Кравчук Д.Д.

СПОСОБИ ЗЛОЧИННОГО ПРОФЕСІОНАЛІЗМУ У СФЕРІ НЕЗАКОННОГО ВИКОРИСТАННЯ ПЛАТІЖНИХ КАРТОК, ПОВ'ЯЗАНИХ ІЗ ВТРУЧАННЯМ У РОБОТУ БАНКОМАТІВ

УДК 343.9:8

Актуальність теми. Однією з найгостріших проблем, з якою зіткнулася Україна і міжнародне співтовариство протягом останнього десятиліття є злочинність у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів.

Зростання банківських технологій, зумовило не тільки швидкий розвиток і ефективне застосування їх в повсякденному житті, а й зростання нових загроз. Легкодоступність до платіжних карток та банкоматів, а також можливість приспособлень різних високотехнологічних пристроїв для використання їх у злочинних цілях є основними причинами використовувати всі ці переваги для вчинення злочинних дій і не бути піймаными.

Важливу роль для вивчення злочинності у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів відіграє дослідження способів вчинення злочину. При цьому у кримінологічній науці вказана проблема залишається однією із найменш досліджених, хоча спосіб вчинення злочину має важливе практичне значення не тільки при розслідуванні злочинів вказаної категорії, але й при попереджувальній діяльності.

Аналіз досліджень даної проблеми. Дослідженню комплексу проблем які пов'язані із способами вчинення злочинів, а зокрема і способів вчинення злочинів у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів у своїх працях висвітлювали А.І. Бойцова, В.М. Валіневич, А.А.Вознюк, В.І. Василинчук, Ю.В. Гавриліна, С.М. Зав'ялов, Г.Г. Зуйкова, О.В. Оропай, Н.В. Павлової, Н.І. Панова, В.В.Тіщенка, С.С.Чернявський, М.Г. Шурухнова та інші.

Не заперечуючи вагомого внеску наукових праць згаданих учених для дослідження даної проблеми існує відсутність комплексної кримінологічної розробки і теоретичного вивчення способів вчинення злочинів у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів професійними злочинцями.

Постановка мети. Метою статті є характеристика основних способів вчинення злочинів у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів професійними злочинцями, які повинні лягти в основу подальшої боротьби з даним негативним явищем.

Виклад основних положень. Спосіб вчинення злочину є елементом злочинної поведінки, та представляє собою певну систему послідовних актів поведінки. Варто звернути увагу, що спосіб вчинення злочину професійними злочинцями є витонченим та складається з взаємопов'язаних та взаємозалежних дій, що спрямовані безпосередньо на підготовку, вчинення, а також приховання злочину використовуючи свої професійні вміння та навички. Як зазначає С.М. Зав'ялов, ці акти поведінки – дії, операції, прийоми – сполучаються за певною ієрархією і субординацією як частини цілеспрямованої вольової діяльності. Автор дотримується думки, що у злочинній діяльності, виконавець має власну систему способів дій, спрямованих на досягнення бажаного результату, а власне спосіб вчинення злочину безпосередньо пов'язаний з фізичними, функціональними та професійними можливостями злочинця, зумовленими багато в чому як самим характером злочину, так і зовнішніми умовами, за яких він вчиняється [1].

Криміналісти зазначають, що спосіб вчинення злочину – це система дій з підготовки, скоєння і приховування злочину, детермінована умовами зовнішнього середовища і психологічними якостями особи, пов'язаними з виборчим використанням відповідних засобів та умов місця і його часу[2,3,4].

Розглянувши дане твердження відповідно до мети нашої роботи можна визначити, що способи вчинення злочинів у сфері незаконного використання платіжних карток пов'язаних із втру-

чанням у роботу банкоматів професійними злочинцями – це стійка система дій спрямована на підготовку, скоєння і приховування злочину, детермінована умовами сучасного середовища, пов'язана з використанням професійних умінь і навичок особи для досягнення мети, та є джерелом засобів її існування.

