УДК: 343.98.06
DOI: 10.15587/2523-4153.2021.235769

ІНТЕРНЕТ-ШАХРАЙСТВА: ТЕХНОЛОГІЇ ВЧИНЕННЯ, ШЛЯХИ ПРОТИДІЇ ТА ЗАПОБІГАННЯ

О. А. Самойленко, К. В. Тітуніна

How to Cite:
Samoilenko, O., Titunina, K. (2021). Internet fraud: technologies of performance, ways of counteraction and prevention. ScienceRise: Juridical Science, 2 (16), 65–70. doi: http://doi.org/10.15587/2523-4153.2021.235769

The article proves that the separation of technologies for committing fraud on the Internet allows you to determine the causal complexes. As a result, it is possible to effectively influence the prevention and counteraction of the corresponding type of crime. The author concludes that it is necessary to introduce into the practice of law enforcement and other government agencies effective tools for preventing and combating Internet fraud. He sees such a tool as outreach activities and modes of action that will block the determinants of criminal behavior in cyberspace. In order to concretize the specified means of prevention, it also deepens the theoretical basis regarding the system for preventing Internet fraud. So, the author comes to the conclusion that counteraction is a system of measures and methods of activity not only of law enforcement agencies, but also of other state and non-state bodies, while among these measures there are measures to prevent certain types of crimes.

The article indicates that in the process of implementing a certain type of cybercrimes by criminals, they talk about the technologies of criminal activity as complexes of interrelated crimes, united by a single criminal purpose. For the commission of Internet fraud in the technology of criminal activity, there are typically ways of committing crimes in the use of computers, systems and computer networks and telecommunication networks (provided for in Section XVI of the Criminal Code of Ukraine) and Art. 200 of the Criminal Code of Ukraine. As a result of the analysis of the materials of the forensic practice of investigating fraud on the Internet, two main technologies have been identified: 1) the seizure of funds using phishing sites (the methods of reporting false information from the victim and its content have been updated) 2) the seizure of funds using a bank payment card and / or ATM (the variability of the method of manipulating information has been updated).

Keywords: *prevention, means, Internet, false information, counteraction, investigation, method, technology, fraud*

© The Author(s) 2021
This is an open access article under the Creative Commons CC BY license

1. Вступ

За офіційними даними Департаменту кіберполіції Національної поліції України в 2020 році понад 80 % повідомлень громадян стосувалися шахрайських дій у віртуальному простор [1]. Це актуалізує такий напрямок в діяльності правоохоронних органів як протидія Інтернет-шахрайствам. Основною ознакою сучасної ситуації у сфері протидії Інтернет-шахрайству в Україні є потреба у оновлення системи запобігання останнім. Для її розроблення обов'язковим є поглиблення теоретичних знань щодо технологій вчинення Інтернет-шахрайств, способів оптимізації досягнення кінцевої злочинної мети шахрая, що діє із використанням кіберпростору.

2. Літературний огляд

У більшості праць питання протидії шахрайствам, учиненим із використанням мережі «Інтернет», розглянуто насамперед в контексті швидкого реагування правоохоронних органів на заяви та повідомлення про вчинення кримінальних правопорушень в мережі Інтернет та здійснення ефективного впливу на процес розслідування конкретного виду такого шахрайського прояву засобами оперативної та слідчої діяльності. Законодавець же, використовуючи терміни «протидія» в численних законах України, міжвідомчих та відомчих нормативно-правових актах Національної поліції України та інших правоохоронних органів, розширено тлумачить зміст цього терміну та виділяє в системі заходів впливу на злочинність протидію та запобігання. Термін «протидія» вживається стосовно різних сфер діяльності: правоохоронних органів по відношенню до певного виду злочинності [2, 3]; злочинців по відношенню до процесу розслідування [4, 5]; міжнародної спіль-

ноти щодо тероризму, корупції тощо [6]. Обґрунтувати це можна етимологією категорії «протидія» – це дія, що перешкоджає іншій дії. Цим і пояснюється різноманітність видів, форм та суб'єктів протидії. Працівник оперативного підрозділу має своїм безпосереднім завданням пошук і фіксація фактичних даних про кримінальні правопорушення, а також їх в інтересах кримінального судочинства, слідчий – здійснення досудового розслідування в ході якого прагне встановити приховувані про кримінальні правопорушення факти і обставини та подолати опору з боку незацікавлених в успішному розслідуванні справи осіб. Злочинець прагне уникнути кримінальної відповідальності або покарання, виконуючи для цього різні способи дії, в тому числі й опосередковано через інших осіб. Наявність протилежних цілей із злочинцем обумовлює конфлікт інтересів, що зазвичай є нормою у кримінально-процесуальних відносинах, оскільки останні виникають у зв'язку із пошуком та залученням до кримінальної відповідальності конкретної особи та припускають настання відносно неї покарання. Державою в цілому з метою протидії злочинності здійснюється низка заходів за різними напрямками діяльності, зокрема: виявлення, припинення (документування), розслідування кримінальних правопорушень; запобігання злочинам шляхом застосування заходів кримінально-правового характеру притягнення винних до відповідальності; забезпечення відшкодування шкоди, розвиток співробітництва з різноманітними інститутами суспільства тощо. Тож, протидія представляє собою систему заходів та способів діяльності не тільки правоохоронних органів, а також й інших державних та недержавних органів, при цьому серед цих заходів присутні заходи запобігання, як злочинності в цілому, так й окремих видів злочинів. Поштовх розробленню науково обґрунтованої системи запобігання Інтернет-шахрайствам може дати розуміння сучасного стану розвитку злочинної поведінки у мережі Інтернет, аналіз існуючих технологій такої шахрайської діяльності. Відокремлення останніх дасть змогу визначити причинні комплекси та ефективно впливати на запобігання відповідного виду злочинності.

3. Мета та завдання дослідження

Метою дослідження є обґрунтування впровадження в практику правоохоронних та інших державних органів ефективних інструментів запобігання та протидії Інтернет-шахрайствам.

Для досягнення мети були поставлені такі завдання:

– класифікувати технологій вчинення Інтернет-шахрайств;

– поглибити теоретичну базу щодо сучасної системи запобігання Інтернет-шахрайствам.

4. Матеріали і методи

Методологічну основу дослідження складає комплекс загальнонаукових методів: діалектичний, системно-структурний, формально-логічні, моделювання. В результаті системного підходу за допомогою методу системного аналізу конкретизовано окремі інструменти запобігання та протидії Інтернет-шахрайствам. Теоретичною базою дослідження стали наукові праці іноземних та вітчизняних учених, закони України та підзаконні акти; емпіричну базу дослідження становлять інтерв'ювання слідчих та узагальнення практики розслідування Інтернет-шахрайств (станом на 1 травня 2021 року).

5. Результати дослідження та їх обговорення

В процесі реалізації злочинцями окремого виду кіберзлочинів ведуть мову про наявність технології злочинної діяльності як комплексу взаємопов'язаних злочинів, що об'єднуються єдиною злочинною метою. Фактично ж вони утворюють алгоритмічну систему способів дії, що й забезпечує настання бажаного злочинного результату. Така система дій забезпечує ефективність злочинного процесу в мережі Інтернет. Для вчинення Інтернет-шахрайства в технології злочинної діяльності типово присутні способи вчинення злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (передбачених розділ XVI КК України) та/або ст. 200 КК України, тому можна визначити дві основні технології.

1. *Заволодіння грошовими коштами за допомогою фішингових сайтів* (30 % діянь, кваліфікованих за ч.3 ст. 190 КК). Використовують сайти фіктивні, спеціально створені злочинцем з метою отримання від жертви інформації (персональних даних, логінів та паролів, зокрема до систем дистанційного банківського обслуговування) або безпосередньо безготівкових коштів. Отримавши в результаті введення в оману доступ до облікових записів жертв, злочинець блокує доступ законних користувачів до аккаунтів шляхом змінення паролів, налаштовує систему в своїх корисливих цілях. Ця технологія постійно удосконалюються, адже злочинець, що вчиняє шахрайство таким способом є впевненим користувачем, здатний підвищувати свій професійний рівень, може відмовитись від участі в організованій злочинній групі та здійснювати індивідуальну злочинну діяльність (більше половини злочинців діють одноособно) [7, с. 126–127]. Як фахівець високої кваліфікації він використовує технології анонімізації доступу до ресурсів мережі Інтернет, через що має

високий ступінь географічної мобільності. Жертвами шахрайства стають, як правило, занадто довірливі або неуважні звичайні користувачі, які самі (добровільно) надають конфіденційну інформацію, коли їх просять перейти за електронним посиланням на нібито справжній сайт сервісу, пошти, платіжної системи, сторінки в соціальній мережі тощо, повторити введення пароля, повідомити номер рахунку та пароль для реєстрації покупки або грошового переказу, зареєструватися на фіктивному сайті Інтернет-магазину, інтернет-аукціону тощо.

Враховуючи варіативність змісту та способу повідомлення неправдивої інформації жертви, у вказаній технологій спосіб введення в оману потерпілого можна класифікувати за способом повідомлення та змістом неправдивої інформації:

1) користувачі-жертви отримують масову електронну розсилки листів, зовнішньо мають вигляд офіційних від сервісів та адміністрацій електронної пошти, банків, платіжних систем, соціальних мереж тощо. Їм повідомляють про нестандартні ситуації на сервісі, наприклад, необхідності оновити реєстраційні дані, здійснити перехід за посиланням. В результаті таких дій користувач заходить на фіктивний сайт, який має подібну до офіціальної сторінки архітектуру, близький за звучанням домен, тим самим вводять в оману потерпілого та добровільно від нього отримують інформацію, що буде використана для отримання доступу до персональних даних, відповідно й електронних рахунків потерпілого, що дає можливість заволодіти коштами останнього.

2) користувачі-жертви через неуважність знаходять та користується за призначенням фіктивною сторінкою сайтів відомих ресурсів мережі Інтернет («Інтернет-магазини», «Дошки оголошень», сервіси електронних платіжних систем тощо). Сайт-копія подібний або наближений до сайту-оригіналу, використовуються також аналогічні доменні імена, що призводить до введення в оману потерпілого та, наприклад, сплати ним вартості обраних товарів чи послуг на підставні рахунки, надання доступу злочинцям до персональних даних та здійснення ними в подальшому платіжних операцій з чужими рахунками.

3) користувачі-жертви масово отримують дзвінок нібито від імені Інтернет-сервіса чи організації, клієнтами яких вони є. Потерпілому називають легендовану причину дзвінка поєднану із проханням оновити персональні дані (логіни, коди, номери кредитних карток, рахунків тощо) шляхом передачі останніх устно або користуючись панеллю телефону. Для реалізації цій технології використовують можливостей «Інтернет-телефонії» (так звана технологія VoIP) гарантуючи надійність та швидкість передачі передачі даних цією технологією, суб'єкти надання таких послуг вказують на можливість передання прихованих даних.

4) користувачі-жертви перенаправляються на фіктивний сайт шляхом «спуфінг» (від англ. «spoof» – містифікація) – це кібер-атака, в рамках якої шахрай видає себе за яке-небудь надійне джерело, щоб дістати доступ до важливих даних або інформації [8]. Така підміна (спуфинг-атака) може відбуватися через веб-сайты, електронну пошту, телефонні дзвінки, текстові повідомлення, IP-адреси і сервери декількома способами: шляхом зміни IP-адреси, MAC-адреси, шляхом підміни адрес IP-пакетів (syslog), в результаті икористанні чужої IP-адреси для обману системи безпеки (як вид хакерської атаки).

5) користувачі-жертви перенаправляються на фіктивний сайт шляхом «фармінг» (англ. «farming» – займатися сільським господарством, тваринництвом). Це спосіб шахрайства э більш модернізованим, при якому шкідливий код встановлюється на комп'ютер або сервер жертви [9, с. 53–54]. Цей код міняє інформацію по IP-адресах, внаслідок чого користувач-жертва перенаправляється на фіктивні веб-сайти без їх відома і згоди. Після того, як користувач переходить на фіктивний сайт, йому пропонується ввести свою персональну інформацію, яка потім й буде використана для заволодіння коштами. Основними цілями для фармінг є користувачі он-лайн-банків або інших фінансових систем і валютно-обмінних сервісів. Його по-суті віднести до фішингу можна умовно, адже фарминг не вимагає від користувачів попередніх дій: вони перенаправляються на фіктивні сайти автоматично без їх відома за рахунок роботи шкідливого програмного засобу. Цей спосіб можна вважати модернізованим (вдосконаленим), бо його механізм реалізації пов'язаний із потаємним перенаправленням користувача на фішингові сайти, що стає можливим завдяки наступним обставинам: а) комп'ютерна система користувача заздалегідь піддається вірусній атаці; б) комп'ютерна система, що тепер містить шкідливий програмний засіб (вірус) автоматично активує вірусний код при першій спробі звернення до неї; в) саме вірусний код і перенаправляє комп'ютерну систему на фішингові сайти. Висока потаємність фармінгу забезпечується завдяки мінімальній участі користувача-жертви у взаємодії з комп'ютерною системою.

2. *Заволодіння грошовими коштами за допомогою банківської платіжної картки та/або банкомату* (20 % діянь). Така злочинна діяльність в Україні найчастіше кваліфікується за сукупністю ст.ст. 200, 190 КК України. Можна навести такі сучасні закономірності названої злочинної діяльності:

1) суть обману з використанням платіжної картки та/або банкомату при вчиненні шахрайств із використанням мережі «Інтернет» полягає у використанні технічні можливості Інтернет, дистанційного керування електронною інформаційною системою;

2) злочинець вдається до маніпулювання інформаційними потоками, змінюючи їх з корисливою метою;

3) складність технологій і тип злочинця нерозривно пов'язані; чим вище професіональний рівень зловмисника, тим складнішою є технологія;

4) початкові дії традиційного злочинця можуть бути, як спрямовані на незаконний вплив на засоби комп'ютерної техніки та інформацію, так й не спрямовані;

5) така злочинна діяльність пов'язана із застосуванням комплексу спеціальних комп'ютерних технологій, що дозволяють отримати доступ до інформації про банківські картки та дані їх власників [10, с. 70–71].

Враховуючи варіативність змісту та способу маніпулювання інформацією, спосіб введення в оману потерпілого можна класифікувати наступним чином:

1) копіювання інформації з магнітної смуги платіжної картки та отримання ПІН-коду до неї шляхом попереднього придбання (або виготовлення) та встановлення на банкомати пристроїв зчитування. Всі ці дії у комплексі отримали назву «скіминг» (з англ. «skimming» – «зняти вершки») [11]. Для реалізації цього способу шахрайства вчиняються різноманітні, в залежності від професійного рівня злочинця підготовчі дії, зокрема можливе: виготовляють банкомат, що за зовнішнім виглядом майже не відрізняється від тих, які використовують справжні банки; банкомат встановлюють у людному місці; через електронні дошки оголошень або соціальні спільноти злочинець замовляє та отримує пристрій, що має функції зчитування, стирання, передання, запису інформації на магнітній смузі пластикової платіжної карти; використовуючи ті самі ресурси, злочинець підшукує так званих виконавців (так званих «дропів» (від англ. drop «скидати, упускати»), які фізично через банкомати будуть встановлювати пристрої та знімати їх та безпосередньо гроші з карткових рахунків); «дропи» встановлюють пристрої на банкомати та знімають їх в подальшому для оброблення інформації тощо.

Після поміщення потерпілим картки до приймального отвору банкомату та ведення ПІН-коду на моніторі банкомату з'являється повідомлення про неможливість виконання запитаної операції з певних причин (відсутність зв'язку із банком або інша причина, через яку виконання запиту є неможливим. Втім, у цей час пристрій в банкоматі або сам банкомат записує інформацію з картки в окремий файл, в тому числі й пін-код карти та передає злочинцю, або мережею «Інтернет», або в подальшому фізично як носій інформації. Таким чином, шахрай отримує необхідні дані для дистанційного керування рахунком потерпілого або створення дубліката банківської картки.

2) «клонування» (підробка) платіжної картки та зняття готівки в банкоматах. Найбільшого поширення сьогодні набув такий алгоритм дій (технологія з визначеними етапами злочинної діяльності):

а) отримання пристрою, що має функції зчитування, стирання, запису інформації на магнітній смузі пластикової платіжної карти;

б) підшукання персональних банківських відомостей (однаково поширеним є, або за допомогою кріпто-валюти (часто «btc») придбання в мережі так званих «дампів» про чужі банківські карти, або шляхом фізичного копіювання інформації з магнітної смуги платіжної картки та отримання ПІН-коду;

в) використання «білого пластику» або підбір платіжних карт у вигляді емітованих в установленому законодавством порядку пластикових карток, що використовуються для переказу грошей з рахунку платника або відповідного рахунку банку, оплати товарів і послуг через банківські термінали;

г) за допомогою придбаного раніше обладнання здійснюється запис інформації на магнітні смуги підібраних для цього платіжних карток, отримуючи таким чином їх копії. Інформація може бути навіть не персоніфікованою, але функціональною за призначенням. Після виготовлення таких копій банківських карток зловмисник проводить низку несанкціонованих трансакцій через банкомати. Злочинець прагне максимально скоротити час між моментом, коли жертва в останнє користувалась карткою в банкоматі, та моментом зняття з карткового рахунку коштів за допомогою картки-клону.

3) фіксація диспенсеру банкомату для привласнення в подальшому злочинцем готівки, яка була списана з карткового рахунку законного держателя картки (в англ.. публікаціях отримав назву «Cash Trapping» – «кеш-траппинг»). Даний спосіб шахрайського заволодіння має два різновиди. В першому випадку кэш-траппинг є разовою крадіжкою грошей безпосередньо у певного клієнта: на зону видачі грошей встановлюється спеціальна пастка (це механічні затиски різних конструкцій і пристрою з суперв'язким клеєм), яка захоплює грошові кошти у момент видачі їх банкоматом. Потерпілий після користування карткою не отримує кошти, а наступна особа-злочинець забирає його кошти з банкомату разом з пристроєм. Другий варіант кэш-траппинга

складніший – злочинець використовує для заволодіння грошима спеціальний механічний пристрій, яка встановлюється всередину механізму видачі готівки банкомату. Алгоритм такий: шахрай самостійно проводить операцію зняття по карті грошових коштів на невелику суму, у момент отримання грошей він механічно віджимає шторку презентера банкомату і вставляє пастку («рогатку»), після чого шторка закривається. Подальша операція зняття готівки тим або іншим добросовісним утримувачем карти закінчується захопленням грошей – купюри впираються в спеціальний ступор «рогатки» і залишаються усередині банкомату. Клієнт, не одержавши грошей, йде, злочинець повертається, виламує шторку презентера і виймає пастку з грошовими коштами, що потрапили в неї. Згідно з доповіддю Європейської асоціації безпечних транзакцій (EAST), було встановлено, що в 2019 році кількість фізичних атак, пов'язаних з банкоматами, збільшилась на 27 % порівняно з 2017 роком, а збитки від них склали 36 мільйонів євро, або на 16 % більше ніж в 2017 году [12].

В подальшому шахраї вдосконалили вищенаведений механізм шахрайства, він отримав назву скасування трансакцій «Transaction Reversal Fraud» – це втручання в роботу банкомату при здійсненні операцій видачі готівки, яку залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником. Такі дії не кваліфікуються за ст.190 ч.3. КК України, але в практиці протидії Інтернет-шахрайству вважаються одним з його способів. На етапі підготовки до вчинення злочину злочинець відкриває в банку карту на ім'я «дропа»; розміщує на картковий рахунок значну суму грошей. Після чого, встановивши по вищеописаній схемі пастку в банкомат при знятті невеликої суми з своєї карти, він проводить операцію зняття готівки на всю суму залишку. Банкомат не може коректно завершити операцію по видачі і «оцінює» ситуацію як збій, про який в банк, процесинговий центр (хост) поступає відповідна інформація з «командою» проведення операції онлайн-відміни операції видачі готівки, внаслідок чого гроші, заблоковані раніше при операції зняття готівки, повертаються на рахунок, а шахрай описаним вище способом забирає гроші з пастки. А оскільки зняті засоби знов «повернулися» на рахунок, шахрай таким же способом знімає їх вже в іншому банкоматі. Такі маніпуляції можуть бути здійснені багато разів, поки банк не виявить ці дії і не заблокує карту.

6. Висновки

1. Визначено дві основні групи технологій шахрайської діяльності у кіберпросторі:

– заволодіння грошовими коштами за допомогою фішингових сайтів (варіативність змісту та способу повідомлення неправдивої інформації жертви дає можливість здійснити їх класифікацію за способом повідомлення та змістом неправдивої інформації);

– заволодіння грошовими коштами за допомогою банківської платіжної картки та/або банкомату (варіативність змісту та способу введення в оману дозволяє виділити її різновиди). На відміну від класичних способів фішингу, коли користувачеві треба довірятись електронним листам, вчиняти дії, наприклад, переходити за електронним посиланням на інші сайти, технологічно-оновлені способи («спуфінг», «фармінг») вимагають від користувачеві просто відвідати офіційний сайт (ввести адресу самостійно чи скористатися закладкою), а комп'ютерна система автоматично його направляє на підроблений.

2. Класифікація технологій Інтернет-шахрайства дозволяє стверджувати, що сучасна система запобігання Інтернет-шахрайствам має включати в себе інформаційно-просвітницьки заходи та способи дії, які будуть нейтралізувати чи блокувати детермінанти злочинної поведінки в кіберпросторі. Така інформаційно-просвітницька діяльність спрямована на постійне збільшення кількості людей, які поінформовані про групу «класичних» способів фішингу та технологічно-оновлених способів («спуфінг», «фармінг»). У систему запобігання Інтернет-шахрайсвам обов'язково повинні входити заходи активізації роботи Інтернет-сервісів, банківських та інших платіжних систем, соціальних мереж та інших служб щодо попередження користувачів щодо потенційних ризиків стати жертвою шахрая, як за допомогою фішингових сайтів, так й з використанням банківської платіжної картки та/або банкомату, зокрема шляхом:

– застосування властивих суб'єктам оперативно-розшукової діяльності засобів та методів;

– оприлюднення офіційних, аналітичних оглядів, статистичних даних щодо виявлення державними органами фактів вчинення таких злочинів;

– доведення з боку суб'єктів ринку телекомунікаційних послуг до користувача технічних аспектів функціонування мережі, які забезпечуватимуть кіберзахист користувача;

– введення додаткових форм перевірки здійснення платежів власником банківської платіжної картки з боку фінансових та банківських установ, платіжних систем;

– висвітлення офіційних заходів з питань кібербезпеки, оприлюднення результатів журналістських розслідувань з боку представників засобів масової інформації. Вказані заходи дозволять в цілому підвищити ефективність спільної діяльності у сфері протидії Інтернет-шахрайствам.

Література

1. У 2020 році до кіберполіції надійшло понад 30 тисяч звернень щодо шахрайства в Інтернеті (2021). Available at: https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/
2. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (2019). Закон України № 361-IX. 06.12.2019. Available at: https://zakon.rada.gov.ua/laws/show/361-20#Text
3. Про затвердження Положення про Департамент кіберполіції НП України (2015). Наказ Національної поліції України № 85. 10.11.2015. Available at: https://cyberpolice.gov.ua/normatyvno-pravovi-akty-yaki-rehlamentuiut-diialnist-politseiskoi-komisii/
4. Орлов, П. І., Волобуєв, А. Ф., Осика, І. М. та ін. (2004). Протидія економічній злочинності. Харків: Нац. ун-т внутр. справ, 568.
5. Бутузов, В. М., Павловський, В. Д., Скалозуб, Л. П. та ін.; Романюк, Б. В., Скулиш, Є. Д. (Ред.) (2011). Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій. Київ, 404.
6. Косенкова, Н. А., Сіродан, Т. О. (2014). Протидія кіберзлочинності. Київ, 48.
7. Самойленко, О. А.; Волобуєв, А. Ф. (Ред.) (2020). Основи методики розслідування злочинів, вчинених у кіберпросторі. Одеса: ТЕС, 372.
8. Wi-Fi-злодії: способи захисту. Незалежна асоціація банків України. Available at: http://anticyber.com.ua/article_detail.php?language=ua&id=108
9. Самойлов, С. В. (2014). Розслідування шахрайств, учинених із використанням мережі Інтернет. Донецьк, 226.
10. Самойленко, О. А. (2018). Характеристика технологій вчинення злочинів у кіберпросторі. Судова та слідча практика в Україні, 7, 64–71.
11. Sidel, R. (2015). Theft of debit card data from ATMs soars. The Wall Street Journal. Available at: https://www.wsj.com/articles/theft-of-debit-card-data-from-atms-soars-1432078912
12. HSBC UK pilot of new, industry-first technology reduces ATM “cash-trapping” fraud losses by 50 % (2015). HSBC Holdings plc. Available at: https://www.atmia.com/news/hsbc-uk-pilot-of-new-industry-first-technology-reduces-atm-cash-trapping-fraud-losses-by-50/9188/

Received date 06.04.2021
Accepted date 12.05.2021
Published date 30.06.2021

Самойленко Олена Анатоліївна, доктор юридичних наук, доцент, Відділ дослідження проблем протидії кіберзлочинам та загрозам інформаційної безпеці, Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, пл. Солом’янська, 1, м. Київ, Україна, 03035

Тітуніна Катерина Вікторівна, кандидат юридичних наук, Відділ дослідження проблем протидії кіберзлочинам та загрозам інформаційної безпеці, Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, пл. Солом’янська, 1, м. Київ, Україна, 03035

***Corresponding author:** Olena Samoilenko, e-mail: samoilenko_elena@ukr.net