18. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58. (Scopus).
19. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256. (Scopus).
20. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114. (Scopus).

УДК 004

І.Шевчук, магістр гр. КІ-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ДАНИХ КАРТИ ТАХОГРАФА

У статті розроблено програмне забезпечення, яке призначено для системи даних карти тахографа. Метою розробки є дослідження та програмна реалізація системи даних карти тахографа. Об'єктом дослідження є процес даних карти тахографа. Предметом дослідження є методи даних карти тахографа. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи даних карти тахографа. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, захисту доступу, тахограф

Постановка проблеми. У цей час пластикові карти одержали широке поширення в додатках захисту інформації: це й таксофонні карти, і SIM-карти в стільникових телефонах, це, звичайно ж, платіжні карти різних типів, карти медичного страхування, проїзду в міському транспорті, карти постійного покупця, що стимулюють попит, називані дисконтними, контейнери криптографічних ключів, карти-ключі, що відкривають електронний замок у дверях, електронні посвідчення особи, засоби підтвердження оплати й дійсності абонента в стільниковій телефонії й супутниковому телебаченні, засоби автентифікації користувачів обчислювальної системи й т.д.

Основними завданнями розвитку технології вітчизняних чіп-карт на сьогодні є:

– пошук методів збільшення ефективності використання ресурсів кристала, в умовах неможливості переходу на іншу норму проектування;

– пошук шляхів інтеграції чіп-карт закордонного виробництва в системи, що використовують вітчизняні криптографічні стандарти;

– проектування захищених малоресурсоємних протоколів електронних платежів і ідентифікації на основі чіп-карт;

– проектування захищених безконтактних карт, що несуть як ідентифікаційну, так і платіжну функціональність, які задовольняють вітчизняним стандартам в області захисту інформації;

– пошук нових областей застосування для чіп-карт.

Рішенню комплексу вищевказаних теоретичних і практичних питань і присвячена дана магістерська робота. Крім того, розроблені методи зменшення ресурсоємності, застосовувані для рішення набору даних прикладних завдань, можуть бути використані й в інших областях, у яких є подібні завдання. Останнє робить магістерську роботу актуальною не тільки для розглянутої предметної області.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи даних карти тахографа.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи даних карти тахографа.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем даних карти тахографа.
– Дослідження системи даних карти тахографа.
– Програмна реалізація системи даних карти тахографа.

Об'єктом дослідження є процес даних карти тахографа.

Предметом дослідження є методи даних карти тахографа.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис функціонування системи

Розглянемо основні уразливості, при роботі з чіп-картами. До основних класів типових атак на АС на основі чіп-карт, відносяться наступні:

– Соціальна інженерія.
– Соціальна інженерія із застосуванням апаратних засобів.
– Доступ до каналів зв'язку.
– Підміна / модифікація устаткування.
– Інженерне проникнення, DPA/ DFA-атаки, криптоаналіз.
– Закладки, залишені розроблювачами системи.

Розглянуті в магістерській роботі протоколи безпеки спроектовані таким чином, що захищають від атак зловмисників описаних рівнів до рівня 3 включно на доступ до каналів зв'язку й підміну / модифікацію устаткування, якщо в описі протоколу не зроблене уточнення. Захист від атак видів "соціальна інженерія", "соціальна інженерія із застосуванням апаратних засобів" повинна бути забезпечена організаційно-адміністративними мірами. Захист від атак класу "інженерне проникнення, DPA/DFA-атаки, криптоаналіз" здійснюється розроблювачами кристалів чіп-карт, і базових криптоалгоритмів. Захист від закладок, залишених розроблювачами системи, не здійснюється.

Вирішимо завдання побудови архітектури компактної файлової системи мікропроцесорної карти, збільшення ефективності використання ресурсів існуючого кристала вітчизняної мікропроцесорної карти (у першу чергу, EEPROM).

Для цього розробимо архітектуру компактної файлової системи, що дозволяє використовувати ресурси EEPROM істотно більш раціональним образом, рекомендації зі зміни архітектури мікроконтролера карти для забезпечення можливості виконання внутрішніх скриптів безпосередньо мікроконтролером карти й швидкодіюча реалізація ДСТ 28147:2009 на чіп-картах.

Самим ресурсномістким і дефіцитним видом пам'яті сьогоднішніх інтелектуальної карти є EEPROM. Вона займає більше половини кристала і його розмір обмежує можливості використання карти. Для рішення поставленого завдання були проведені:

– Розробка організації файлової системи таким чином, щоб перенести незмінні частини файлів додатків карти (а їх – до 90% від усього обсягу прикладних даних) у більше дешеве й менш дефіцитне масочне ПЗП. Таким чином, байти того самого файлу зберігаються, залежно від їхнього призначення, у різних пристроях зберігання. При цьому таке зберігання є прозорим для операційної системи й додатків карти (

– Рисунок 1). Дане завдання було вирішено за допомогою FAT із кластерами змінної довжини.

– Зменшення розмірів службових областей.

– Був зроблений перехід від блок-орієнтованої організації файлової системи (що приводить до втрат при вирівнюванні до границі блоку) до байт-байт-орієнтованого.

– Замість розрахунку CRC на файл (коли для читання хоча б одного байта було потрібно перечитати весь файл, щоб перевірити CRC) був реалізований підрахунок CRC на сектор (рис.2).

Розроблена архітектура файлової системи має наступні властивості:

– Мінімізовано втрати від вирівнювань.