Для дослідження способів вчинення злочинів у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів було досліджено останні доступні статистичні матеріали. Адже, слід мати на увазі те, що банки, як правило, не прагнуть розголошення інформації щодо збитків, які їм були заподіяні успішними шахрайськими діями, оскільки ці факти негативно позначаються на іміджі банку, тому проблема може носити більш загрозливий характер. Отож дане процентне відношення може мати набагато більший показник. Кількість махінацій у банківській сфері із використанням платіжних карток, накладок та інших способів незаконного заволодіння коштами за 2 квартал 2016 року виросло на 80 % [5]. За вересень 2016 року згідно отриманої інформації з центрального офісу ПАТ «Райффайзен Банк Аваль» злочинцями вчинено 15 крадіжок способом вилучення банкнот через шаттер банкомату. Внаслідок цих незаконних дій злочинцями було викрадено 102,2 тисяч гривень банківських коштів. Окрім того, протягом двох тижнів жовтня 2016 року банком втрачено понад 1,8 мільйона гривень способом вирізання отворів на лицевій панелі банкомату поруч з картко приймачем та клавіатурою [6].

Сервіс банківських установ дозволяє здійснювати більшість операцій дистанційно, управляти рахунками з будь-якого місця з використанням програмно-апаратних засобів. Понад сотні банків в Україні використовують внутрішньодержавні й міжнародні платіжні системи, здійснюють емісію і еквайринг платіжних карток, тож способи незаконного втручання в роботу банкоматів та розміри збитків через це щорічно збільшуються. Сучасний стан злочинів, що вчиняються у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів, характеризується високим рівнем професіоналізму, постійним удосконалюванням злочинцями способів вчинення таких діянь.

Спираючись на практику боротьби зі злочинами у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів дозволяє виділити дві основні групи способів їх вчинення:

1) пов'язані з незаконним використанням платіжних карток, технічних пристроїв з подальшим зняттям готівки з банкомату до яких можна віднести наступні: викрадення платіжних карток у законного держателя, створення ситуацій, коли інформація про картку розголошується законним держателем, створення фіктивних фірм по обслуговуванню розрахунків з використанням банківських платіжних карток (у т. ч. у мережі Інтернет), одержання справжньої платіжної картки за підробленими документами, злочинна змова з працівниками банківських структур, використання неодержаних законним держателем платіжних карток.

2) пов'язані з незаконним проникненням до банкомату шляхом використання технічних пристроїв, знищення чи пошкодження корпусу банкомату або встановлення фальшивого банкомату[7].

Проте з поданих вище груп потрібно виділити ті способи які потребують певних умінь і навичок, та характеризують особу, як «професійного злочинця».

До першої групи можна віднести такі злочинні дії як траппінг (ліванська петля), фішінг, вішінг, скімінг (шимінг), фальсифікація карток. Дані способи, злочинних дій ми постараємось детально описати.

Траппінг (ліванська петля) (*Lebanese loops)* - це новий спосіб шахрайства, який дозволяє сторонній особі заволодіти вашою пластиковою карткою.«Ліванська петля» в більшості випадків являє собою пластиковий конверт, який не перевищує розмірів звичайної пластикової карти. Принцип виготовлення пристрою є досить простий. З фотоплівки або будь-якого іншого матеріал шахрай виготовляє петлю. Потім цей пристрій швидко встановлюється в картрідер банкомату, а кінці «ліванської петлі» непомітно закріплюються зовні. У момент, коли карта потрапляє в пастку, зловмисник виявляється поруч з потерпілим і пропонує йому ввести повторно ПІН-код, мотивуючи це тим, що з ним наперe-

додні сталася подібна ситуація і це допомогло повернути карту. Після «неуспішних» вводів ПІН-коду пластик, природно, не повертається, і шахрай радить звернутися в банк. Коли потерпілий йде, конверт разом з картою витягується шахраєм з банкомату. В результаті у злочинця не тільки виявляється картка потерпілого, а й інформація про її ПІН-код[8].

Так званий Фішінг – (*phishing*) вид злочинних дій, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти, інтернет-магазинів[9]. Злочинці використовують усілякі способи, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані. Типовий приклад фішінгу, коли клієнти якої-небудь платіжної системи отримують повідомлення по електронній пошті нібито від адміністрації або служби безпеки даної системи з проханням вказати свої рахунки, паролі і т.п. При цьому посилання в повідомленні веде на підроблений сайт, на якому і відбувається крадіжка інформації. Сайт цей знищується через деякий час, і відстежити його творців в інтернеті досить складно.

