УДК 343
DOI https://doi.org/10.32782/2524-0374/2022-8/60

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТА ВИДИ РОЗКРАДАНЬ ШЛЯХОМ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ЯК ОДНОГО З НАЙПОШИРЕНІШИХ ВИДІВ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ

GENERAL CHARACTERISTICS AND TYPES OF EMBEZZLEMENT THROUGH THE USE OF INFORMATION TECHNOLOGY AS ONE OF THE MOST COMMON TYPES OF CRIMINAL OFFENSES IN CYBERSPACE

Думчиков М.О., старший викладач
кафедри кримінально-правових дисциплін та судочинства
Навчально-науковий інститут права Сумського державного університету

Малетов Д.В., викладач-стажист
кафедри кримінально-правових дисциплін та судочинства
Навчально-науковий інститут права Сумського державного університету

Світовий науково-технологічний прогрес призвів до появи великої кількості нових технологій. Такі технології впровадили велику кількість інновацій в суспільне життя людей. Важливою точкою розвитку вважається поява перших комп'ютерів та комп'ютерних мереж, що в свою чергу відкрило для людства велику кількість можливостей. Беручи до уваги всі особливості прогресу та інші фактори, можна вважати закономірним появу нової кримінальної ланки в кіберпросторі.

Кримінальні правопорушення у кіберпросторі сьогодні є дуже актуальною проблемою суспільства. Про її актуальність свідчать новини по всьому світу, кримінальна статистика, проблемні питання науці кримінального права, а також проблеми в кримінальному процесі. Все це пов'язано з тим, що як явище, кримінально протиправних діянь у кіберпросторі є дуже специфічною категорією, яка постійно розвивається паралельно з технічним прогресом.

У науковій статті проаналізовано такі види кримінальних правопорушень у кіберпросторі, як «кардинг» та «фішинг». Визначені основні проблеми з якими зіштовхуються слідчі під час розслідування кримінальних правопорушень у кіберпросторі у формі розкрадань. Наголошено на необхідності розроблення методики розслідування кримінальних правопорушень у кіберпросторі. Розглянуто можливості, комп'ютерно-технічної експертизи в якості важливого підмоги в розкритті та розслідуванні кримінальних правопорушень, пов'язаних з розкраданнями коштів з банківських карт.

Метою наукової статті є дослідження розкрадань майна та грошових коштів шляхом використання інформаційних технологій, визначити особливості та тактичні прийоми під час розслідування такого кримінального правопорушення, дослідити загальну характеристику суміжних явищ, а також визначити загальну суспільну небезпечність кіберзлочинності а також вивчення шляхів протидії цій кримінальній категорії.

Об'єктом наукової статті є відносини, що виникають у зв'язку з функціонуванням розкрадання у сфері інформаційних технологій як одного із найпопулярніших видів кіберзлочинності.

Предметом наукової роботи є особливості розкрадання у сфері інформаційних технологій як одного із найпопулярніших видів кіберзлочинності.

Ключові слова: кримінальні правопорушення у кіберпросторі, кіберзлочини, кіберпроступки, розкрадання майна шляхом використання інформаційних технологій, кардинг, фішинг.

World scientific and technological progress has led to the emergence of a large number of new technologies. Such technologies introduced a large number of innovations into people's social life. The appearance of the first computers and computer networks is considered an important point of development, which in turn opened up a large number of opportunities for mankind. Taking into account all the features of progress and other factors, the emergence of a new criminal link in cyberspace can be considered natural.

Criminal offenses in cyberspace are a very urgent problem of society today. Its relevance is evidenced by news around the world, criminal statistics, problematic issues of the science of criminal law, as well as problems in the criminal process. All this is due to the fact that, as a phenomenon, criminal acts in cyberspace are a very specific category that is constantly developing in parallel with technological progress.

The scientific article analyzes such types of criminal offenses in cyberspace as "carding" and "phishing". The main problems faced by investigators during the investigation of criminal offenses in cyberspace in the form of embezzlement have been identified. The need to develop a methodology for investigating criminal offenses in cyberspace is emphasized. The possibility of computer and technical examination as an important aid in the disclosure and investigation of criminal offenses related to embezzlement of funds from bank cards is considered.