– Кількість рівнів файлової системи становить не менш трьох.

– Для додатків, емісія яких становить достатній обсяг, з'являється можливість переміщення всіх константних даних з EEPROM у вільну область масочного ПЗП.

– Реалізовано можливість видалення з карти додатків, що мають константні дані в масочному ПЗП для забезпечення можливості використання карти в інших додатках. Оскільки видалення даних з масочного ПЗП неможливо, віддаляються лише посилання на них з EEPROM.

– Для забезпечення можливості використання кристалів з окремими збійними ділянками EEPROM, зсуву даних, збережених в EEPROM, не зберігаються в масочному ПЗП.

– Можливе видалення файлів (що дозволяється лише в деяких файлових системах чіп-карт), однак видалення файлів і додатків не повинні носити масового характеру.

– Залежно від типу, файли можуть мати заголовки різної довжини.

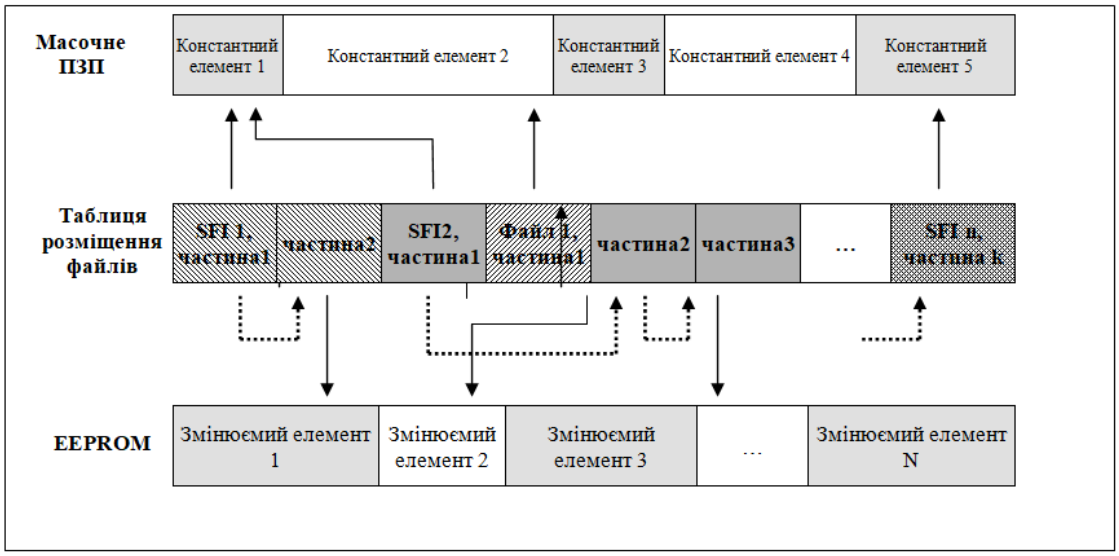

Рисунок 1 – Таблиця розміщення файлів

– Структура даних файлової системи поліпшена з погляду мінімізації часу звертання до файлів.

– Файлова система дозволяє забезпечувати збалансоване навантаження по перезапису на сектори EEPROM, тобто немає секторів, перезаписуваних істотно частіше, ніж інші.

Оцінка практичної ефективності (на прикладі EMV-сумісного додатка) запропонованої методики показала, що розмір що вимагається EEPROM може зменшуватися до 3-4 разів.

Далі розглянемо завдання вироблення рекомендацій зі зміни архітектури мікроконтролера карти для забезпечення можливості виконання внутрішніх скриптів безпосередньо мікроконтролером карти, що має метою зменшення простору масочного ПЗП, займаного кодом ОС карти, а також забезпечення можливості кастомізації конфігурації ОС на етапі персоналізації шляхом додавання різних додаткових модулів ОС в EEPROM.

Для забезпечення ізольованості друг від друга додатків, що перебувають на карті, виберемо шлях введення програмного супервізора й введемо аналог захищеного режиму, що

дозволяє додатку робити лише безпечні операції, а виконання операцій, критичних з погляду безпеки, здійснюється під контролем (або за допомогою) супервізора.

Рекомендуємо, до застосування, реалізацію мінімального достатнього набору модифікацій в архітектурі кристала інтелектуальної карти КБ5004ВЕ1 (An15M04):

– введення прапора наявності віртуального режиму в регістрі стану процесора;

– об'єднання адресного простору масочного ПЗП і EEPROM в один адресний простір, для того, щоб програмний код, збережений в EEPROM, був доступний для виконання кристалом;

– поділ набору команд на привілейовані й непривілейовані;

– введення в систему команд кристала додаткової команди перемикання на супервізор;

– використання двох переривань під порушення захисту й під супервізор;

– спроектовані протоколи дозволяють захиститися від атак зловмисників рівнів 1-3, описаних у розділі 1 на доступ до каналів зв'язку й підміну / модифікацію устаткування.