Вішінг (*vishing - voice phishing*) названий так за аналогією з фішінгом. Подібність назв підкреслює той факт, що принципової різниці між вішінг і фішингом немає. Основна відмінність вішінгу в тому, що так чи інакше задіюється телефон. Схеми обману у випадку вішінг, ті ж самі що і у фішінгу. Тільки у випадку вішінгу в повідомленні міститься прохання зателефонувати на певний міський номер. При цьому зачитується повідомлення, в якому потенційну жертву просять повідомити свої конфіденційні дані. Наприклад, ввести номер картки, паролі, PIN-коди, коди доступу або іншу особисту інформацію в тоновому наборі. Перші епідемії вішінгу в Україні зафіксовані у 2006 році[10].

Скімінг (*skim*) є найбільш розповсюдженим способом заволодіння інформації про реквізити картки. Треба зауважити, що технологія копіювання запису магнітної смуги за допомогою підставних пристроїв зчитування дістала широкого застосування серед професійних злочинців. Сучасні «скімери» мають розмір сірникової коробки, працюють від пальчикових батарейок і

вміщують до 200 номерів карток. На таку операцію витрачається 1–2 с. Відповідний електронний пристрій накладається на витвір для приймання картки. Спеціалізоване обладнання для кодування магнітних стрічок або обладнання, функціональність якого надає можливість зчитувати / записувати інформацію на магнітну смугу, є загально поширеним і може бути зроблене тільки людиною з відповідною технічною освітою, тобто «професійними злочинцями».

При здійсненні цієї злочинної операції може використовуватися комплекс скімінгових пристроїв:

1. Інструмент для зчитування магнітної доріжки платіжної картки – пристрій, що встановлюється на картоприймач, також може встановлюватися і картрідер на вхідних дверях в зону обслуговування клієнтів у приміщенні банку. Зовні воно являє собою пристрій з системою зчитування магнітної голівкою, підсилювачем – перетворювачем, пам'яттю і перехідником для підключення до комп'ютера.

Скімери можуть бути портативними, мініатюрними. Основне завдання скімінгу – копіювати необхідні дані (вміст доріжки / трека) магнітної смуги карти для подальшого відтворення її на підроблену карту, так званий «білий пластик». Таким чином, при оформленні операції з підробленою карткою авторизаційний запит і списання грошових коштів за шахрайською транзакції будуть здійснені з рахунку оригінальної, «скіммірованної» карти.

2. Мініатюрна відеокамера, залежно від моделі банкомата, може бути вмонтована в сам «скімер», або виготовлятися у вигляді планки під козирок банкомату або сторонніх накладок над вікном видачі купюр. Головне завдання встановити на банкомат і направити на клавіатуру введення – використовується разом зі скімерами для отримання ПІН-кода держателя, який використовується шахраями для отримання готівки в банкоматах за підробленою картою.

Ці пристрої живляться від автономних джерел енергії – мініатюрних батарей електроживлення, і, для ускладнення виявлення, як правило, виготовляються і маскуються під колір і форму банкомату. Шиммінг являє собою різновид скімінгу. У цьому випадку в

картрідер банкомату поміщається електронний пристрій (шимер), що дозволяє отримати інформацію про банківську карту. Товщина шиммера– близько 0,2 мм. Зовнішнє визначення використання шиммера вкрай ускладнено.

3. Клавіатурні насадки накривають існуючі клавіатури справжніх банкоматів, запам'ятовують і накопичують інформацію про набраний PIN-код. Злочинці можуть застосовувати спеціальне (одноразове) прозоре напилювання на клавіатуру. Після користування банкоматом на клавішах клавіатури залишаються сліди, що відповідають задіяним цифрам PIN-коду.

Фальсифікація платіжних карток визначають носії інформації, які, у свою чергу, обумовлюють наявність обов'язкових реквізитів і певних засобів захисту картки від підроблення. Трапляється два типи підроблення:

– фальсифікація справжньої картки (часткове підроблення);

– незаконне виготовлення нової картки(повне підроблення).

Часткове підроблення – це фізична зміна інформації на поверхні картки та/або перекодування електронної інформації на магнітній стрічці з подальшим її використанням. З цією метою використовуються чужі (викрадені, знайдені) або власні картки.

Основним способом часткового підроблення є перекодування вмісту магнітної смуги, що призводить до зміни інформації, яка міститься у картці. Цей спосіб є складним і потребує досконалого обладнання та певного професіоналізму. Для цього використовують спеціальний прилад –«декодер», який при з'єднанні з комп'ютером зчитує та розкодовує інформацію, що міститься на магнітній смузі і записує нову інформацію.

