бути негайною [4, с. 112–113]. До таких поліцейських заходів уявляється за можливе віднести застосування примусових поліцейських заходів.

Підсумовуючи викладене, можемо констатувати, що поліцейські заходи, застосування яких урегульовано адміністративно-правовими нормами, є втіленням адміністративного примусу у правоохоронній діяльності поліції.

Список бібліографічних посилань

1. Про Національну поліцію : закон України від 02.07.2015 № 580-VIII. *Відомості Верховної Ради України.* 2015. № 40–41. Ст. 379.

2. Адміністративна діяльність. Частина особлива : підручник / за заг. ред. О. М. Бандурки. Харків : Еспада, 2000. 368 с.

3. Адміністративна діяльність : навч. посіб. / М. В. Ковалів, З. Р. Кісіль, Д. П. Калаянов та ін. Київ : Прав. єдність, 2009. 432 с.

4. Коломоєць Т. О. Адміністративний примус у публічному праві України: теорія, досвід та практика реалізації : монографія / за заг. ред. В. К. Шкарупи. Запоріжжя : Поліграф, 2004. 404 с.

Одержано 27.10.2017

УДК 004.056:55(043.2)(477)

Ксенія Олександрівна КРАТАСЮК,
курсант групи Ф4-202 факультету № 4
Харківського національного університету внутрішніх справ

Науковий керівник:
Віталій Анатолійович СВІТЛИЧНИЙ,
кандидат технічних наук,
доцент кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ

ПРОТИДІЯ КІБЕРШАХРАЙСТВУ ЩОДО ВИКОРИСТАННЯ ПРИСТРОЇВ ДЛЯ НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ БАНКОМАТІВ

На сучасному етапі розвитку українського суспільства банківські пластикові картки впевнено займають одне з головних місць в системі фінансово-економічних відносин

громадян. Проте разом з перевагами використання даного засобу електронного розрахунку або зберігання грошового капіталу, пересічний громадянин може стикнутися з деякими проблемними ситуаціями, що можуть загрожувати його економічному добробуту. Однією з таких проблем є шахрайство з використанням віртуального електронного простору (кіберпростору), коли зловмисник з одного боку використовує конфіденційні реквізити електронних платіжних карток для особистого збагачення, а з іншого використовує пластикові електронні картки для отримання коштів, які були зараховані на рахунок від довірливих громадян.

Ще одна очевидна причина пожвавлення скіммінгу в Україні – збільшення обсягу грошових коштів, які проходять через банківські карти. На даний момент він збільшився в кілька разів, тому шахрайство в даному секторі залишається дуже прибутковою справою. При великому ринку шахрайства в онлайн-банкінгу і системах дистанційного банківського обслуговування для юридичних осіб, новий ринок привернув українських та іноземних хакерів, тому що населення країни набагато гірше навчено правилам безпеки при використанні пластикових карт, як в банкоматі, так і в Інтернеті. Свою роль відіграють і інші особливості української кіберзлочинності: надприбутки, ілюзія безкарності і слабке законодавство.

Скіммінг (від англ. skim – знімати вершки) – створення копії магнітної смуги для виготовлення клону карти користувача за допомогою спеціалізованих пристроїв, які називаються скімери і шиммери і найчастіше встановлюються на банкомати. За принципом дії ці пристрої не відрізняються один від одного і потребують використання прихованих відеокамер або накладок на клавіатуру банкомату для отримання PIN – коду [1]. Скіммер – технологічно просте, велике за розміром і незначне за ціною пристрій. А ось шиммер – абсолютно непомітний при підключенні до банкомату. Скіммер, крім того, що він помітний неозброєним оком на картридері, може відчуватися як перешкоди при введенні банківської карти в картрідер. «Шимер» підсаджується за допомогою спеціальної карти – носія: її просовують у щілину банкомату, де тонкий «шиммер» приєднується до контактів, що прочитує дані з карт, після чого картканосій видаляється. Далі все працює, як і при традиційному скіммінгу – тобто вставляються в банкомат пластикових

карт, де зчитуються всі важливі дані «дампи», які потім використовуються зловмисниками для виробництва карток – дублікатів та зняття з їх допомогою грошей. Єдине, але дуже важливе на відміну від скіммінгу полягає у відсутності будь-яких зовнішніх ознак шиммінгу того, що в банкоматі сидить «жучок». Виходячи зі специфікацій, що регулюють розміри щілини картрідера, товщина «шиммера» не повинна перевищувати 0,1 мм [1], інакше він буде заважати пластиковим картам. Це приблизно вдвічі тонше людської волосини. На щастя вартість таких пристроїв відносно скіммерів велика, тому вони поки ще не поширені в Україні. Тобто в нашій країні почастішали випадки саме скімінгу [2]. Діють шахраї приблизно таким чином: на щілину банкомату, куди вставляється картка, а також на клавіатуру поміщаються спеціальні пристрої – накладки. Перша копіює інформацію з магнітної смуги картки, друга – запам'ятовує персональний ідентифікаційний номер (далі – PIN-код). Буває, що PIN-код «підлягає» мініатюрна замаскована (наприклад рекламними матеріалами) відеокамера, яка також непомітно розміщується десь на банкоматі або десь біля нього.