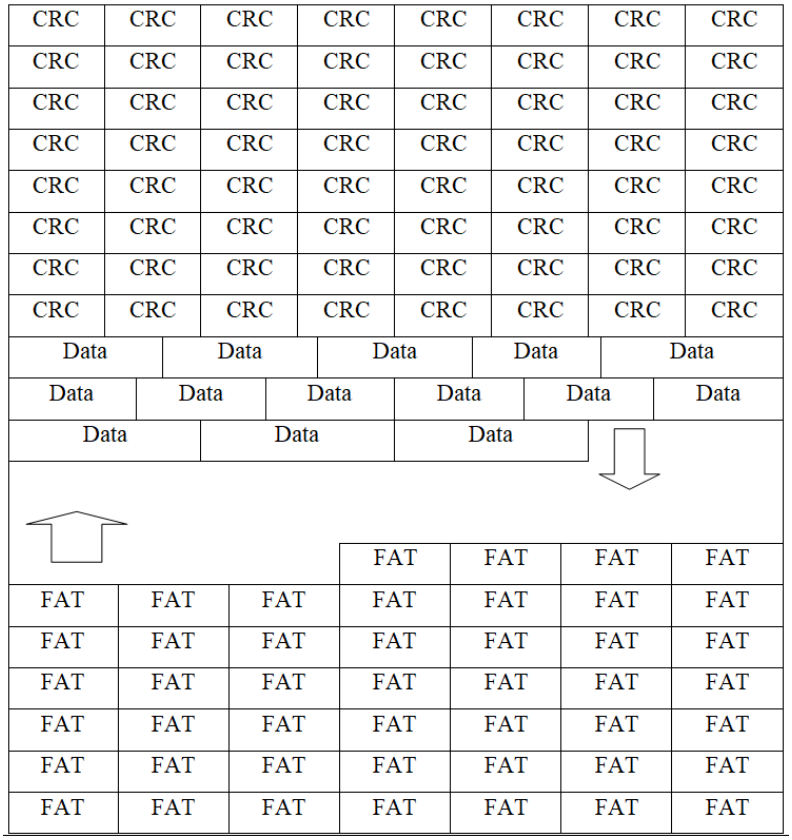

Рисунок 2 – Заповнення EEPROM карти файловою системою

Вироблені рекомендації дозволять розвантажити простір у масочному ПЗП, тому що розмір реалізації супервізора представляється істотно меншим у порівнянні із традиційним інтерпретатором скриптів віртуальної машини. По оцінці, заснованій на розмірах реалізацій інтерпретаторів віртуальної машини в існуючих операційних системах для кристала КБ5004ВЕ1, абсолютна величина виграшу може скласти від одного до півтора кілобайт із шістнадцяти на сьогоднішній день.

Розглянемо реалізацію вітчизняного криптоалгоритму ДСТ 28147:2009 на закордонних картах без необхідності модифікації їх масочного ПЗП, з поліпшеними швидкісними характеристиками. Дане рішення необхідно для забезпечення можливості використання закордонних чіп-карт (не підтримуючих ДСТ 28147:2009) у додатках, що вимагає використання вітчизняної криптографії й наявності обсягів EEPROM, істотно перевищуючих існуючі EEPROM чіп-карт російського виробництва.

ДСТ 28147:2009 орієнтований на мікропроцесори із тридцятидвобітною архітектурою, з порядком байтів BigEndian. Ніяких складностей у реалізації ДСТ 28147:2009 на інтелектуальній карті в принципі немає, якщо тільки карта підтримує опціональний для інтелектуальної карти тридцятидвобітний тип int. На жаль, на сьогоднішній день більшість реалізацій інтелектуальної карти тип int не підтримують, а карти, на яких інтелектуальної карти підтримують int, мають досить високу вартість. Виходить, необхідно робити тридцятидвобітне додавання як пари шістнадцятибітних, контролюючи переповнення, благо шістнадцятибітний тип short зобов'язаний бути присутнім у будь-якій реалізації інтелектуальної карти. Однак в інтелектуальній карті неможливо здійснити контроль переповнення за допомогою прапора, тому для контролю переповнення при додаванні двох чисел певного типу доводиться перетворювати їх до старшого типу й потім порівнювати з маскою, переконуючись, що результат приводиться до вихідного типу без втрат. Таким чином, при традиційному підході, одне додавання тридцятидвобітних чисел виливається в додавання чотирьох восьмибайтових чисел, і це навіть без обліку інкрементів.

Пропонована схема дозволить здійснювати додавання тридцятидвобітних чисел з будь-якими значеннями шляхом виконання двох шістнадцятибітних додавань, одного інкремента й трьох шістнадцятибітних операцій перевірки знака.

Для прискорення реалізації криптоалгоритма були отримані наступні теоретичні результати:

Визначення 1: Назвемо знаковою інтерпретацією беззнакового числа $x \in \overline{0,2^n-1}$ конструкцію виду:

$$s(x) := \begin{cases} x, & x < 2^{n-1} \\ x - 2^{n-1}, & x \geq 2^{n-1} \end{cases}, \qquad (1)$$

Уведемо знакові інтерпретації для що складаються A, B і їхньої суми:

$$a := s(A),\ b := s(B),\ c := s((A+B) \bmod 2^n). \qquad (2)$$

Під сумою доданків у цьому випадку розуміється операція додавання без обліку переповнення, тобто за модулем 2^n.

Лема 1: $c \geq 0 \Leftrightarrow A + B \in \left[0, 2^{n-1}\right) \cup \left[2 \cdot 2^{n-1}, 3 \cdot 2^{n-1}\right)$.

Лема 2: $\forall n \geq 2 \qquad 2 \cdot (2^n - 1) \geq 3 \cdot 2^{n-1}$.

Твердження 1 (Критерій наявності переносу): Перенос при додаванні чисел A і B (тобто $A + B \geq 2^n$) виникає тоді й тільки тоді, коли щира умова:

$$\begin{cases} b < 0 \,\&\, c \geq 0, & a \geq 0 \\ b < 0 \vee c \geq 0, & a < 0 \end{cases}. \qquad (2)$$

Отриманий результат дозволяє одержати реалізацію, істотно більш швидку в порівнянні з існуючими аналогами.

