

УДК 681.322

Іщук Г. П., к.е.н.; Пелешенко А. В., студент

(Державний університет телекомунікацій. +380 (44) 249 25 22, +380 (63)679-42-93. temi4.root@gmail.com)

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ КАРТКОВИХ ПЛАТІЖНИХ СИСТЕМ ПРИ ПРОВЕДЕННІ ПЛАТІЖНИХ ОПЕРАЦІЙ

Іщук Г. П., Пелешенко А. В. Забезпечення безпеки даних карткових платіжних систем при проведенні платіжних операцій. У статті розглянуто типи платіжних карток із врахуванням технічних засобів забезпечення безпеки картки, забезпечення безпеки даних держателів платіжних карток та критичних автентифікаційних даних. Розглянуто нормативно-правове забезпечення безпеки платіжних систем та операцій в них. Проаналізовані новітні загрози щодо компрометації платіжних карток, а також рівні і способи захисту карткового бізнесу та правила проведення платежу, зокрема інструкція використання картки в торгівельно-сервісній мережі, процес ідентифікації та авторизації держателя платіжної картки при проведенні операції. Надано рекомендації щодо безпеки використання платіжних карток у повсякденному житті. Зроблено висновок з приводу того, що проведення операцій з платіжними картками становить ряд загроз даним держателів платіжних карток, а тому їх необхідно захищати на всіх рівнях обробки та зберігання.

Ключові слова: електронні платіжні системи, безпека даних, платіжна картка, карткова платіжна система

Ищук Г. П., Пелешенко А. В. Обеспечение безопасности данных карточных платежных систем при проведении платежных операций. В статье рассмотрены типы платежных карточек с учетом технических средств обеспечения безопасности карточки, обеспечения безопасности данных держателей платежных карточек, и критических аутентификационных данных. Рассмотрено нормативно правовое обеспечение безопасности платежных систем и операций в них. Проанализированы новейшие угрозы относительно компрометации платежных карточек, а также уровни и способы защиты карточного бизнеса и правила проведение платежа, в частности инструкция использования карточки в торгово-сервисной сети, процесс идентификации и авторизации держателя платежной карточки при проведении операции. Даны рекомендации относительно безопасности использования платежных карточек в повседневной жизни. Сделан вывод по поводу того, что проведение операций с платежными карточками составляет ряд угроз данным держателей платежных карточек, а потому их необходимо защищать на всех уровнях обработки и хранения.

Ключевые слова: электронные платежные системы, безопасность данных, платежная карточка, карточная платежная система

Ishchuk H.P., Peleshenko A.V. Providing data security of the payment services during payment transactions. This article deals with the types of payment cards including the technical means of providing card security, cardholders data security and important authentication data. It is examined the regulatory and legal framework for the payment systems and security operations in them, the latest threats related to the payment card compromises as well as the level and ways to protect the card business and rules for making card payment, in particular: a card usage guide in the sales service network, the process of identification and authorization of a card holder during the transactions. The article provides the recommendations on the secure use of payment cards in our everyday payment activities as well as a conclusion that the execution of transactions using the payment cards represents by itself a number of threats directed against the cardholders, and so they should be protected at all processing and storage levels.

Keywords: electronic payment service, payment card, card payment service, money security

Вступ. В Україні зростає популярність електронних платіжних систем. Разом зі зручністю використання електронних грошей зазначимо й супутні ризики. Платіжні системи можна розділити на карткові та безкарткові.

Розглянемо переваги та недоліки використання карткових платіжних систем в Україні.

До переваг віднесемо: *захищеність грошей* – при втраті картки та своєчасному виконанню всіх вимог договору держателя платіжної картки (ПК) ризик отримання збитків мінімізується; *зручність* – не потрібно використовувати готівку та підтримувати ризик її втрати, досить мати при собі одну або декілька ПК; *простота використання* – розрахунок без додаткових комісій на відміну від отримання готівки за допомогою банкомату або в пункті видачі готівки (тариф залежить від банківської установи).

