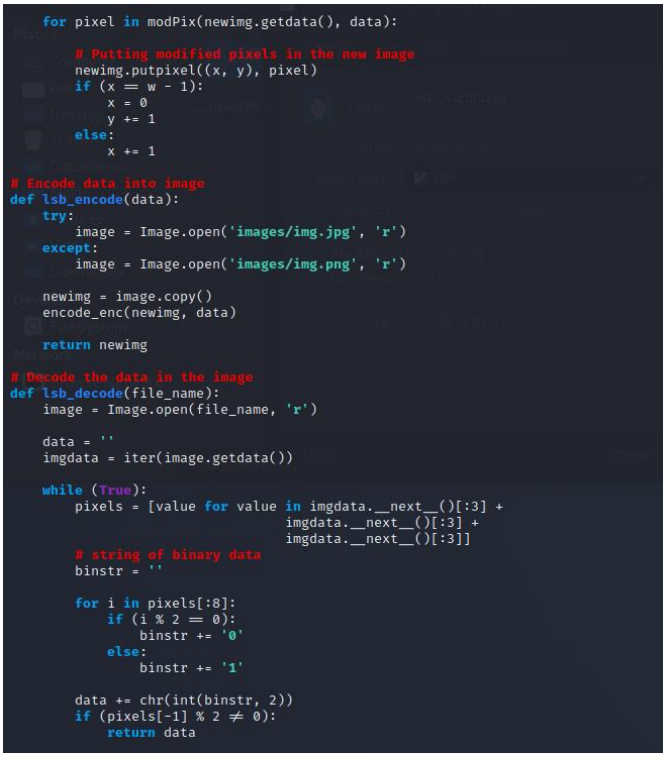
Рисунок 2.3 Код основного компоненту

Модуль криптографії відповідає за формування секрету із використанням зображення-секрету.

```
from PIL import Image
import numpy as np

# Convert encoding data into 8-bit binary
# form using ASCII value of characters
def genData(data):

        # list of binary codes
        # of given data
        newd = []

        for i in data:
            newd.append(format(ord(i), '08b'))
        return newd

# Pixels are modified according to the
# 8-bit binary data and finally returned
def modPix(pix, data):

    datalist = genData(data)
    lendata = len(datalist)
    imdata = iter(pix)

    for i in range(lendata):

        # Extracting 3 pixels at a time
        pix = [value for value in imdata.__next__()[:3] +
                                  imdata.__next__()[:3] +
                                  imdata.__next__()[:3]]

        # Pixel value should be made
        # odd for 1 and even for 0
        for j in range(0, 8):
            if (datalist[i][j]=='0') and (pix[j]% 2 != 0):

                if (pix[j]% 2 != 0):
                    pix[j] -= 1

            elif (datalist[i][j] == '1') and (pix[j] % 2 == 0):
                pix[j] -= 1

        # Eigh^th pixel of every set tells
        # whether to stop ot read further.
        # 0 means keep reading; 1 means the
        # message is over.
        if (i == lendata - 1):
            if (pix[-1] % 2 == 0):
                pix[-1] -= 1
```

Рисунок 2.4 Код компоненту стеганографії

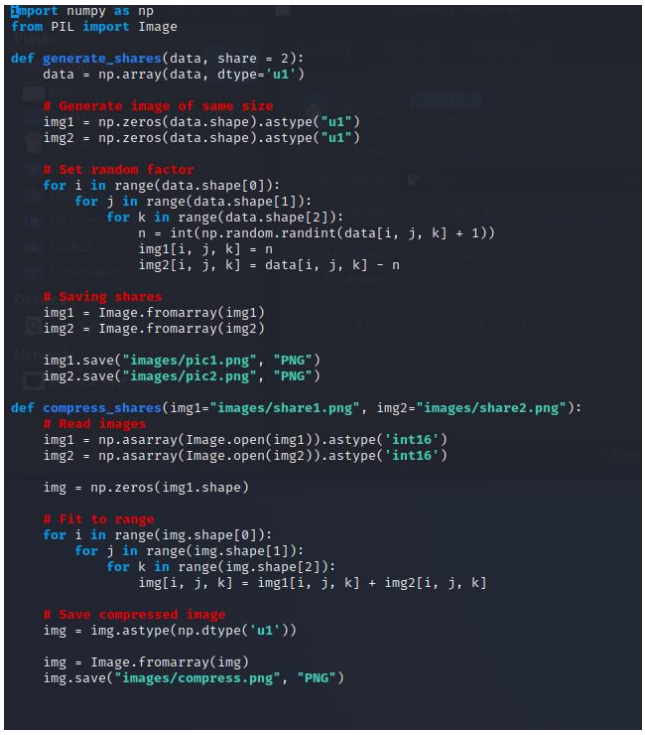
Як показано на Рисунку 2.5, методи цього модулю виконують перетворення над зображенням, створюючи дві видозмінені версії зображення.



```
    for pixel in modPix(newimg.getdata(), data):

        # Putting modified pixels in the new image
        newimg.putpixel((x, y), pixel)
        if (x == w - 1):
            x = 0
            y += 1
        else:
            x += 1

# Encode data into image
def lsb_encode(data):
    try:
        image = Image.open('images/img.jpg', 'r')
    except:
        image = Image.open('images/img.png', 'r')

    newimg = image.copy()
    encode_enc(newimg, data)

    return newimg

# Decode the data in the image
def lsb_decode(file_name):
    image = Image.open(file_name, 'r')

    data = ''
    imgdata = iter(image.getdata())

    while (True):
        pixels = [value for value in imgdata.__next__()[:3] +
                                imgdata.__next__()[:3] +
                                imgdata.__next__()[:3]]
        # string of binary data
        binstr = ''

        for i in pixels[:8]:
            if (i % 2 == 0):
                binstr += '0'
            else:
                binstr += '1'

        data += chr(int(binstr, 2))
        if (pixels[-1] % 2 != 0):
            return data
```

Рисунок 2.5 Код стенографічного модуля

Модуль стискання та розділення зображень позначено на Рисунку 2.6.



```
import numpy as np
from PIL import Image

def generate_shares(data, share = 2):
    data = np.array(data, dtype='u1')

    # Generate image of same size
    img1 = np.zeros(data.shape).astype("u1")
    img2 = np.zeros(data.shape).astype("u1")

    # Set random factor
    for i in range(data.shape[0]):
        for j in range(data.shape[1]):
            for k in range(data.shape[2]):
                n = int(np.random.randint(data[i, j, k] + 1))
                img1[i, j, k] = n
                img2[i, j, k] = data[i, j, k] - n

    # Saving shares
    img1 = Image.fromarray(img1)
    img2 = Image.fromarray(img2)

    img1.save("images/pic1.png", "PNG")
    img2.save("images/pic2.png", "PNG")

def compress_shares(img1="images/share1.png", img2="images/share2.png"):
    # Read images
    img1 = np.asarray(Image.open(img1)).astype('int16')
    img2 = np.asarray(Image.open(img2)).astype('int16')

    img = np.zeros(img1.shape)

    # Fit to range
    for i in range(img.shape[0]):
        for j in range(img.shape[1]):
            for k in range(img.shape[2]):
                img[i, j, k] = img1[i, j, k] + img2[i, j, k]

    # Save compressed image
    img = img.astype(np.dtype('u1'))

    img = Image.fromarray(img)
    img.save("images/compress.png", "PNG")
```

Рисунок 2.6 Код модуля для обробки зображень

У запропонованій системі обговорено реалізацію безпечного використання стеганографічної техніки з використанням генетичного алгоритму та візуальної криптографії з використанням псевдовипадкового числа. Можна зробити висновок, що звичайний захист зображень із застосуванням стеганографічної та візуальної криптографічної техніки робить завдання слідчих розшифрувати зашифроване секретне повідомлення нездійсненним.

