

2. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. Вип. 1. С. 312-320. URL: http://nbuv.gov.ua/UJRN/boz_2012_1_37 (дата звернення: 31.10.2018).

Одержано 31.10.2018

УДК 004.056.53:004.89

Олег Вікторович ЗОЛОТУХІН,

кандидат технічних наук, доцент

доцент кафедри штучного інтелекту

Харківського національного університету радіоелектроніки;

ORCID: <https://orcid.org/0000-0002-0152-7600>;

Олексій Феліксович ЛАНОВИЙ,

кандидат технічних наук, доцент

доцент кафедри програмної інженерії

Харківського національного університету радіоелектроніки;

ORCID: <https://orcid.org/0000-0002-4504-4301>

ІДЕНТИФІКАЦІЯ БЕЗКОНТАКТНИХ ПЛАТЕЖІВ В СИСТЕМАХ КІБЕРБЕЗПЕКИ

В даний час інтернет-комерція стала невід'ємною частиною бізнесу в сфері інформаційних технологій. При цьому важливу роль в системах інтернет-комерції грають системи електронних платежів.

Як технології для безконтактних платежів розглядається технологія NFC (Near Field Communication), яка реалізується у вигляді чіпа (адаптера), вбудованого в мобільний телефон.

Технологія NFC об'єднує інтерфейс смарт-картки зчитувача в єдиний пристрій. Це дозволяє охопити в стандарті більш широкий спектр завдань і стандартизувати набагато більший набір пристроїв. На даний момент NFC технологія активно використовується перш за все у величезній кількості цифрових мобільних пристроїв, таких як мобільні телефони, в які NFC чіпи вбудовуються за замовчуванням, а також використовується в громадському транспорті і різноманітних платіжних системах (наприклад, системи АЗС).

Безконтактні технології платежів засновані на стандарті радіозв'язку ближнього радіусу дії NFC, активно впроваджуються зараз в різноманітні мобільні пристрої – смартфони, планшети, ноутбуки.

Технології безконтактних платежів дозволяють проходження операцій на малі суми тільки прикладанням карти до магнітного зчитувача – без введення ПІН-коду. При цьому карта не передається в руки касирів. Крім того, передбачена можливість «вбудовування» пристроїв (чіпів) в будь-які форми (мобільний телефон, годинник,

брелоки), можливість суміщення безконтактної карти з іншими пристроями (пропуски, проїзні, студентські квитки тощо).

Основними методами ідентифікації, застосовуваними різними платіжними системами, є:

- ідентифікація по PIN паролю;
- ідентифікація клієнта довіреною особою з перевіркою документів клієнта;
- використання набору AES (Advanced Encryption Standard) і DES (Data Encryption Standard) ключів всередині призначеного для користувача пристрої;

- використання одноразових ключів;
- Fraud-контроль шахрайства.

В якості методів, пропонованих в якості удосконалення процедури ідентифікації, пропонується, крім основних і додаткових методів, використовувати методи ідентифікації за становищем і методи біометричної ідентифікації.

Пропонується використовувати наступні методи:

- ідентифікація по фотографії
- метод біометричної ідентифікації. Під час здійснення платежу з додатком необхідно надати фотокартку особи користувача. Цю фотографію аналізують нейронні мережі та набір алгоритмів для визначення параметрів особи. В результаті оцінки виходить ймовірність того, що людина, яка робить платіж, є власником карти. Для цього попередньо потрібно зробити кілька знімків особи власника картки під час реєстрації в платіжній системі.

Метод має обмеження:

а) не використовується перевірка властивостей, які можуть бути вкрадені під час перевірки, наприклад, PIN код може бути підглянутий;

б) недосконалість алгоритмів обробки і аналізу особи по фотографії. На даний момент для того, щоб точно визначити по фотографії, чи є людина власником карти, чи ні, необхідно провести складні і «важкі» обчислення, навантажуючи процесор мобільного пристрою, витрачаючи багато енергії акумулятора мобільного пристрою, а також тривалий час на якісну обробку;