Потім досить швидко шахраї знімають накладки з банкомату та виготовляють дублікат картки. Знаючи PIN-код, вони можуть вичистити її «під нуль».

Основні способи захисту:

1. По можливості обмежте використання банкоматів в принципі, тому що більшість карт компрометуються саме в них, використовуйте віртуальні картки для оплати покупок і мережі Internet.

2. Кожен раз, навіть користуючись знайомим Вам банкоматом, оглядайте його на предмет наявності підозрілих пристроїв (накладок на кардрідер, прихованих камер відеоспостереження, підозрілих панелей на банкоматі).

3. Спробуйте підчепити край клавіатури для введення ПІН-коду нігтем, банковською карткою або іншим плоским предметом. Якщо на клавіатурі є шахрайська накладка, вона може відокремитися, тому що приклеюють її зазвичай двостороннім скотчем, або суперклеєм.

4. Не соромтесь активно перевірити антискіммінгову накладку на картрідері. Санкціонована накладка не відірветься, тому що вона антивандальна, шахрайська ж може від'єднатися.

5. Вводячи ПІН-код прикривайте долоню і клавіатуру другою рукою або гаманцем, щоб навіть встановлена біля банкомату відеокамера не зняла введені цифри.

6. Встановіть ліміт на зняття готівки в банкоматі максимум одну операцію в день. Можливо, Вам буде складніше користуватися банкоматом, зате шахраї не зможуть «обнулити» весь Ваш рахунок.

7. По можливості використовуйте картки з чіпом. Такі карти більше захищені від скіммінгу, і опротестувати шахрайську операцію буде простіше.

8. Якщо банкомат встановлено в офісі банку не є гарантією, що на ньому не встановлено скіммінговий пристрій. Кожен раз, навіть користуючись знайомим вам банкоматом, оглядайте його на предмет наявності підозрілих пристроїв (накладок на картрідер, прихованих камер відеоспостереження, підозрілих панелей на банкоматі).

9. У випадку некоректної роботи банкомату – якщо він довгий час перебуває в режимі очікування або мимоволі перезавантажується – відмовтеся від його використання. Велика ймовірність того, що він перепрограмований зловмисниками.

10. Ніколи не піддавайтесь допомозі порадам сторонніх осіб при проведенні операцій з банківської картки в банкоматах. Зв'яжіться з Вашим банком – він зобов'язаний надати консультаційні послуги по роботі з картою.

11. У торгових точках, ресторанах і кафе всі дії з Вашою картою повинні відбуватися у Вашій присутності. В іншому випадку шахраї можуть отримати реквізити Вашої картки за допомогою спеціальних пристроїв і використовувати їх в подальшому для виготовлення підробки.

12. Найголовніше. Банківська картка як і гаманець не є засобом для накопичення фінансових коштів або здійснення значних платежів.

Список бібліографічних посилань

1. Світличний В. А. Сучасні кіберзлочини з втручанням в роботу банкоматів // Використання сучасних інформаційних технологій в діяльності національної поліції України : матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 25 листоп. 2016 р.). Дніпро : Дніпропетровськ. держ. ун-т внутр. справ, 2016. С. 84–85.

2. Сюрприз для банкомата: вирусы и способы защиты от них // Prostobankir.com.ua : сайт. URL: http://www.prostobankir.com.ua/it/stati/syurpriz_dlya_bankomata_virusy_i_sposoby_zaschity_ot_nih (дата звернення: 28.10.2017).

Одержано 30.10.2017

УДК 159.9(477)

Марина Олександрівна МАЛЬКОВА,
курсант групи ФЗ-109 факультету № 3
Харківського національного університету внутрішніх справ

Науковий керівник:
Вікторія В'ячеславівна ДОЦЕНКО,
кандидат психологічних наук, доцент,
доцент кафедри педагогіки та психології факультету № 3
Харківського національного університету внутрішніх справ

РОБОТА ПСИХОЛОГА З ДІТЬМИ, ЯКІ ЗАЗНАЛИ НАСИЛЬСТВА В СІМ'Ї

Насильство в сім'ї – це комплексна проблема сучасного суспільства, що має всебічно вирішуватися державними органами та зусиллями громадськості. Жертвою насильства в сім'ї може стати будь-яка людина, незалежно від віку, статті, освіти, фізичної підготовки. Проте, особливо незахищеною і вразливою частиною населення є діти, які повністю залежать від дорослих, і, перебуваючи в ситуації насилля, часто не здатні впоратися з нею самостійно.

Дитина, яка постраждала від жорстокого ставлення з боку батьків чи близьких людей відчуває різні негативні емоції і почуття. Але в силу відсутності життєвого досвіду може вважати, що насильницькі взаємини, є нормальними. Тому дитина мовчить і не просить допомоги, що ускладнює як процес виявлення насилля так і процес надання їй психологічної допомоги. Тоді як кваліфікована допомога фахівця вкрай необхідна постраждалій від насильства дитині, адже наслідки можуть мати як безпосередній так і відстрочений характер впливу на її незрілу психіку. Так, найближчими наслідками пережитого дитиною насилля є [1–3]:

– фізичні травми, пошкодження частин тіла і внутрішніх органів;