Функції безпеки стеганографії дуже оптимізовані за допомогою генетичного алгоритму. Запропонована система має високу стійкість до RS-атак і оптимально використовується як для відтінків сірого, так і для кольорового виведення у візуальних секретних ресурсах, що робить її дуже сумісною для додатків реального часу. Майбутня робота може бути спрямована на вдосконалення алгоритму з використанням нейронної мережі для візуальної криптографії, щоб система могла генерувати секретні спільні ресурси, які не можна виявити, використовуючи певний набір навчальних даних, які можуть бути автоматично згенеровані та утилізовані після виконання завдання. Такий підхід може надати найбільш безпечну стеганографічну та візуальну криптографічну схему.

2.5 Висновки до розділу 2

Безпека стала найважливішим аспектом у сучасній системі банківських операцій, оскільки банки зобов’язані надавати своїм клієнтам безпечні основні банківські послуги. Для досягнення цієї мети потрібна автентичність користувачів, тобто тільки авторизовані користувачі можуть брати участь у транзакції. З цією метою банки використовують системи аутентифікації на основі біометричних даних, але через неминучу шкідливу діяльність база даних банківської системи більше не є захищеною. Досвідчені хакери можуть отримати біометричні дані клієнтів із бази даних банку, а потім використовувати їх для фальшивих транзакцій. Щоб уникнути всіх цих катастрофічних речей, використовується візуальна криптографічна техніка разом з алгоритмом AES.

Візуальна криптографія [48] — це ефективна схема шифрування, в якій інформація ховається всередині зображень і розшифровується лише візуальною системою людини. У запропонованому рішенні використовується візуальна криптографія на основі безпечної операції XOR разом з алгоритмом AES та технікою обробки зображень для захисту банківських транзакцій.

РОЗДІЛ 3
ТЕСТУВАННЯ ТА ЕКСПЛУАТАЦІЯ ПРОГРАМНОГО РІШЕННЯ

3.1. Запуск та тестування графічної оболонки

3.1.1 Установка необхідних для роботи компонентів

Для візуалізації роботи програмного рішення, було розроблено візуальну оболонку, яка демонструватиме роботу процесів шифрування та дешифрування. Графічна версія програми запускається у браузері користувача на основі локального хосту.

Для навігації та зручного використання програми розроблено файл README.md, який описує принципи використання програмного рішення.

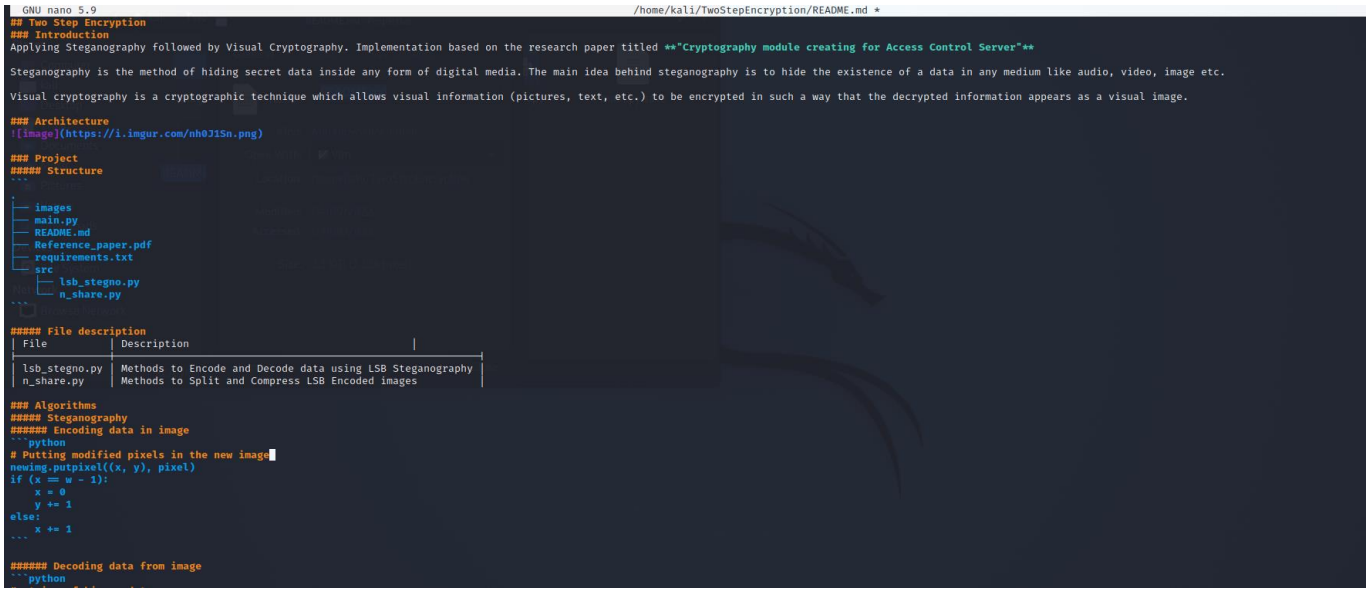


Рисунок 3.1 Файл REAMDE.md

Файл README.md знаходиться у кореневій папці, з якої буде запускатись скрипт.

Рисунок 3.2. Опис логіки системи у файлі README.md

Враховуючи те, що програмне рішення написане на мові Python, для роботи із програмним кодом та запуску програми необхідно встановити утиліту Streamlit.

Streamlit - це фреймворк з відкритим вихідним кодом на мові Python [49]. Це допомагає нам створювати веб-додатки для науки про дані та машинного навчання за короткий час. Він сумісний з основними бібліотеками Python, такими як scikit-learn, Keras, PyTorch, SymPy(latex), NumPy, pandas, Matplotlib тощо.

Роботу програми буде продемонстровано на базі операційнох системи Kali Linux. Враховуючи це, команди, необхідні для інсталяції утиліт, орієнтовані на ОС Kali.

