[23] Smuggling of migrants – A Global Review and Annotated Bibliography of Recent Publications // United Nations Office on Drugs and Crime : [Електронний ресурс]. – Режим доступу: https://www.unodc.org/documents/human-trafficking/Migrant-Smuggling/Smuggling_of_Migrants_A_Global_Review.pdf – Заголовок з екрана.

[24] *Spijkerboer T.* The Human Costs of Border Control / T. Spijkerboer // European Journal of Migration and Law. – 2007. – № 9. – P. 127–139.

[25] *Голіна В.В.* Сучасна кримінологія: досягнення, проблеми, перспективи / В.В. Голіна // Сучасна кримінологія: досягнення, проблеми, перспективи : матеріали Міжнар. наук. конф., присвяч. 50-річчю каф. кримінології та кримінально-виконавчого права (м. Харків, 9 грудня 2016 р.) / за ред. В.Я. Тація, Б.М. Головкіна. – Х. : Право, 2016. – С. 5.

[26] *G.E. Sanchez.* Human Smuggling and Border Crossings // Routledge Studies in Criminal Justice, Borders and Citizenship, 2014. – 146 p.

[27] *Shelley L.* Human Smuggling and Trafficking into Europe: A Comparative Perspective / L. Shelley. – Washington, DC: Migration Policy Institute, 2014. – 24 p.

Резюме

Кібальник С.О. **Незаконне переправлення осіб через державний кордон у кримінологічній науці ЄС та США.**

Стаття присвячена характеристиці та аналізу стану розробки проблеми незаконного переправлення осіб через державний кордон з позицій кримінології вченими Західної Європи та Сполучених Штатів Америки. Основну увагу приділено формулюванню загальних тенденцій та закономірностей її висвітлення західними фахівцями, а також виявленню спільних та суперечливих аспектів у їх точках зору.

Ключові слова: незаконне переправлення осіб через державний кордон, незаконна міграція, організована злочинність, транскордонна злочинність, запобігання злочинності.

Резюме

Кибальник С.О. **Незаконная переправка лиц через государственную границу в криминологической науке ЕС и США.**

Статья посвящена характеристике и анализу состояния разработки проблемы незаконной переправки лиц через государственную границу учеными Западной Европы и Соединенных Штатов Америки. Основное внимание уделено формулированию общих тенденций и закономерностей ее освещения западными специалистами, а также выявлению общих и дискуссионных аспектов в их точках зрения.

Ключевые слова: незаконная переправка лиц через государственную границу, незаконная миграция, организованная преступность, международная преступность, трансграничная преступность, предотвращение преступности.

Summary

Kibalnyk S. **Human smuggling in the criminological science of the EU and the USA.**

The article is devoted to characteristic and analysis of the scientific development of the human smuggling problem in Western Europe and the United States of America. The main attention is drawn to the formulation of general trends and patterns in its coverage by Western experts, as well as the revealing of common and controversial aspects in their points of view.

Key words: human smuggling, illegal migration, organized crime, cross-border crime, crime prevention.

УДК 343.3/.7

В.М. КРИВОЛАПОВ

Володимир Михайлович Криволапов, *ад'юнкт Національної академії внутрішніх справ*

КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ПРОТИДІЇ ЗЛОЧИНАМ, ПОВ'ЯЗАНИМ ІЗ ЗАВОЛОДІННЯМ КОШТАМИ ШЛЯХОМ УТРУЧАННЯ В РОБОТУ БАНКОМАТІВ

Швидкі темпи розвитку фінансових ринків та все більш зростаюча масштабність проведення розрахунків у міжнародних платіжних системах супроводжуються одночасним виникненням різного роду ризиків, пов'язаних із застосуванням платіжних терміналів. У зв'язку з цим здійснення оцінювання ризиків шахрайства та дослідження їх економічних наслідків для учасників розрахункових процесів, а також розробка системи заходів щодо мінімізації даних ризиків є актуальною в умовах інтернаціоналізації систем масових електронних платежів.