До недоліків віднесемо: *неможливість* розрахунку картою у торгових точках, де відсутній POS-термінал; *додаткові витрати*, пов'язані з утриманням карткового рахунку.

Мета роботи: дослідити засоби компрометації ПК при проведенні платіжних операцій, сформулювати правила та рекомендувати превентивні заходи протидії.

Проблема забезпечення безпеки ПК розслідування злочинів у цій сфері досліджуються в багатьох публікаціях зарубіжних та вітчизняних вчених [1...7]. Ця проблема потребує комплексного рішення на законодавчому, координаційному та технічному рівнях. Далеко не всі злочини з використанням ПК у полі зору правоохоронних органів, оскільки нелегко довести провину внаслідок недосконалої законодавчої бази [5].

Для недопущення шахрайського використання даних ПК був розроблений стандарт PCI DSS (Payment Card Industry Data Security Standard), що вказує на правила зберігання, передачі та обробки даних ПК та Закон України [8] тощо.

Для забезпечення безпеки платіжних операцій всі фінансові установи періодично проходять аудити Національного Банку України та незалежні аудити на відповідність міжнародним стандартам безпеки, проводять цілодобовий моніторинг фінансових операцій з метою виявлення підозрілих транзакцій за територіальним критерієм, за критеріями суми та типу операції. За вимогами міжнародних платіжних систем, фахівці з питань безпеки платіжних операцій повинні проходити навчання щодо новітніх засобів шахрайства в області ПК, та ознайомлюватись з новітніми методиками боротьби з ним.

У кожній фінансовій установі має бути підрозділ, що займається забезпеченням безпеки платіжних операцій, фінансовим моніторингом та реагуванням на спроби порушення безпеки платіжних карток, а також тісно взаємодіє з аналогічними підрозділом інших фінансових установ в Україні, представниками міжнародних платіжних систем.

Основні терміни та визначення. *Платіжна Система* (payment institution) – платіжна організація, учасники платіжної системи та сукупність відносин, що виникають між ними при проведенні переказу коштів. Обов'язковою функцією, що має виконувати платіжна система – є проведення переказу коштів [8].

Платіжна картка (payment card) – спеціальний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для ініціювання переказу коштів з рахунку платника або з відповідного рахунку банку з метою оплати вартості товарів і послуг, перерахування коштів зі своїх рахунків на рахунки інших осіб, отримання коштів у готівковій формі в касах банків через банківські автомати, а також здійснення інших операцій, передбачених відповідним договором [8].

Держатель картки (держатель спеціального платіжного засобу) – фізична особа, яка на законних підставах використовує спеціальний платіжний засіб для ініціювання переказу коштів з відповідного рахунку в банку або здійснює інші операції із застосуванням зазначеного спеціального платіжного засобу.

Платіжна операція – дія, ініційована держателем спеціального платіжного засобу, з внесення або зняття готівки з рахунку, здійснення розрахунків у безготівковій формі з використанням цього спеціального платіжного засобу за банківськими рахунками.

Еквайринг – діяльність щодо технологічного, інформаційного обслуговування суб'єктів господарювання і здійснення операцій з видачі готівки користувачам спеціальних платіжних засобів, які не є клієнтами емітента, а також проведення розрахунків з ними за операції, які здійснені із застосуванням спеціальних платіжних засобів.

Емісія спеціальних платіжних засобів (емісія) – проведення операцій з випуску спеціальних платіжних засобів певної платіжної системи.

Емітент спеціальних платіжних засобів (емітент) – банк, що є членом платіжної системи та здійснює емісію спеціальних платіжних засобів.

Авторизація – процедура отримання дозволу на проведення операції з використанням спеціального платіжного засобу.

Код авторизації – набір цифр або набір букв і цифр, що формується і надається емітентом або юридичною особою – учасником платіжної системи, яка діє за його дорученням, за результатами авторизації.

Персональний ідентифікаційний номер (ПІН) – набір цифр або набір букв і цифр, відомий лише держателю спеціального платіжного засобу і потрібний для його ідентифікації під час здійснення операцій із використанням спеціального платіжного засобу.

