УДК 336.71

Галіцейська Ю. М.
Леськів О. М.
Тернопільський національний економічний університет

ОСОБЛИВОСТІ ПРОЯВУ КАРТКОВОГО РИЗИКУ В СФЕРІ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ: МІЖНАРОДНІ АСПЕКТИ ТА ВІТЧИЗНЯНІ РЕАЛІЇ

У статті аналізується стан ринку платіжних карток в Україні, розглядаються питання виникнення ризику операцій з платіжними картками. Пропонуються заходи для мінімізації ризиків усіх основних учасників карткових розрахунків: емітента, клієнта-користувача, еквайра. Досліджуються випадки шахрайства з платіжними картками та інструменти зменшення ризиків карткового бізнесу.
Ключові слова: платіжні картки, картковий бізнес, емітент, еквайр, скімінг, ризики.

Постановка проблеми. Будь-яка діяльність в середовищі банківського бізнесу є не тільки прибутковою, але й характеризується достатньо великим рівнем ризику, оскільки здійснення фінансових операцій часто пов'язане із невизначеністю, яка має як матеріальне, так і нематеріальне вираження. При цьому втрати, що виникають в результаті реалізації ризикової ситуації, мають значний вплив не лише на національну банківську систему, але й відображаються на міжнародних платіжних системах і впливають на вибір методів мінімізації ризику, а також спричиняють активізацію систем моніторингу і наднаціонального регулювання через посилення взаємодії між контрольними органами різних країн. Організація такого виду відносин характерна і для боротьби із так званим «картковим» ризиком, що в сучасному комп'ютеризованому суспільстві набуває особливої актуальності, оскільки більше половини всіх банківських операцій та розрахунків здійснюється за допомогою спеціальних платіжних засобів – платіжних карток.

Банківська діяльність в напрямку організації карткового бізнесу зумовлює виникнення ситуації, коли банк має обрати певну стратегію щодо допустимого рівня ризику, на який він погоджується, або йти на уникнення від ризику, що веде до відмови від виконання тих чи інших операцій, які в цілому можуть бути більш прибутковими і забезпечити стійкий притік клієнтів.

Аналіз останніх досліджень і публікацій. Багато вітчизняних науковців присвятили свої праці вивченню проблем виникнення карткових ризиків і пошуку найбільш оптимальних шляхів щодо їх мінімізації. Серед них: В.Берніков, Ф. Бутинець, Н. Вядрова, А. Герасимович, І. Дорошенко, К. Жидко, В. Кравець, М. Колдовський, О. Махаєва, А. Одарюк, О. Сокольська, В. Харченко, Н. Шульга та інші.

Виділення невирішених раніше частин загальної проблеми. Однак загалом досить незначна кількість дослідників зосереджують свою увагу на вивченні взаємозв'язку між різними проявами ризику використання платіжних карток, які реалізуються на тих чи інших рівнях регулювання (це, зокрема, міжнародні та національні платіжні системи), проведенні аналізу їх кількісних масштабів та розробці найбільш оптимальної системи захисту відповідно до визначених загроз, які притаманні банківським операціям, що зумовлюють застосування спеціальних платіжних засобів.

Мета статті. Головною метою даної роботи є виявлення і конкретизація характерних особливостей прояву карткового ризику в банківській сфері з урахуванням міжнародних і вітчизняних реалій та виділення комплексу найбільш дієвих заходів щодо його мінімізації з огляду на структурні тенденції розвитку національного сектору безготівкових розрахунків.

Виклад основного матеріалу. За даними, які оприлюднила Американська асоціація банкірів (American Bankers Association), в світі здійснюється більш як 2,5 трлн. операцій по кредитних картках у рік [5].

Вітчизняний ринок платіжних карток звичайно не можна порівняти із світовими показниками, але зрушення у цій сфері є вже достатньо вагомими, зокрема протягом 2013 року кількість активних платіжних карт банків в Україні зросла на 7,6% (до 35,6 млн. шт.), а їх частка в загальній кількості емітованих платіжних карт за вказаний період збільшилася з 47,4% до 51,1%. Крім того, майже на 5,4 млн. (12,1%) збільшилася кількість власників банківських платіжних карт – до 49,7 млн. Як бачимо, нарощування обсягу операцій із платіжними картками здійснюється доволі прогресуючими темпами і спрямоване на досягнення відповідності визначеним міжнародними стандартам структури грошового обігу.