Специфічні риси та властивості електронних грошей, а також масштабний характер їх розвитку і поширення в повсякденному житті суспільства привернули увагу не тільки потенційних користувачів, але також контролюючих і регулюючих організацій. Нині підвищений інтерес до вдосконалення процедур їх звернення пояснюється успішним функціонуванням приватних систем електронних грошей і криптовалюти, впливом

глобальної економічної кризи, зниженням надійності світової валютної системи, наявністю кіберзагроз у фінансовій сфері. Сьогодні як окремі господарюючі суб'єкти, так і країни в цілому відчувають потреба в легітимному використанні децентралізованого підходу до організації електронних розрахунково-платіжних систем, побудованих з застосуванням технології блокчейн, оскільки вони позбавлені основних недоліків централізованих систем в частині безпеки здійснення розрахунків і платежів, а також зберігання фінансової інформації.

Питання розслідування злочинів у різні часи були об'єктом дослідження широкого кола вчених, зокрема таких як Ю.П. Аленін, В.Д. Басай, В.П. Бахін, П.Д. Біленчук, В.К. Весельський, А.Ф. Волобуєв, Д.Ю. В'юнник, О.М. Джужа, О.П. Дубовий, В.Ф. Єрмолович, Ю.Л. Заросинський, А.В. Іщенко, В.С. Кузьмічов, В.Т. Маляренко, І.О. Манжос, Г.І. Прокопенко, М.В. Салтевський, П.Ю. Тимошенко, О.А. Федотов, С.С. Чернявський, В.В. Чернєй, В.М. Шевчук, В.Ю. Шепітько, М.Є. Шумило та ін. Однак, незважаючи на велику кількість публікацій з цієї тематики, питання аналізу та мінімізації ризиків шахрайства учасників міжнародних платіжних систем в Україні залишається відкритим.

Отже, **метою** статті є визначення елементного складу зазначеної категорії злочинів, яка зумовлена нагальною потребою аналізу криміналістичної характеристики зазначеної категорії злочинів та з урахуванням їх специфіки.

Розслідування будь-яких злочинів повинно ґрунтуватися на узагальненій слідчій практиці, у поєднанні з використанням апробованих криміналістичних рекомендацій та наукових знань. Уже існуючі наукові напрацювання розкривають значну кількість питань з цієї проблематики. Водночас, об'єктивно враховуючи соціальні й правові реалії сьогодення, дослідження питання незаконного втручання в роботу банкоматів залишається досить актуальним.

Дедалі частіше банки прагнуть знизити власні витрати і спонукати клієнтів до оплати товарів, послуг, податків і т.д. не через касира, а через банківські термінали або за допомогою інтернет-банкінгу. Проте в Україні обсяг операцій зі зняття готівки з банкоматів перевищує обсяг оплат товарів і послуг за банківськими картками більш ніж удвічі і за дев'ять місяців 2017 р становив понад 5 млрд грн. І весь цей грошовий потік проходить через банкомати, яких більше 38 тис. по всій Україні[1].

Будапештська Конвенція, як основоположний документ у сфері боротьби з кіберзлочинністю, надає таку класифікацію кіберзлочинів:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, зокрема:

– незаконний доступ, наприклад, шляхом злому, обману та іншими засобами;

– нелегальне перехоплення комп'ютерних даних;

– втручання в дані, включаючи навмисне пошкодження,

– знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

– втручання в систему, включаючи умисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;

– зловживання пристроями, тобто виготовлення, продаж, придбання для використання, поширення пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу з метою здійснення кіберзлочинів;

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;

3) правопорушення, пов'язані з утриманням інформації, зокрема дитяча порнографія, расизм і ксенофобія;

4) правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

Разом із тим, з урахуванням мотивації злочинців, кіберзлочини можна умовно розділити на наступні категорії:

– кібершахрайство з метою заволодіння коштами;

– кібершахрайство з метою заволодіння інформацією (для власного користування або для наступного продажу);

– втручання в роботу інформаційних систем з метою отримання доступу до автоматизованих систем управління (для умисного пошкодження за винагороду або для нанесення збитку конкурентам);

– інші злочини.

Перша категорія злочинів – привласнення грошових коштів, при якому шахраї використовують різні способи, іноді змушуючи користувачів самостійно розкривати конфіденційні дані.

Найпоширеніші злочини, що належать до другої – третьої категорії – це злом баз даних і виведення з ладу комп'ютерних систем компаній і державних організацій, а також крадіжка інновацій або технологій.

У рамках даного дослідження найбільш детально розглянуто кіберзлочини, в результаті яких виникає фінансова чи інша матеріальна вигода у вигляді незаконно отриманих доходів. Йдеться насамперед про використання інформаційно-комунікаційних систем і комп'ютерних технологій для доступу до приватної власності юридичних і фізичних осіб та подальших дій з управління або розпорядження цією власністю. Зокрема, найбільш популярним нині серед кіберзлочинів є отримання доступу до засобів клієнтів банківських установ.

У цій категорії найбільш поширеними є такі види злочинів:

1) шахрайство в мережі Інтернет, зокрема:

– створення «фінансових пірамід» в мережі Інтернет;

– шахрайство при продажу товарів (послуг) через Інтернет або на Інтернет-аукціонах;

– діяльність по створенню програмних засобів з метою розкрадання фінансової, комерційної або персональної інформації (створення фіктивних WEB-сайтів, поширення комп'ютерних вірусів і троянських програм, перехоплення трафіку тощо);

2) шахрайство в системах дистанційного банківського обслуговування (далі – ДБО), зокрема:

– створення комп'ютерних вірусів і троянських програм для прихованого перехоплення управління комп'ютером клієнта з встановленим програмним забезпеченням ДБО;

– відкриття рахунків, проведення несанкціонованих операцій і отримання готівкових коштів в результаті несанкціонованих операцій в системах ДБО;

– отримання платежів від іноземних відправників через міжнародну систему SWIFT внаслідок втручання в роботу комп'ютерів і систем ДБО клієнтів іноземних банківських установ;

3) підробка платіжних карт і банкоматне шахрайство, зокрема:

– використання втрачених/викрадених/підроблених платіжних карт;

– викрадення реквізитів платіжних карт, в тому числі із застосуванням технічних засобів їх «клонування»;

– скімінг – виготовлення, збут і установка на банкомати пристроїв зчитування/копіювання інформації з магнітної смуги платіжної карти і 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 здійсненні операцій видачі готівки, яке залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником;

– Cash Trapping – заклеювання диспенсера для присвоєння зловмисником готівки, яка була списана з карткового рахунку законного власника картки.

Слід зазначити, що стрімкий розвиток сфери інформаційних технологій постійно генерує нові види послуг, в тому числі в фінансовій сфері. Це, в свою чергу, змушує злочинців удосконалювати свої здібності і придумувати нові способи незаконного заробітку в кіберсередовищі.

Такий оборот готівки не може не привертати зловмисників, охочих ними заволодіти. Почастішали випадки як нападів на інкасаторів, так і крадіжки грошей з банкоматів і пристроїв самообслуговування. Якщо напад на інкасаторів – це дуже ретельно підготовлений, смертельно небезпечний шлях, по якому йдуть в основному люди, яким вже нічого втрачати, то крадіжка грошей із банкоматів є більш поширеною та безпечнішою. Спокуса велика: кілька сотень тисяч гривень лежать усього лише за тонкою стінкою сейфа.

Для більш детального аналізу ми розберемо категорії злочинців, які вчиняють незаконні дії щодо банкоматів, а саме: зломщики, грабіжники(викрадачі), кіберзлочинці (хакери) та шахраї.

Основною метою злочинців, що спеціалізуються на зломі банкомату, є крадіжка готівки з нижнього кабінету (сейфа) банкомату, нерідко сполучена з незаконним проникненням у приміщення, де встановлений банкомат. Часто таких осіб називають «ведмежатниками». Для досягнення своєї мети вони використовують три основні способи:

– злом сейфа банкомату на місці його розміщення;

– протиправне відкривання замка сейфа банкомату;

– несанкціоноване переміщення (крадіжка) банкомату і відкриття його в іншому віддаленому місці.

Для злому сейфа банкомату «ведмежатники» найчастіше використовують звичайний слюсарний інструмент (ручний або електричний), який вільно можна придбати в будівельному магазині (кувалду, лом, ножівку, дискову пилу типу «болгарка», газовий різак і т.д.). Однак останнім часом почастішали й випадки руйнування оболонки сейфа банкомату за допомогою вибуху. Для цього зловмисники або закачують в нижній кабінет банкомату вибухонебезпечний газ, або встановлюють кумулятивний заряд зовні сейфа.

Протиправне відкриття замикаючого пристрою сейфа банкомату здійснюється найчастіше за допомогою спеціалізованого інструменту (відмичок), що дає змогу відкрити замок без використання ключа або його руйнування, а в деяких випадках – шляхом використання штатних ключів чи кодів (якщо мала місце змова злочинців з працівниками фінансової або обслуговуючої організації).

Для несанкціонованого переміщення банкомату зловмисники використовують підручні, автотранспортні або спеціальні засоби. За допомогою даних засобів злочинці витягують банкомат з приміщення і відвозять у віддалене приховане місце, де й здійснюють безпосередній злом сейфа та викрадення готівки.

Слід підкреслити: якщо ж банкомат або платіжний термінал розміщено в закритому приміщенні (іншими словами, до нього немає вільного доступу в будь-який час доби), порушникам доводиться спочатку проникнути в приміщення, «обійти» заходи охоронної сигналізації та відеоспостереження (при їх наявності), і тільки після цього добиратися до готівки, зламуючи сейф банкомату. Як показує статистика такого роду злочинів, порушників не зупиняє навіть наявність фізичної охорони на об'єкті, особливо якщо це літнього віку сторож або вахтерка.

Зазначеними видами злочинів займаються як кустарі-одинаки з найпростішими підручними інструментами, так і організовані злочинні групи, оснащені за останнім словом техніки.

Наступна категорія зловмисників – це грабіжники. Це найбільш небезпечний вид злочинців, які діють у сфері дистанційного банківського обслуговування. Під загрозу збройного пограбування можуть потрапити як звичайні громадяни (при знятті готівки з банкомату), так і інкасатори (при завантаженні, вивантаженні або транспортуванні готівкових коштів). У цій категорії зустрічаються як відчайдушні «одинаки», так і організовані злочинні групи, які мають спеціальні знання, підготовку, автотранспорт, засоби придушення радіозв'язку, вогнепальну зброю.

Для протидії цій категорії злочинців необхідне оснащення банкоматів системами «інтелектуального» відеоспостереження, а також засобами тривожної сигналізації. Крім того, на обговорення може бути винесене питання про негласне формуванні сигналу тривоги шляхом набору спеціальної комбінації цифр на панелі введення ПІН-коду.

Окремої уваги заслуговують кіберзлочинці, так звані хакери, методи «роботи» яких можуть бути різними. В одних випадках – це може бути крадіжка готівки з нижнього кабінету банкомату, в інших – отримання незаконного доступу до конфіденційної інформації банківських карт клієнтів[2].

У першому випадку, на відміну від вищеописаних зломщиків, хакерам потрібен безпосередній доступ не в нижній кабінет банкомату, де розташовані касети з готівкою, а в верхній кабінет банкомату, де розташований комп'ютерний блок з операційною системою. Шляхом розтину верхнього кабінету і несанкціонованого підключення до комп'ютера банкомату вони встановлюють (інсталюють) шкідливі програми або підміняють програмне забезпечення банкомату. Після чого банкомат стає «слухняним» і або видає гроші зі свого нижнього кабінету по команді злочинця, або здійснює безготівкові перекази грошових коштів з чужих рахунків, до яких був отриманий доступ.

В Україну з Європи прийшов інноваційний спосіб крадіжки грошей з банкоматів і терміналів – пристрої заражають вірусами-шпигунами. Найчастіше в якості об'єктів для атаки зловмисники використовують АТМ і POS-термінали великих мережевих магазинів. Їх заражають шкідливим програмним забезпеченням для автоматичного запису технічної інформації та ПІН-кодів банківських карток клієнтів фінансових установ, які скористалися послугами терміналу.

У зв'язку з цим для забезпечення безпеки банкомату від таких загроз необхідно, по-перше, заблокувати (захистити від несанкціонованого відкривання) верхній кабінет, наприклад, за допомогою магнітоконтактного сповіщувача. По-друге, здійснити програмний захист операційної системи та програмного забезпечення банкомату від хакерських атак.

Досить згадати, якого шуму в кінці 2014 р. наробив вірус Backdoor.MSIL.Tyupkin, виявлений «Лабораторією Касперського». Цей вірус заражав банкомати по всьому світу і дозволяв кіберзлочинцям спустошувати касети з грошима. Окремо слід згадати про Росію, на яку припав найбільший відсоток «пограбувань» банкоматів з його використанням. Як повідомили експерти «Лабораторії Касперського», пограбування здійснювалися без використання кодів карт фізичних осіб шляхом прямих маніпуляцій з банкоматами. Фахівці проаналізували відеоматеріали з камер відеоспостереження, які були встановлені в місцях розміщення заражених банкоматів, і виявили, що зловмисники отримували гроші з банкоматів, попередньо встановивши шкідливий код із завантажувального диска. Цей вірус виявився актуальним для банкоматів, що працюють на 32-розрядної платформі Microsoft Windows.

Після проведення розслідування по новому вірусу «Лабораторія Касперського» були розроблені практичні рекомендації[3] для кредитно-фінансових організацій, компаній, що займаються обслуговуванням банківських пристроїв самообслуговування, і розробників програмного забезпечення (далі – ПО) для банкоматів. Відповідно до цих рекомендацій, щоб уникнути ризиків зараження банкоматів шкідливими програмами необхідно:

– посилити фізичний захист банкоматів (важливо, щоб банкомат надійно стояв на місці – був прикріплений до стіни або підлоги приміщення чи поміщений у спеціальний бокс);

– встановити охоронну сигналізацію (за даними «Лабораторії Касперського» Backdoor.MSIL.Tyupkin заражав тільки банкомати без сигналізації);

– замінити всі замки і майстер-ключі від виробника, що замикають верхні відсіки (кабінети) банкоматів;

– змінити встановлені за замовчуванням паролі BIOS (розробникам ПО слід приділяти більше уваги безпеці пристроїв: унікальні паролі BIOS повинні бути складними, містити не тільки цифри, а й букви та спецсимволи);

– встановити і регулярно оновлювати антивірусний захист банкоматів;

– регулярно виконувати повну перевірку файлової системи кожного банкомату;

– регулярно перевіряти банкомати на наявність сторонніх пристроїв (скімерів);

– використовувати тільки перевірені Whitelisting-продукти на банкоматах, щоб знизити ймовірність визначення антивірусами чистого програмного забезпечення як шкідливого так і навпаки.

Окремої уваги заслуговують шахраї, що займаються вчиненням злочинів, пов'язаних із втручанням в роботу банкомату. Ця кримінальна категорія найбільш «різношерста» й винахідлива. Цілі таких правопорушників і методи їх діянь можуть бути найрізноманітнішими, часом непередбачуваними. Зазначимо лише найбільш відомі:

– крадіжка конфіденційної інформації банківських карт клієнтів (скімінг);

– крадіжка банківської карти шляхом її механічного блокування в картрідер банкомату («ліванська петля»);

– крадіжка готівки клієнта шляхом захоплення і утримання банкнот в презентери банкомату;

– помилкове скасування банківської або платіжної операції;
– установка підроблених банкоматів («банкоматів-клонів»);
– створення «сайтів-клонів» кредитних організацій;
– розсилка на стільникові телефони власників банківських карт повідомлень від імені банку про блокування банківської карти.

В Україні загальний рівень шахрайства за платіжними картками поступово набирає обертів. Уже у 2012 р. від карткового шахрайства постраждали клієнти 51 банку, в той час як у 2011 р. причетними до незаконних операцій були картки, емітовані лише 43 фінансовими установами. За даними НБУ, протягом 2012 р. було здійснено 7,6 тис. неправомірних операцій, що на 2,5 тис. операцій менше, ніж у 2010 році. При цьому, у 2011 р. кількість шахрайських операцій становила лише 2,9 тис., тобто у 3,5 раза (на 7,2 тис.) менше, ніж у 2010 р., та на 4,7 тис. операцій менше, ніж у 2012 році. Відповідно до змін кількості шахрайських трансакцій у 2011 р. втрати від них зменшилися на 6,7 млн гривень порівняно з попереднім періодом – з 13 млн гривень до 6,3 млн гривень. Але вже у 2012 р. збитки збільшилися до 9,1 млн гривень, причому середній обсяг однієї несанкціонованої операції становив приблизно 1 тис. гривень.

У 2011 р. практично усі операції (99,7 % від їх загальної кількості), що заподіяли збитків банкам, держателям платіжних карток та торговцям, були здійснені з картками міжнародних платіжних систем Visa (55,27 %), на яку припадає найбільша частка ринку, та MasterCard (44,45 %)[4]. Обсяг втрат держателів карток міжнародної платіжної системи Visa у 2011 р. становив понад 6,2 млн гривень. У 2012 р. зросла кількість шахрайських операцій, здійснених за допомогою карток платіжної системи MasterCard, які використовувалися вдвічі частіше, ніж у попередньому році, і становила 1883 операції. Це завдало збитків держателям платіжних карток даної системи на суму 2,8 млн гривень[5]. Щодо вітчизняних платіжних систем НСМЕП та УкрКарт, то вони не зазнали втрат взагалі.

Проблеми боротьби із шахрайством у сфері дистанційного банківського обслуговування вимагають окремої ґрунтовної розмови.

Підсумовуючи вищезазначене, слід підкреслити, що питання організації заходів охорони в зоні розміщення банкоматів, платіжних терміналів та інших засобів дистанційного банківського обслуговування, а також особливості застосування систем активного захисту, що встановлюються як в самих банкоматах, так і в клієнтських зонах, потребує значно більшої уваги, аніж є сьогодні. В даний час ці напрями в сфері безпеки об'єктів дистанційного банківського обслуговування активно розвиваються і допомагають істотно підвищити ефективність застосовуваних заходів захисту.

---

[1] *Сахно Д.* Загальна інформація про систему міжбанківського обміну інформацією «Exchange-online» / Д. Сахно // Українська міжбанківська Асоціація членів платіжних систем «ЄМА». – 2012. – 5 жовтня : [Електронний ресурс]. – Режим доступу: http://ema.com.ua/exchange-online/info-exchange/

[2] *Богомолов А.Н.* Банковские платежные карты как предмет состава изготовления или сбыта поддельных кредитных либо расчетных карт и иных платежных документов / А.Н. Богомолов // Территория науки. – 2015. – № 2. – С. 158–165.

[3] *Голованов С.* Банкоматный вирус Tyupkin: будут ли новые атаки? / С. Голованов // Банкноты стран мира. – М., 2015. – № 4. – С. 26–27.

[4] О безопасности рынка платежных карт Украины // Карт Бланш: информационно-аналитический журнал. – 2012. – № 2. – С. 37–38.

[5] Аналіз масштабів та основні напрями мінімізації ризиків шахрайства членів міжнародних платіжних систем : [Електронний ресурс]. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=2120

Резюме

Криволапов В.М. **Криміналістична характеристика протидії злочинам, пов'язаним із заволодінням коштами шляхом утручання в роботу банкоматів.**

У статті розглянуто основні категорії порушників і види кримінальних правопорушень, у тому числі вчинених ними злочинів на об'єктах дистанційного банківського обслуговування, а також відомі на сьогодні способи протидії таким злочинам. Аналіз статистики злочинів, пов'язаних із заволодінням коштами шляхом утручання в роботу банкоматів (платіжні термінали), дає змогу із усього різноманіття порушників виділити кілька основних категорій.

Ключові слова: банкомат, банк, телекомунікаційна мережа, мережа інтернет, програмне забезпечення, інформаційні технології.

Резюме

Криволапов В.М. **Криминалистическая характеристика противодействия преступлениям, связанным с завладением денежными средствами путем вмешательства в работу банкоматов.**

В статье рассмотрены основные категории нарушителей и виды уголовных преступлений, в том числе совершенных ими преступлений на объектах дистанционного банковского обслуживания, а также известные на сегодня способы противодействия таким преступлениям. Анализ статистики преступлений, связанных с завладением денежными средствами путем вмешательства в работу банкоматов (платежные терминалы), позволяет из всего многообразия нарушителей выделить несколько основных категорий.

Ключевые слова: банкомат, банк, телекоммуникационная сеть, сеть интернет, программное обеспечение, информационные технологии.

Summary

Krivolapov V. **Forensic characteristic of counteraction to crimes connected with the acquisition of funds by means of the delivery of ATMs.**

The article deals with the main categories of violators and types of criminal offenses, as well as crimes committed by them at remote banking facilities, as well as methods known today for counteracting such crimes. Analysis of the statistics of crimes associated with the acquisition of funds through intervention in the work of ATMs (payment terminals), allows you to distinguish several main categories from a variety of offenders.

Key words: ATM, bank, Telecommunication network, Internet, software, information technologies.

УДК 343.132

Л.В. ПІВНЕНКО

Людмила Володимирівна Півненко, *старший викладач Харківського національного технічного університету сільського господарства імені Петра Василенка*

ОСОБЛИВОСТІ ПРЕД'ЯВЛЕННЯ ОСОБИ ДЛЯ ВПІЗНАННЯ ЗА ФУНКЦІОНАЛЬНИМИ ОЗНАКАМИ

В основу впізнання можуть бути покладені будь-які ознаки (прикмети, особливості), якщо вони мають особистий характер, тобто невіддільні від даної особи і проявляються зовні, створюючи можливість сприйняття, запам'ятовування і відтворення в ході пред'явлення особи для впізнання.

Доведено, що у випадках, коли у слідчого виникають сумніви щодо об'єктивності результатів пред'явлення особи для впізнання за функціональними ознаками, доцільним є залучення фахівців. Слідчий може призначати логопедичну експертизу, а після пред'явлення для впізнання за ходою – біомеханічну експертизу, що в свою чергу дасть змогу повно і об'єктивно дослідити обставини вчиненого злочину і сформувати належну доказову базу.

З огляду на складність в організації і проведенні впізнання особи за функціональними ознаками вказана слідча дія повинна проводитися із чітким дотриманням процесуальних норм, тактико-криміналістичних прийомів і рекомендацій.

Ефективна діяльність органів досудового розслідування щодо розкриття і розслідування злочинів залежить передусім від належної організації і проведення слідчих (розшукових) дій. Слідча (розшукова) дія – це передбачений Кримінальним процесуальним кодексом захід, який застосовується компетентними особами для збирання, дослідження, оцінки та використання доказів у ході кримінального провадження. Слідчі дії мають пізнавальний і водночас процесуальний характер та розшукову спрямованість, сутність якої полягає у діяльності слідчого чи іншої уповноваженої особи відшукати та належним чином процесуально закріпити фактичні дані, що мають значення для розкриття злочину та встановлення особи, яка його вчинила.

Перелік слідчих (розшукових) дій чітко регламентовано Кримінальним процесуальним кодексом України, в якому чинне місце займає така слідча (розшукова) дія, як пред'явлення особи для впізнання. Пред'явлення особи для впізнання є важливим засобом збирання доказової інформації, дає змогу перевірити показання осіб, які були допитані раніше (потерпілого, свідка, підозрюваного), висунути й перевірити слідчі версії, отримати нові докази у кримінальному провадженні.

Одним із видів пред'явлення особи для впізнання є впізнання за функціональними ознаками (голосом, ходою). Це надто складна слідча дія, що викликає певні труднощі в ході її практичного застосування. За умови неналежної підготовки і порушення процесуального порядку проведення вказаної слідчої дії може бути втрачена доказова інформація, яка має суттєве значення для розкриття злочину та встановлення особи, яка його вчинила.

Питання процесуальної регламентації та тактики проведення впізнання завжди привертали увагу вчених-криміналістів. Багатоаспектність даної проблеми, а також важливість результатів впізнання для практики кримінального судочинства визначають актуальність подальшого дослідження цих питань.

Проблемам законодавчого регулювання слідчих дій і, зокрема, пред'явлення для впізнання присвятили свої наукові праці відомі вчені: Р.С. Бєлкін, Ю.М. Грошевий, А.В. Іщенко, І.П. Козаченко, В.І. Комісаров, В.О. Коновалова, Є.Д. Лук'янчиков, В.Т. Томін, Л.Д. Удалова, П.П. Цвєтков, В.Ю. Шепітько, М.Є. Шумило та інші. Не зважаючи на значні наукові доробки вчених-правознавців, необхідно зазначити, що в роботах багатьох авторів пред'явлення для впізнання досліджувалося фрагментарно, а питанням пред'явлення особи для впізнання за функціональними ознаками приділялося зовсім мало уваги. Аналізуючи викладене вище, можна констатувати, що не вирішеність процесуальних і криміналістичних проблем вимагає більш ґрунтов-