Установка pip:

sudo apt-get install python3-pip

pip3 install pipenv

Створення нового середовища для Streamlit:

cd encryption

pipenv shell

Установка Streamlit у середовище, яке щойно створено:

pip install streamlit

3.2.2 Експлуатація програмного рішення

Тепер, для запуску програми, необхідно запустити команду:

python3 -m streamlit run /folder/file

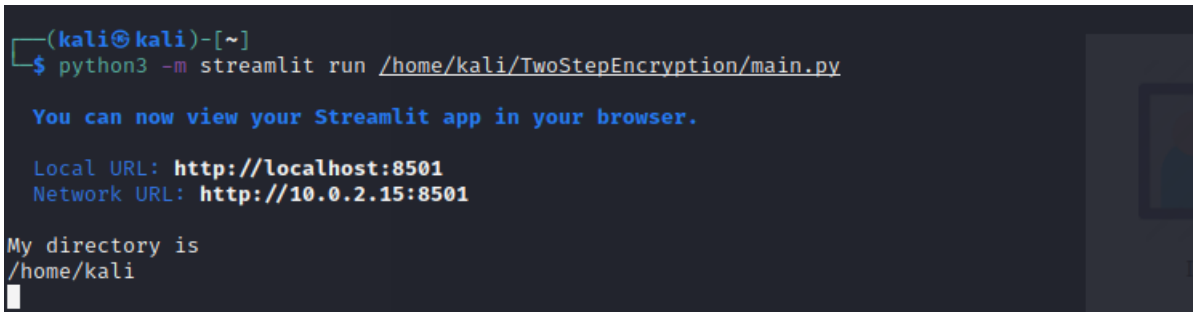


Рисунок 3.3 Запуск програми із консолі

Як результат, стартова сторінка програми буде запущена у вікні браузера:

Рисунок 3.4 Запуск програми у браузері

Для того, щоб перевірити шифрування повідомлення, необхідно використати функцію Encode. Для початку роботи необхідно завантажити вхідне зображення та записати повідомлення, яке повинно бути приховане. Таким чином, створюється пароль, який повинен бути переданий користувачу безпечним шляхом.

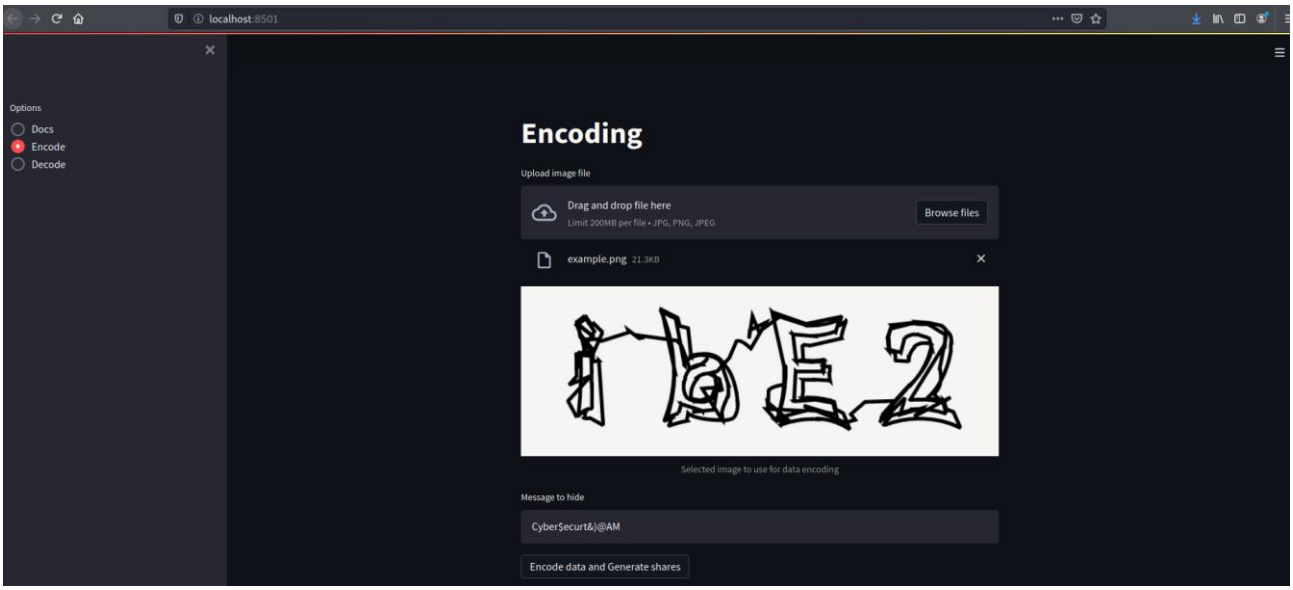


Рисунок 3.5 Етап шифрування

Після того, як повідомлення та вхідне зображення завантажені, виконується шифрування.

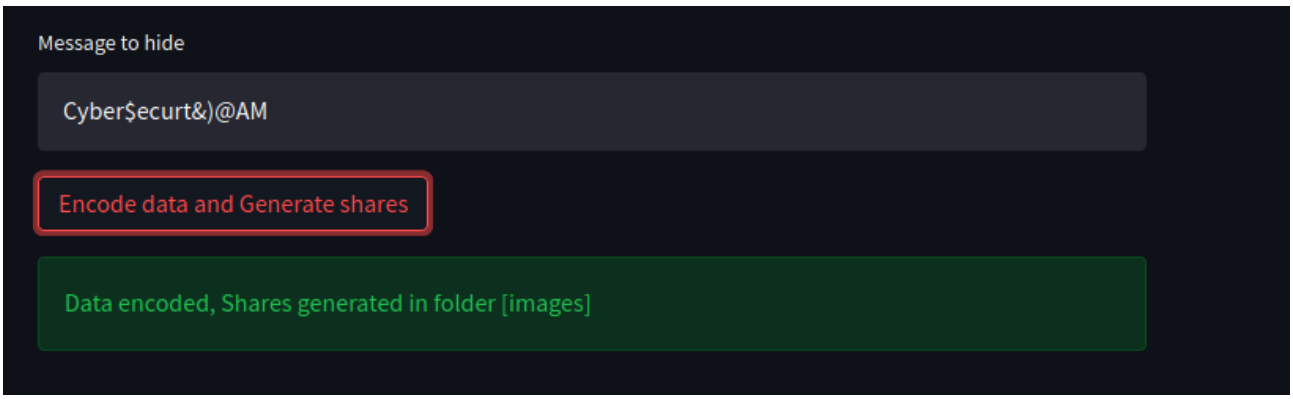


Рисунок 3.6 Результат роботи команди шифрування

Після того, як шифрування завершено, буде створено два файли із стеганографічними зображеннями.

Рисунок 3.7 Збереження стеганографічних зображень

Стеганографічні повідомлення є результатом роботи першого етапу схеми. Таким чином, створено стеганографічні зображення, за допомогою яких секретне повідомлення повинно бути передано на особистий засіб користувача.

Для дешифрування повідомлення необхідно використати функцію Decode.