Розробимо протокол гнучких і малоресурсоємних типових додатків чіп-карт, що відповідають сучасним вимогам безпеки, придатних до використання в широкому колі виникаючих прикладних завдань, у тому числі з урахуванням специфіки додатків безконтактних карт.

Уведемо поняття універсального облікового додатка й розробимо його в також виробимо ряд рекомендацій з розробки архітектури вітчизняних безконтактних карт, що задовольняють вимогам вітчизняних стандартів в області захисту інформації, на базі кристала MIFARE компанії Philips Semiconductor.

Основною проблемою в даній області є складність розбору виникаючих нестандартних ситуацій, що виникають внаслідок атак або ненавмисних аварійних ситуацій, таких як, переривання живлення або розриви зв'язку в процесі виконання транзакції.

Звичайно в подібній ситуації тримач карти приречений очікувати два тижні – час, протягом якого банк повинен зібрати всі оффлайн-журнали для відновлення послідовності подій.

Для забезпечення можливості невідкладного й однозначного трактування всіх відомих атак і помилок, що виникають у процесі проведення платіжних транзакцій були уведені три платіжних лічильники:

– лічильник запитів сертифіката балансу;
– лічильник дебетований;
– лічильник онлайн-операцій.

Розроблено алгоритм виявлення атак шляхом трактування станів лічильників.

Розроблена архітектура універсального платіжного додатка задовольняє наступним вимогам:

– можливість захищеного онлайн-поповнення, дебетування, синхронізації й віддаленої зміни платіжних лімітів;

– можливість безпечних оффлайн-дебетування й, можливо, оффлайн-скасування з виконанням всіх вимог безпеки.

– можливість безпечного дебетування на дрібні суми без уведення PIN-коду;

– стійкість до збоїв зв'язку під час онлайн-транзакції: у цьому випадку клієнт не повинен втратити кошти з балансу карти, навіть тимчасово;

– оффлайн- і онлайн-операції рознесені, тобто клієнт навіть після невдало завершеної онлайн-транзакції повинен мати можливість, як і колись, проводити оффлайн-операції;

– можливість використання симетричних криптоалгоритмів, і можливість застосування (у випадку потреби й наявності криптографічного співпроцесора на кристалі карти) асиметричних криптоалгоритмів без серйозних архітектурних змін.

Спроектовані протоколи дозволяють захиститися від атак зловмисників рівнів 1-3, описаних у розділі 1 на доступ до каналів зв'язку й підміну / модифікацію устаткування.

Спроектовано універсальний механізм, називаний універсальним обліковим додатком, на зразок універсального платіжного додатка, що має однакові принципи функціонування в зовсім різних платіжних проектах. Забезпечується унікальність криптограм, передані дані захищаються від модифікації при читанні/запису.

Були зроблені наступні кроки:

– Вичленовано загальні прикладні особливості в різних по призначенню облікових додатків.

– Виходячи з вимог атомарності перезапису секторів з урахуванням контролю автентичності записуваних даних був обраний розмір сектора.

– Обрано й описана конфігурація маски доступу.

– Розроблено набір прикладних команд універсального облікового додатка.

Отриманий універсальний обліковий додаток має наступні властивості:

– Універсальність: наскільки це можливо, додаток задовольняє вимогам різних дисконтних схем.

– Низька ресурсоємність. Функціональність додатка легко реалізується на різних чіп-картах, як вітчизняних, так і закордонних, що дозволяють розширювати набір команд за допомогою скриптів або апплетів інтелектуальної карти. Також повинна бути можливість апаратної реалізації додатку в безконтактній карті без мікропроцесора.

– Для спрощення реалізації додатка на безконтактних картах додаток не вимагає наявності апаратного ДВЧ.

– Гнучка схема розмежування доступу.

– Можливість реалізації декількох облікових додатків на одній карті.

– Можливість розмежування доступу до прикладним даних шляхом двосторонньої криптографічної автентифікації між картою й пристроєм прийому карт (ППК).

– Можливість автентифікації тримача карти за паролем.

– Наявність убудованого в додаток криптографічного контролю цілісності прикладних даних, переданих як з карти, так і на карту.

– Мінімізовано кількість обмінів між картою й ППК.

– Наявність механізму забезпечення унікальності криптограм.

– Спроектовані протоколи дозволяють захиститися від атак зловмисників рівнів 1-3, описаних у розділі 1 на доступ до каналів зв'язку й підміну / модифікацію устаткування.

Розробимо архітектуру вітчизняної безконтактної карти. Вирішимо наступні підзадачи:

– Вибір продукту з лінійки MIFARE як прототип вітчизняної безконтактної карти. Після детального дослідження лінійки кристалів MIFARE компанії Phillips Semiconductors, як прототип кристала вітчизняної безконтактної карти був обраний кристал MF1 IC S50.

– Механізми криптографічної автентифікації були наведені у відповідність із вітчизняними стандартами.

– Організація пам'яті була наведена у відповідність із розмірами ключа застосовуваного криптоалгоритмом ДСТ 28147:2009;

– Механізм автентифікації став забезпечувати можливість контролю цілісності переданих в обох напрямках по ефіру даних.

– Забезпечено унікальність (неповторюваність) даних, записуваних на карту.