Банківський автомат самообслуговування (банкомат) – програмно-технічний комплекс, що дає змогу держателю спеціального платіжного засобу здійснити самообслуговування за операціями з одержання коштів у готівковій формі, внесення їх для зарахування на відповідні рахунки, одержання інформації щодо стану рахунків, а також виконати інші операції згідно з функціональними можливостями цього комплексу.

Платіжний термінал (POS-термінал) – електронний пристрій, призначений для здійснення платіжних операцій, отримання довідкової інформації і друкування документа за операцією із застосуванням спеціального платіжного засобу [9].

Шахрайські методи, направлені на платіжні картки. Небезпеку при використанні ПК становить її втрата – неможливість здійснення держателем контролю (володіння) над спеціальним платіжним засобом, незаконне заволодіння та/або використання спеціального платіжного засобу чи його реквізитів. Цій небезпеці підконтрольні всі типи платіжних карток; відповідальність за збереження картки покладається на держателя.

Компрометація картки – процес, при якому відбувається заволодіння оригіналом картки або виготовлення її дублікату та втрата держателем особистої інформації, що необхідна для авторизації (наприклад передача в будь-який спосіб ПІН-коду третій особі).

У разі втрати коштів з картки через її компрометацію з вини держателя банк емітент картки або платіжна система не повертають втрачені кошти.

Розглянемо деякі технічні методи компрометації карток.

Скімінг – різновид карткового шахрайства, при якому для отримання потрібних реквізитів ПК (цифрова інформація, ПІН-код) використовуються спеціальні зчитувальні пристрої (скімери, накладки на клавіатуру, відеокамери) з метою подальшого виготовлення та несанкціонованого використання копії/дублікату ПК [10]. До даного методу компрометації схильні ПК з магнітною стрічкою. При використанні скімеру (електронний пристрій у вигляді накладки на карткоприймач банкомату, або у вигляді POS-терміналу) здійснюється зчитування та збереження дампу всіх даних, що записані на магнітну стрічку. Ці дії дозволяють шахраю зробити дублікат картки на так званий “білий пластик” (заготівка без ознак будь-якої платіжної системи та банку емітента), щоб потім вступивши у злочинну змову з касиром, або підробивши вигляд картки будь-якого банку розрахуватись у торгівельно-сервісній мережі.

Разом зі скімером використовують наступні методи отримання ПІН-коду:

– підглядання ПІН в процесі набору особисто або за допомогою камери. Цей метод є найдешевшим, але становить загрозу для самого шахрая;

– використання додаткового обладнання – накладки на клавіатуру. Є досить багато різновидів цих накладок – одні з них мають власну пам'ять, інші передають дані зловмиснику за допомогою безпроводових каналів зв'язку.

Скімінг дуже дорогий у виконанні та нерентабельний у випадку чіпованих карт, адже чіп на карті – це мікропроцесор який не тільки зберігає дані платіжної картки, а й виконує операції по їх розшифруванню та шифруванню.

Зазвичай при використанні гібридних карток (картки з чіпом та магнітною стрічкою) проводити операцію по магнітній стрічці дозволяється після ініціалізації чіпу та лише у випадку відсутності технічної можливості провести транзакцію за допомогою чіпу.

Розглянемо інші шахрайські методи, що становлять загрозу для платіжних карток.

– “*Ліванська петля*” – спеціальний пристрій, що блокує так вікно подачі карти, щоб вона застрягла в банкоматі [3]. Цей вид шахрайства небезпечний для всіх видів карток, тому що він направлений на вилучення картки.

– *Фотографування* або інший вид фіксації даних зазначених на картці. Особливу увагу слід приділяти збереженню CVC2 коду, повного номеру картки (PAN) та строку дії картки, адже ці дані необхідні для розрахунку карткою в мережі Internet.