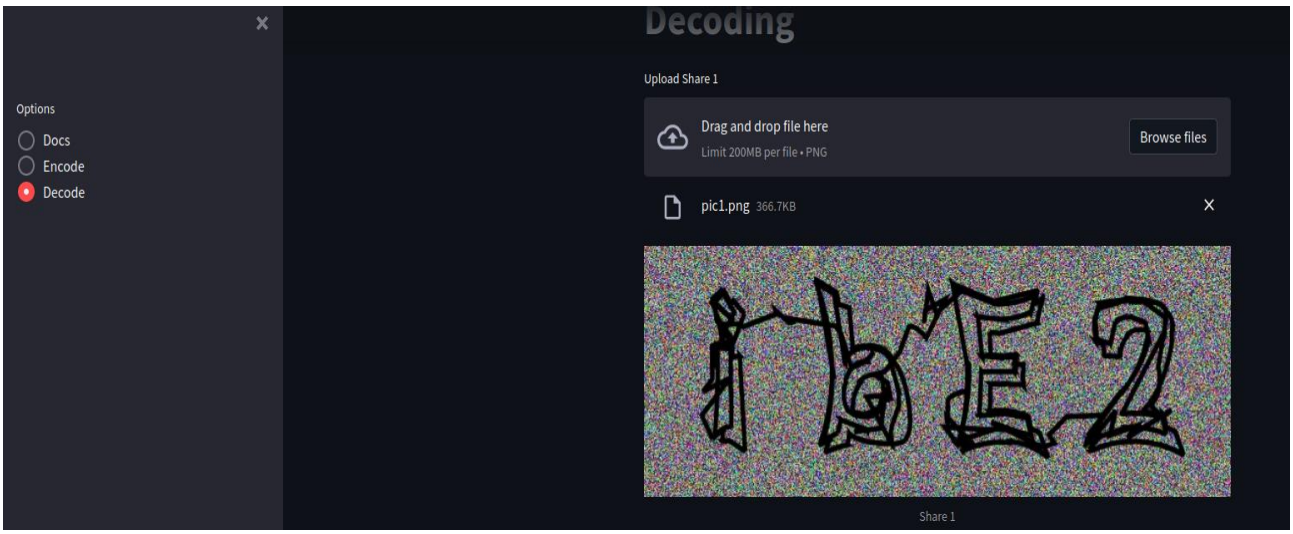


Рисунок 3.8 Завантаження зображення 1 для дешифрування

Для дешифрування отримувач повідомлення повинен завантажити у декриптор обидва стеганографічні зображення.

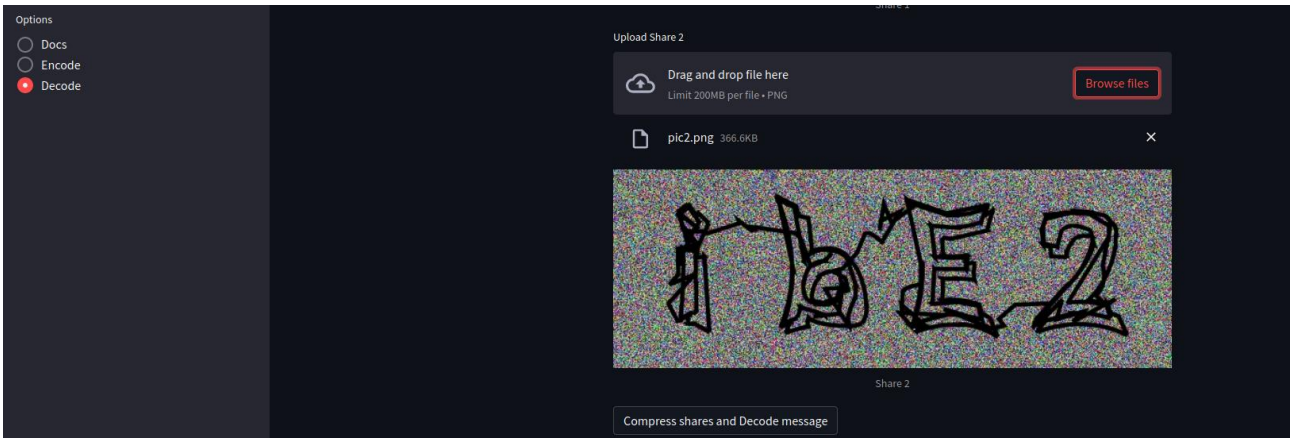


Рисунок 3.9 Завантаження зображення 2 для дешифрування

У результаті дешифрування буде отримано секретне повідомлення, яке може бути використане покупцем для підтвердження своєї операції, ввівши код на ACS сторінці свого банку.

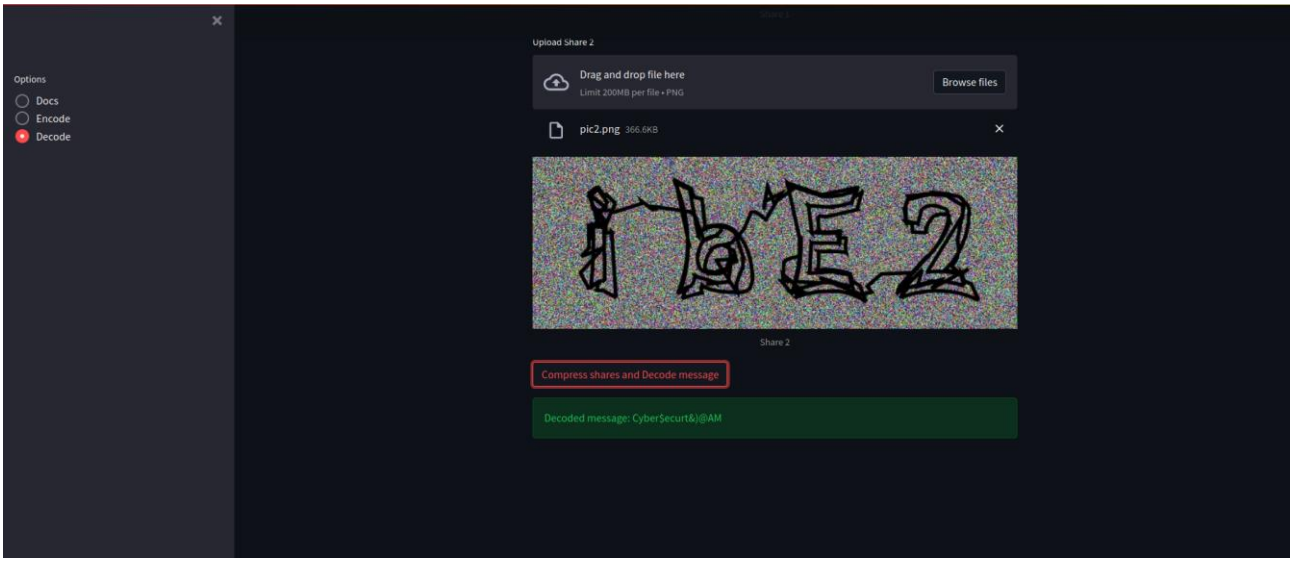


Рисунок 3.10 Результат дешифрування

Кеш після обробки повідомлення зберігається у кореневу папку, де знаходиться програма.