Знайдемо шляхи застосування чіп-карт вітчизняного виробництва в системах захисту ПЗ від несанкціонованого копіювання. У ній вирішуються проблеми:

– Можливості використання вітчизняних чіп-карт у системах захисту ПЗ від несанкціонованого копіювання шляхом розробки протоколу симетричної автентифікації суб'єктом, що не зберігає секретний ключ автентифікації.

– Криптографічний протокол голосової активації ПЗ, що захищається від несанкціонованого копіювання, що володіє архітектурою, схожою з попереднім протоколом архітектурою.

– Спроектовані протоколи дозволяють захиститися від атак зловмисників рівнів 1-3, описаних у розділі 1 на доступ до каналів зв'язку й підміну / модифікацію устаткування.

Пропонується протокол симетричної однобічної автентифікації. Загалом, на автентифікуючій стороні зберігається таблиця еталонних відповідей на запити автентифікації, що не дозволяє, проте, відтворювати свій вміст в емуляторі зловмисника.

Стійкість протоколу забезпечується тимчасовими і ємнісними міркуваннями, а сам протокол показує можливість застосування чіп-карт, що здійснюють лише симетричні криптографічні перетворення, у системах захисту ПЗ від несанкціонованого копіювання.

Діаграма обмінів протоколу автентифікації, наведена в таблиці 1.

Істотною вимогою є забезпечення цілісності програмно-апаратного середовища автентифікуючій сторони. При цьому допускається можливість дослідження зловмисником алгоритмів функціонування автентифікуючій сторони, у т.ч. можливість читання зловмисником таблиці еталонних відповідей.

Розробимо криптопротокол віддаленої активації що захищається ПЗ через голосовий телефонний канал, що задовольняє наступним вимогам:

– можлива передача даних тільки один раз від клієнта до сервера й потім один раз назад;

– розмір переданих даних для кожного напрямку не повинен перевищувати 64-128 бітів, більший обсяг передати через голосовий телефонний канал (диктування) представляється скрутним;

– ПЗ, що захищається від несанкціонованого копіювання, повинне бути захищене від модифікації зловмисником;

– допускається наявність у зловмисника повної інформації про протокол активації;

– ПЗ, що захищається від несанкціонованого копіювання, повинне бути захищене від надання апаратним середовищем і операційною системою нав'язувальних зловмисником даних, що представляють собою ідентифікатори й метрики устаткування, а також джерела інформації для програмних ДВЧ;

– на стороні клієнта не повинні вимагатися які-небудь додаткові апаратні засоби;

– на клієнті не повинні зберігатися секретні криптографічні ключі;

– повинно бути розрахунково складно для зловмисника земулювати відповідь сервера на запит клієнта;

– можливе використання різних базових криптоалгоритмів одного класу в криптографічному протоколі активації.

Обмеження, що накладаються у вищеописаних вимогах, на розмір і кількість переданих повідомлень унеможливлюють використання асиметричних криптоалгоритмів у силу того, що розміри ЕЦП відомих авторові криптоалгоритмів істотно перевищують задані межі. Використання ж традиційної схеми автентифікації на базі симетричного криптоалгоритма, що припускає зберігання секретного ключа на обох сторонах, також неможливо.

Таблиця 1 – Діаграма обмінів протоколу автентифікації

Мікропроцесорна карта		Система захисту ПЗ від несанкціонованого копіювання
Ініціалізація даних		
Ключ K генерується й міститься на карту		Таблиця $T'=\{h(i) \mid 0 \le i < N\}$, що відповідає ключу K генерується й міститься до пам'яті ПЗ, що захищається, де $h(i) = H(v(i))$, $N = 2^{25} = 33\,554\,432$, розмір таблиці T' складе 128Мб.
Автентифікація карти		
		Генерується випадкове число $r \in \overline{0, N-1}$, і передається карті.
	←	
Формується й вертається відповідь $t = v(r)$ довжиною більше 1 кб		
	→	
		Обчислюється хеш-значення $w = H(t)$, потім по таблиці T', перевіряється рівність $w = h(r)$. Автентифікація вважається успішною у випадку збігу, і неуспішною в противному випадку.

Для підготовки до виконання криптопротоколу на сервері пропонується згенерувати таблицю пар виду:

$$\{(r,c) \mid r = H(c)\}, \qquad (4)$$

де:

r – двійковий вектор розміром l_r від 8 до 16 байт, називаний запитом активації (або, просто, запитом);

c – двійковий вектор розміром l_c від 8 до 16 байт, називаний підтвердженням активації (або, просто, підтвердженням), вибирається довільно, можливо, випадковим образом.

Вибір діапазону значень параметрів l_r і l_c обмежений знизу міркуваннями колізійної стійкості, а зверху – міркуваннями зручності й зменшення ймовірності помилки при диктуванні криптограми по голосовому каналі зв'язку.

$H(x)$ – криптографічна хеш-функція, значення якої усікається до необхідного розміру.

Параметри $\{c\}$ пар таблиці будуть секретними параметрами.

На клієнті зберігається таблиця запитів активації, що є підмножиною першого стовпця таблиці пар на сервері. Розмір таблиці – 2^{16} записів, тобто 0.5 – 1 Мб. Вибір підмножини здійснюється довільно.

Активація що захищається ПЗ здійснюється в такий спосіб. Клієнт здійснює збір прив'язочних значень обчислювального середовища E, зберігає його й потім хеширует цей набір значень у двійковий вектор $e = h(E)$ довжиною 16 біт.