Українські банківські установи, в свою чергу, продовжують нарощувати обсяг інвестицій у розвиток інфраструктури обслуговування карткового бізнесу. Так, кількість банкоматів збільшилася на 11,6% (до 40,35 тис.), кількість банківських терміналів – на 0,5% (до 28,89 тис.), кількість торговельних терміналів – на 43,6% (до 192,33 тис.). У перерахунку на 100 тисяч активних платіжних карт кількість банкоматів за рік зросла з 109 до 113, кількість торговельних терміналів – з 405 до 540 [1].

Лідерство за кількістю активних банківських платіжних карт, як і раніше, зберігають ПриватБанк, Ощадбанк та Райффайзен Банк Аваль – на початок року на їх частку припадало понад 66% активних платіжних карт БСУ. Ці ж установи мають і найбільш розвинену банкоматну мережу.

Обсяг операцій з банківськими картами у 2013 році склав 916,03 млрд. грн., що на 23,5% перевищує аналогічний показник попереднього року. Не дивлячись на те, що в структурі операцій з платіжними картами ще значною мірою переважають операції з отримання готівки, питома вага безготівкових розрахунків поступово збільшується: за обсягом – до 17,4% у 2013 році проти 12,3% у 2012 році; за кількістю операцій – до 43,6% у 2013 році проти 32,4% у 2012 році [1].

З вищенаведеного вже можемо зробити висновок, що наростання масштабів операцій з використанням платіжних карток на сьогодні вимагає запровадження єдиної системи ризик-менеджменту в українських банках, яка була б спрямована саме на виявлення і мінімізацію всіх основних ви-

дів карткового ризику і зменшення втрат від його можливої реалізації.

Як правило, до процесу використання платіжних карток причетні різні суб'єкти ринку. Від шахрайських операцій з пластиковими банківськими картками, в першу чергу, страждають клієнти банків, зазнаючи фінансових збитків, а також самі банки, які втрачають не лише гроші, а й репутацію.

На нашу думку, варто здійснити розподіл всіх можливих втрат, які напряму залежать від дій учасників ринку карткового обслуговування, на три групи:

а) ризик зі сторони емітента (банку): випуск паралельних карток на одного клієнта; неправомірне регламентування авторизаційного ліміту; недотримання вимог платіжної системи стосовно оформлення платежів чи передачі даних;

б) ризик зі сторони клієнта-користувача, який передбачає як правило, ризик втрати коштів з рахунку: списання коштів за рахунком клієнта за підробленими та втраченими платіжними картками; несвоєчасне звернення клієнта до банку з приводу втраченої картки; розповсюдження конфіденційної клієнтської інформації серед третіх осіб;

в) ризик зі сторони еквайра (торговця): овердрафт за рахунком клієнта, що виник у результаті незаконних дій клієнта при масових операціях у торговельній мережі за карткою нижче авторизаційних лімітів торгових точок; часта зміна робочих кадрів та відмова від проведення інструктажу по роботі з платіжними картками; відмова від застосування елементарних методів перевірки якості та справжності платіжних карток [6].

На жаль, збільшення кількості карткових операцій і кількості їх власників спричинило одночасне збільшення і числа випадків шахрайства з картками, а їхній характер став більш витонченим. Особливої актуальності це питання набуло в Україні та країнах СНД, де рівень шахрайства з пластиковими картами значно перевищує навіть середні показники по світу як по відношенню до емітента, так і по відношенню до еквайра. Зокрема, у міжнародній практиці дії з загубленими та вкраденими картами мають найбільшу питому вагу в структурі шахрайства: на їхню частку зазвичай припадає більше 50% випадків шахрайства з банківськими картками.

Ендрю Хелдейн, керівник відділу фінансової стабільності Банку Англії, стверджував, що найбільші 5 банків Великобританії бояться кіберзлочинів навіть більше, ніж боргової кризи. За його словами, система захисту від хакерських атак у банківському секторі досі перебуває в зародковому стані: «фінансисти більше дбали про ліквідність, аніж про безпеку» [5]. За експертними оцінками, щорічні втрати від шахрайства, зокрема, з банківськими картами в світі сягають 10-12 млрд. дол. Частково оцінювання та регулювання карткових ризиків здійснює Європейська група з безпеки банкоматів (EAST).

Що стосується банкоматних шахрайств, зокрема у європейських країнах, то, за даними EAST (European ATM Security Team), членом якої, серед інших 29 країн Європи із загальним розміщенням 619 603 банкоматів, є і Українська Асоціація «ЕМА», протягом 2013 р. випадки готівкового трапінгу збільшилися, в той час як число випадків скімінгу та обсяг втрат від банкоматних шахрайств знизилися. Усього кількість інцидентів банкоматних шахрайств знизилася на 6% – з 22450 у 2012 році до 21346 у 2013 році (рис. 1).

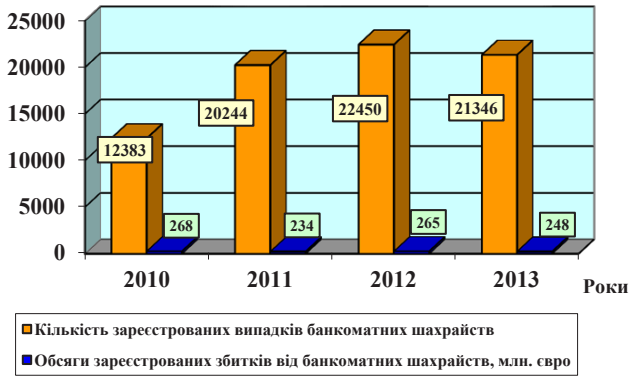

Рис. 1. Динаміка кількості зареєстрованих EAST інцидентів та збитків від банкоматних шахрайств у 2010-2013 рр.

Джерело: розроблено авторами за даними [9]

Кількість випадків скімінгу у 2012-2013 рр. знизилася на 26% до найнижчого рівня ще з 2009 року. Сумарна величина збитків зменшилася на 6,5% з 265 млн. євро до 248 млн. євро [9].

Щодо загальних тенденцій, то у 2013 році кількість випадків скімінгу та обсяг втрат від нього знизилися по всій Європі в цілому, але в окремих країнах спостерігалося їх збільшення (іноді досить значне). Завдяки оперативному обміну інформацією та статистикою члени EAST мали змогу надавати один одному допомогу для вирішення виникаючих загроз і прогнозування тенденцій. У 2013 році кількість фізичних атак на банкомати збільшилася на 9,5% порівняно з 2012 роком – з 1920 до 2102 інцидентів (рис. 2), хоча в середньому оцінені втрати грошових коштів внаслідок пограбувань банкоматів зросли на 24% – від 19 млн. євро у 2012 році до 23 млн. євро у 2013 році [9].

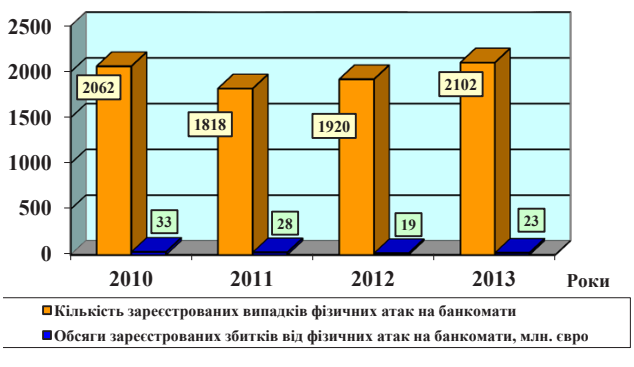

Рис. 2. Динаміка кількості зареєстрованих EAST фізичних атак на банкомати та сумарна величина збитків у 2010-2013 рр.

Джерело: розроблено авторами за даними [9]

Представлені дані свідчать, що загалом ситуація в міжнародному платіжному середовищі є в деякій мірі досить неоднозначною та вимагає більш детального аналізу з боку відповідних контролінгових органів.

За інформацією Національного банку України, в банківській системі України найбільш розповсюдженими є наступні види кіберзлочинів у сфері карткового бізнесу:

1) банкоматне шахрайство: скімінг – виготовлення, збут та встановлення на банкомати пристроїв зчитування/копіювання інформації з магнітної смуги платіжної картки та отримання ПІН-коду до неї; використання «білого пластику» для «клонування» (підробки) платіжної картки та

зняття готівки в банкоматах; Transaction Reversal Fraud – втручання в роботу банкомату при проведенні операцій з видачі готівки, яке залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником; Cash Trapping – це заклеювання диспансеру банкомата для присвоєння зловмисником готівки, яка була списана з карткового рахунку законного держателя картки [8];

