Розділ 1

АКТУАЛЬНІ НАПРЯМИ ЗМІЦНЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

УДК 336.051

М. В. Бодрецький

АНТИКРИЗОВЕ УПРАВЛІННЯ: БОРОТЬБА З ШАХРАЙСТВОМ ІЗ ВИКОРИСТАННЯМ ЕЛЕКТРОННОГО ОБЛАДНАННЯ (ПТКС)

Доведено, що розвиток електроніки в світі зумовив перехід готівкового грошового обігу в безготівкову форму не тільки серед суб'єктів господарювання, а й фізичних осіб. Визначено, що основним засобом здійснення безготівкових розрахунків фізичними особами залишається пластикова картка. Подано результати останніх досліджень у сфері методів і принципів, що застосовуються кібершахраями в Україні, описано обладнання шахраїв, надано науково обґрунтовані рекомендації для забезпечення мінімізації витрат банківської установи як складової антикризових дій у сфері управління банком.

Ключові слова: *кіберзлочин, ПТКС, шахрайство, кібершахраї, антикризове управління, банкомат, захист від шахрайства.*

Постановка проблеми. Антикризове управління охоплює методи та механізми протидії всім можливим подіям та/чи процесам, що можуть негативно впливати на банківську установу. Складовими потенційно небезпечних подій є більшість процесів банку. Що більше операцій здійснюється організацією, в тому чи іншому напрямі, то більша вірогідність збоїв і втрат. У ході аналізу можливостей забезпечення ефективного антикризового управління банківською установою автор аналізує різні процеси, які проводять банківські установи. В цій статті викладено результати дослідження питання створення механізмів захисту банківської установи від кіберзлочинів та шахрайських дій, пов'язаних із використанням електронного обладнання банку, такого, як банкомат, електронний кіоск тощо [1; 2].

Розвиток електроніки в світі обумовив переведення готівкового обігу в безготівковий не тільки серед суб'єктів господарювання, а й серед фізичних осіб. Основним засобом здійснення безготівкових

розрахунків фізичними особами залишається пластикова картка. Вона як «ключ» до рахунку фізичної особи (клієнта банку) є основною ціллю шахраїв, які за допомогою картки, або інформації, що міститься на ній, намагаються заволодіти грошовими коштами клієнтів банківських установ [3–5].

Стан дослідження. Науковцями, що активно займаються питаннями кіберзлочинів та протидії шахрайствам із використанням пластикових карток та електронного обладнання, є: Т. С. Вайда, Д. О. Губська, М. В. Іщук, О. В. Косаревська, О. І. Олійничук, О. М. Сарахман, В. Ю. Чуприна тощо. Науковий пошук у зазначеному напрямі ведеться не достатньо активно.

Метою цієї статті є збір, аналіз та донесення до фахівців (науковців і практиків) даних про методи роботи та обладнання шахраїв, які спеціалізуються на кіберзлочинах зі залученням ПТКС.

Виклад основних положень. Банки вимушені дедалі більше приділяти уваги протидії кіберзлочинцям та шахраям, що націлені на високотехнологічні злочини. Насамперед це пов'язано зі зростанням важливості для банків операцій, що здійснюються з використанням пластикових карток (далі – ПК, БПК, платіжна катка або картка). Чимраз більше банківських продуктів продається й обслуговується з використанням ПК. Нині з використанням ПК та системи Інтернет-банку клієнти мають можливість отримувати кредити, розміщати депозити, здійснювати платежі тощо. Банк, що не приділяє уваги емісії власних банківських ПК, майже виштовхується з ринку банківського обслуговування фізичних осіб, а це відображається на прибутках [6–10].

Окрім уваги до емісії як такої, важливою частиною роботи банківської установи є підтримання якості обслуговування ПК (або рахунків / карткових рахунків клієнтів). Важливе значення має впевненість клієнтів у захищеності їх коштів. А цей показник у довгостроковій перспективі погіршується. Хоча необхідно відзначити, що заходи, які здійснюються банківськими установами, регуляторами локальних банківських ринків, міжнародними платіжними системами та правоохоронцями майже всіх країн світу, значно стримують зростання шахрайських операцій в зазначеній сфері.

Так, 2017 року, за даними Національного банку України, кількість злочинів, у зіставленні з 2016 роком, знизилась. Однак загальний довгостроковий тренд спрямований на підвищення кількості кіберзлочинів та шахрайства з банківськими пластиковими картками [11; 12].

