

ПРОТИДІЯ СУЧАСНИМ ЗАСОБАМ ПЕРЕХОПЛЕННЯ ІНФОРМАЦІЇ З БАНКІВСЬКИХ АВТОМАТІВ

М. С. Хрущов¹, В. М. Степаненко¹

¹ Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Фізико-технічний інститут

Анотація

В даній статті було розглянуто основні загрози зняття інформації з банківського автомату, проаналізоване сучасне покоління скімерів на базі нових мікросхем, у тому числі, з технологією Bluetooth/GSM та надані рекомендації щодо виявлення каналів витіку інформації та мінімізації ризиків перехоплення даних.

Ключові слова: скімер, банкомат, кардинг.

Вступ

Кредитні та дебетові картки стрімко витісняють готівку у сучасній платіжній сфері (рис. 1).

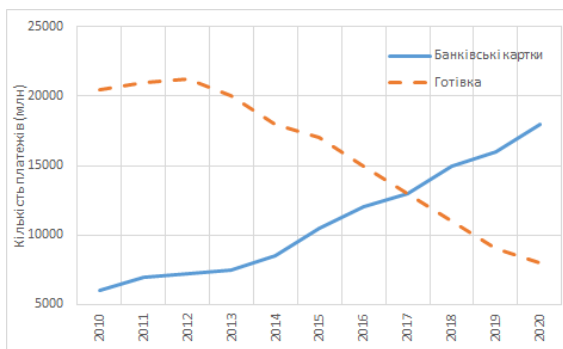


Рис. 1. Графік кількості платежів у період 2010-2020

Найбільший їх недолік – це можливість отримання даних у злочинних цілях. Дані з магнітної стрічки або з чіпу картки отримують за допомогою скімерів – пристроїв, які таємно встановлені у банкомати, або термінали, призначених для незаконної фіксації даних з картки. Після викрадення інформації зловмисники вдаються до кардингу – виду шахрайства, при якому проводиться операція з використанням платіжних карток, що не ініційована або не підтверджена її власником. В інших випадках зловмисники можуть продавати викрадені з карток дані чи підроблювати їх для подальшого зняття коштів. Усі дані, що містяться на доріжках картки, написані як простий текст і шахрай із доступом до магнітної смуги (наприклад, зі скімером) може створити повну копію. Ці клоновані картки містять ті самі ж дані що й оригінали.

1. Огляд існуючих скімерів

Покоління скімерів, які потребували приховану відеокамеру чи накладну клавіатуру, для того щоб

дізнатися PIN-код, на даний час втрачають актуальність (рис 2). Їх заміняє нове покоління скімерів на основі технологічніших мікросхем, більш ємнісних акумуляторів та безконтактним способом передачі викрадених даних. Нові типи пристроїв не потребують використання камер та клавіатур, замість цього викрадення PIN-коду відбувається іншими методами.

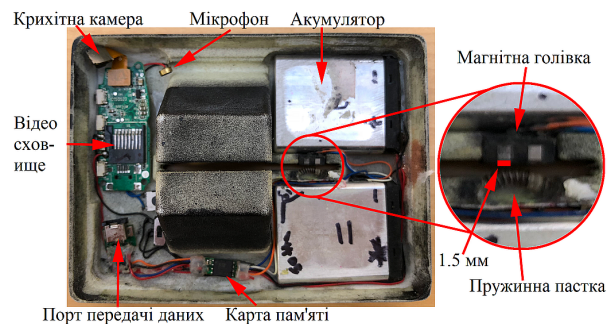


Рис. 2. Накладний скімер всередині

Крім накладних скімерів, що розміщуються на гнізді магнітної смуги, можливі й інші місця їх встановлення. Скімери, що вміщуються у проріз для магнітної смуги (рис. 3), є покращеною та більш прихованою версією накладних скімерів. Також існують скімери, що під'єднані до фізичної лінії зв'язку, під'єднавшись до якої можливо зчитувати дані (прослуховування) і такі, що вміщуються у гніздо та зчитують інформацію з чіпу картки (EMV шимери) (рис 4). EMV (Europay + MasterCard + VISA) – це міжнародний стандарт карток із чіпом.