– *Фантом банкомату* – шахраями виставляється, по суті, муляж апарату, обладнаного скімінговими пристроями, накладними клавіатурами тощо. На вигляд звичайний банкомат,

зчитувальні пристрої не привертають до себе уваги, так як вони не є чужорідними тілами на заводському корпусі. Банкомат буде реагувати на запити. На екрані відобразяться звичні зображення. Єдине, на остаточній стадії отримання грошей висвітлиться повідомлення на кшталт «у банкоматі немає запитаної суми» або «технічні несправності, просимо вибачення за тимчасові незручності» [9]. В цьому випадку єдина рекомендація – не користуватись банкоматами, які з'явилися раптово у місцях скупчення людей, краще використати банкомат розташований у відділенні банку або перевірений часом.

– Крадіжка ПІН-коду за допомогою банкомату з використанням високочутливої інфрачервоної камери. Зловмисник робить знімок клавіатури, на якій попередній користувач набирав ПІН-код. Клавіші, до яких торкалися, трохи тепліші, причому остання натиснута клавіша тепліша від передостанньої і т.д. Причому успішність цього методу залежить від типу клавіатури (металеві клавіатури мають більшу теплопровідність і температура їх клавіш швидко вирівнюється) і від того, чи не набирав клієнт ще якісь комбінації, наприклад, суму. Для уникнення зняття ПІН-коду за тепловим відбитком достатньо після роботи з клавіатурою на короткий час покласти на неї долоню.

Технічні способи скомпрометувати картку не єдині. Частіше за все сам держатель повідомляє конфіденційні дані шахраям. Метод так-званої «соціальної інженерії».

Наприклад, на номер телефону власника картки здійснюється дзвінок, або надсилається коротке текстове повідомлення (SMS) з подібним змістом: «Ваша картка заблокована, тому що є підозра її компрометації. Будь ласка, зверніться до служби підтримки користувачів за номером (номер шахраїв). У випадку дзвінка жертви на тій стороні знаходиться дуже хороший психолог, який входить у довіру та запитує конфіденційну інформацію.

Протидіяти такому виду шахрайства можна лише одним способом – при отриманні такого повідомлення або дзвінка, перервіть розмову під будь-яким приводом. Наприклад, вам зараз незручно розмовляти та запропонуйте зателефонувати вам через годину. Тим часом потрібно звернутися до служби підтримки клієнтів банку за номером зазначеним на зворотному боці картки та повідомити про інцидент.

Правила проведення операцій в торгово-сервісній мережі. Платіжна картка є зручним інструментом для проведення розрахунків за товари та послуги в магазинах, кафе, на АЗС тощо. Отже, для забезпечення безпеки використання платіжної картки слід знати загальні правила здійснення розрахунків в торгівельно-сервісній мережі [10].

1. Оператор зобов'язаний здійснювати операції з використанням спеціального платіжного засобу лише в присутності клієнта [11].

2. Слід ідентифікувати ПК. Провести візуальну перевірку платіжної картки та визначити чи не має вона фізичних пошкоджень.

Платіжна картка в цілому та окремі її реквізити (місце для підпису, магнітна смуга, голограма, номер, захисні символи) не повинні мати зовнішніх пошкоджень.

Отже слід: *перевірити* елементи захисту ПК; *провести* зовнішній огляд ПК на предмет наявності обов'язкових реквізитів; *переконатись*, що ПК відповідає стандартам зазначеної платіжної системи і її використання не обмежено однією країною (надпис на лицьовій стороні VALID ONLY IN (дійсно в ...), за винятком тих ПК, що діють на території України; *звернути* увагу на термін дії ПК. Картка дійсна до останнього дня місяця, вказаного на ній; *перевірити*, чи не підроблена смуга для підпису держателя ПК: смуга для підпису має бути гладенькою і не має бути відірваною чи сколупнутою, підпис має бути зроблений кульковою ручкою (в жодному випадку не фломастером, олівцем, тощо); *перевірити*, чи немає на ПК сторонніх наклейок (якщо вони є, потрібно запропонувати клієнту їх зняти, а у разі відмови клієнта зняти наклейки – відмовити в оплаті цією платіжною картою); *перевірити* наявність підпису держателя ПК на зворотній стороні картки (якщо підпис відсутній на неперсоніфікованій картці (НПК) – проводити операції з такою картою заборонено).