в) особу просто «підробити». Зловмисник може поставити фотографію власника карти перед камерою мобільного пристрою в момент скоєння фінансової транзакції, і на поточному рівні розвитку мобільних пристроїв буде дуже складно або навіть неможливо визначити ідентифіковану особистість;

– ідентифікація по ході – метод біометричної ідентифікації. У фоновому режимі мобільний пристрій, з якого здійснюються платежі, відстежує дані з датчиків прискорення (акселерометрів). Ці дані зберігаються в одному великому масиві. Після з цього масиву за допомогою статистичних методів рядів Фур'є відбувається виділення патернів ходи власника карти. У момент скоєння фінансової транзакції

мобільний пристрій бере дані з акселерометрів за останні дві хвилини і звіряє їх з існуючими довіреними паттернами. На підставі цього виходить імовірна оцінка того, що останні дві хвилини телефон був у руках у свого власника, відповідно саме він і робить платіж.

Метод не вимагає ніяких дій від користувача. Для оплати необхідно лише піднести телефон до терміналу. У цьому методі не використовується перевірка властивостей, які можуть бути вкрадені під час перевірки. Наприклад, PIN код може бути підглянутий. Дані акселерометрів дуже складно підробити через відмінності в анатомії двох будь-яких людей. І навіть якщо вдасться підібрати потрібні параметри, то це буде дуже складно для крадіжки одного телефону, і майже неможливо для систематичних крадіжок. Не дає хибно позитивних результатів.

Метод має недоліки. Через постійне відстежування даних акселерометра відбувається постійний розряд батареї пристрою, що негативно позначається на тривалість періоду, після і стан батареї.

Незважаючи на те, що метод не дає помилково позитивних результатів, метод дуже часто дає помилково негативні результати, через що його дуже складно застосовувати як основний метод ідентифікації. Як правило, його застосовують у сукупності з іншими методами. Наприклад, з перевіркою PIN коду застосовують тоді, коли оцінка ходи вказує, що платіж виконує не власник карти;

– ідентифікація за даними про пересування – метод ідентифікації за становищем (геолокація). У фоновому режимі мобільний пристрій, з якого здійснюються платежі, відстежує дані про переміщення власника пристрою за допомогою отримання даних з датчиків системи глобального позиціонування GPS (Global Positioning System), а також отримання ідентифікаторів всіх найближчих Wi-Fi точок. Ці дані зберігаються в одному великому масиві. Після цього за допомогою різних методів, наприклад, методів машинного навчання або простого статистичного аналізу, визначаються патерни переміщення людини в залежності від часу доби і дня тижня. На підставі цих даних можна визначити ймовірність того, що власник карти буде здійснювати фінансову транзакцію в даному місці, в даний час доби, на дану суму. На підставі цього можна оцінити в момент скоєння користувачем фінансової транзакції, ймовірність того, що людина, яка виконує платіж є власником мобільного пристрою.

На основі дослідження існуючих систем безконтактних електронних платежів: Google Pay, Apple Pay, Samsung Pay, MasterCard Contactless визначені характеристики, переваги та критичні недоліки систем у вигляді рекомендацій вибору конкретного рішення.

Висновок. Згідно з дослідженнями європейських компаній, на сьогоднішній день на частку безконтактних технологій припадає близько 10% всіх здійснюваних транзакцій.

Основним фактором зростання для інвестицій компаній в безконтактні технології є збільшення швидкості обробки платежів

(74%), можливість знайти імідж новатора (43%), підвищення ефективності витрат (42%). Для споживачів найбільш важливим фактором є підвищення зручності (47%), більш високий ступінь задоволеності (43%) і спрощення процесів оплати (43%).

Однак впровадження безконтактних технологій не є простим завданням, і щоб скористатися перевагами нової технології компаніям належить подолати ряд труднощів. Європейські компанії, які вже підтримують безконтактні технології, в числі основних труднощів при їх впровадженні називають високу вартість установки платіжних терміналів і загрозу безпеці – ці питання актуальні для 46% респондентів. Потім вони відзначають високу вартість обслуговування нових терміналів (44%), труднощі з формуванням довіри у клієнтів до різних методів оплати (35%), питання відповідальності в разі шахрайських транзакцій (26%), відсутність або недостатність інфраструктури (20%), складності, пов'язані інтеграцією нових платіжних технологій в уже наявні технології (20%), труднощі з пошуком надійного партнера, з яким доведеться працювати (11%).