The purpose of the scientific article is to study the theft of property and money through the use of information technologies, to determine the peculiarities and tactical techniques during the investigation of such a criminal offense, to investigate the general characteristics of related phenomena, as well as to determine the general public danger of cybercrime, as well as to study ways of countering this criminal category.

The object of the scientific article is the relations arising in connection with the operation of theft in the field of information technologies as one of the most popular types of cybercrime.

The subject of the research paper is the peculiarities of theft in the field of information technologies as one of the most popular types of cybercrime.

Key words: criminal offenses in cyberspace, cybercrimes, cybermisdemeanors, theft of property through the use of information technologies, carding, phishing.

Виклад основного матеріалу. Сучасні технології міцно увійшли в наше повсякденне життя і тепер є невід'ємною її частиною. Говорячи про Інтернет, можна сказати, що дана сфера взаємодії людей стрімко розвивається. Зараз там можна знайти будь-яку інформацію, в тому числі і кримінального характеру. А що можна сказати про злочини, скоєних за допомогою мережі Інтернет?

На відміну від традиційних видів злочинів, історія яких охоплює століття, такі як вбивство або крадіжка, явище кіберзлочинності є відносно молодим і новим, яке виникло майже одночасно з появою Інтернету.

На разі в сучасній Україні терміни «розкрадання у сфері інформаційних технологій» в нормативно-правових актах офіційно не визначено. У той же час сама концепція була сформована завдяки діяльності правоохоронних органів розвинутих країн Європи та світу, це стосується злочинів у сфері комп'ютерних технологій, незаконного обігу радіоелектронних та спеціальних технічних засобів, розповсюдження неліцензованого програмного забезпечення для комп'ютерів, а також деякі інші види злочинів [1, с. 247].

Найпоширенішим злочином в Інтернеті є розкрадання. Саме в сфері інформаційних технологій розкрадання

розвинулося досить добре і тому має безліч видів. Одним з таких є «кардинг» або інакше кажучи, розкрадання, пов'язане з банківськими картами. Зловмисник може зробити дане діяння шляхом злому серверів інтернет-магазинів, де зберігаються дані про платежі, системи платежів в цілому або злом персонального комп'ютера якогось користувача з метою отримання персональних даних банківських карт, рахунків і т.д.

Викрадення реквізитів, що ідентифікують користувачів в мережі Інтернет як власників банківських кредитних карт, з їх можливим подальшим використанням для здійснення незаконних фінансових операцій (купівля товарів або відмивання грошей) прийнято називати кардинг [2, с. 121].

Підвищений інтерес делінквентов до збільшення кількості онлайн-платежів обумовлює необхідність вдосконалення законодавства в сфері протидії кардингу. Більш того, низький рівень протидії в цій області перетворив кардинг в самостійну сферу кримінального бізнесу з величезною прибутком. Аналіз спеціальної та наукової літератури дозволяє зробити висновок про те, що протидії розкраданням грошових коштів з банківських карт приділяється увага з боку наукового співтовариства.

Актуальність питань, пов'язаних з кримінальною відповідальністю за розкрадання, вчинені з використанням інформаційних технологій, обумовлена тим, що в даний час правопорушення, що посягають на відносини власності, і безпосередньо пов'язані з використанням комп'ютерних технологій і мережі Інтернет, набули широкого поширення і набули яскраво виражений інтернаціональний характер. В абсолютній більшості випадків особи не знають один одного в реальному житті і їх взаємодія реалізується за допомогою віртуальних засобів ідентифікації [3].

Відповідно, забезпечення безпеки в інформаційній сфері вимагає постійного пошуку нових механізмів протидії кіберзлочинності, включаючи правові інструменти, аналізу причин, ризиків і загроз високотехнологічних кримінальних правопорушень проти власності.

Найпоширенішим кримінальними правопорушеннями в мережі Інтернет є розкрадання. Саме в сфері інформаційних технологій розкрадання розвинулося досить добре і тому має безліч видів. Одним з таких є «кардинг» або інакше кажучи, розкрадання, пов'язане з банківськими картами. Зловмисник може зробити дане діяння шляхом злому серверів інтернет-магазинів, де зберігаються дані про платежі, системи платежів в цілому або злом персонального комп'ютера якогось користувача з метою отримання персональних даних банківських карт, рахунків і т.д.

Останнім часом набирає популярність веб-кардинг, т. е. розкрадання грошових коштів з рахунків платіжних карт, віртуальних рахунків, криптовалюта з використанням мережі Інтернет. Низький рівень взаємодії між правоохоронними органами різних держав ускладнює процес протидії вебкардінгу. Для здійснення розкрадань, наприклад, з американських платіжних карт, переходять на режим неспання і сну, схожий до часового поясу США (ведуть свою діяльність вночі, вдень сплять) [4, с. 411].

Звернемося до одного з найбільш важко пізнавальних його видів – скіммінгу, (таке розкрадання здійснюється з використанням спеціальних пристроїв і інструментів, що дозволяють зчитувати відомості платіжних карт (наприклад, магнітної доріжки)). Способи зчитування інформації в даний час існують різні, при цьому безперервний технічний розвиток науки і техніки визначає постійне вдосконалення цих способів злочинцями.

Правоохоронним органам на сьогоднішній день відомі такі способи зчитування магнітних стрічок платіжних карт, як використання спеціальних пристроїв що зчитує магнітною головкою і перехідником для підключення до комп'ютера, які дозволяють обробляти необхідні дані магнітної стрічки карти для подальшого відтворення її вже на підробленої. Крім того, злочинці використовують і мініатюрні відеокамери, завданням яких є отримання даних про PIN-коди платіжних карток [5, с. 148].

Основною проблемою виявлення цих пристроїв на банкоматі або інших терміналах, бензозаправках, вендінгових машинах є їх ретельна маскування і відсутність знань про достовірне зовнішньому вигляді цих терміналів серед громадян. Так, не фахівцеві в даній галузі знань навряд чи вдасться напевно відрізнити банкомат з оригінальними елементами від приймального лотка з накладкою у вигляді магнітної головки. Насамперед, такі пристрої не кидаються в очі, накладки мають оригінальний колір, форму і інші зовнішні дані.

Сутність використання скімерів полягає в можливості таких пристроїв концентрувати здобуту злочинним шляхом інформацію про платіжні картки, а також передавати її по каналах зв'язку в цілях подальшого виготовлення дубліката картки, як для переведення в готівку грошових коштів, так і для здійснення різних покупок без безпосереднього зняття коштів з карти [6, с. 145].

Суттєвою проблемою розкриття таких злочинів є досить високий рівень розвитку так званої «кримінальної електроніки ». Удосконалення способів розкрадань грошових коштів з банківських карт ускладнює створення певного алгоритму дій співробітників правоохоронних органів, що дозволяє грамотно реагувати на подібні факти протиправних дій злочинців.

«Фішинг» – це особливо небезпечний злочин, пов'язаний з помилковими повідомленнями від банків, адміністраторів платіжних систем або розсилка повідомлень в соціальних мережах і ін. В даних повідомленнях найчастіше просять перейти за посиланням для зміни пароля або інших дій, тим самим отримуючи справжні логін і пароль користувача. Метою таких маніпуляцій може бути рахунок в банку, обліковий запис в платіжних системах, електронна пошта і соціальні мережі. Як тільки шахраї отримують те, що їм потрібно, то вони швидко застосовують це для доступу до рахунку банку користувача.

Фішинг можна визначити як отримання шляхом обману або методів соціальної інженерії (Хакерства з використанням людського фактора) персональних даних для використання в корисливих, злочинних цілях. Реалізація фішингу має два механізми: по-перше, посередницьке отримання персональних даних, по-друге, отримання особистих даних у самого їх власника [7, с. 75].

Принцип роботи «фішингу» полягає в перенаправленні користувача на підроблені мережеві ресурси, створені зловмисниками, зовні нічим не відрізняються від справжніх інтернет-сторінок.