Особливу увагу слід приділити контролю ембосованих даних:

– Усі ембосовані номери та символи повинні бути виконані чітко та рівномірно з пропусками. Якщо вони виявилися кривими або реембосованими (перебиті зверху), платіжна картка може бути шахрайською. Також потрібно переконаватися, що останні 4 цифри номеру картки надруковані на голограмі (для MasterCard). Часто на шахрайських ПК ембосовані номери знаходяться під голограмою.

– Порівняти перші чотири цифри номера платіжної картки, які ембосовані або надруковані з чотирма цифрами, надрукованими меншим шрифтом нижче ембосованого/надрукованого номеру картки (крім карток CIRRUS/MAESTRO, на яких маленький чотиризначний номер відсутній). Вони повинні співпадати.

– Порівняти 16-значний номер, нанесений на панелі для підпису з номером картки на лицьовій стороні. Вони повинні співпадати.

Якщо на панелі для підпису нанесені 4 останні цифри номеру картки – порівняти чотири цифри, надруковані на панелі для підпису з чотирма останніми цифрами номеру картки, ембосованому або надрукованому на лицьовій стороні картки (крім карток MAESTRO, на яких номер на панелі для підпису відсутній). Вони повинні співпадати.

3. У деяких випадках оператор може запропонувати держателю пройти процедуру ідентифікації. Ситуація, в якій рекомендується ідентифікація держателя платіжної картки:

– **поведінка клієнта** є підозрілою, а саме; *клієнт* нервує, намагається відволікти оператора під час проведення операції або чинить психологічний тиск; *невпевнено* розписується і намагається підробити підпис; *своїм* зовнішнім виглядом викликає підозру щодо суми операції; *намагається* зробити декілька операцій протягом короткого часу;

– **стать Клієнта** явно не відповідає імені на картці;

– **вигляд Клієнта** та культура його поведінки не відповідають статусу утримувача даного типу картки; *своїм зовнішнім виглядом* не відповідає високій вартості послуги/товару, який збирається оплатити за допомогою картки;

– **у разі, коли Клієнт** безладно здійснює вибір товарів на значну суму, або, навпаки, купує товар на одну суму й у разі позитивної авторизації робить спробу добору товару на додаткову суму – все це може бути серйозною підставою для підозри в шахрайських діях.

4. Під час процедури ідентифікації держателя ПК слід перевірити документ, що засвідчує особу держателя ПК.

Таким документом можуть бути: *внутрішній* громадянський паспорт або документ, що його замінює – для громадян України; *закордонний* паспорт, або документ, що його замінює – для громадян України або для іноземних громадян, які тимчасово перебувають в Україні; *посвідчення* особи військовослужбовця або військовий квиток для військовослужбовців; *права водія* – для громадян України (крім неперсонифікованих ПК).

Далі слід впевнитись у тому, що держатель ПК є та особа, чия фотокартка представлена у документі, співпадають.

5. Якщо держатель вводив ПІН код, то підпис на чеку вимагати заборонено.

6. При вводі ПІН коду через додаткову або основну клавіатуру POS-терміналу слід переконаватися, що клавіатура не знаходиться в полі зору сторонніх осіб або камер спостереження.

7. Вимагати та зберігати чек, що підтверджує операцію.

Розглянемо детальніше процедуру авторизації платежу.

При проведенні розрахунку в торгівельно-сервісній мережі сума операції не знімається з рахунку держателя, а блокується в середньому на три доби, доки еквайер не отримає підтвердження транзакції від торгівельно-сервісної організації.

Ця дія призначена для можливості повернення коштів при поверненні товару. При цьому оператор зобов'язаний відмінити транзакцію за допомогою POS-терміналу, а еквайер повідомити банк емітент картки. Емітент знімає блокування з суми відміненої транзакції та гроші стають доступними на рахунку.