Очевидно, що безконтактні технології надовго закріпилися в нашому житті і будуть активно розвиватися і застосовуватися у всіх аспектах нашого життя. Дослідження показує, наскільки важливу роль безконтактні платежі відіграють у житті європейських компаній - незалежно від їх форми або розмірів, і наскільки високі очікування покладають компанії на ці технології в найближчі кілька років.

У найближчому майбутньому безконтактні платіжні картки, як одна з найбільш сталих форм безконтактних рішень, продовжить домінувати на ринку, при цьому платежі з застосуванням мобільних технологій і носяться пристроїв будуть стрімко нарощувати свою частку.

Виявлення та протидія шахрайським операціям—одна з ключових завдань всіх міжнародних платіжних систем. Безпека онлайн-платіжних транзакцій відстежується безліччю систем на різних рівнях і етапах проходження платежу.

На сьогоднішній день з використанням безконтактної технології платіжні технології мають безліч переваг, серед яких інноваційність, оперативність здійснення платежів, простота, зручність, швидкість проведення операцій, значна економія часу, зниження черг і, в результаті використання модифікації методу ідентифікації платежів, більш високий рівень безпеки проведення операцій, зниження злочинності.

Запропонована в роботі система безконтактних електронних платежів дозволяє підвищити ефективність роботи більшості сучасних телефонів і планшетів, оснащених NFC адаптерами, з можливістю швидкого обміну контентом і безконтактної оплати послуг.

Актуальність завдання обумовлена гнучкістю використання даної технології, сумісністю з різними пристроями, спрощення процесів

оплати, що сприяють підвищенню привабливості впровадження даної технології банками.

Для поліпшення ідентифікації безпеки пропонується також використовувати метод автентифікації в роботі автомобільного іммобілайзера як RFID (Radio Frequency IDentification) – мітки, яка є невід'ємною частиною ключа сучасного автомобіля. Це мікросхема, яка містить пам'ять з секретним кодом, мініатюрний передавач і приймач радіосигналу. Енергії електромагнітних хвиль вистачає, щоб мікросхема відправила у відповідь секретний код. Отримавши правильну відповідь, іммобілайзер дозволяє блоку управління двигуном включитися. У найближчому майбутньому автомобільний ключ може взяти на себе куди більше функцій, ніж просте відкривання дверей і захист від викрадення. Еволюція буде пов'язана з поширенням технології передачі даних на короткі відстані NFC. Пристрої, сумісні з NFC, такі як автомобільний ключ, мобільні телефони, комп'ютери, банкомати, можуть обмінюватися даними, тільки перебуваючи на відстані щонайменше 10 см.

Список бібліографічних посилань

1. MasterCard Cloud-Based Payments Product Description, MasterCard Digital Enablemet Service, 2015.

2. Kulkarni M., Im D. J., Saputra S. J. SamsungPay Payment Method // Maheshkk.github.io. 15 September 2016. URL: <https://maheshkk.github.io/webpayments/proposals/SamsungPay-payment-method.html> [Accessed: 18 Jul 2018].

3. MasterCard Cloud-Based Payments Credential Managment System Functional Description, MasterCard Digital Enablemet Service, 2015.

Одержано 01.11.2018

УДК 621.34

Василь Миколайович КЛОЧКО,

студент 2 курсу факультету № 6

Харківського національного університету внутрішніх справ

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ РУХОМОГО ЗВ'ЯЗКУ

На сучасному етапі розвитку людство майже не уявляє свого існування без звичного мобільного зв'язку, тому питання дослідження та вдосконалення моделей захисту інформації в мережах рухомого зв'язку постає дедалі частіше. В основі забезпечення захисту інформації в мережах рухомого зв'язку лежать законодавчі та нормативно-правові норми, морально-етичні звичаї суспільства, організаційні та апаратно-програмні засоби та способи функціонального забезпечення інформаційної безпеки цифрових систем, каналів, мереж зв'язку.