2) шахрайські операції в торгівельно-сервісних мережах: укладання фіктивних угод торговельного еквайрингу для обслуговування підроблених платіжних карток; викрадення реквізитів платіжних карток, у тому числі також із застосуванням технічних засобів їх «клонування»; операції на суму нижче встановленого ліміту без проведення авторизації; використання у ПС втрачених/викрадених/підроблених платіжних карток;

3) шахрайство в мережі Інтернет: викрадення реквізитів платіжних карток; проведення операцій із використанням викрадених реквізитів платіжних карток; діяльність щодо створення програмних засобів для викрадення реквізитів платіжних карток (фішинг – створення фіктивних WEB-сайтів та здійснення фальсифікованої інформаційної розсилки повідомлень, поширення комп'ютерних вірусів та троянських програм, перехоплення трафіку тощо).

4) шахрайські схеми в системах дистанційного банківського обслуговування (далі – ДБО): впровадження комп'ютерних вірусів та троянських програм для прихованого перехоплення управління ПК клієнта з встановленим програмним забезпеченням ДБО (віруси типу Gamker і Carberp, банківські трояни для крадіжки інформації (Neverquest)); відкриття рахунків, проведення несанкціонованих операцій та отримання готівки в результаті неправомірних операцій у системах ДБО; незаконне одержання платежів від закордонних відправників через міжнародну систему SWIFT внаслідок втручання у роботу комп'ютерів та клієнтських систем ДБО закордонних банків.

Вітчизняні реалії на сьогодні репрезентують нам лише посилення негативних тенденцій, а винахідливість у реалізації шахрайських операцій справді вражає. Ось лише окремі факти: Українська міжбанківська асоціація членів платіжних систем ЕМА розмістила інформацію про те, що в січні-вересні 2013 року було зроблено 257 спроб списання коштів з рахунків клієнтів банків (їх загальна сума 108,7 млн. грн.), у 2012 році таких спроб було 179 (150,1 млн. грн.), в 2011 році – всього шість (14,9 млн. грн.) [8]. Також МВС України було опубліковано інформацію щодо кількості злочинних трансакцій у 2013 році, зокрема протягом цього періоду правоохоронні органи зафіксували 270 спроб злому систем ДБО на суму понад 100 млн. грн. Із зареєстрованих списань на 67 млн. грн. вдалося заблокувати і повернути близько 47 млн. грн. [2].

Протягом квітня та жовтня 2013 року близько 30 банків в один день піддалися системним масованим кібератакам типу «відмова від обслуговування» (DDoS-атаки), в результаті яких клієнти банків не могли скористатися сервісами дистанційного банківського обслуговування від декількох годин до декількох днів [2]. Одна така DDoS-атака обходиться шахраям приблизно в 100 тис. грн. За словами начальника відділу протидії кіберзагрозам ПУМБ Олександра Третяка, у другому півріччі 2013 року порівняно з першим кількість зафіксованих кібератак збільшилася на 40% [2]. Проте вже після першої такої атаки в квітні більшість банків посилили загальні елементи захисту позабанківського середовища. На ці заходи українські фінустанови витратили близько 3 млн. грн., однак зрозуміло, що цих коштів на сьогодні все одно недостатньо для надання повної гарантії клієнтам щодо захисту їх коштів та особистої інформації, оскільки час не стоїть на місці і з'являються все нові способи, які, на жаль, допомагають зловмисникам більш майстерно обходити наявні обмеження і системи безпеки.

За інформацією прес-служби МВС у 2013 році було виявлено близько 160 скімінгових пристроїв на банкоматах, в 2012 р. – 73, у 2011 р. – 45. Зокрема за даними Української міжбанківської асоціації членів платіжної системи ЕМА у другому кварталі 2013 р. були виявлені скімінгові пристрої по ряду регіонів України: у м. Київ – 100 шт., у м. Кривий Ріг – 18 шт., в Одеській обл. – 14 шт., у Дніпропетровську – 11 шт., у Запорізькій обл. – 8 шт., у м. Чернівці – 8 шт., у м. Харків – 2 шт., у Донецькій обл. – 2 шт. [8]

Якщо ж говорити про конкретні випадки в розрізі українських банків, ці пристрої були зафіксовані: ПАТ «Укрсиббанк» – 1 шт., АТ «Сбербанк Росії» – 1 шт., ПАТ АБ «Південний» – 1 шт., ПАТ КБ «Надра» – 1 шт., АТ банк «Фінанси та кредит» – 2 шт., ПАТ «Міський комерційний банк» – 2 шт., ПАТ «Укрексімбанк» – 3 шт., ПАТ «VAB Банк» – 3 шт., ПАТ «Банк Кіпру – 4 шт., ПАТ «Укрінбанк» – 5 шт., ПАТ «Укрсоцбанк» – 7 шт., ПАТ КБ «Правекс-Банк» – 9 шт., ПАТ «Райффайзен Банк Аваль» – 10 шт., ПАТ «ПриватБанк» – 101 шт. [8].

Аналіз вітчизняних тенденцій справді не залишає сумнівів у тому, що широкомасштабне впровадження системи розрахунків на основі карткових платіжних засобів є особливо важливим в умовах постійного зростання частки тіньового сектора економіки, рівня доларизації, широко розповсюдженого небажання населення тримати свої заощадження на рахунках у банківських установах, значного уникнення від сплати податків та загальної недовіри до банків на тлі поширення соціально-економічних та політичних проблем.

Однак все ж є очевидним і той факт, що проблема виникнення ризиків при проведенні операцій з пластиковими картками в практиці українських банків все ж залишається дуже актуальною й потребує якомога швидшого вирішення через реалізацію комплексної системи якісних заходів та прийомів карткового контролінгу.

В загальному управління ризиками при емісії платіжних карток зводиться до мінімізації впливу ризикових факторів використання банківських карток на прибутковість бізнесу в цілому. Управління картковими ризиками при обслуговуванні торгово-сервісної мережі (еквайринг) полягає в реалізації комплексу організаційних і технологічних процедур, спрямованих на обмеження можливості проведення несанкціонованих платежів та створення стійкого непривабливого іміджу торгово-сервісної мережі банку у шахраїв.

В Україні значний вклад в розвиток управління картковими ризиками зробила Асоціація «ЕМА». Завдячуючи зусиллям Асоціації «ЕМА» та її членів спільно з Українським Процесинговим Центром було розроблено систему міжбанківського обміну банківською інформацією «Exchange-OnLine»; успішно реалізовується щорічна програма преміювання кадрових спеціалістів підрозділів ризик-менеджменту банків та правоохоронних органів; також відбува-

ється проведення щоквартальних засідань Форуму з безпеки розрахунків і операцій з платіжними картками та інші різноманітні процедури.

Але, зважаючи на те, що ці ризики є невід'ємною складовою карткового бізнесу, то, відповідно, для їх зменшення та подальшого усунення банківським установам слід забезпечити реалізацію системи таких внутрішніх заходів:

1) для зменшення ризиків зі сторони емітента (банку): кваліфіковано організовувати процеси управління ризиковою ситуацією; формувати страхові фонди за рахунок власних коштів або коштів клієнтів; здійснювати постійний оперативний контроль в самому банку та налагоджувати позапланові перевірки; використовувати процедуру не знижувального залишку за картковим рахунком; здійснювати постійне тестування та вибіркову перевірку персоналу.

2) для зменшення ризиків зі сторони клієнта-користувача: створити в банківській системі єдину захищену базу даних користувачів платіжних карток; здійснювати поступове удосконалення всіх систем моніторингу; впроваджувати ефективні IT-технології забезпечення безпеки безготівкових розрахунків [4, с. 48].

3) для зменшення ризиків зі сторони еквайра (торговця): разом з місцевими відділеннями зв'язку забезпечити банкомати та POS-термінали надійними лініями зв'язку; забезпечення цілодобової авторизації платежів за картками; вчасне складання та розсилка стоп-листів [4, с. 46].

Наприклад, одним з інструментів зменшення ризиків карткового бізнесу, що пов'язані з електронною природою операцій/ трансакцій в режимі «он-лайн», є впровадження спеціалізованих систем моніторингу, що використовують технології «соціальної інженерії» та передових інформаційних технологій, рекомендованих міжнародними платіжними системами. Зокрема, для програмних систем, які було створено фахівцями Процесингового центру «Українська фінансова мережа», розроблені ефективні критерії виявлення підозрілих та/або шахрайських трансакцій, засновані на рекомендаціях VISA International Risk Management (застосування методів статистичного аналізу, негайна реакція на події, статистична обробка потоку транзакцій з метою виявлення закономірностей в поведінці карток, банкоматів, терміналів за визначеними параметрами). Моніторинг при цьому здійснюється за допомогою систем «IFM», «Online Reporting» та «UFN Acquirer GUARD» [7].

Технології моніторингу шахрайських операції в цих системах надаються в двох режимах:

– режим online – тут повідомлення про неправомірну транзакцію поступає безпосередньо відповідальній особі в банку;

– режим offline – щоденна звітність по операціях у відповідності з вимогами платіжних систем.

В кожній із всіх систем online-моніторингу функціонує більше 15 правил. Правила моніторингу можуть бути розширені з урахуванням вимог банку та специфіки обслуговування карток.

Issuer Fraud Monitoring (IFM). IFM – це offline-система моніторингу шахрайських транзакцій, яка включає необхідний набір вимог міжнародних платіжних систем до моніторингу шахрайських операцій. Моніторинг здійснюється шляхом перевірки кожної транзакції за встановленими в системі правилами [7]. По закінченню бізнес-дня (один раз на добу) IFM формуються звіти, які направляються до банку з використанням спеціальних засобів поштового зв'язку.

Online Reporting. Система Online Reporting забезпечує моніторинг потоку емітентських авторизацій на підозру в проведенні шахрайських операцій по ряду визначених правил. Online Reporting дозволяє в режимі online розсилати повідомлення операторам. Після чого оператор може прийняти рішення про зміну статусу (блокування) карти або самостійно зателефонувати клієнту для підтвердження або спростування шахрайства. Також оператор має можливість на деякий період часу внести карту клієнта в стоп-список. Якщо авторизація потрапляє під визначений критерій правила, результат роботи системи Online Reporting відображається в системі віддаленого доступу UFN Info в розділі «Моніторинг» [7]. За допомогою UFN Info оператор може бачити всі попередження і правила, за якими спостерігалося спрацювання системи, а також встановлює обов'язкову відмітку про перегляд даного попередження.

UFN Acquirer GUARD. Система моніторингу шахрайських транзакцій UFN Acquirer GUARD в еквайєрській мережі банку застосовується для регулярного контролю за можливим перевищенням сукупності граничних значень за чітко визначеними критеріями. Вказані порогові значення встановлюються для певних груп підприємств, які об'єднуються за ідентичністю сфер діяльності. Існує три рівні перевищення: низьке (L), середнє (M) і високе (H), по кожному з яких встановлюється відповідна реакція системи [7].

Новинка на українському ринку – це електронні пристрої класу Trust Screen, які використовуються для запобігання злочинності в сфері безготівкових розрахунків. Вони мають спеціальний екран для відображення інформації платіжного доручення. Цифровий підпис накладається за дорученням в самому пристрої і повертається в клієнтське ПЗ вже підписаним [1].

Висновки і пропозиції. З огляду на зростаючі темпи розвитку ринку платіжних карток, які в свою чергу зумовлюють і значне наростання масштабів карткового ризику, можемо зробити висновок, що забезпечити зменшення числа шахрайських операцій з платіжними картками в Україні, і в тому числі значної частки сумарного карткового ризику, банки можуть за реалізації таких заходів: широко застосовувати інформативні екранні заставки в банкоматах із зображенням банкомату (терміналу) без сторонніх пристроїв і елементів; проводити комплексну роз'яснювальну діяльність серед банківських працівників (співробітників служб безпеки, моніторингу, інкасаторів) щодо всіх наявних проявів карткового шахрайства та можливих способів боротьби з ним; проводити регулярний огляд банкоматів на предмет наявності сторонніх предметів або слідів їх встановлення; розробити внутрішні стандарти та процедури реагування при виявленні сторонніх пристроїв на банкоматах або слідів їх встановлення; встановити камери відео-спостереження на банкоматах; використовувати програмні способи виявлення накладок на банкоматах в момент їх встановлення та/або використання; забезпечення використання у термінальному обладнанні шифрування з використанням алгоритму Triple DBS; постійне впровадження серед клієнтів роз'яснювальної діяльності щодо дотримання правил безпеки та збереження конфіденційності при користуванні платіжними картками. Також, вітчизняним банкам необхідно прискорити процес переходу на карткові чіп-технології [3]. При використанні, для розрахунків за товари, роботи чи послуги в Інтернеті,

чіпових (EMV-стандарт) карток потрібна їх фізична наявність у особи, що намагається здійснити транзакцію, на відміну від пластикових карток із магнітною смужкою, що унеможливлює проведення незаконних операцій.

