1)експертизу мережених пристроїв; 2) експертизу програмних продуктів, що застосовуються в телекомунікаційних технологіях; 3) експертиза мобільних телекомунікаційних пристроїв [7, с. 98–99].

Підсумовуючи зазначимо, що ефективне розслідування злочинів проти правосуддя можливе за умови використання допомоги спеціалістів, в тому числі й шляхом призначення судових експертиз, які в свою чергу, потребують подальшого теоретичного осмислення та розроблення експертних методик з врахуванням потреб сьогодення.

Список бібліографічних посилань: 1. Книженко С. О. Криміналістична класифікація злочинів проти правосуддя. *Право і Безпека*. 2013. № 1 (48). С. 113–118. **2.** Ямашкин А. С. Методика расследования побегов с мест лишения свободы. М. : Юрлитинформ, 2012. 208 с. **3.** Якименко Р. В. Щодо способів фальсифікації слідів капілярних узорів рук людини та можливостей їх виявлення при проведенні дактилоскопічної експертизи. *Криміналістика і судова експертиза.* 2019. Вип. 64. С. 464–480. **4.** Гайдук О. Г. Особливості проведення дактилоскопічної експертизи з урахуванням можливості фальсифікації слідів. *Наукові записки Національного університету «Острозька академія». Серія «Право».* 2006. Вип. 7. С. 237–238. **5.** Богословська М. О. Деякі аспекти судово-лінгвістичної експертизи. *Вісник Академії адвокатури України.* 2009. № 1 (14). С. 152–158. 6. Кихтюк О. До методологічної проблеми психолінгвістичної експертизи // inforum : сайт. URL: https://www.inforum.in.ua/conferences/19/46/319 (дата звернення: 12.10.2019). **7.** Практикум з криміналістики : навч. посіб. / за ред. В. Ю. Шепітька. Київ : Ін Юре, 2013. 128 с.

Одержано 15.10.2019

УДК 343.98

Ілля Олександрович КОВАЛЕНКО,
аспірант кафедри криміналістики, судової медицини та психіатрії, викладач кафедри кримінально правових дисциплін Дніпропетровського державного університету внутрішніх справ

ДЕЯКІ АСПЕКТИ ПРОВЕДЕННЯ ДОПИТУ ПОТЕРПІЛОГО ПРИ РОЗСЛІДУВАННІ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Вивчення судової та слідчої практики показує, що одним з найпоширеніших та складних в тактичному відношенні слідчих (розшукових) дій у справах про шахрайство, вчинене у сфері використання

банківських електронних платежів, є допит потерпілих та свідків. Провівши аналіз кримінальних правопорушень про шахрайство у сфері банківських електронних платежів, допит потерпілого проводиться практично у кожному випадку. Як зазначають ряд авторів, допит спрямований на встановлення безпосереднього предмета розкрадання, його кількість, види та стану, способу розкрадань чи зловживань, осіб, які брали участь у цих операціях, їх способу життя, майнового стану, оточення та іншої інформації, яка може зацікавити слідство [2, с. 19].

Для досягнення більшої ефективності слід заздалегідь скласти перелік питань, що підлягають з'ясуванню, це дозволить уникнути проведення повторного допиту. В ході допиту потерпілого або свідка, за умови повного усвідомлення нею того, що сталося, і бажанні допомогти, встановленні істини, використовуються наступні тактичні прийоми, розроблені в криміналістиці: бесіда, відновлення в пам'яті забутого, уточнення і деталізація показань. Як правило, слідчі при підготовці до допиту звертаються за допомогою до фахівців-криміналістів в галузі ІТ-безпеки, яких, на превеликий жаль, не вистачає.

Кримінальні правопорушення у вигляді шахрайства у сфері банківських електронних платежів відносять до злочинів з використанням інформаційних технологій, які здійснюються, як правило, віртуально за допомогою всесвітньої мережі інтернет, і в криміналістиці характеризуються як комп'ютерні злочини (кіберзлочини) з економічним напрямом.

Серед науковців, які періодично пропонують різні правки і доповнення щодо удосконалення організаційно-правових засад протидії кіберзлочинності в Україні, є: С. С. Чернявський, О. М. Бандурка, Ю. М. Батурін, В. Б. Вехов, В. А. Голубев, М. Д. Діхтяренко, Ю. В. Онищенко, О. В. Орлов, Б. В. Романюк.

Такі злочини, як правило, здійснюються за допомогою спеціальних програм, які маскують реальне місце знаходження особи злочинця, так званих анонімайзерів, таких як: VPN – скорочена назва від англ. Virtual Privat Network – віртуальна приватна мережа, Socks – скорочена назва від англ.Socked Secure – мережевий протокол, та ін. Здебільшого такі злочини вчиняються організованими злочинними групами та кваліфікуються за ознаками ч. 3 ст. 190 КК України [1].

Якщо брати міжнародний досвід таких розвинутих країн як США, шахрайство в сфері банківських електронних платежів також відносять до комп'ютерних злочинів і входять в програму NTCP, а органи які розслідують такі види злочинів відносяться до спеціального відділу FBI [3, с. 9].

Підводячи висновки, зазначимо, що допит потерпілих є важливою складовою при розкритті шахрайства, вчиненого в сфері банківських електронних платежів, і спрямований на встановлення безпосереднього предмета розкрадання. Головною проблемою є нестача відповідних фахівців- криміналістів в галузі ІТ-безпеки, які б пришвидшували розкриття даних злочинів та розробляли відповідні методики для протидії.

Список бібліографічних посилань: 1. Кримінально процесуальний кодекс України : закон України від 18.10.2019 № 4651-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 10.10.2019). **2.** Пчеліна О. В., Корнієнко В. В. Особливості розслідування злочинів, вчинених шляхом кредитнофінансових операцій : метод. рек. Харків : Харків. нац. ун-т внутр. справ, 2011. 36 с. **3.** Преступления, связанные с компьютерной информацией. *Зарубежный опыт.* 2000. Вып. 5. С. 7–12.

Одержано 12.10.2019

УДК 343.1

Валентина Павлівна КОРЖ,
доктор юридичних наук, професор,
почесний працівник прокуратури України,
професор кафедри кримінального процесу,
криміналістики та експертології факультету № 6
Харківського національного університету внутрішніх справ;
https://orcid.org/0000-0002-9431-8727

ТАКТИЧНІ ОСОБЛИВОСТІ ОГЛЯДУ СЛУЖБОВОГО ПРИМІЩЕННЯ БАНКІВСЬКОЇ УСТАНОВИ, НА ЯКУ ЗДІЙСНЕНО ОЗБРОЄНИЙ НАПАД

Найбільш розповсюдженими видами бандитизму є озброєні напади членів банди на банківські, фінансові установи. Місцем події у цій ситуації є приміщення, офіси банківських установ.

Завдання огляду:

– вивчити обстановку події озброєного нападу на банківську установу;

– з'ясувати характер і механізм нападу;

– встановити час, спосіб вчинення нападу, зброю, знаряддя злочину, його наслідки, ймовірну кількість злочинців;

– встановити особу потерпілого;