Для цього рекомендується використовувати криптографічний алгоритм хешування. Даний хеш буде індексом у таблиці запитів активації клієнта. Обраний запит $r[e]$ активації відправляється клієнтом на сервер. Сервер знаходить у своїй таблиці пар запит-підтвердження $c = H^{-1}(r[e])$ необхідне підтвердження й відправляє його клієнтові. Клієнт шляхом обчислення хеш-функції від підтвердження й порівняння результату із запитом активації $H(c) = r[e]$ переконується в автентичності підтвердження. Після чого клієнт зберігає підтвердження у своїй області даних.

Для перевірки прив'язки в обчислювальному середовищі, клієнт, аналогічно вищеописаному, здійснює збір прив'язочних значень обчислювального середовища *E*' і робить порівняння векторів *E* і *E*'. У випадку успішного порівняння, клієнт переконується у відповідності підтвердження активації збереженому еталону, тобто перевіряє рівність $H(c) = r[h(E)]$.

Розробка структурної схеми

Структурна схема розробленої системи зображена на рисунку 3. На ній показано структурні блоки, з яких складається система, та структурні взаємозв'язки між цими блоками.

Структурна схема складається з трьох основних блоків:

– Інтелектуальна мікропроцесорна карта з EEPROM.
– Програмне забезпечення на серверній частині.
– Банкомат (Картрідер).

Розглянемо ці блоки більш детально.

Інтелектуальна мікропроцесорна карта з EEPROM являє собою пластикову картку, яку можливо використовувати для операцій з грошима. EEPROM – (Electrically Erasable Programmable Read-Only Memory, електрично стираємий перепрограмувальний постійний запам'ятовувальний пристрій ЕСППЗП). Пам'ять такого типу може стиратися й заповнюватися даними кілька десятків тисяч разів. Використовується у твердотільних накопичувачах. Однією з різновидів EEPROM є флеш-память.

Структурно вона включає в себе наступні блоки:

– Блок автентифікації користувача.
– Блок захисту даних на пластиковій карті.
– Блок здійснення операцій над рахунком.

Блок автентифікації користувача включає в себе наступні дані:

– Дані про користувача – прізвище, ім'я та по батькові.
– PIN-код користувача.

Блок захисту даних на пластиковій карті включає в себе наступні складові:

– Номер банківського рахунку користувача.
– Кількість грошей на рахунку.

– Криптоалгоритм ДСТ 28147:2009, яким зашифровані перераховані вище дані користувача.

Блок здійснення операцій над рахунком включає в себе наступні операції:

– читання про стан рахунку;
– зняття грошей з рахунку;
– поповнення рахунку;
– переведення грошей на інший рахунок.

Розглянувши структурний склад інтелектуальної мікропроцесорної карти з EEPROM, перейдемо до розгляду іншої складової – програмного забезпечення на серверній частині.

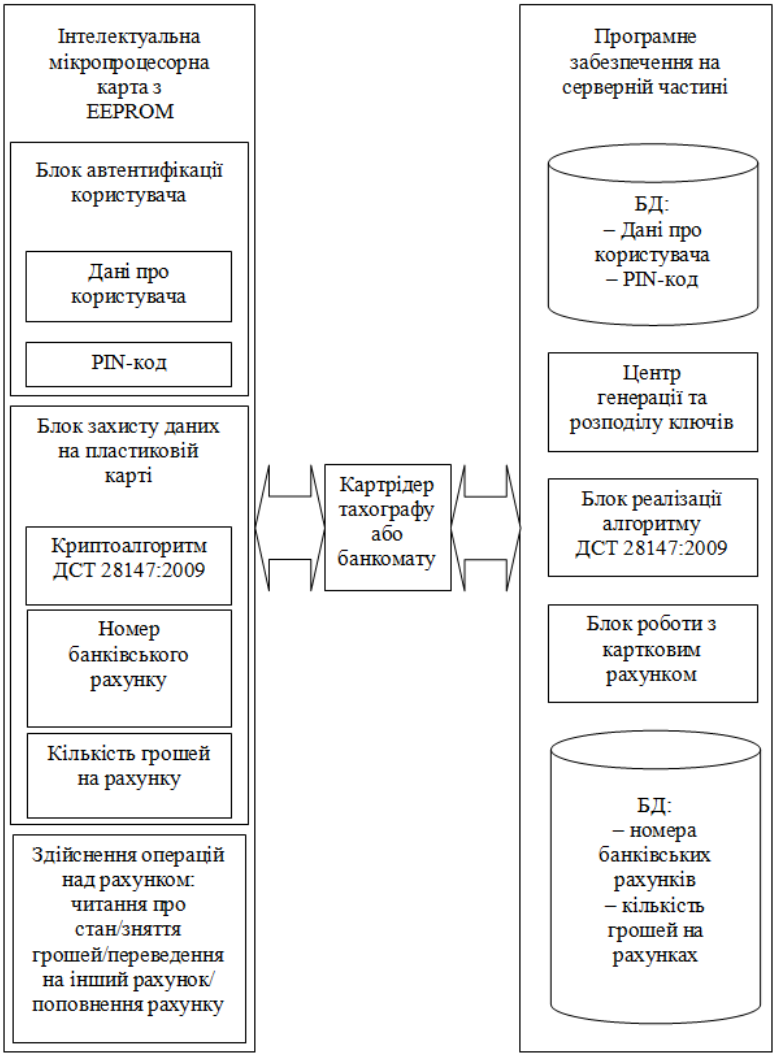

Рисунок 3 – Структурна схема системи

Програмне забезпечення на серверній частині складається з наступних структурних блоків:

– База даних про користувача.
– Центр генерації та розподілу ключів.
– Блок реалізації алгоритму ДСТ 28147:2009.
– Блок роботи з картковим рахунком.
– База даних про рахунок.

