

БЕЗПЕКА БЕЗКОНТАКТНОЇ ОПЛАТИ

Жданкін А. В.

Національний аерокосмічний університет ім. М. Е. Жуковського
«ХАІ»

Науковий керівник Землянко Г. А.

Актуальність. За останні п'ять років в Україні, як і у всьому світі, широке поширення набула технологія безконтактної оплати, що закономірно: вона спрощує процес оплати, дозволяючи використовувати для цих цілей пристрої, що носяться, такі як смарт-годинник або смартфон замість традиційної оплати пластиковою картою. При цьому з'являється питанням: наскільки безпечно її використання.

Метою даної роботи є аналіз безпеки безконтактної форми оплати та її види і особливості.

Основні положення. Банківські картки є сьогодні поширеним платіжним засобом: переважна більшість українців (82 %) – власники банківських карток, причому за останні 11 років їхня частка зросла з 31 % до 82 %. Українці вважають технологію безконтактної оплати зручною. Ті, хто знайомий з цією технологією, частіше відзначали зручність платежів за допомогою банківської картки (80%) та смартфона (70%). Більшість людей впевнені, що оплату товарів та послуг зручно здійснювати за допомогою смарт-годинників (63%), браслетів (60%) та брелків (56%) [1].

Провівши аналіз було зрозуміло, що, наприклад, з банківською картою, що володіє тільки контактним способом оплати - зазвичай магнітна смуга та/або мікропроцесор, пластикова карта, що підтримує можливість безконтактного платежу більш вразлива [2]. Розглянувши це питання, було вирішено, що більшість переживань простих користувачів пов'язані з можливістю без підтвердження ПІН-кодом проводити так звані мікро-транзакції. Передбачається, що зловмисник, який використовує POS термінал для оплати, може зробити незаконне списання коштів з банківського рахунку без відома власника, наприклад, у громадському транспорті притулити термінал із запитом на списання до сумки чи кишені. Такий варіант розвитку подій, безумовно, можливий, проте на практиці складно реалізуємо через такі обставини: Для здійснення цієї операції необхідна невелика відстань

між платіжним терміналом та картою – менше 10 см [3]. Завдання значно ускладнюються, якщо в одному місці розташовано кілька карток з можливістю безконтактної оплати, у разі виявлення кількох карток у полі дії деякі види терміналів не здатні зробити списання коштів. Важливо розуміти, що термінал не можна так просто взяти – він має бути зареєстрований, підключений, мати доступ до Інтернету, на нього має бути відкритий рахунок, а організація, на яку відкрито рахунок, має пройти перевірку служби безпеки банку. Зловмисник може користуватися POS терміналом юридичної особи, оформленої на підставні особи, але все це, на чорному ринку, значно перевищить потенційні вигоди від цього виду шахрайства, що робить його недоцільним. Навіть у разі успішного списання коштів у законних власників їх зарахування на рахунок зловмисника відбудеться не відразу, а через кілька днів. При цьому ймовірність того, що ніхто з жертв не помітить зникнення і не звернеться до свого банку-емітенту карти, а той, у свою чергу, до банку-еквайєра з метою встановлення підозрілих операцій за рахунком, який буде після заблоковано, вкрай низька.

Висновки. Використання пристрою з одним із перелічених вище сервісів безпечніше, ніж користування звичайною картою, що підтримує безконтактні платежі. Для виключення ймовірності несанкціонованого читання безконтактних карток можна застосувати екранування, обернувши картки фольгою або використовувати гаманець із RFID захистом.

Список літератури

1. Безконтактні платежі: повернення до готівки не буде. *Нафи*. URL: <https://bit.ly/3p44ur0> (дата звернення: 14.11.2021);
2. Ідентифікаційні картки. Картки на інтегральних схемах безконтактні. Картки близької дії. Частина 1. Фізичні характеристики. *Електронний фонд ПНТД*. URL: <http://docs.cntd.ru/document/1200108020> (дата звернення: 15.11.2021);
3. Як вкрати гроші з безконтактної картки та Apple Pay. *Хабр*. URL: <https://habr.com/ru/post/422551/> (дата звернення: 16.11.2021).

Відомості про авторів

Жданкін Артем Вікторович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 066-248-54-55, a.zhdankin@student.csn.khai.edu

Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu