УДК 343.3

О. М. Лепеха

ОПЕРАТИВНО-РОЗШУКОВА ХАРАКТЕРИСТИКА СПОСОБІВ ЗАВОЛОДІННЯ ГРОШИМА ТА ОСОБЛИВОСТІ ОПЕРАТИВНОГО ВИЯВЛЕННЯ ПІДРОБКИ ПЛАТІЖНИХ КАРТОК

Розглянуто зміст методів та способів реалізації злочинного наміру щодо викрадення інформації з подальшим її використанням за допомогою підроблених платіжних карток як невід'ємних елементів оперативно-розшукової характеристики злочинності із платіжними картками. Описано технологічні особливості підробки пластикових карток. Обґрунтовано необхідність орієнтування в специфіці підробки пластикових карток із метою підвищення ефективності організації оперативно-розшукової діяльності підрозділами кіберполіції Національної поліції України. Проаналізовано особливості оперативного виявлення підробки платіжних карток як превентивних заходів учинення класифікованих злочинів більшої тяжкості. Наведено приклади припинення злочинних дій із платіжними картками.

Ключові слова: *платіжна картка, підробка, оперативно-розшукова характеристика, оперативна розробка, оперативне документування.*

Постановка проблеми. Злочинність із використанням платіжних карток зростає швидше, ніж обсяги законних операцій із легальними платіжними картками. За оцінками фахівців, близько 40% всього незаконного зняття грошових коштів відбувається саме за допомогою фальшивих платіжок. На другому місці розкрадання, що стали можливими через крадіжку-втрату власниками платіжної картки, – на їх частку припадає 35% «ринку» [6]. НБУ заявляє про приховування банками реальних збитків, а самі банкіри стверджують, що рівень латентності таких злочинів становить близько 60% [12]. Протидія злочинам із використанням платіжних карток залишається одним із пріоритетних напрямів, широко підтримуваних європейською спільнотою, правоохоронної діяльності із протидії транснаціональній злочинності.

Стан дослідження. Проблема протидії злочинам, спрямованим на протиправне заволодіння коштами за допомогою платіжних карток, досліджувалася у наукових працях В. М. Бутузова, В. І. Василинчука, Н. Л. Волкової, І. О. Воронова, В. Д. Гавловського, С. Ю. Гаврика, В. О. Глушкова, С. В. Демедюка, Г. В. Загіки, О. М. Комара, М. Ю. Літвінова, О. В. Манжая, С. І. Ніколаюка, Д. Й. Никифорчука, В. П. Поїзда, С. М. Рогозіна, О. В. Сидоренка, Л. П. Скалозуба, О. В. Сухачова,

А. В. Тарасюка, Л. Л. Тимченка, К. В. Тітуніної, В. Є. Ткаліча, О. А. Федотова, І. Ф. Хараберюша, Д. М. Цехана, В. П. Шеломенцева, О. М. Юрченка.

Аналіз наукових праць дає змогу стверджувати про недостатню дослідженість питання оперативно-розшукового виявлення та оперативного документування фактів готування чи підробки платіжних карток, що підкреслює його теоретичну та практичну значущість.

Мета статті – виокремити елементи оперативно-розшукової характеристики підробки пластикових платіжних карток, які необхідно враховувати під час планування оперативно-розшукової діяльності, та обґрунтувати необхідність удосконалення нормативно-правового врегулювання застосування оперативно-розшукової діяльності із виявлення та припинення підробки платіжних карток із метою забезпечення превентивної функції правоохоронної діяльності підрозділів кіберполіції Національної поліції України – недопущення та попередження викрадення грошових коштів фізичних та юридичних осіб.

Виклад основних положень. Про стрімкий розвиток ринку платіжних карток свідчать дані НБУ, відповідно до яких станом на 01.01.2002 року в Україні налічувалось 3 млн 214 тис. держателів платіжних карток із обсягом активних готівкових операцій на суму 20 млн 48 тис. грн, станом на 01.01.2015 – 43 млн 58 тис. платіжних карток із операціями на суму 1 млрд 232 млн грн [11].