Рис. 3. Скімер, встановлюється у проріз

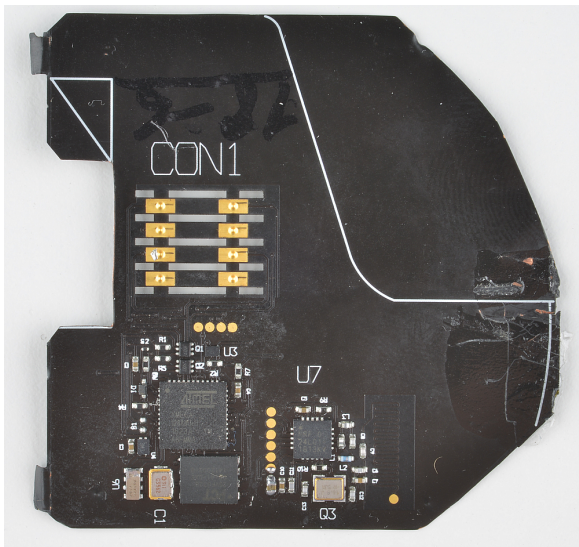


Рис. 4. EMV шимер



Рис. 5. Накладка на POS термінал

Та найнебезпечніший зі скімерів – це скімер із внутрішнім доступом. Такі пристрої перехоплюють інформацію, що передається між зчитувачем карток та іншими компонентами. В результаті цей пристрій отримує як дані картки, так і PIN-код. Також існують різноманітні накладки на лицеву панель POS-терміналів, які неможливо відрізнити від оригіналу (рис. 5).

На рисунку 6 представлена схема банкомату з розміщенням кожного типу скімера.

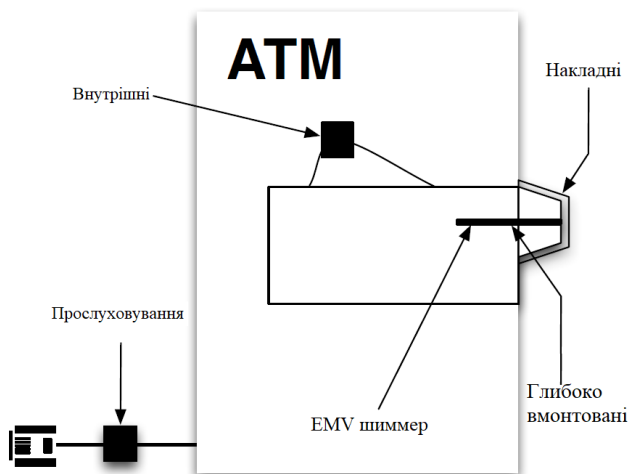


Рис. 6. Місця встановлення скімерів

2. Зняття інформації зі скімера

Усі скімери, що потребують внутрішнього доступу, живляться від банкомату та містять апаратне забезпечення для бездротової передачі даних: Bluetooth або GSM. Більшість інших скімерів потребують фізичного доступу для подальшого зняття інформації та підживлення акумуляторів. В міських умовах дальність стабільної роботи Bluetooth складає до 5 метрів. У випадку GSM – дальність прийому з чутливою антеною не перевищує 20 метрів. За допомогою спе-

ціалізованих приладів або смартфон-додатків можна дізнатися про можливий скімер із Bluetooth модулем неподалік. Великий недолік таких додатків є те, що вони сигналізують про небезпеку, виявивши деякі типи відомих Bluetooth-чипів, що розповсюджені у побутових приладах: Bluetooth-динаміки, фітнестрекери, смарт-кросівки та інші. При близькості цих пристроїв відбувається хибне попередження про наявність скімерів, що є неподалік.

Висновки

Скімери нового покоління використовують новітні технології, стають стійкішими до виявлення та розповсюдились на інші пристрої безготівкової оплати. Виходячи з цього можна дати такі поради:

- Використовувати банкомати всередині банківських відділень.
- Використовувати банківські карти з вбудованим мікročіпом або смартфон із NFC, якщо це можливо.
- Використовувати додатки для пошуку скімерів через Bluetooth.
- Бути пильним і уважним при користуванні банкоматом або POS-терміналом, звертати увагу на нестандартні елементи конструкції.

Перелік використаних джерел

1. Krebs B. Krebs on Security – 2017. — URL:: <https://krebsonsecurity.com/all-about-skimmers/>
2. Credit Card Skimmers Evolved: Shimming – 2018. — URL:: <https://www.sparkfun.com/news/2673>
3. Изотов Д. С., Быкова Н. Н. Виды мошенничества с банковскими картами. — Вестник НГИЭИ. — 2015. — № 3. — С. 49-52 —
4. Ивлеева Г. И., Тишина В. Н. Анализ рынка банковских карт России. — Молодой ученый. — 2013. — С. 309 с. —