УДК 004.382.001.25.343.3/7

Максим Анатолійович Ведмідь,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Аналіз методів захисту інтернет- і мобільного банкінгу

Українці все частіше використовують безготівковий метод оплати, про що свідчить статистика Національного банку України. Так, за останні 9 місяців 2019 року частка безготівкових розрахунків в загальному обсязі операцій з використанням платіжних карток, емітованих українськими банками, зросла з 5% – до 44,3% [1].

За 2019 рік кількість операцій з використанням платіжних карток склала 2,8 млрд грн, а їх обсяг – 2 трлн грн. Ці показники, якщо порівнювати з минулим роком, зросли на 27,2% і 38,5% відповідно.

Кількість безготівкових операцій склало більше 2,2 млрд шт., З яких 1,1 млрд операцій (51,7%) припадало на розрахунки в торговельних мережах [1].

На сучасному етапі розвитку України є дуже велика кількість варіантів безготівкового розрахунку: смартфон, платіжна система, блокчейн систем. Більшість з вище перерахованих платіжних систем для оплати використовують банківські карти, та мають власні методи захисту платіжних даних.

Головна перевага для клієнтів, котрі використовують банківські картки це їх зручність. Головним недоліком стає велика кількість протиправних дій по відношенню до тримачів карт, карти постійно стають мішенню для зловмисників. За даними Асоціації членів платіжних систем ЕМА, в 2018 році шахраї вкрали в українців 669,6 млн гривень, з яких близько 160 млн гривень було викрадено за допомогою банкоматів. Більш 509 млн гривень шахраї отримали використовуючи соціальну інженерію. У кіберполіції відзначають, що в 2018 році в порівнянні з 2017 роком на 70% зросла кількість заяв про крадіжки з банківських карт. Всього у 2017 році було зареєстровано 3820 звернень [3].

Жодна фінансова установа не має в своєму розпорядженні універсального способу або технічного пристосування, здатного забезпечити 100-відсотковий захист карт від зазіхань зловмисників. Більшість банків фінансово не спроможні організувати власні процесингові центри, які зможуть підтримувати достатній рівень безпеки. В зв'язку з цим банки використовують сторонні процесінгові центри, в наслідок чого операції з платіжними картками більш захищені та правоохоронним органам легше викрити шахрайські операції.

Найбільш поширені фінансові злочини з банківськими картами умовно можна розділити на дві категорії. Перша – це крадіжка даних банківської карти за допомогою стороннього технічного забезпечення. Друга – це використання зловмисниками соціальної інженерії для отримання обманним шляхом даних банківських карт та інших даних, котрі допоможуть в скоєнні противоправних дій.

Методи шахрайства, котрі можна віднести до першої категорії.

1. Крадіжка даних банківської карти при здійсненні операцій в банкоматі шляхом установки зчитувальних пристроїв (скіммінг, шиммінг).

2. Отримання доступу до картрахунку шляхом фішингу, вивідування даних обманним шляхом.

3. Використання спеціальних пристосувань для блокування пластикової карти в банкоматах (траппінг).

Методи шахрайства, котрі можна віднести до другої категорії.

1. Зловмисники телефонують власнику карти представляючись працівниками банку. Дзвінок може бути здійснений як з звичайного незарезервованого банком номеру так і з банківського. Шахраї застосовують методи підміни номера за допомогою SIP/VOIP телефонії. Зловмисники зазвичай повідомляють клієнта про блокування його карти, або про «Підозрілу транзакцію». Іноді, коли зловмисник співробітник банку, він має доступ до приватних даних клієнтів, а саме:кількість грошей на рахунку, номери телефонів, що прив'язані до рахунку та інше. У наслідок чого зловмисники вимагають повідомити їм дані банківської карти, чи даних онлайн кабінету для ідентифікації користувача та урегулювання проблеми.

2. За допомогою підміни номеру зловмисники здійснюють дзвінки безпосередньо з різних фінансових організацій. Крім того, попутно вам навіть можуть приходити «підтверджуючі» легітимність співрозмов-

ника СМС. Ввічливий співробітник повідомляє, що з вашої карти були списані кошти і система безпеки банку маркувала його «підозрілим». Раптово з'ясовується, що на скасування переведення у вас є всього 10 хвилин і для скасування потрібно назвати код, який вам прийде за допомогою СМС. Звичайно, цей код – для проведення транзакції, тільки він зловмисникам і потрібен.

3. Також є повністю автоматизований спосіб здійснення противоправних дій по відношенню до клієнтів банку. Клієнт завантажує різні додатки з непідтверджених джерел, в наслідок чого заражає свій смартфон вірусом. Вірус в свою чергу виконує крадіжку платіжних даних та організовує переадресацію СМС та дзвінків з пристрою жертви на пристрій зловмисника. Такі дії вірусу дають змогу зловмисникам використовувати платіжні інструменти без відома власника рахунків.

Щоб мінімізувати ризики попадання фінансових даних до рук шахраїв та в перспективі викрадення даних з картки, розглянемо способи захисту цієї інформації:

1. Використання технології SMS-інформування власників. При використанні цього методу клієнт має можливість відстежувати всі операції з його банківською карткою і відмовити у вчиненні несанкціонованого трансакції. Недоліками SMS-інформування є те, що не всі клієнти усвідомлюють його ефективність і виявляють бажання на підключення даного сервісу, а у банку відсутні законні права підключити клієнта примусово.

2. Впровадження технології додаткової ідентифікації користувача системи дистанційного банківського обслуговування, використання надійних алгоритмів шифрування електронно-цифрового підпису для підтвердження фінансових операцій.

3. Застосування чіпових технологій VSDC в процесі випуску міжнародних банківських карт, найефективнішого способу захисту від скіммінгу (крадіжки персональних даних при обслуговуванні в банкоматі).

4. Управління емітентськими обмеженнями (автоматичну відмову в операції на стадії авторизаційного запиту) за операціями, проведеними в торгово-сервісній мережі та Інтернет-магазині, які відносяться банком до ризикових точках.

5. Використання спеціальних програмних систем Fraud-моніторингу, що дозволяють за допомогою критичних правил проводити аналіз і

виявляти шахрайські операції в процесі обігу банківських карт з більшою ймовірністю [4].

Запропоновані методи не можуть гарантувати стовідсоткової безпеки платіжних даних, але можуть значно знизити ризик противоправних дій по відношенню до клієнтів банку. Також подібні заходи дають змогу правоохоронним органам отримати більш повний обсяг інформації про зловмисників.

Список бібліографічних посилань

1. Украинцы стали чаще использовать безналичный расчет // delo.ua : сайт. URL: https://delo.ua/econonomyandpoliticsinukraine/za-9-mesjacev-ukraincy-rasschitalis-po-beznalu-n-348030 (дата звернення: 24.10.2019).
2. Мошенничество с банковскими картами, что такое кардинг, скимминг и шимминг // Fingramota.org : сайт. 11.06.2013. URL: http://www.fingramota.org/bezopasnost/v-bankakh-i-s-kred-kartami/item/88-moshennichestvo-s-bankovskimi-kartami-chto-takoe-karding-skimming-i-shimming (дата звернення: 24.10.2019).
3. Как с вашей карты могут украсть деньги: пять актуальных схем // Лига.Финансы : сайт. 01.02.2019. URL: https://finance.liga.net/personal/article/kak-s-vashey-karty-mogut-ukrast-dengi-pyat-aktualnyh-shem (дата звернення: 24.10.2019).

Одержано 25.10.2019