Розвиток сучасних технологій дозволяє злочинцям незаконно привласнювати та витрачати гроші громадян, до яких останні мають доступ через платіжні картки, без таких карток, а лише за допомогою викраденої інформації, носіями якої є самі платіжні картки. Здебільшого трапляються випадки незаконного заволодіння платіжними картками з подальшим отриманням доступу до інформації, яка у них міститься. Також трапляються випадки підробки платіжних карток із внесенням раніше викраденої інформації. Для реалізації злочинного наміру використовують різні методи. Виокремлюють три типи методів згаданої злочинної діяльності:

– інформаційний (передбачає контакт картки з банкоматом або втручання в діяльність POS-термінала);

– соціальна інженерія – метод, який передбачає отримання інформації в особи шляхом введення її в оману;

– механічний тип – встановлення накладок на банкомати, в яких затримується готівка, а також банальна крадіжка карток [14].

Розрізняють способи викрадення грошей, доступ до яких законослухняні громадяни здійснюють, використовуючи платіжні картки. Здебільшого їх узагальнено так:

Фізичний скімінг – встановлення накладок на банкомат, які допомагають отримати відомості про картку та доступ до неї (копіювання даних із магнітної смуги картки, електронного чіпа та запису ПІН-коду).

Програмний скімінг – встановлення на банкоматі шкідливого програмного забезпечення для запису даних із магнітної смуги карток та ПІН-кодів.

Прямий диспенс (jackpotting) – втручання в програмне забезпечення банкомата, яке дає диспенсеру команду на видачу всіх завантажених у касети грошей.

Reversal transaction – операція в режимі реального часу з метою відміни попередньої транзакції, яка була виконана з порушенням процедури або містила неправильні дані (наприклад, у разі неуспішної банкоматної операції внаслідок технічного збою, відсутності грошей у банкоматі тощо).

Cash Trapping (захват готівки) – встановлення на банкоматі спеціального пристрою, який дає змогу здійснити захват готівки під час операції, котру проводить законний держатель картки, яка згодом привласнюється зловмисником.

Card Trapping (захват картки) – розміщення в картрідері банкомата пристрою («ліванська петля», «пружинний тримач»), який перешкоджає отриманню картки її держателем, після чого її вилучає зловмисник та проводить операції зняття готівки в банкоматі, попередньо вивідавши ПІН-код [13].

Перехоплення даних, які банкомат відправляє в банк, щоб упевнитися в наявності запитуваної суми грошей на рахунку.

Установлення «власного» банкомата, який «не видає грошей», зате успішно зчитує з картки всі необхідні дані. Зауважу, що це «задоволення» є дорогим, але набуває поширення через викрадення банкоматів зі Сходу України внаслідок війни із РФ. Фальшивий банкомат зазвичай встановлюється злочинцями в торгово-розважальних центрах або інших місцях скупчення великої кількості людей, і є пристроєм, який ззовні виглядає як банкомат, має наклейки з логотипами платіжних систем, банків, банківських мереж тощо, але не містить у сейфовій частині грошових коштів та не підключений до банківського процесингового центру.

Отримання інформації від службових осіб (злочинна змова із працівниками банківських установ, торгових центрів тощо) [6]. За умови ефективної роботи служби безпеки банків легко відрізнити помилку персоналу банку від шахрайських дій співробітників. Основними показниками є дії співробітника, які були довершені задля

отримання вигоди для себе чи будь-якої іншої приватної особи або організації, а саме внаслідок підробки, зміни, використання фальшивих письмових розпоряджень щодо операцій із кредитними картами [7].

Крадіжка картки. Досвідчені злочинці крадуть платіжну картку після того, як дізналися ПІН-код.

Крадіжка банкомата, внаслідок чого злочинці отримують не тільки гроші, а й інформацію про всі карти, які проходили через кардрідер банкомата.

Атака на POS-термінал. Через POS-системи, які встановлюються у великих торгових центрах для прийому платежів (зокрема за допомогою кредиток), можна отримати персональну інформацію з тисяч, а то і мільйонів кредитних карток. Крадіжку персональних даних вчиняють за допомогою установки програми або технічного пристрою.

Дистанційне зчитування інформації з платіжної картки пристроєм із чіпом RFID. У транспорті, на ринку, в магазині зробити це не складно. Людина може навіть не помітити «злодійства» [2].

Розглянемо детальніше спосіб заволодіння грошима із використанням підроблених платіжних карток. Науковці та практики зауважують, що найбільші збитки платіжні системи несуть унаслідок використання підроблених платіжних карток. Підроблення платіжних карток поділяють на повне (виготовлення підробки з дотриманням усіх реквізитів справжньої платіжної карти); часткове (заміна окремих зовнішніх реквізитів, перекодування магнітної смуги тощо); виготовлення карток типу «білий пластик» [1, с. 64]. Під час зняття коштів із банківських карток обраних жертв шахраї використовують «білий пластик». Технологія виготовлення такої картки передбачає нанесення на пластик реквізитів реальних платіжних карток, інформацію про які було отримано незаконним шляхом. Візуально від справжньої платіжної картки «білий пластик» відрізняється відсутністю класичних символів розпізнавання банку-емітента та відповідної платіжної системи. Департамент комунікації Національної поліції України повідомляє, що професійні підробки зловмисниками використовуються в торговельних мережах для розрахунку за товари і послуги, а менш досконалі – під час зняття готівки у банкоматах [3].

Технологія виготовлення пластикових карток є доволі складною та потребує спеціалізованого обладнання. Детально згаданий процес є описаним у багатьох підручниках. Нагадаємо лише основні моменти, які необхідно враховувати оперативним підрозділом кіберполіції як елемент оперативно-розшукової характеристики під час організації та планування оперативно-розшукової діяльності. Основним матеріа-

лом для виготовлення пластикових карток слугує полівінілхлорид. Він легко піддається обробці та нейтральний до фарб, що дає змогу одержувати на готових картках дуже чисті кольори. Етапи виготовлення пластикових карток такі: підготовка макета; друк; способи захисту поверхні карток (лакування поверхні картки, ламінування карток, яке дозволяє «ховати» всередину картки мікрочіп і антену безконтактних карток або наносити на картку «втоплену (не виступає над поверхнею картки) магнітну смугу»; персоналізація (на картку або партію карток наносяться персональні дані: ПІН-код, ембосування, штрих-код, запис магнітної смуги тощо); нанесення додаткових елементів (магнітна смуга, смуга для підпису, ембосування, нумерація/текстова персоналізація, штрих-код, Scratch-смуги, голограма, «металічні» фарби (золото, срібло), ірідісцентні фарби, ультрафіолетові фарби, мікросхема (чіп), тиснення фольгою). Сучасні технології дають змогу виготовляти захищені пластикові картки. Елементами захисту є: мікрошрифт, голограма, ультрафіолетове зображення та чорна пластикова вставка (для scratch-карток) тощо [8].

До основних елементів підроблених пластикових карток із магнітною смугою (на прикладі Visa й EuroCard/MasterCard), які нині найчастіше трапляються в Україні, належать: голограма (на підроблених голограмах зображення може переливатися всіма барвами веселки, проте немає об'єму зображення); панель для підпису (натомість наклеюється смужка паперу, яка виступає над поверхнею карти. Краї панелі для підпису легко задираються. На панелі у низці випадків немає або стертий фон у вигляді трикольорового напису «MasterCard» (картки MasterCard/EuroCard), синьої або трикольорової «Visa» (картки Visa). Часто не відповідає оригіналу відтінок фарби, яким нанесений напис; ламінування на лицьовому (іноді й на зворотному) боці картки може бути нанесена прозора плівка, що клеїться на ламінат. Ламінувальна плівка відшаровується по краях картки, а іноді в межах підробленої голограми й ембосування нещільно прилягає до пластика; препринт (перші чотири цифри номера картки продубльовані під або над номером чорною фарбою) може стиратися з картки, що неможливо на справжній картці. Часто препринт не збігається з першими чотирма цифрами ембосованого номера картки; логотип відрізняється за кольором, розміром, взаємним розташуванням елементів від стандартного та може стиратися з картки; мікрошрифт навкруги логотипа Visa практично не читається і легко стирається з картки. Часто мікрошрифт навкруги логотипа замінюється рівною лінією; стилізовані символи «V» або «MC» зроблені грубо і відрізняються від стандартних. Не відповідає оригіналу нахил, взаєморозташування частин, місце ембосування

на лицьовому боці картки. Іноді елементів взагалі немає; ультрафіолетові символи: в ультрафіолетовому світлі на картках можуть бути відсутні зображення голуба, що летить у Visa або букви «МС» у EuroCard/MasterCard. На деяких підробках ці символи є, проте вони нечіткі та розмиті, розташовані не в тих місцях; магнітна смуга може відчуватись на дотик на межі смуги і картки, оскільки часто просто наклеюється зверху, а не впаюється в поверхню. Дані магнітної смуги можуть не відповідати ембосуванню (наприклад, не збігаються номер картки та прізвище держателя, зчитані з магнітної смуги і надруковані на чекові (екрані термінала) з нанесеними на лицьову сторону картки); торцева частина картки не білого кольору; можлива невідповідність найменування банку на лицьовій і зворотній стороні картки, на якій вигравіюваний голуб і, відповідно, зображення не об'ємне й абсолютно позбавлене будь-якої кольорової градації [8].

Зазначене є складовою оперативно-розшукової характеристики злочинних дій із платіжними картками і мають інформативно-пошуковий характер для оперативно-розшукової діяльності підрозділів кіберполіції Національної поліції України. Розглянемо оперативно-розшуковий аспект правоохоронної діяльності оперативних підрозділів кіберполіції із виявлення та припинення підробки платіжних карток із метою попередження викрадення грошових коштів. В опублікованих раніше наукових працях вказувалося, що, на відміну від незаконного використання платіжних карток, факти якого найчастіше виявляються гласно (службою моніторингу банку за результатами сумнівних операцій; працівниками банку, які виявляють вилучені банкоматами підроблені картки; під час затримання правопорушника біля банкомата, в якого під час огляду виявлено та вилучено підроблені картки; під час розслідування кримінального провадження, коли встановлено факти незаконного зняття готівки з банкоматів, виявлено та вилучено підроблені картки), інформація щодо злочинних дій із платіжними картками отримується переважно під час оперативного пошуку, а тому не вноситься до єдиного реєстру досудових розслідувань, а відтак процес перевірки наявності злочинної діяльності відбувається в межах оперативно-розшукової діяльності. Оперативне документування можливо проводити і під час оперативно-розшукової діяльності без заведення оперативно-розшукової справи (далі – ОРС), і під час оперативної розробки в межах ОРС, але із застосуванням усіх сил, засобів та заходів оперативно-розшукової діяльності [5]. Варто зауважити, що підробка платіжних карток (ч. 2 ст. 200 КК України) належить до злочинів середньої тяжкості, а це, своєю чергою, унеможливлює застосовування в процесі оперативного документування такого інструмента опера-

тивно-розшукової діяльності, як оперативно-розшукові заходи. Також дискусійним є питання доцільності залучення спеціалізованої агентури для виявлення та припинення злочинів середньої тяжкості. А відтак використання лише заходів оперативного пошуку, передбачених відомчими нормативно-правовими актами із грифом секретності, значно ускладнює процес оперативного документування злочинних дій із готування та вчинення підробки платіжних карток не в сукупності з іншим тяжким злочином. Нагадуємо, що законність заведення ОРС, окрім безпосередніх і прямих керівників оперативного (територіального) підрозділу НП, перевіряється прокурором, до повноважень якого входить право скасування незаконних постанов про заведення ОРС із усіма наслідками дисциплінарного, а інколи і кримінально-правового характеру. Фальсифікація матеріалів оперативно-розшукової діяльності для заведення ОРС із кваліфікацією діянь сукупно із тяжким чи особливо тяжким злочином є невиправданою навіть із метою припинення суспільно небезпечної діяльності. Крім того, межі оперативного документування обмежені вимогами положення ст. 7 Закону України «Про оперативно-розшукову діяльність», яким зобов'язано оперативний підрозділ при виявленні ознак злочину невідкладно направити до органу досудового розслідування зібрані матеріали, в яких зафіксовано фактичні дані про протиправні діяння у вигляді злочинних дій з платіжними картками, відповідальність за які передбачена Кримінальним кодексом України, для проведення досудового розслідування [10]. Приблизний до викладеного за змістом алгоритм дій передбачений відомчим наказом № 700 від 14 серпня 2012 року [9].