Перекодування смуги може здійснюватись у сукупності зі зміною інформації на пластикові, так і самостійно. В останньому випадку злочинці використовують не лише викрадені або загублені картки, а й свої. Як правило, ці картки використовують під час розрахунків за речі та послуги і зовні не викликають підозри. За наявності інформації щодо ПІН-коду за допомогою перекодованої картки можливе зняття готівки з банкомату, оскільки цей програмно-апаратний комплекс сприймає лише вміст магнітної смуги.

Повне підроблення полягає у виготовленні картки з використанням чистого шматка пластику, на який наносять усі необхідні реквізити, включаючи магнітну смугу, в якості якої використовується звичайна відеоплівка. Як пластиковий бланк картки використовують інші картки, що не є платіжними, але також мають магнітну смугу (перепустки, клубні та дисконтні картки, готельні картки-ключі тощо) або бланки пластикових карток з вмонтованою магнітною стрічкою, що можуть викрадатися з підприємств-виробників банківських платіжних карток. Цей спосіб підроблення дістав назву «білого пластику» («WhitePlasticFraud»). Для приховання ознак підроблення і надання їй вигляду справжньої картки на її поверхню наклеюють спеціальну кольорову плівку, що робить білий пластик схожим на справжню банківську картку. На магнітну смугу наносять інформацію щодо реквізитів картки, отриманої незаконним шляхом. Ця картка зовні виглядає як справжня і використовується до сплати як у крамницях, так і банкоматом для отримання готівки[7].

До другої групи можна віднести способи пов'язані з незаконним проникненням до банкомату шляхом використання технічних пристроїв, встановлення фальшивого банкомату (фантома), перелаштування справжніх банкоматів таким чином, щоб кошти, які видає банкомат згідно запиту клієнта, застрягали в слоті отримання готівки(шаттерінг).

Дані способи потребують більш детальнішого теоретичного обґрунтування.

Фантоми - це встановленні фальшиві банкомати, які зовнішнім виглядом мало чим відрізняються від справжніх (програмне забезпечення подібне), але готівки не видають. Після введення картки та набирання персонального ідентифікаційного номеру (ПІН-коду) на дисплеї фальшивого банкомату з'являється напис про те, що грошей у банкоматі немає (або про будь-яку несправність). Фальшивий банкомат не підключений ні до однієї з платіжних систем, а просто збирає дані магнітної стрічки та ПІН-коди держателів карток. До того ж у режимі реального часу він може передавати отриману протиправним шляхом інформацію про справжні платіжні картки через Інтернет до будь-якої точку світу.

Шаттерінг - це використання спеціального пристрою, який встановлюється всередині «презент ера» банкомату через «шаттер», що відкривається для видачі коштів під час отримання клієнтом готівки.

Злочинець, використовуючи справжню карту, маніпулює пристроєм у вигляді вилки, який використовується злочинцями для фіксації шторки та виймання готівки з банкомату. Зловмисник ініціює операцію на невелику суму з метою установки в диспенсер (в отвір для видачі готівки) такої «вилки». Далі замовляє велику суму та одночасно, притримуючи шторку диспенсера, симулює ситуацію «помилки запиту в умовах відсутності доступу до грошей».

Одночасно «софт» банкомата направляє «solicitedstatus», який каже про те, що «при видачі відбувся збій обладнання, клієнт до набраної суми доступу не мав». Злочинець робить відміну раніше списаної суми та баланс його карти не змінюється. Між тим, «вилка» з грошима виймається з банкомата з можливим одночасним пошкодженням «шаттера» (шторки). Кількість повторів в одному банкоматі залежить від працездатності АТМ та лінії поведінки злочинця.

Висновки. Способи вчинення злочинів у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів професійними злочинцями – це стійка система дій спрямована на підготовку, скоєння і приховування злочину, детермінована умовами сучасного середовища, пов'язана з використанням професійних умінь і навичок особи для досягнення мети, та є джерелом засобів її існування.

Характеристика способів вчинення злочинів дозволяє виявити мотиви, цілі, життєві установки, потреби, що дозволяють розкрити проблеми не тільки окремого злочину даної групи, але й загалом злочинності в сфері незаконного використання платіжних карток пов'язаних із втручання у роботу банкоматів професійними злочинцями, і як наслідок більш ефективно боротися з нею.

1. Зав'ялов С. М. Спосіб вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю : автореф. дис... канд.

юрид. наук: 12.00.09 / С. М. Зав'ялов ; Нац. акад. внутр. справ України. – К., 2005. – 19 с.