Переходячи по прикріпленою до листа посиланням, користувач потрапляє на підроблений сайт, який виглядає так само як справжній сайт будь-якого банку, магазину чи соцмережі. Після того як користувач заповнює форму з логіном і паролем, щоб увійти в свій аккаунт, вони виявляються в розпорядженні зловмисників. Злочинець, отримуючи доступ до логіну та паролю від аккаунта в інтернет банкінг, здійснює переказ грошових коштів з рахунку потерпілого, тим самим здійснюючи розкрадання.

Наприклад існує відомий сервіс криптовалютних платежів www.myetherwallet.com На такому сервісі можна завести віртуальний криптовалютний гаманець і купити та зберігати криптовалюту. Зловмисники в своїх повідомленнях або повідомленнях, надсилаючи посилання нібито цього сайту змінюють декілька або взагалі одну букв на інші знаки так, щоб це було непомітно. Наприклад, справжня посилання даної системи виглядає наступним чином: www.myetherwallet.com, а посилання зловмисника буде виглядати приблизно так: www.myetherwalIet.com.

Необхідно наголосити, що за допомогою «фішингу» впливу програмних засобів на комп'ютер жертви не відбувається. Потерпілий сам переходить за надісланим лінком і вводить логін і пароль. Надалі розкрадання грошових коштів

проводиться за допомогою отриманих логіна і пароля, але не в результаті впливу на пристрій потерпілого.

«Кардінг» і «Фішинг» на даний момент є найпопулярнішим способом отримання чужих грошових коштів або іншої інформації. Найчастіший метод здійснення даних видів розкрадання відбувається шляхом так званого клонування.

Великого поширення в даний час набуває розкрадання, пов'язане з безконтактної оплатою, тобто завдяки NFC, технології бездротової передачі даних малого радіусу дії, яка дає можливість обміну даними між пристроями, що знаходяться на відстані 4 сантиметрів. Дана технологія зараз присутня майже в кожних банківській картці і смартфоні і дозволяє оплачувати покупки до певної суми лише прикладаючи банківську карту без введення пароля.

Сенс роботи злочинців полягає в перехопленні NFC-сигналів, використовуючи незаконні пристрої-зчитувачі. RFID-перехоплювачі – це більш розроблені аналоги звичайних безконтактних карткових терміналів ПОС з збільшеною функціональністю, які вловлюють і обробляють електромагнітні хвилі. Такий прилад зазвичай обладнаний антеною, спеціальним контролером, роз'ємами для вилучення зі зчитувача інформації та піратського комп'ютерного ПО, тобто програмного забезпечення.

Для отримання грошових коштів зловмиснику досить знаходиться в 10 сантиметрах від банківської карти, що дозволить отримати не тільки гроші, але і все її дані. Однак, прогрес не стоїть на місці і вже на сьогоднішній день існують деякі способи захисту від зловмисників: багато виробники почали продаж спеціальних алюмінієвих чохлів для карт, які приглушують електромагнітні хвилі, тим самим обмеживши використання безконтактної оплати, далі існує варіант самостійної установки ліміту для безконтактної оплати без введення пароля та інші [8, с. 201].

У зв'язку з цим важливим бачиться відзначити одне з досягнень останніх років у сфері розкриття і розслідування розглянутих кримінальних правопорушень а саме – поява комп'ютерно-технічної експертизи, яка включена до відповідного переліку родів (видів) судових експертиз, вироблених в експертно-криміналістичних підрозділах [9].

Володіючи спеціальними знаннями в сфері комп'ютерної техніки, фахівці (експерти) здатні внести неоціненний вклад в діяльність слідчого по встановленню істини при розслідуванні злочинів.

Можливості судової експертизи важко переоцінити. За даним фактом досить точно висловилися А. В. Варданян і О. П. Грібунов, що відзначили, що в даний час правозастосовна практика орієнтована на призначення і проведення експертиз, які дозволять виявити зведення про механізм злочинної діяльності, особистості невстановленого злочинця та інших ознаках і властивостей , тим самим буде слугувати доказом у кримінальній справі [10, с. 277].

