УДК 336.71

ПІДТРИМКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОЦЕСИНГУ ПЛАТІЖНИХ КАРТ

О.В. НИКИТЧЕНКО,
доцент

Дніпропетровський державний аграрно-економічний університет, Україна
E-mail: nickavic@i.ua

Розглянуто роль банківських установ у забезпеченні динамічного розвитку економіки, впровадженні сучасних банківських технологій та інструментів. Визначено проблеми надійного та ефективного процесингу платіжних карт, інформаційної та фінансової безпеки, протидії випадкам фроду, кардингу, скімингу тощо. Запропоновано методи і програмні засоби для оперативного визначення точок компрометації та скомпрометованих платіжних карт з метою запобігання випадкам шахрайства у сфері банківського обслуговування та організації боротьби з його проявами.

Ключові слова: *платіжна карта, мікропроцесорна карта, еквайринг, трансакція, фрод, кардинг, Excel, код CVV, точка компрометації, скомпрометована карта.*

Постановка проблеми. Провідну роль у динамічному розвитку аграрно-промислового комплексу України відіграє фінансове забезпечення та банківське обслуговування суб'єктів АПК системними фінансовими установами. Вплив банківської системи на економіку невпинно зростає. Діяльність банківських установ не обмежується акумуляцією і розміщенням зростаючої маси грошових коштів компаній, підприємств і населення. Банки сприяють накопиченню капіталу, не лише активно втручаючись в усі сторони господарського життя, але й безпосередньо беручи участь у діяльності функціонуючого капіталу або здійснюючи контроль над ним. Останнім часом спостерігається щорічне збільшення суми банківських портфелів з кредитування сільгоспвиробників, так як з'явилося багато комерційних аграрних підприємств, зростає інвестування останніх з боку власників і пайовиків.

Важливим сегментом банківського обслуговування клієнтів є робота процесингових центрів фінансових установ, які сертифіковані міжнародними платіжними системами на випуск і підтримку великої кількості фінансових продуктів, у тому числі платіжних карт. За швидкого ритму життя та сучасних технологій платіжна карта є не лише засобом для отримання заробітної плати, пенсії або інших зарахувань, але й надійним та зручним інструментом для повноцінного банківського обслуговування. З метою підтримки високого рівня безпеки і побудови технологічного процесу процесингові центри щорічно перевіряються на відповідність правилам організації випуску та функціонування платіжних карт.

Банківська платіжна карта (payment card) стала засобом, прив'язаним до банківських рахунків, який може бути використаний власником карти для оплати товарів і послуг, у тому числі через інтернет. На ринку існують декілька типів платіжних карт: кредитна карта (credit card і charge card), дебетова карта (debit card, bank card, check card), картка банкомату (ATM card), карта передоплати або карта зі збереженою вартістю (stored-value card), паливна карта (fuel card або fleet card – пластикова карта для автоматизації

122

оплати заправки на АЗС), подарункова карта (gift card) тощо.

У банківському обслуговуванні серед головних, поміж іншого, стоїть питання вирішення задач безпеки процесингу банківських карт, протидія випадкам різного виду шахрайства на сайтах інтернет-магазинів, у банкоматах, точках оплати тощо. Ситуація не виходить з-під контролю, і ці задачі в цілому вирішуються. Поява мікропроцесорних карт стала центральною подією в індустрії пластикових карт останніх років. Це докорінно змінило ситуацію з картковим шахрайством. Проте присутність карт із магнітною смугою все ще велика, тому старі види шахрайства продовжують існувати і розвиватися. Зокрема, набуває нових форм скімінг. Найбільша загроза виходить від так званого банкоматного скімінгу, коли для запису даних магнітної смуги карти, а також компрометації PIN-коду на банкоматі встановлюються накладний рідер і накладна клавіатура / відеокамера. Відомі випадки, коли для крадіжки карткових даних застосовувалося спеціальне шкідливе програмне забезпечення. Гостро постає питання виявлення випадків скімінгових атак з метою проведення своєчасних заходів, спрямованих на блокування платіжних карт, які були скомпрометовані в точках компрометації: банкоматах, підприємствах торгівлі та сервісу з виявленими скімінговими пристроями. У даній роботі розглядається вирішення задачі оперативного виявлення точок компрометації та скомпрометованих платіжних карт.

Аналіз матеріалів за темою. Функціонування платіжних систем в Україні регламентується Законом "Про платіжні системи та переказ коштів в Україні" (№ 2346-14 від 19.04.2014 р.). Згідно зі статею 1.19-2 даного Закону, "моніторинг – діяльність емітента/еквайра щодо контролю за операціями, які здійснюються із застосуванням електронних платіжних засобів, з метою виявлення та запобігання помилковим та неналежним переказам. За дорученням емітента/еквайра моніторинг за умови дотримання вимог щодо збереження конфіденційності інформації може проводити юридична особа, що надає емітенту/еквайру послуги з оброблення даних (послуги процесингу)" [1].