Підсумовуючи все вищесказане, слід відзначити, що всі без винятку банківські установи повинні постійно моніторити можливість виникнення будь-яких втрат при здійсненні всіх видів електронних розрахунків, належним чином оцінювати рівень ризиковості та ймовірність реалізації ймовірних загроз, при цьому забезпечуючи дієвість системи ризик-менджменту щодо попередження та протидії різного роду злочинам або шахрайствам, які можуть виникнути як під впливом зовнішніх, так і внутрішніх чинників. Розуміння ризиків, що виникають при здійсненні електронних розрахунків, зокрема ризиків шахрайства з платіжними картками, та реалізація ефективної політики управління ризиками, дасть змогу не тільки забезпечити фінансову стійкість і стабільну роботу банків, а й підвищити довіру населення до банківського сектора України загалом та всіх форм карткових розрахунків зокрема.

Список літератури:

1. Банківський сектор активно інвестує у розвиток карткового бізнесу [Електронний ресурс]. – Режим доступу : http://www.siogodennya.org.ua/?p=19602.
2. В Україні зростає фінансова кіберзлочинність [Електронний ресурс].– Режим доступу : http://news.finance.ua/ua/~/2/0/all/2013/12/15/314801.
3. Вядрова Н.Г. Шляхи протидії шахрайствам у сфері електронних розрахунків [Електронний ресурс].– Режим доступу : http://univd.edu.ua/general/publishing/konf/finbezpeka/24_vyadrova.pdf.
4. Колдовський М. В. Ризики використання банківських платіжних карток / М. В. Колдовський, О. М. Ващенко // Вісник Української академії банківської справи. – 2010. – № 1. – С. 45-49.
5. Круглый стол «Киберпреступность: украинские банки на линии удара» (информационно-аналитические материалы) [Електронний ресурс]. – Режим доступу : http://lfr.org.ua/ru/analytics/822-2013-26-11-analytics.html.
6. Мельник Ю.Б. Ризики у сфері банківського карткового бізнесу [Електронний ресурс]. – Режим доступу : http://www.cibs.ck.ua/parts/scien/stconf/10/tezy.pdf.
7. Моніторинг шахрайських операцій [Електронний ресурс]. – Режим доступу : http://www.ufn.com.ua/monitoring_fraud.html?lang=ua.
8. Офіційний сайт Української міжбанківської асоціації членів платіжної системи ЕМА [Електронний ресурс]. – Режим доступу : www.ema.com.ua/infoassociation /struktura-i-ustav.
9. Офіційний сайт European ATM Security Team (EAST) [Електронний ресурс]. – Режим доступу : http://www.european-atm-security.eu.

Галицейская Ю. Н.
Леськив О. М.
Тернопольский национальный экономический университет

ОСОБЕННОСТИ ПРОЯВЛЕНИЯ КАРТОЧНОГО РИСКА В СФЕРЕ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ: МЕЖДУНАРОДНЫЕ АСПЕКТЫ И ОТЕЧЕСТВЕННЫЕ РЕАЛИИ

Резюме
В статье анализируется состояние рынка платежных карт в Украине, рассматриваются вопросы возникновения риска операций с платежными картами. Предлагаются меры по минимизации рисков всех основных участников карточных расчетов: эмитента, клиента-пользователя, эквайера. Исследуются случаи мошенничества с платежными картами и инструменты снижения рисков карточного бизнеса.

Ключевые слова: платежные карты, карточный бизнес, эмитент, эквайер, скиминг, риски.

Halitseyska Ju. M.
Leskiv O. M.
Ternopil National Economic University

PECULIARITIES OF THE EXPRESSION OF CARD RISK IN THE SPHERE OF BANKING ACTIVITY: INTERNATIONAL ASPECTS AND NATIONAL REALITIES

Summary
The state of the payment cards market in Ukraine is analyzed and the issues of risk appearance with payment cards are revealed in the article. The measures to minimize the issuer's, client-user's and acquirer's risks are suggested. The cases of fraudulent transactions with payment cards and the instruments of card business risk reduction are investigated.

Key words: payment cards, card business, an issuer, a client-user, an acquirer, skimming, risks.