Значна частина випадків шахрайства з картками здійснюється із використанням точок контакту картки з обладнанням, спрямованим

на зчитування інформації з неї і здійснення платежів, оплат, переказів тощо. До такого обладнання відносяться банкомати, POS-термінали, електронні кіоски тощо. Зазначене обладнання має загальну назву – програмно-технічні комплекси самообслуговування. В ході дослідження питань боротьби з шахрайськими діями основна увага приділялась кіберзлочинам, що пов'язані саме з програмно-технічними комплексами самообслуговування [13–16].

У визначеному напрямі зусилля шахраїв зосереджені на отриманні даних магнітної смуги платіжної картки та ПІН-коду до неї, зловмисниками використовуються пристрої для незаконного зчитування інформації, які загалом іменують скімери або скімінгові пристрої. Для виявлення цих пристроїв при огляді банкоматів необхідно запам'ятати принципи та можливі місця їх встановлення.

Оскільки для будь-якої операції по отриманню готівкових коштів у банкоматі необхідні дані, що містяться на магнітній смузі та дані ПІН-коду, будь-який пристрій для незаконного зчитування цієї інформації можна умовно поділити на два окремі пристрої, які можуть бути і пов'язані між собою, і ні:

– пристрої для отримання даних магнітної смуги;
– пристрої для отримання даних ПІН-коду.

Такі пристрої містять магнітну головку зчитування, елементи живлення та елементи, що накопичують (або передають) отриману інформацію.

Властивістю встановлення таких пристроїв є те, що магнітна головка, яка завжди має бути на пристрої зчитування, має бути встановлена вздовж осі, по якій картка потрапляє в картоприймач або рухається в картоприймачі. Тобто магнітна головка має мати контакт із магнітною смугою картки під час проведення операції клієнтом.

Розрізняють два типи установки таких пристроїв:

– зовні банкомата;
– зсередини банкомата.

Зовнішні пристрої монтуються на лицьовій панелі банкомата, добре підібрані і по кольору, і по фактурі матеріалів із яких виготовляються. Шахрайське обладнання може встановлюватися на штатні картоприймачі, або замість них, а також імітувати їх передню частину. Головне завдання шахраїв виробити і встановити пристрій так, щоб клієнт уважав його стандартним елементом банкомата. З розвитком 3D-друку виготовити або придбати такі види «накладок» стає дедалі простішим. Якість пластику майже завжди висока. Виявити їх можливо при візуальному огляді банкомата з лицьової сторони. Пристрої можуть бути і приклеєні, і закріплені якісніше та жорсткіше. Основне

завдання при огляді виявити магнітну головку зчитування в разі зміни зовнішнього вигляду місця входу картки в картоприймач.

У ході дослідження вдалося виявити декілька видів (типів) скімерів, які використовуються для отримання інформації з ПК. В якості досліджуваного ПТКС використовувалися банкомати виробництва NCR Corporation.

Отримання доступу до коштів клієнтів на банківських рахунках за допомогою ПК є отримання даних про ПІН-код та ідентифікаційних даних ПК (її номера, строку дії, CVV-коду). Для отримання інформації про ПІН-код від картки використовуються такі види пристроїв:

– відеокамери;
– накладки на ПІН-клавіатуру.

Відеокамери розміщуються в різних місцях, але вони завжди направлені на ПІН-клавіатуру. Варіанти розміщення розмаїті. Ці пристрої можуть бути виконані і як фрагменти панелей, і мати вигляд лотка для розміщення рекламної продукції тощо. Будь-які зміни в зовнішньому вигляді лицьової панелі банкомата можуть свідчити про встановлення камери. Такі пристрої містять відеокамеру (найчастіше використовуються готові плати від мобільних пристроїв), накопичувач інформації (найчастіше використовуються флеш накопичувачі) та елементи живлення. Зазвичай від відеопристрою вимагається функціонування від 24-х годин. Однак нині трапляються й довгодіючі пристрої, і навіть пристрої, що передають інформацію на відповідний приймач, а також до мережі Інтернет. Особливістю цих пристроїв є доволі значні розміри, порівняно з іншими, оскільки енергоспоживання відеокамер порівняно з фальш-накладками на ПІН-клавіатуру або скімерами, які встановлюються на картридер, є значно більшим. Тому при виготовлені накладок зловмисники змушені використовувати акумуляторні батареї (наприклад, від мобільних телефонів) та інші джерела струму, які мають доволі габаритні розміри.

Окрім варіантів установлення камер на банкомат зафіксовані випадки монтажу камер на стелю/стіни приміщення розташування банкомата, що утруднює їх пошук та виявлення.