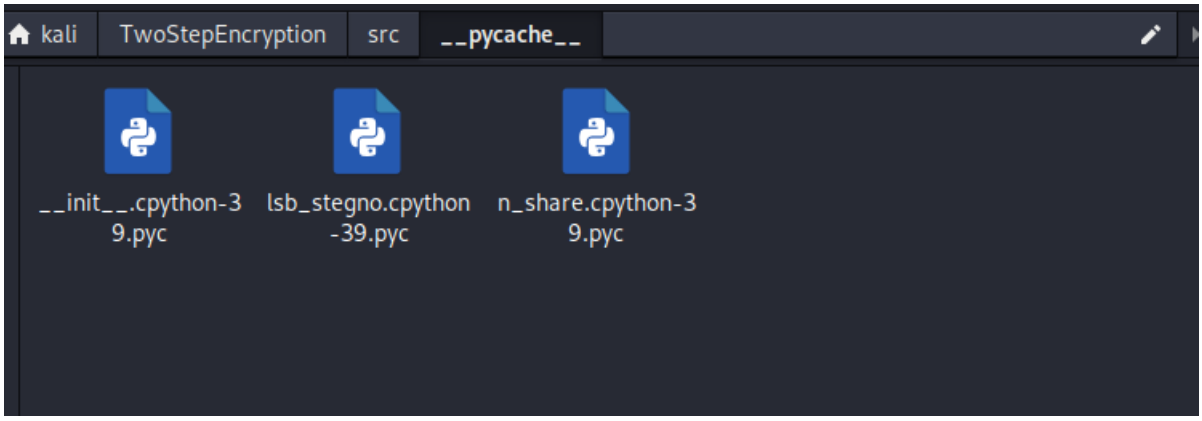


Рисунок 3.11 Кеш за результатами роботи програми

3.2.3 Тестування методів атаки

Враховуючи те, що повідомлення повинно передаватись по каналах зв’язку між банком та клієнтом, необхідно перевірити, чи може зловмисник отримати доступ до секретного повідомлення, що передається.

Для цього необхідно застосувати технологію стеганоаналізу.

Стеганоаліз – це технологія, яка намагається подолати стеганографію, виявляючи приховану інформацію та витягуючи або знищуючи її [49].

Існують різні методи аналізу залежно від того, яка інформація доступна:

Атака, коли відомо лише стего: для аналізу доступний лише об’єкт стего.

Відома атака прикриття: доступний стего-об'єкт, а також оригінальний носій. Стего-об’єкт порівнюється з оригінальним об’єктом покриття, щоб виявити будь-яку приховану інформацію.

Атака на відомі повідомлення: відомі приховане повідомлення та відповідне стего-зображення. Аналіз закономірностей, які відповідають прихованій інформації, може допомогти розшифрувати такі повідомлення в майбутньому.

Відома стего-атака: Алгоритм стеганографії відомий, і доступні як оригінал, так і стего-об’єкт.

Вибрана стего-атака: Алгоритм стеганографії та стего-об'єкт відомі.

Атака з обраним повідомленням: стеганалітик генерує стего-об'єкт з якогось інструмента стеганографії або алгоритму вибраного повідомлення. Метою цієї атаки є визначення шаблонів у стего-об’єкті, які можуть вказувати на використання певних інструментів або алгоритмів стеганографії.

Для перевірки роботи механізму застосуємо різні утиліти, створені для стегоаналізу, та порівняємо результати.

Утиліта Stegosuite — це графічний інструмент стеганографії. Він використовується для приховування секретних даних або інформації у файлах зображень, а також для дешифрування повідомлень. Для роботи утиліти необхідно отримати стего зображення та пароль, що використовувався для його формування.

З цього випливає, що задана утиліта або подібні до неї не можуть виконати атаку на повідомлення, що передається у запропонованій системі.

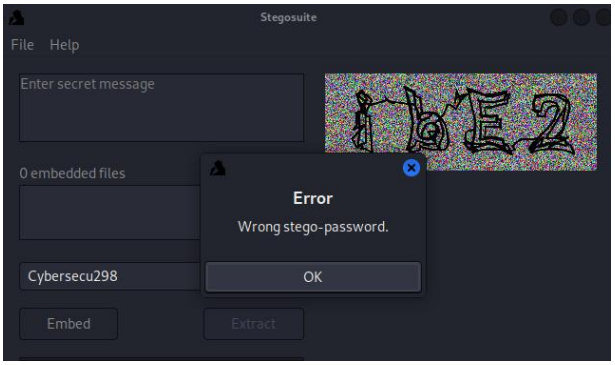


Рисунок 3.12 Результат роботи StegoSuite

Binwalk — це інструмент для пошуку вбудованих файлів і виконуваного коду в заданому двійковому зображенні. Зокрема, він призначений для ідентифікації файлів і коду, вбудованого в образи мікропрограми. Binwalk використовує бібліотеку libmagic, тому вона сумісна з магічними сигнатурами, створеними для утиліти файлів Unix.

Для перевірки виконаємо команди:

binwalk –B – для аналізу підпису зазначеного файлу.

binwalk -A – вказує binwalk шукати у вказаному файлі коди виконуваних інструкцій, загальні для різних збірок CPU.

Як результат, після аналізу за допомогою утиліти, не виявлено вказівки на те, що зображення є стеганографічним файлом.

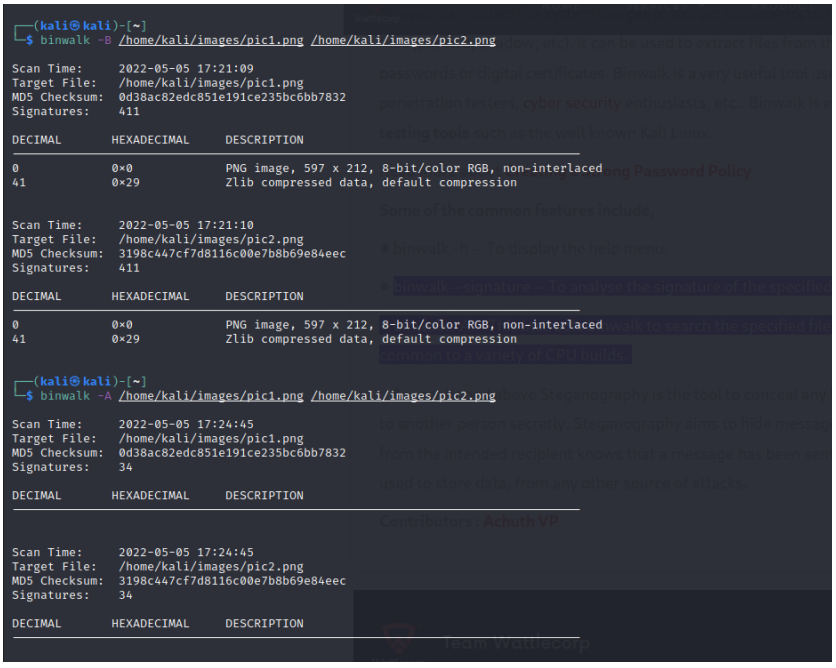


Рисунок 3.13 Результати роботи BinWalker

StegCracker — це утиліта для стеганографії для виявлення прихованих даних у файлах методом грубого перебору.

У випадку, якщо пароль зловмиснику не відомий, використовується перебір всіх значень словника з паролями та їх можливих комбінацій, таким чином

повідомлення із стеганографічного зображення запропонованої системи не може бути декодовано.