База даних про користувача включає в себе наступні дані:

– Дані про користувача – прізвище, ім’я та по батькові.
– PIN-код користувача.

База даних про рахунок включає в себе наступні дані:

– Номер банківського рахунку користувача.

– Кількість грошей на рахунку.

Опишемо алгоритм ДСТ 28147:2009. Для захисту даних на мікропроцесорній карті запропоновано використовувати алгоритм ДСТ 28147:2009, що є класичним алгоритмом симетричного шифрування на основі мережі Фейстеля (Рисунок 4). Даний алгоритм шифрує інформацію блоками по 64 біта (такі алгоритми називаються "блоковими"). Зміст мережі Фейстеля полягає в тому, що блок шифруемої інформації розбивається на два або більше субблоків, частина яких обробляється за певним законом, після чого результат цієї обробки накладається (операцією побітового додавання за модулем 2) на необроблювані субблоки. Потім субблоки міняються місцями, після чого обробляються знову й т.д. певне для кожного алгоритму число раз – раундів.

$L_i = R_{i-1}$

$R_i = L_i \oplus f\ (R_{i-1}, K_i)$

Функція F проста. Спочатку права половина й і-ий підключ складаються за модулем 2^{32}. Потім результат розбивається на вісім 4-бітових значень, кожне з яких подається на вхід S-box. ДЕРЖСТАНДАРТ 28147 використовує вісім різних S-boxes, кожний з яких має 4-бітовий вхід і 4-бітовий вихід.

Виходи всіх S-boxes поєднуються в 32-бітне слово, що потім циклічно зсувається на 11 бітів вліво. Нарешті, за допомогою XOR результат поєднується з лівою половиною, у результаті чого виходить нова права половина.

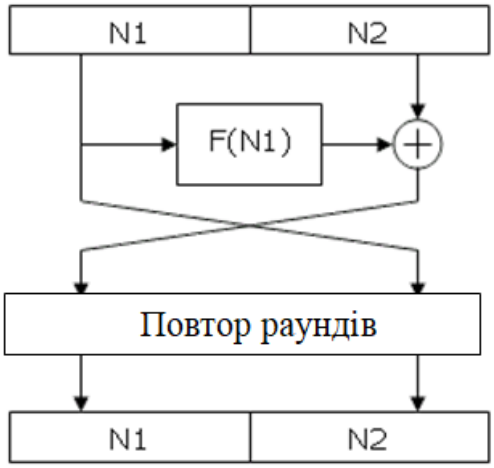

Рисунок 4 – Мережа Фейстеля

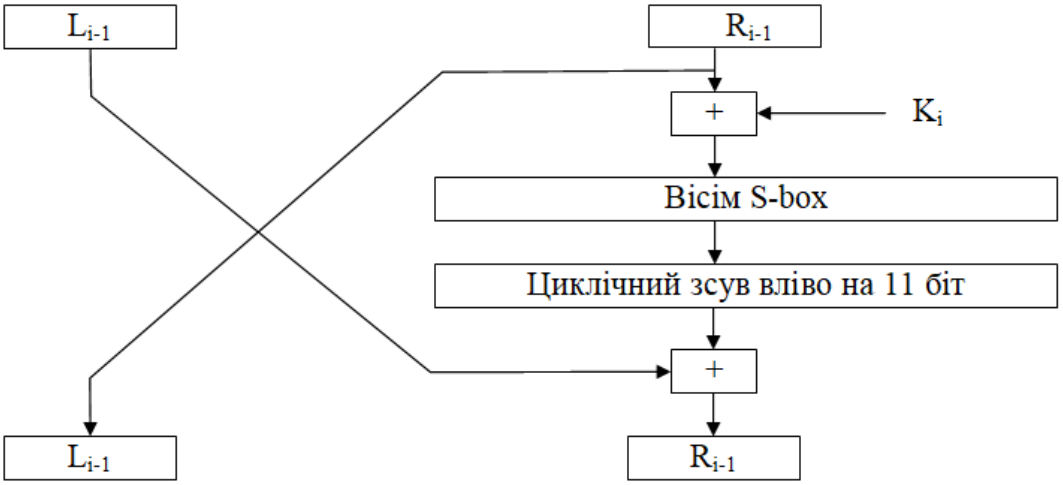

Рисунок 5 – і-ий раунд ГОСТ 28147:2009

Основна відмінність алгоритмів симетричного шифрування друг від друга складається саме в різних функціях обробки субблоків.

Дана функція часто називається "основним криптографічним перетворенням", оскільки саме вона несе основне навантаження при шифруванні інформації.

Основне перетворення алгоритму ДСТ 28147:2009 є досить простим, що забезпечує високу швидкодію алгоритму; у ньому виконуються наступні операції (Рисунок 6).