Для отримання даних про ПІН-код власника рахунку з коштами використовується накладка на ПІН-клавіатуру, яка є фальш-панеллю, що монтується на справжню клавіатуру та імітує її. Така накладка фіксує ПІН-код при вводі його клієнтом. Може бути використана і як накладка тільки над ПІН-клавіатурою, і закривати собою всю нижню панель, де встановлена ПІН-клавіатура.

Потрібно зазначити, що першим і головним етапом виявлення пристроїв для незаконного зчитування (отримання) інформації є вияв-

лення саме пристрою для отримання даних магнітної смуги, оскільки місце його встановлення завжди локалізовано біля картрідеру. Головка для зчитування даних завжди встановлена в місці, де є контакт з магнітною смугою картки, яка вставляється в банкомат. Теж саме відноситься до отворів через які проводиться підключення до плати картрідеру. В разі виявлення пристрою для отримання даних магнітної полоси, або характерних пошкоджень лицьової панелі тощо, наступним етапом є виявлення пристрою для фіксації ПІН-коду, оскільки одразу зрозуміти де встановлена фальш-панель з камерою або накладка на ПІН-клавіатурі не завжди вдається, особливо якщо камера добре замаскована або накладка на ПІН-клавіатуру виконана дуже якісно.

Джерелами отримання інформації про встановлення шахрайського обладнання на банкомати можуть виступати:

– працівники банку (інкасатори, відповідальні працівники за робочий стан ПТКС, працівники служби безпеки банку тощо);

– підрозділи інкасації інших банківських установ (юридичних осіб перевізників), з якими укладено договір на послуги з інкасації;

– клієнти банку;

– правоохоронці;

– інші особи.

За результатами проведеного обговорення з фахівцями банків сформовано такі рекомендовані дії для уникнення (або зменшення) витрат від шахрайських дій.

Після отримання інформації (чи самостійного виявлення) про встановлені скімінгові пристрої та накладки на ПТКС, необхідно негайно проінформувати керівництво банку (або службу безпеки банку).

Керівництву банку, після отримання інформації щодо виявлення шахрайського обладнання на ПТКС банку, доцільно:

– забезпечити інформування місцевого підрозділу правоохоронних органів про дану подію;

– надати доступ до ПТКС та можливість його огляду правоохоронцям, які задокументують факт виявлення шахрайського обладнання;

– здійснити фотофіксацію виду та способу встановлення шахрайського обладнання.

В разі виявлення пошкоджень банкомата, що характерні для підключення скімерів типу «зовнішня плата», доцільно розглянути питання віднесення пошкодження до страхового випадку. Задля чого необхідно проінформувати відповідного страховика.

Висновки. Проведене дослідження питань організації антикризових дій при боротьбі з шахрайством із використанням електронного

обладнання (ПТКС) надає якісний матеріал для вивчення варіантів шахрайського обладнання, їх видів та методів встановлення. Ознайомлення зі зібраними даними фахівців банків можуть бути як дієві антикризові заходи, що підвищать швидкість та вірогідність виявлення шахрайського обладнання. Сформовані рекомендації щодо реагування допоможуть виграти час та знизити вірогідні збитки.

1. Сарахман О. М., Шурпенкова Р. К. Аналітичні аспекти операцій з платіжними картками для розвитку сфери послуг. *Туристичні послуги на світовому ринку як фактор розвитку міжнародного туризму*: зб. матер. Міжнар. наук.-практ. конф. (м. Львів, 10 травня 2018 р.). Львів, 2018. С. 210–215.

2. Водовозов Є. Н., Палант О. Ю. Економіко-правові аспекти забезпечення електронних розрахунків на громадському транспорті. *Економічний вісник Запорізької державної інженерної академії* / ред. О. В. Коваленко. Запоріжжя, 2018. Вип. 1 (13). С. 92–98.

3. Губська Д. О. Правові питання забезпечення інформаційної і кібернетичної безпеки платежів. *Інформаційні технології та безпека*: матер. XVII Міжнар. наук.-практ. конференції. К., 2017. С. 52–62.

4. Косаревська О. В., Олексієнко Д., Дарвін О. Кіберзлочини у фінансово-банківській сфері: скімінг та способи його викорінення. *Кібербезпека в Україні: правові та організаційні питання*: матер. Всеукр. наук.-практ. конференції. Одеса, 2017. С. 101–102.

5. Олійничук О. І. Банківські картки як об'єкт шахрайства: стан і протидія явищу. *Актуальні проблеми правознавства*. 2017. Вип. 1 (9). С. 91–94.

6. Мельник С. С. Типологія фінансового шахрайства в українських комерційних банках. *Вісник Університету банківської справи.* 2017. № 1 (28). С. 65–70.