2. *Гаврилин Ю. В. Криминалистика: методика расследования отдельных видов пре ступлений : курс лекций / Ю. В. Гаврилин, Н. Г. Шурухнов ; под ред. профессора Н. Г. Шурухнова. – М. : Книжный мир, 2004. – С. 52.*
3. *Зуйков Г. Г. Криминалистическое учение о способе совершения преступления : дис. ... д-ра юрид. наук: 12.00.09 / Г. Г. Зуйков. – М., 1970. – С. 205.*
4. *Тищенко В. В. Подготовка преступления как объект криминалистического исследования / В. В. Тищенко // Актуальные проблемы криминалистики : материалы международной научно-практической конференции. – Х., 2003. – С. 94.*
5. *Платежное мошенничество: актуальная инфографика (итоги 2-го квартала 2016 года) [Електронний ресурс] //Режим доступу до ресурсу: http://ema.com.ua/payment-fraud-actual-infographics-results-2-q-2016/*
6. *Статистика пошкодження та викрадення готівкових коштів із банкоматів [Електронний ресурс] // ПАТ «Райффазен Банк Аваль» – Режим доступу до ресурсу: https://www.aval.ua/press*
7. *Організація розслідування злочинів, пов'язаних із заволодінням грошима шляхом утручання в роботу банкоматів [Текст] : метод. рек. / [С. С. Чернявський, В. І. Василинчук, В.М, Валіневич, О.В. Оропай та ін.]. – К. : Нац. акад. внутр. справ, 2013. –68 с.*
8. *Трапінг [Електронний ресурс] // Незалежна асоціація банків України. – Режим доступу до ресурсу: http://anticyber.com.ua/article_detail.php?id=140*
9. *Глосарій: фішінг [Електронний ресурс] // Українська міжбанківська асоціація членів платіжних систем «Ема». – Режим доступу до ресурсу: http://ema.com.ua/terms/#16*
10. *Вішинг [Електронний ресурс] // Матеріали вільної енциклопедії «Вікіпедія».– Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D1%88%D0%B8%D0%BD%D0%B3*

Кравчук Д.Д. Способи злочинного професіоналізму у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів.

Важливу роль для вивчення злочинного професіоналізму у сфері незаконного використання платіжних карток пов'язаних із втручанням у роботу банкоматів відіграє дослідження способів вчинення злочину. При цьому у кримінологічній науці вказана проблема залишається однією із найменш досліджених,

хоча спосіб вчинення злочину має важливе практичне значення не тільки при розслідуванні злочинів вказаної категорії, але й при попереджувальній діяльності.

Ключові слова: спосіб, злочинність, професійна злочинність, платіжні картки, банкомат.

Кравчук Д.Д. Способы преступного профессионализма в сфере незаконного использования платежных карточек связанных с вмешательством в работу банкоматов.

Важную роль для изучения преступного профессионализма в сфере незаконного использования платежных карточек связанных с вмешательством в работу банкоматов играет исследование способов совершения преступления. При этом в криминологической науке данная проблема остается одной из наименее исследованных, хотя способ совершения преступления имеет важное практическое значение не только при расследовании преступлений указанной категории, но и при предупредительной деятельности.

Ключевые слова: способ, преступность, профессиональная преступность, платежные карточки, банкомат.

Kravchuk D.D. Methods of criminal professionalism in the illegal use of payment cards associated with interference in the work of ATMs.

An important role for the study of criminal professionalism in the illegal use of payment cards relating to interfere with the ATM plays a research ways of commiting a crime. Thus in criminological science specific problem remains one of the least studied, although the way the offense is of great practical significance not only in the investigation of crimes of this category, but also in preventive activities.

Keywords: way, crime, professional crime, credit cards, ATM.

Красій М.О.

ВИРОК З ТОЧКИ ЗОРУ КРИМІНАЛЬНО-ПРАВОВОЇ, КРИМІНАЛЬНОЇ ПРОЦЕСУАЛЬНОЇ ТА КРИМІНАЛЬНО-ВИКОНАВЧОЇ ПОЛІТИКИ

УДК 343.13

Постановка проблеми. Винесення вироку є завершальною стадією судового розгляду, а вирок є найважливішим актом правосуддя. Від рішення суду залежить доля підсудного, тому доктрина, законодавець та практика спрямовані на винесення законних, обґрунтованих та вмотивованих вироків для досягнення завдань кримінального судочинства. Важливим є також питання,