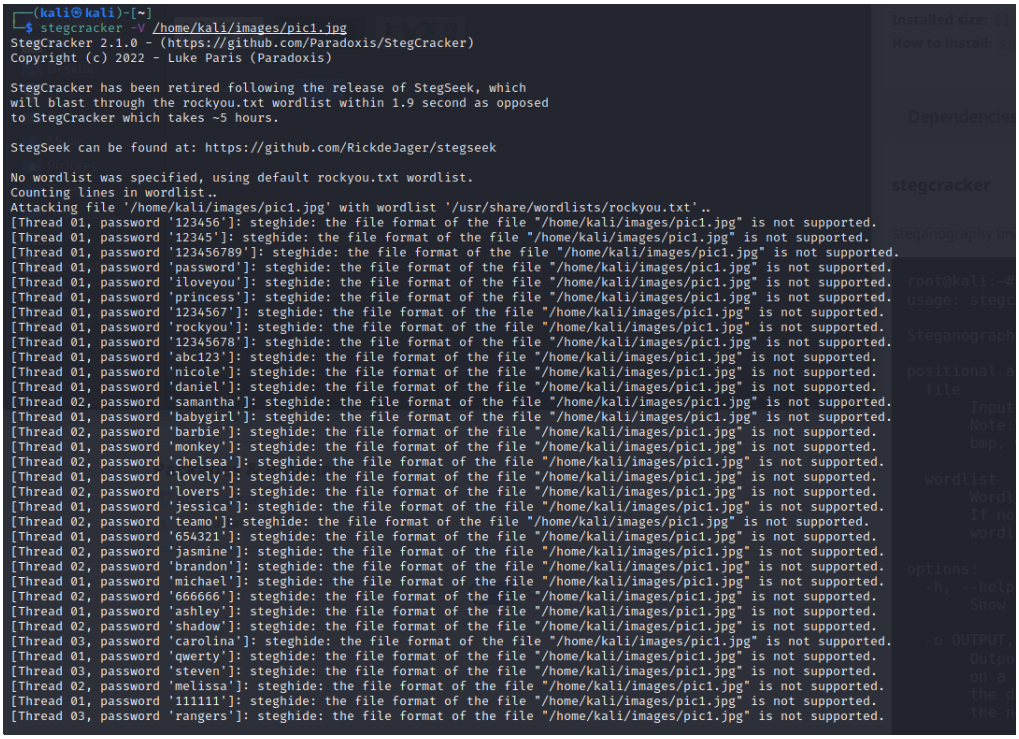


Рисунок 3.14 Результат роботи StegCracker

3.2. Переваги запропонованого рішення

1. Використовуючи цей процес, якщо є порушення безпеки на рівні бази даних роздрібного продавця, ми можемо бути впевнені, що особиста або банківська інформація кінцевих користувачів не постраждає. Це також захищає від неетичного використання особистої або банківської інформації кінцевих користувачів на веб-сайті роздрібного продавця.

2. Крім того, центральний центр сертифікації (ЦС) четвертої сторони може досягти більшої безпеки. Це дозволить кінцевому користувачу отримати більш безпечний переказ коштів, оскільки кількість сторін і рівень безпеки будуть збільшені.

3. Стеганографія використовується таким чином, що навіть центральний центр сертифікації (ЦС) не зможе зрозуміти пароль аутентифікації кінцевого користувача. Таким чином, ми забезпечуємо більшу безпеку для кінцевого користувача.

4. Зв'язок між центральним засвідчуючим органом (ЦА) та банком кінцевих користувачів буде завершуватися за допомогою безпечної поштової служби, щоб цей код можна було захистити від неправильного використання.

5. Завжди існує ймовірність злому або скомпрометації бази даних, оскільки дані кінцевого користувача пересилаються кільком сторонам.

3.3. Аналіз рішення на предмет виконання міжнародних стандартів безпеки

Для прийняття рішення, чи може запропонований продукт бути застосований у сучасних банківських продуктах, необхідно провести аналіз на предмет відповідності системи міжнародному стандарту PCI 3DS, виконання вимог якого є обов’язковим для участі інформаційної системи у роботі протоколу 3D-Secure і надання відповідних сервісів користувачам.

Враховуючи те, що вимоги стандарту стосуються всіх сфер менеджменту інформаційною системою, до розгляду буде прийнято лише вимоги, які можуть бути застосовані до програмного забезпечення, що обслуговує ACS.

Таблиця 3.1

Аналіз вимог до ACS

Вимога PCI 3DS	**Чи застосовується**	**Чи задовольняється**	**Коментар**
P2-3.1 Захист кордонів	Ні		Вимога стосується визначення, фізичного та логічного обмеження кордонів інформаційних підсистем.
P2-3.2 Захист базових конфігурацій	Частково	Так	Криптографічний модуль не має функції захисту конфігурації системи, проте кеш роботи програми дозволить адміністраторам системи якісно відслідковувати роботу модуля і виявляти аномалії.
P2-3.3 Захист	Так	Так	Робота модуля підлягає

Вимога PCI 3DS	**Чи застосовується**	**Чи задовольняється**	**Коментар**
програм та інтерфейсів програм			моніторингу і при ретельному дослідженні кешу аномалії в роботі можуть бути оперативно виявлені.
P2-3.4 Захищені веб-конфігурації	Ні		Функція захисту від незахищеного та неперевіреного з'єднання покладається на мережеві компоненти системи.
P2-3.5 Підтримка доступності операцій 3DS	Так	Так	Робота модуля не вимагає великої обчислювальної потужності як з боку шифрування (на боці серверу), так і з боку дешифрування (на боці клієнта), відповідно використання модуля не може викликати збої/переривання у роботі протоколу
P2-4.1 Захист з'єднання для клієнтів-емітентів і продавців	Так	Так	Запроповноване рішення впроваджує схему приховування повідомлення між емітентом та користувачем, завдяки чому повідомлення може бути безпечно передане, без втручання третіх осіб у процес.

3.4. Висновки до розділу 3

Зі сказаного вище можна зробити висновок, що, використовуючи існуючий метод під час здійснення покупок через веб-сайт інтернет-магазину, завжди існує ймовірність вторгнень та витоку інформації. Під час зазначеного процесу життєво важлива інформація, як-от банківські реквізити та персональні дані кінцевих користувачів, може бути зламана та використана неправомірно. Щоб захистити дані кінцевих користувачів і зробити фінансові операції більш безпечними, ми

пропонуємо цю систему. У якому через ЦС кінцеві користувачі платіжної інформації надаватимуть платіжному порталу, а не надсилатимуть її на веб-сайт продавця.

Для цього підходу нам потрібна підтримка довіреної третьої сторони, відомої як центральний сертифікований орган із текстовою стеганографією та RG-візуальною криптографією. CA авторизував та аутентифікував особу кінцевого користувача шляхом поєднання текстових зображень share1 та share2 перед обробкою платежу. Комбінований підхід текстової стеганографії та RG-візуальної криптографії з CA забезпечить кінцевому користувачеві конфіденційність інформації та захистить дані від неправомірного використання. Отже, використовуючи цей комбінований підхід у запропонованій платіжній системі, можна реалізувати функції безпеки та захистити платіжні дані користувачів від втручання зловмисників.