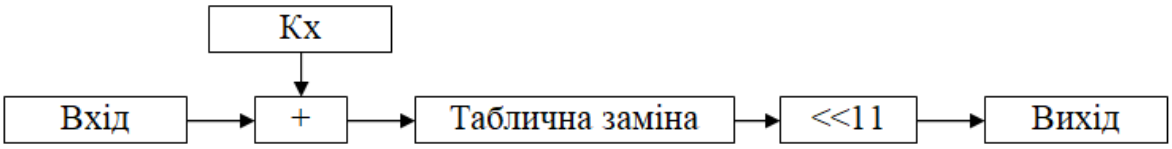

Рисунок 6 – Основне перетворення алгоритму ДСТ 28147:2009

1. Додавання субблоку з певним фрагменом ключа шифрування за модулем 2^{32}. Кх – це 32-бітна частина ("підключ") 256-бітного ключа шифрування, якому можна представити як конкатенацію 8 підключей: $К = К_0К_1К_2К_3К_4К_5К_6К_7$. Залежно від номера раунду й режиму роботи алгоритму (про їх – нижче), для даної операції вибирається один з підключей.

2. Таблична заміна. Для її виконання субблок розбивається на 8 4-бітних фрагментів, кожний з яких прогоняється через свою таблицю заміни. Таблиця заміни містить у певній послідовності значення від 0 до 15 (тобто всі варіанти значень 4-бітні фрагменти даних); на вхід таблиці подається блок даних, числове подання якого визначає номер вихідного значення. Наприклад, подається значення 5 на вхід наступної таблиці: "13 0 11 74 91 10 143 5 122 15 8 6". У результаті на виході виходить значення 9 (оскільки 0 заміняється на 13, 1 – на 0, 2 – на 11 і т.д.).

3. Побітове циклічне зрушення даних усередині субблока на 11 біт уліво.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів даних карти тахографа. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем даних карти тахографа. Досліджена система даних карти тахографа. На основі отриманих результатів досліджень створена програмна реалізація системи даних карти тахографа. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання даних карти тахографа. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kovalenko Oleksandr Qualitative risk analysis of software development / Oleksandr Kovalenko, Jamil Al-Azzeh, Oleksii Smirnov, Anna Kovalenko, Serhii Smirnov // Asian Journal of Information Technology. – Volume 17 Issue 3. – Medwell Journals. – 2018. – P. 218-230. ISSN: 1682-3915. URL: http://medwelljournals.com/abstract/?doi=ajit.2018.218.230 Doi: ajit.2018.218.230

2. Kovalenko Oleksandr, The mathematical model of the testing technology for DOM XSS vulnerabilities / O. Kovalenko, O. Smirnov, A.Kovalenko, S. Smirnov, V. Vialkova // Scientific & practical cyber security journal (SPCSJ) Volume 2 Issue 1, P. 22-28. Georgia. Tbilisi. Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667.

3. Kovalenko O.V. Method of testing the dom xss vulnerability / Kovalenko Oleksandr, Kovalenko Anna, Smirnov Oleksii, Smirnov Serhii // International Conference «information technologies, systems and networks ITSN-2017». Chisinau, Republic of Moldova. 17 – 18 October 2017. – Chisinau: Academy of Sciences of Moldova, Military Academy of Armed Forces "Alexandru cel Bun". – 2017. – P. 7.

4. Коваленко О.В. Метод тестування DOM XSS уразливості / О.В. Коваленко, О.А. Смірнов, А.С. Коваленко, С.А. Смірнов // Збірник тез всеукраїнської науково-практичної інтернет-конференції «Автоматика та комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті». м. Кропивницький. 16-17 листопада 2017 р. – Кропивницький: ЦНТУ. – 2017. – С. 198-199.

5. Коваленко О.В. GERT-модель технології тестування DOM XSS уразливості / О.В. Коваленко, А.С. Коваленко, О.А. Смірнов, С.А. Смірнов // Збірник наукових праць IV міжнародної науково-практичної

конференції «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації». м. Київ. 21-24 лютого 2018 р. – Київ: Європейський університет. – 2018. – С. 65-70.
6. Коваленко О.В. Технології тестування уразливостей Web-застосунків з використанням GERT-моделі / О.В. Коваленко, А.С. Коваленко, О.А. Смірнов, С.А. Смірнов // Збірник тез всеукраїнської науково-практичної конференції "Комп'ютерні інтелектуальні системи та мережі (КІСМ-2018)". м. Кривий Ріг. 21-23 березня 2018 р. – Кривий Ріг.: ДВНЗ КНУ – 2018. – С. 227-230.
7. Коваленко А.В. Тестирование уязвимости Web-приложений к атаке вида межсайтовый скриптинг / А.В. Коваленко, А.С. Коваленко, А.А. Смирнов, С.А. Смирнов // Збірник тез «Securitea informationala 2018». Conferenta internationala (editia a XIV-a). Chisinau. Moldova. 20-21 martie 2018. – Chisinau: ADSEM. – 2018. – P. 54-56.
8. Коваленко А.В. Комплекс математических моделей технологии тестирования web-приложений / А.В. Коваленко, А.С. Коваленко, А.А. Смирнов, С.А. Смирнов // Збірник тез X міжнародної науково-практичної конференції “Проблеми і перспективи розвитку ІТ-індустрії”. м. Харків. 19-20 квітня 2018 р. – Харків: ХНЕУ. – 2018. – С. 38.
9. Smirnov O.A., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346. (Scopus).
10. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131. (Scopus).
11. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14. (Scopus).
12. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84. (Scopus).
13. Smirnov O., Kuznetsov A., Pushkar’ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587. (Scopus).
14. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136. (Scopus).
15. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379. (Scopus).
16. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43. (Scopus).
17. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645. (Scopus).
18. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660., (Scopus).
19. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407. (Scopus).
20. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019. (Scopus).