Оперативний пошук інформації щодо виявлення та припинення підробки платіжних карток необхідно сконцентрувати на особах, які підозрюються у шахрайстві чи раніше судимих за аналогічні злочини. Питання оперативного обслуговування об'єктів, на яких може відбуватися крадіжка особистої інформації та/або підроблення платіжних карток, є складним, оскільки технічна оснащеність і суб'єктів підприємницької діяльності, і можливості придбання технічних пристроїв є надзвичайно поширеними, побутово необхідними та не підконтрольними державним органам. Згадане питання може розглядатися лише у разі наявності перевіреної інформації щодо конкретного місця вчинення злочинної діяльності, наприклад, аналіз інформації від осіб (потерпілих) про факти викрадення грошових коштів після їх використання у «спільних» торгових точках. Зробити такий висновок можна внаслідок зіставлення та аналізу проведення розрахунків платіжними картками самими потерпілими, через що можна встановити ймовірні місця викрадення інформації із платіжної картки. Наслідком цілеспрямованого

оперативного відпрацювання таких місць повинно стати визначення кола причетних до злочинної діяльності осіб із подальшою їх ідентифікацією та оперативною розробкою з метою виявлення всіх складових злочинного ланцюжка.

За фактами виявлення підроблених платіжних карток без осіб (наприклад, вилучення із банкомата) повинно бути відкрите кримінальне провадження (не завжди банки повідомляють про такі факти). В процесі досудового розслідування необхідно ідентифікувати картковy інформацію із встановленням її приналежності конкретній особі (справжній платіжній картці клієнта). Виключаючи версію із втрати картки, необхідно проаналізувати місця проведення розрахунків цією карткою, а також можливості стороннього доступу до неї. Існує невелика перспектива встановлення ймовірного місця викрадення персональної інформації клієнта із платіжної картки.

Наведемо декілька прикладів із виявлення фактів злочинної діяльності з платіжними картками.

16 грудня 2015 року працівниками Поліського Управління кіберполіції ДКП НП України викрито групу громадян Білорусі, яка складалася з 3-ох осіб, що здійснювали обготівкування грошей у торговельній мережі Волинської області шляхом списання коштів із банківських рахунків громадян США за купівлю товарів. Попередньо зловмисники замовляли в мережі Інтернет інформацію щодо електронних дампів та пін-кодів банківських карток іноземних громадян, які записували на магнітні стрічки банківських карток, що були відкриті на самих зловмисників у банківських установах Республіки Білорусь. Перед розрахунками останні уточняли в торговельних закладах, що мають намір розраховуватися іноземними банківськими картками.

Нещодавно співробітники Слобожанського управління кіберполіції Полтавщини викрили та затримали злочинця, який, маючи скомпрометовані банківські карти (дампи, пін-коди, слу-коди), для прикриття своєї протиправної діяльності зареєстрував приватне підприємство, після чого уклав договір із банківською установою на отримання торгового термінала. Зловмисник здійснив 650 успішних операції з використанням скомпрометованих карток (білий пластик) та незаконно отримав із банківських рахунків громадян майже півмільйона гривень [3].

В іншому випадку київський «фахівець» тривалий час викрадав гроші з рахунків одного з банків, де керівництво залучило його до розробки відповідної програми для банкоматів і їх сервісного обслуговування. Технічно злочинець мав можливість копіювати дані з пластикових карток власників, які користувалися послугами фінансової устано-

ви, після чого виготовляв підроблені пластикові картки та знімав гроші через банкомати.

Класичний приклад злочинів, пов'язаних із платіжними банківськими картками, викладений у вироку Піщанського районного суду Вінницької області, яким засуджено 30-річну жінку, яка, керуючи місцевим відділенням відомого банку, порушуючи Закон України «Про банки і банківську діяльність», а також внутрішні службові інструкції, організувала виготовлення 25 підроблених кредитних карток із кредитним ресурсом 10 тис. грн кожна. На підставі копій документів (паспортів та довідок про податкові номери) померлих людей, підсудна від їх імені писала заяви з проханням укласти кредитний договір із банком, оформляла ці договори та реєструвала, віддавала розпорядження підлеглим (молодим дівчатам без досвіду роботи) виписувати на ім'я померлих банківські картки та перераховувати на їхні рахунки гроші, після чого отримувала картки разом із пін-кодами та знімала гроші, які привласнювала. У результаті злочинної діяльності підсудна привласнила близько 200 тис. грн, що належать банку.