Аналіз статистичних даних моніторингу, результатів міжбанківського обміну інформацією і матеріалів, отриманих від платіжних систем MasterCard і Visa про шахрайство з платіжними картами, підтверджує збереження в Україні у 2013–2014 рр. [2, 3]:

– стабільно високого рівня банкоматного шахрайства (скімінгові атаки, у тому числі встановлення шахраями скімінгових пристроїв у зовнішні антискімінгові накладки на кардрідери, використання "білого пластику" для зняття готівкових коштів у банкоматах тощо);

– істотного скорочення часового інтервалу між копіюванням інформації з платіжної карти / викраденням реквізитів платіжної картки та проведенням шахрайських операцій з використанням підробки викрадених реквізитів платіжної картки;

– туризму міжнародних злочинних угруповань для зняття інформації в українській банкоматній мережі та використання в магазинах і банкоматах підроблених карт іноземних банків-емітентів.

У випадках шахрайських атак, здійснених відносно банкоматів, терміналів тощо, фахівці банківського сегменту мають задачу оперативного виявлення точок компрометації та скомпрометованих платіжних карт.

Мета дослідження – розробити технологію та програмне забезпечення для виявлення скомпрометованих платіжних карт. Платіжні системи використовують термін, який визначає точки компрометації як CPP – Common Point of Purchase. Отримана інформація вводиться у так звану базу даних CPP у форматі .xls. Знаючи точку і час компрометації, першорядним стає питання виявлення наявності транзакцій за картками банку в даній CPP з метою запобігання використанню прочитаної інформації з карти шахраєм і, як наслідок, здійсненню шахрайських операцій.

Водночас існують зворотні ситуації, коли шахрайські операції по карті (картках) вже здійснені (транзакції не підтверджуються клієнтом) і необхідно виявити точку компрометації (CPP).

Обговорення матеріалів досліджень. Для вирішення поставленої задачі достатньо мати такі вихідні дані по транзакціях:

• дата здійснення транзакції;

• TID – TerminalID, код терміналу (банкомат, торговельний ПОС- термінал), що присвоюється при реєстрації в платіжній системі;

• MID – MerchantID, код торгової точки (банк, магазин, пункт сервісного обслуговування), що присвоюється при реєстрації;

• AID – AcquirerID, код банку – еквайр-банку, що обслуговує дану торговельну точку / банкомат.

Для пошуку можливої СРР формуються виписки за певний період по картках клієнтів, за якими пройшли шахрайські операції, у форматі .xls .

Порівнюючи дані за виписками клієнтів (усі транзакції, проведені до шахрайської операції по карті), можна знайти точку перетину, яка швидше за все і буде СРР. Подібний метод порівняння застосуємо і для пошуку перетинань даних з виписки клієнта з базою даних, відомих у результаті міжбанківського обміну інформацією по СРР. Простий метод вирішення поставленої задачі – порівняти дані двох відповідних Excel-таблиць. Задачу досить нескладно розв'язати в середовищі VBA.

Електронна таблиця містить дві Excel-таблиці, які мають бути порівнянні для пошуку перетину TID, MID, AID кодів. У наведеному прикладі ці таблиці отримані технологією імпорту з бази даних транзакцій. Інтерфейсна кнопка "Find", яка створена у надбудові Excel-VBA, викликає до виконання програмний код відповідного макросу. Після аналізу даних порівнюваних таблиць програма макросу повертає знайдені співпадіння шуканих TID, MID, AID кодів, ідентифікуючи таким чином скомпрометовані об'єкти.

Отже, для банків, фінансових установ і суб'єктів господарювання проблема безпеки є пріоритетною. Наведена інформаційна технологія дозволяє своєчасно виявляти випадки скімингових атак з метою проведення оперативних заходів, спрямованих на блокування скомпрометованих платіжних карт та недопущення матеріальних збитків, загроз і незручностей для клієнтів.

Розв'язана задача доводить, що інформаційні технології захисту від випадків шахрайства у банківській сфері можуть і мають бути розширені, у тому числі й засобами MS Excel-VBA.

Бібліографія

1. Закон України "Про платіжні системи та переказ коштів в Україні" № 2346-14, редакція від 19.04.2014. – [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2346-14

2. *Щербина В.М.* Інформаційне забезпечення економічної безпеки підприємств та установ / *В.М. Щербина* // Актуальні проблеми економіки. – 2006. – № 10. – С. 220–225.

3. Информационная безопасность банков. – [Електронний ресурс]. – Режим доступу: http://www.infowatch.ru/solutions/finance.

Рецензент – доктор економічних наук, професор ***І.І. Вініченко***