ВИСНОВКИ

Під час виконання роботи було проведено аналіз наявних методів захисту платіжних транзакцій та участь серверу контролю доступу у протоколі 3D-Secure, на основі чого сформовано висновки про необхідність впровадження ефективних методів захисту ACS як об'єкта інформаційної безпеки.

На ACS покладаються функції обробки операції із аутентифікації клієнта, з чого випливає, що програмний модуль ACS повинен забезпечувати такі функції як: цілісність, конфіденційність, доступність, оперативність, програмна сумісність.

В ході роботи було запропоновано та розроблено рішення для криптографічного модуля, яке може бути впроваджене у будь-яку сучасну банківську систему. Запропоноване рішення працює на основі об’єднання методів стеганографії та візуальної криптографії, що дозволить безпечно передавати дані для аутентифікації (на сучасному етапі такими даними є одноразовий пароль) користувачу без ризику, що ці дані можуть бути перехоплені або скомпрометовані третьою стороною.

Були проведені роботи із експлуатації та тестування програмного рішення, за результатом яких доведено, що технології, які можуть бути використані зловмисником, не дають змоги отримати доступ до даних, що передаються. Окрім цього, аналіз сучасної нормативної бази щодо вимог до систем, які приймають участь у забезпеченні платіжних операцій, показує, що запропоноване рішення відповідає вимогам, які до нього застосовуються.

Таким чином, запропонований криптографічний модуль може бути використаний під час розробки банківської системи, яка підтримує участь у протоколі 3D-Secure 2, а також майбутніх версій протоколу, які будуть впроваджуватись.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A Review on Electronic Payments Security [Електронний ресурс] // National University Malaysia. – 2020. – Режим доступу до ресурсу: https://www.researchgate.net/publication/343598898_A_Review_on_Electronic_Payments_Security.

2. New banking security system iTAN not as secure as claimed [Електронний ресурс] // RedTeam Pentesting GmbH. – 2005. – Режим доступу до ресурсу: https://www.redteam-pentesting.de/en/advisories/rt-sa-2005-014/-new-banking-security-system-itan-not-as-secure-as-claimed.

3. Formal analysis of card-based payment systems in mobile devices [Електронний ресурс] // Macquarie University/. – 2006. – Режим доступу до ресурсу: https://www.researchgate.net/publication/221149707_Formal_analysis_of_card-based_payment_systems_in_mobile_devices.

4. Cybersecurity in payments: what you need to know about payment authentication [Електронний ресурс] // PayXpert. – 2021. – Режим доступу до ресурсу: https://blog.payxpert.com/cybersecurity-in-payments-what-you-need-to-know-about-payment-authentication.

5. The adoption of mobile payment services for “fintech” [Електронний ресурс] // Nanyang Technological University. – 2016. – Режим доступу до ресурсу: https://www.researchgate.net/publication/298714824_The_adoption_of_mobile_payment_services_for_fintech.

6. Protocol and Core Functions Specification. // EMVCo. – 2021. – С. 35–38.

7. Summary of 3D Secure 2.0 and How CA Can Help. // CA ViewPint. – 2016. – С. 1–3.

8. Payment Card Industry 3-D Secure (PCI 3DS) [Електронний ресурс] // PCI Security Standards Council. – 2017. – Режим доступу до ресурсу: https://www.pcisecuritystandards.org/documents/PCI-3DS-Core-Security-Standard-v1.pdf?agreement=true&time=1647803414606.

9. Payment Card Industry EMV® 3-D Secure 3DS SDK [Електронний ресурс] // PCI Security Standards Council. – 2018. – Режим доступу до ресурсу: https://www.pcisecuritystandards.org/documents/3DS-SDK-Program-Guide-v1-0.pdf?agreement=true&time=1647803414637.

10. Visa Secure EMV 3DS Approved Product List [Електронний ресурс] // Visa. – 2021. – Режим доступу до ресурсу: https://technologypartner.visa.com/Download.aspx?id=698.

11. Vulnerability Summary for the Week of October 11, 2021 [Електронний ресурс] // Cybersecurity & Infrastructure Security Agency. – 2021. – Режим доступу до ресурсу: https://www.cisa.gov/uscert/ncas/bulletins/sb21-291.

12. Top 10 Things to Know About EMV 3-D Secure [Електронний ресурс] // Mastercard. – 2019. – Режим доступу до ресурсу: https://www.mastercard.com/content/dam/public/mastercardcom/globalrisk/pdf/Top-10-Things-to-Know-About-3DS.pdf.

13. TranzWare e-Commerce [Електронний ресурс] // CompassPlus – Режим доступу до ресурсу: https://compassplus.ru/static/materials/leaflets/TranzWare_e-Commerce.pdf.

14. 3DS Server Hosted Service ActiveServer Service [Електронний ресурс] // GPayments Pty Ltd – Режим доступу до ресурсу: https://www.gpayments.com/solutions/3ds-server-activeserver-saas/.

15. ActiveServer Authentication API Reference [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://docs.activeserver.cloud/en/api/auth/.

16. Investigation of 3-D Secure's Model for Fraud Detection [Електронний ресурс] // School of ComputingNewcastle University. – 2020. – Режим доступу до ресурсу: https://www.researchgate.net/publication/344410820_Investigation_of_3-D_Secure%27s_Model_for_Fraud_Detection

17. EMV 3-D Secure: Enhanced Data Driving Better Customer Experiences [Електронний ресурс] // CA Technologies. – 2018. – Режим доступу до ресурсу: https://docs.broadcom.com/doc/emv-3-d-secure-enhanced-data-driving-better-customer-experiences.

18. EMV 3-D Secure [Електронний ресурс] // U.S. Payments Forum. – 2020. – Режим доступу до ресурсу: https://www.uspaymentsforum.org/wp-content/uploads/2020/03/EMV-3DS-WP-FINAL-March-2020.pdf.

19. Netcetera 3DS Server - Release Notes - Version 2.5.2.0 [Електронний ресурс] // NetCetera. – 2022. – Режим доступу до ресурсу: https://3dss.netcetera.com/3dsserver/doc/2.5.2.0/v2.5.2.0.

20. Credit Card Encryption and Secure Transactions [Електронний ресурс] // Medium. – 2019. – Режим доступу до ресурсу: https://medium.com/@chaityachheda/credit-card-encryption-and-secure-transactions-98b54dc09d51.

21. Visual cryptography and image processing based approach for secure transactions in banking sector [Електронний ресурс] // 2nd International Conference on Telecommunication and Networks. – 2017. – Режим доступу до ресурсу: https://www.semanticscholar.org/paper/Visual-cryptography-and-image-processing-based-for-Jain-Soni/174e99388c090b0f068b198025f757e1a28cb231.

22. Survey Paper on Utilizing Visual Cryptography for Secure Bank Transaction [Електронний ресурс] // College of Engineering. – 2018. – Режим доступу до ресурсу: https://www.ijsr.net/archive/v8i11/ART20201982.pdf.

23. Jeyavadhanam R. Visual Cryptography for Biometric Privacy, Authentication and General Access Structure: A review / R. Jeyavadhanam, A. Rubavathy. // Journal of Critical Reviews. – 2020. – С. 7213–7230.