Окрім того, очікуються вироки у кримінальних провадженнях стосовно злочинної діяльності групи менеджерів у банківських установах, які перераховували на рахунки підставних осіб великі суми грошей. Для зняття грошей із банкоматів за допомогою підроблених карток наймалися люди з соціально вразливих категорій (алкоголіки, наркомани) [4].

Висновки. Доступність до бланків платіжних карток як матеріальних носіїв персональної інформації про клієнта, компактність технічних пристроїв для внесення викраденої інформації на «пластик», відсутність необхідності високої кваліфікованої підготовки для використання зазначених технічних засобів, латентність таких злочинів ускладнюють процес оперативного пошуку об'єктів та фактів, які становлять оперативний інтерес для підрозділів кіберполіції. Знання елементів оперативно-розшукової характеристики способів викрадення інформації та підробки пластикових платіжних карток дають змогу ухвалити ефективні рішення з організації та планування оперативної розробки.

Оперативне обслуговування об'єктів, які використовують для проведення розрахункових операцій платіжними картками, а відповідно і спеціальне обладнання, яке створює можливості для злочинців із викрадення інформації та подальшої підробки платіжних карток, в умовах стрімкого технічного прогресу та розпорошеності сил та засобів оперативно-розшукової діяльності підрозділів кіберполіції Національної поліції України, є неможливим. Лише взаємодія підрозділів

безпеки банківських установ із оперативними підрозділами Національної поліції дає змогу мінімально протидіяти злочинності із платіжними картками. Без такої взаємодії, яка ґрунтується лише на зацікавленості банків, протидія злочинності із платіжними картками мала б виключно тимчасовий характер та виявлялася в одиничних випадках, які б залежали від помилок злочинців та майстерності правоохоронних органів. Виявлення та припинення фактів готування підроблення платіжних карток можна вважати превентивними заходами більшої суспільно небезпечної діяльності, шкідливі наслідки якої усувати складніше. Нині єдиним дієвим заходом ефективної протидії підробленню платіжних карток у стратегічному вимірі є ускладнення захисту платіжної картки як матеріального носія індивідуальної інформації стосовно клієнта.

Цей процес є витратним, але фінансові установи мають необхідний матеріальний ресурс, який, на нашу думку, буде задіяний лише тоді, коли матеріальні збитки та збитки для ділової репутації банківських установ в рази перевищать згадані витрати на вдосконалення захисту.

Для ефективного використання потенціалу оперативно-розшукової діяльності оперативними підрозділами кіберполіції Національної поліції України необхідно ініціювати внесення змін у законодавче та відомче забезпечення оперативно-розшукової діяльності, зокрема у дозволі проведення повноцінної оперативної розробки (із використанням наявних засобів та заходів оперативно-розшукової діяльності) із виявлення та припинення протиправної діяльності груп осіб незалежно від тяжкості вчинюваного ними злочину.

---

1. Бутузов В. М. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток: навч. посібник / В. М. Бутузов, В. І. Василинчук, В. П. Шеломенцев. – К.: Типографія ТОВ «СТ-стиль», 2006. – 139 с.

2. [Електронний ресурс]. – Режим доступу: http://blogbankir.ru/top-8-sposobov-krazhi-sredstv-s-bankovskoj-karty.html.

3. І цим пристроєм зловмисник вкрав півмільйона гривень [Електронний ресурс]. – Режим доступу: https://ukr.media/business/256022/.

4. Котнюк Ю. Злочини з платіжними картками: судова практика / Ю. Котнюк // Судебно-Юридическая газета [Електронний ресурс]. – Режим доступу: http://anticyber.com.ua/article_detail.php?id=16

5. Лепеха О. М. Можливості оперативно-розшукової діяльності підрозділів боротьби з кіберзлочинністю МВС України з оперативного документування злочинних дій з платіжними картками (ст. 200 КК України) /

О. М. Лепеха, О. В. Кондратюк // Науковий вісник Харківського національного університету внутрішніх справ. Серія юридична (спеціальний випуск): збірник наукових праць. – Спецвип. 1. – Х.: ХНУВС, 2015. – С. 62–67.

6. Марков Д. Як крадуть гроші з картки / Д. Марков [Електронний ресурс]. – Режим доступу: http://i-cent.org.ua/jak-kradut-groshi-z-kartki-2/.

7. Перспективи співпраці страхових компаній та банків в Україні [Електронний ресурс]. – Режим доступу: http://jenessi.net/economi/131-perspektivi-spvprac-strakhovikh.html.