7. Олійничук О. І. Шахрайство з банківськими картками та шляхи протидії. *Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід*: матер. ІІ Міжнар. наук.-практ. конф.: *Економічна думка*. 2017. С. 374–377.

8. Вайда Т. С. Фішинг як сучасний вид інтернет-шахрайства з банківськими платіжними картками та заходи з профілактики цього кримінального злочину. *Кібербезпека в Україні: правові та організаційні питання*: матер. Всеукр. наук.-практ. конференції. Одеса, 2017. С. 61–65.

9. Лаврик С. С. Тенденції тіньової економіки України у розрізі схем і негативних факторів. *Фінанси, облік, банки.* 2017. № 1 (22). С. 241–249.

10. Іщук М. В. Безпека діяльності комерційних банків у мережі Інтернет: диплом. робота за освіт.-кваліф. рівнем «магістр»: спец. 8.18010014 «Управління фінансово-економічною безпекою магістер. програма – управління фінансово-економічною безпекою». Тернопіль, 2017. 104 с.

11. Некрасов В. Соціальна інженерія збагатила кібершахраїв на півмільярда: як українці стають жертвами. *Економічна правда.* 2018. URL: https://www.epravda.com.ua/publications/2018/01/31/633572/

12. Збитки українських банків від незаконних дій з платіжними картками зменшилися вперше з 2015 року / Прес-реліз Національного банку України від 31.01.2018. URL: https://bank.gov.ua/control/uk/publish/printable_article?art_id=63383127&showTitle=true

13. Степанова Н. М., Білошкурський М. В. Особливості управління міжнародним рухом фінансового капіталу у формі IPO. *Збірник матеріалів міжнародної науково-практичної Інтернет-конференції молодих учених і студентів «Фінансово-кредитні механізми розвитку національної економіки».* 2017. С. 91–92.

14. Чуприна В. Ю., Соболева А. Ю., Буряков Г. А. Безналичные расчеты и платежи в разрезе качественных изменений национальной платежной системы. *Инновационные технологии в науке и образовании*: материалы IX Междунар. науч.-практ. конф.: в 2 т. Т. 2. 2017. № 1. С. 195–201.

15. Чуприна В. Ю., Зайцева Т. В. Тенденции и перспективы развития рынка банковских продуктов и услуг в Российской Федерации. *Экономическая наука сегодня: теория и практика*: материалы IV Междунар. науч.-практ. конф. 2016. С. 163–166.

16. Сергєєва О. С., Матвієнко С. О. Перспективи розвитку Cashless Economy в Україні. *Східна Європа: економіка, бізнес та управління.* Вип. 3 (08). 2017. С. 313–316.

Bodretskiy M. V. Anti-crisis management: combating fraudsters which using electronic equipment (payment terminals and ATMs)

The development of electronics in the world led to the transfer of cash circulation to non-cash form, not only among business entities, but also among individuals. The main tool for the implementation of cashless payments by individuals, since its inception, remains a plastic card. A plastic card as a «key» to an account of an individual (a bank client) is the main purpose of fraudsters who, using a card or information contained on a card, try to seize funds from customers of banking institutions. The article reflects the results of recent research in the field of methods and principles of actions by cyber-cheaters in Ukraine, describes the equipment of fraudsters and provides scientifically based recommendations to ensure minimization of costs for a banking institution as a component of anti-crisis actions in banks.

The study found that banks are forced to increasingly focus on countering cybercriminals and fraudsters targeting high-tech crime. This is due to the growing importance of plastic cards for banks. More and more banking products are sold and serviced using plastic cards. Today, with the use of plastic cards and the Internet Bank system, customers have the opportunity to receive loans, place deposits, make payments, etc. The bank, which does not pay attention to the issue of its own bank plastic cards, practically does not have the opportunity to work in the market of banking services of individuals.

The maintenance of the quality of service of plastic cards is an important part of the work of a banking institution. And here the role of the customer's confidence in the security of their funds plays a huge role. This indicator is deteriorating in the long run. Although it has been determined that measures taken

by banking institutions, central banks, international payment systems and law enforcement in almost all countries of the world significantly restrain the growth of fraudulent operations in this area. It was established that in 2017, according to the National Bank of Ukraine, the number of crimes has decreased (in comparison with 2016). However, the overall long-term trend is aimed at increasing the number of cybercrime and fraud with bank plastic cards.

Key words: *Cyber-crime, Payment terminals, Fraud, cyber-cheaters, anti-crisis management, ATM, fraud protection*

Стаття надійшла 29 жовтня 2018 р.