24. Online Payment System using Steganography and Visual Cryptography [Електронний ресурс] // Department of Electronics & Tele-Communication Engineering Jadavpur University. – 2014. – Режим доступу до ресурсу: http://www.logicsystems.org.in/Base%20Papers/2014%20.Net/LSD1452%20-%20Online%20Payment%20System%20using%20Steganography%20and%20Visual%20Cryptography.pdf.

25. Secured Bank Authentication using Image Processing and Visual Cryptography [Електронний ресурс] // International Journal of Computer Science and Information

Technologies. – 2014. – Режим доступу до ресурсу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.661.35&rep=rep1&type=pdf.

26. A novel image encryption algorithm using AES and visual cryptography [Електронний ресурс] // 2nd International Conference on Next Generation Computing Technologies. – 2016. – Режим доступу до ресурсу: https://www.researchgate.net/publication/315365473_A_novel_image_encryption_algorithm_using_AES_and_visual_cryptography

27. Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics [Електронний ресурс] //) International Journal of Computer Science and Information Technologies. – 2012. – Режим доступу до ресурсу: http://ijcsit.com/docs/Volume%203/vol3Issue3/ijcsit20120303112.pdf.

28. Linguistic steganography: survey, analysis, and robustness concerns for hiding information in text [Електронний ресурс] // Center for Education and Research in Information Assurance and Security. – 2004. – Режим доступу до ресурсу: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2004-13.pdf.

29. Improved E-Banking System With Advanced Encryption Standards And Security Models [Електронний ресурс] // International Journal of Scientific & Technology. – 2016. – Режим доступу до ресурсу: https://www.ijstr.org/final-print/oct2016/Improved-E-banking-System-With-Advanced-Encryption-Standards-And-Security-Models-.pdf.

30. Secured Transaction System Using Steganography and Visual Cryptography [Електронний ресурс] // Savitribai Phule Pune University. – 2016. – Режим доступу до ресурсу: https://ijesc.org/upload/89cb6e2252d75357ed02b55593b0bf91.Secured%20Transaction%20System%20Using%20Steganography%20and%20Visual%20Cryptography.pdf.

31. Combine Use of Steganography and Visual Cryptography for Online Payment System [Електронний ресурс] // International Journal of Computer Applications. – 2015. – Режим доступу до ресурсу: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.735.5448&rep=rep1&type=pdf

.

32. Combination of Steganography and Cryptography: A short Survey [Електронний ресурс] // IOP Conference Series: Materials Science and Engineering. – 2019. – Режим доступу до ресурсу: https://iopscience.iop.org/article/10.1088/1757-899X/518/5/052003/pdf.

33. Enhanced Security of Symmetric Encryption Using Combination of Steganography with Visual Cryptography [Електронний ресурс] // International Journal of Engineering Trends and Technology. – 2018. – Режим доступу до ресурсу: https://arxiv.org/ftp/arxiv/papers/1902/1902.11167.pdf.

34. Survey on Visual Cryptography: Techniques, Advantages and Applications [Електронний ресурс] // Journal of Computer Engineering. – 2016. – Режим доступу до ресурсу: https://www.iosrjournals.org/iosr-jce/papers/conf.15013/Volume%201/2%20.06-12.pdf?id=7557.

35. Payment services (PSD 2) - Directive (EU) 2015/2366 [Електронний ресурс] // EU Council. – 2015. – Режим доступу до ресурсу: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en.

36. The Fourth Annual CardinalCommerce Survey [Електронний ресурс] // CardinalCommerce. – 2017. – Режим доступу до ресурсу: https://www.cardinalcommerce.com/news-and-events/press-releases/2017/march/fourth-annual-cardinal-survey.

37. Harvesting High Value Foreign Currency Transactions from EMV Contactless Credit Cards Without the PIN [Електронний ресурс] // Conference on Computer and Communications Security. – 2019. – Режим доступу до ресурсу: https://dl.acm.org/doi/10.1145/2660267.2660312.

38. MasterCard SecureCode Merchant Implementation Guide [Електронний ресурс] // Mastercard. – 2014. – Режим доступу до ресурсу: https://www.mastercard.us/content/dam/mccom/en-us/documents/SMI_Manual.pdf.

39. European EMV 3DS 2.2.0 Implementation Guide [Електронний ресурс] // Visa. – 2019. – Режим доступу до ресурсу: https://www.visa.co.uk/dam/VCOM/regional/ve/unitedkingdom/PDF/sca/visa-european-emv-3ds-220-implementation-guide.pdf.

40. Cryptographic Algorithms for the Payment Card Industry [Електронний ресурс] // Atsec information security corporation. – 2006. – Режим доступу до ресурсу: https://www.atsec.cn/fileadmin/user_upload_us/pci/cryptographic_algorithms_PCI.pdf.

41. Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding [Електронний ресурс] // Foundation of Technical Education. – 2015. – Режим доступу до ресурсу: https://www.academia.edu/26314028/Cryptography_and_Image_Steganography_Using_Dynamic_Encryption_on_LSB_and_Color_Image_Based_Data_Hiding.

42. A Hybrid Approach For Image Security By Combining Cryptography and Steganography. – 2020. – Режим доступу до ресурсу: http://cse.anits.edu.in/projects/projects1920B10.pdf.

43. Steganalysis Techniques: A Comparative Study [Електронний ресурс] // University of New Orleans. – 2007. – Режим доступу до ресурсу: https://scholarworks.uno.edu/cgi/viewcontent.cgi?article=1562&context=td.

44. Classification of steganalysis techniques: A study [Електронний ресурс] // Digital Signal Processing. – 2010. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/abs/pii/S1051200410000412.

45. Visual Cryptography [Електронний ресурс] // Eurocrypt. – 1994. – Режим доступу до ресурсу: https://www.cs.jhu.edu/~fabian/courses/CS600.624/NaorShamir-VisualCryptography.pdf.

46. Review on Various Visual Cryptography Schemes [Електронний ресурс] // International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). – 2017. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8455136.

47. Passwords: If We’re So Smart, Why Are We Still Using Them? [Електронний ресурс] // Mastercard. – 2009. – Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007/978-3-642-03549-4_14#:~:text=Passwords%20remain%20the%20dominant%20means,more%20passwords%20than%20ever%20before..

48. Technological Factors of Mobile Payment: A Systematic Literature Review [Електронний ресурс] // International Conference on Computer Science and Computional Intelligence. – 2019. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S1877050919311615.

49. New Algorithm For Halftone Image Visual Cryptography [Електронний ресурс] // King Fahd University of Pet. & Min.. – 2006. – Режим доступу до ресурсу: https://www.researchgate.net/publication/228980617_New_Algorithm_For_Halftone_Image_Visual_Cryptography.

50. A steganographic method based on Integer Wavelet Transform and Genetic Algorithm [Електронний ресурс] // IEEE. – 2011. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/5739395?arnumber=5739395.

ДОДАТОК А

Наукові публікації

1. VII міжнародна конференція «Information Technology and Implementation» (IT&I-2021). – 2021
2. V Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)”. – 2022