8. Пиріг С. О. Основні характеристики підроблених пластикових карток і методи їх виявлення, платіжні системи / С. О. Пиріг // Бібліотека українських підручників [Електронний ресурс]. – Режим доступу: http://libfree.com/159783537_finansitehnologiya_vigotovlennya_plastikovih_kartok.html.

9. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами внутрішніх справ у попередженні, виявленні та розслідуванні кримінальних правопорушень: Наказ МВС України від 14 серпня 2012 року № 700.

10. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135–XII // Відомості Верховної Ради України (ВВР). – 1992. – № 22. – Ст. 303.

11. Сайт НБУ [Електронний ресурс]. – Режим доступу: http://www.bank.gov.ua/control/uk/publish/category?cat_id=79219.

12. Святенко А. Втрати від карткового шахрайства в семеро більші від допустимих: час серйозно зайнятися системою безпеки електронних гаманців / А. Святенко // Дзеркало тижня. – 2002. – № 40 (415).

13. Тимченко Л. Виявлення пристроїв незаконного втручання в роботу банкоматів та протиправних дій у сфері використання платіжних карток: навчальні матеріали слухачів курсів первинної підготовки працівників патрульної поліції / Л. Тимченко, Р. Федоровська [Електронний ресурс]. – Режим доступу: http://ema.com.ua/ema-academy/trainings/social-responsibility/#.

14. Як крадуть гроші з банківських карток [TechToday від 17 листопада, 2015] [Електронний ресурс]. – Режим доступу: http://today.mts.com.ua/posts/yak-kradut-groshi-z-bankivskix-kartok.

Лепеха О. М. Оперативно-розыскная характеристика способа завладения деньгами и особенности оперативного обнаружения подделки платежных карт

Рассмотрено содержание методов и способов реализации преступного умысла касательно похищения информации с последующим ее использованием с помощью поддельных платежных карт как неотъемлемых элементов оперативно-розыскной характеристики преступности с платежными картами. Описаны технологические особенности подделки пластиковых карт.

Обоснована необходимость ориентирования в специфике подделки пластиковых карт с целью повышения эффективности организации оперативно-розыскной деятельности подразделениями киберполиции Национальной полиции Украины.

Проанализированы особенности оперативного выявления подделки платежных карт как превентивные меры совершения классифицированных преступлений большей тяжести.

Приведены примеры прекращения преступных действий с платежными картами.

Ключевые слова: *платежная карта, подделка, оперативно-розыскная характеристика, оперативная разработка, оперативное документирование.*

Lepekha O. M. Operational-investigative characteristics of the ways to misappropriate money and peculiarities of operational revealing of payment card frauds

The article deals with the methods and ways to fulfill criminal intention to steal information with its further use by means of fake payment cards as inevitable elements of operational-investigative characteristics of criminality related to payment cards.

Technological peculiarities of payment card frauds have been described. The necessity of detectives to be aware of the specificity of payment card frauds has been substantiated due to the increase of effectiveness of operational-investigative arrangements by the divisions of cyberpolice of the National Police of Ukraine.

There has also been analysis of the peculiarities of operational revealing of payment card frauds as preventive measures of committing crimes classified as a serious one.

It was reasoned that effective operational servicing of entities using payment cards to conduct payment transactions in the speedy technological progress and dispersed forces and means of operational-investigative activities of the divisions of cyberpolice of the National Police of Ukraine is impossible.

The focus has been made on the fact that only thanks to the cooperation of the safety divisions of bank institutions with the divisions of the National Police there is a possibility to prevent criminality related to payment cards. Without such cooperation being efficient only if banks are interested, prevention of criminality related to payment cards would have been just of temporary nature and of single instances depending on miscount of criminals and proficiency of law enforcement agencies.

For the purpose of effective use of operational-investigative activities it has been offered to initiate amendments to the legal and official provisions of operational-investigative activities, namely allowing conducting fully valid operational cultivation (with the use of available means and measures of operational-investigative activities) in order to reveal and stop illegal actions of the groups of people irregardless of the seriousness of the committed crime by them.

Key words: *payment card, fraud, operational-investigative characteristics, operational cultivation, operational documentation.*

Стаття надійшла 5 квітня 2016 р.