Авторизація є обов'язковою для всіх ПК. В залежності від коду авторизації операція вважається успішною або не успішною.

В разі успішної авторизації проводиться верифікація держателя картки за допомогою ПІН-коду (якщо це вимагається даним типом картки) або за допомогою підпису.

У разі неуспішної авторизації повідомлення виводиться на екран POS-терміналу, а код друкується на чеку. В залежності від коду оператор повертає картку клієнту або затримує її, сповістивши міліцію чи службу безпеки банку екваера або емітента картки. Транзакція може бути завершена лише в разі позитивної відповіді на авторизаційний запит.

Висновки. Можемо стверджувати, що найбільш безпечним типом платіжних карток є чіповані або гібридні платіжні картки.

Для забезпечення безпеки платіжної картки слід дотримуватись наступних правил:

1. ПІН код потрібно запам'ятати або записати та зберігати окремо від картки в недоступному місці.
2. Підключити послугу SMS інформування та у разі наявності повідомлень про транзакцію яка не була ініційована держателем – негайно звернутись у службу клієнтської підтримки банку емітенту та заблокувати картку.
3. Потрібно встановити ліміти на операції з видачі готівки, розрахунків в мережі Internet та торгово-сервісній мережі.
4. Перед проведенням операцій за допомогою банкомату переконатись в відсутності сторонніх пристроїв на карткоприймачі та корпусі банкомату.
5. При вводі ПІН коду прикривати клавіатуру рукою.
6. Після завершення операції з банкоматом переконатись що банкомат повернув картку, видав готівку та чек.
7. При проведенні розрахунку в торгово-сервісній мережі слідкувати щоб всі дії оператора (касира, офіціанта) над картою були в полі зору держателя.
8. Для розрахунків в мережі Internet використовувати окрему картку наприклад Visa Virtuon та поставити нульовий ліміт для даного типу операцій на основну картку.

Література

1. Андрей Белоусов. Проблемы безопасности в области использования пластиковых карточек [Електронний ресурс] // – Режим доступу: <http://www.crime-research.ru/library/>
2. Голубев В. А. Проблемы преступности и банковские технологии / В. А. Голубев // Корпоративные системы. – 2002. – № 3. – С.78-82.
3. Машин Сергей. Пластиковая карта – мишень для мошенников [Електронний ресурс]. // – Режим доступу: <http://www.aferizm.ru/>
4. Карнаухова Е. Ю. Мошенничество в сфере безналичных расчетов с использованием банковских платежных карт / Е. Ю. Карнаухова // Юридические науки: проблемы и перспективы: материалы II междунар. науч. конф. (г. Пермь, январь 2014 г.). – Пермь : Меркурий, 2014. – С. 42-44.
5. Причина Е. В. Правонарушения в области использования пластиковых карточек [Електронний ресурс] // – Режим доступу: http://www.rusnauka.com/12_KPSN_2010/
6. Bob Arden. Credit card scam [Електронний ресурс] // – Режим доступу: <http://www.crime-research.org/analytics/Credit-card-scam/>
7. Ali Hussain. Internet banking: security [Електронний ресурс] // – Режим доступу: <http://www.crime-research.org/analytics/Internet-banking-security/>
8. Про платіжні системи та переказ коштів в Україні // Закон України від 05.04.2001 р. № 2346-III [Електронний ресурс] // – Режим доступу: <http://zakon.rada.gov.ua>.
9. Постанова Національного Банку України від 04.11.2010 N 481 [Електронний ресурс]. // – Режим доступу : <http://zakon.rada.gov.ua>.
10. Проект Незалежної асоціації банків України (НАБУ) «Протидія кіберзлочинності» [Електронний ресурс] // – Режим доступу: <http://214104.football8.web.hosting-test.net/>
11. Інструкція по прийому до оплати карток міжнародних платіжних систем VISA та MASTERCARD [Електронний ресурс] // – Режим доступу: https://my.ukrsibbank.com/common/upload/Instruktsiya_po_priyomu_do_oplati_PK.pdf