Розглянемо можливості комп'ютерно-технічної експертизи в якості важливого підмоги в розкритті та розслідуванні кримінальних правопорушень, пов'язаних з розкраданнями коштів з банківських карт. Злочинці в більшості випадків з точки зору способів вчинення протиправних діянь використовують об'єкти радіоелектронних пристроїв, призначені для перехоплення інформації про клієнтів систем дистанційного банківського обслуговування.

Предметом комп'ютерно-технічної експертизи, яка проводиться з метою встановлення фактів розкрадань грошових коштів з платіжних карт, є наступні категорії:

– встановлення фактичних обставин, що мають значення для розслідуваної кримінальної справи;

– встановлення фактичних обставин, пов'язаних з використанням радіоелектронних пристроїв, що дозволяють заволодіти даними платіжної банківської картки, а також інформацією про PIN-коді.

Об'єктами комп'ютерно-технічної експертизи є спеціальні пристрої і інструменти, що дозволяють зчитувати відомості платіжних карт, що встановлюються на елементи і вузли терміналів систем дистанційного банківського обслуговування (банкоматів), які вилучаються безпосередньо з банкоматів або під час огляду і в ході проведення обшуків [11, с. 14].

Завданнями даної експертизи, яка призначається при розслідуванні кримінальних справ, порушених за фактами вчинення досліджуваних розкрадань, є: – визначення безпосередньої можливості перехоплення інформації про клієнтів, представленим на дослідження обладнанням; – діагностування індивідуальних номерів банківських карт, їм перехоплених [12].

Встановлення зазначених завдань дозволить отримати інформацію про причетність до вчинення злочину, що розслідується конкретних осіб, а також послужить одним з доказів при виявленні скомпрометованих платіжних карт і для визначення можливої шкоди, заподіяної потерпілому по кримінальній справі. В ході виробництва радіотехнічної експертизи, яка призначається з даної категорії злочинів, експерт може відповісти на наступні питання:

1. Чи можливо за допомогою представлених пристроїв отримувати інформацію, наявну на пластикових платіжних картах, а також інформацію про натисканні клавіш на клавіатурі банкомату (в тому числі про PINкодах)?

2. Чи містяться на представлених об'єктах дані про номери пластикових платіжних карт і їх PIN-коди?

3. Яким способом передбачається отримання з представленого обладнання (пристрою) даних про отриману інформацію? Досить вузький перелік питань, що підлягають для вирішення експертами, пояснюється тим, що даний вид судових експертиз ще досить «молодий», потенціал і можливості дослідження розкриті не в повній мірі, при цьому вказане відбивається і на формуванні якісної доказової бази по кримінальній справі.

Більш того, в даний час відсутня спеціалізована методика виробництва таких експертиз, яка повинна містити в собі всі аспекти даного виду діяльності, точний алгоритм і шляхи вирішення спірних ситуацій, що виникають на етапі формулювання висновків. Безперервне вдосконалення вмінь і навичок злочинців в частині удосконалення приховування слідів злочинної діяльності щодо запропонованих злочинів говорить про необхідність постійного моніторингу розвитку споживчих технологій радіозв'язку, а також про важливість розробки нових актуальних засобів і методів встановлення фактів вчинення протиправних дій, а саме розкрадань грошових коштів з платіжних банківських карт.

ЛІТЕРАТУРА

1. Бондаренко, О.С. Кіберзлочинність в Україні: причини, ознаки та заходи протидії. *Порівняльно-аналітичне право*. 2018. № 1. – С. 246–248. – URL: http://www.pap.in.ua/1_2018/73.pdf

2. Сачков Д.И., Смирнова И.Г. Обеспечение информационной безопасности в органах власти: учебное пособие. Иркутск. 2015. – 121 с.

3. Шемчук В.В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : *Юридичні науки*. 2018. – Т. 29(68), № 6. – С. 119-124.

4. URL: http://nbuv.gov.ua/UJRN/UZTNU_law_2018_29(68)_6_23

5. Протидія кіберзлочинності в Україні: правові та організаційні засади : [навч. посіб.] / О. Є Користін, В. М. Бутузов, О. А. Безуглий та ін. – К. : «Скіф», 2012. – 728. Х628.3 П834

6. І. І. Васильковский. Поняття, класифікація та характеристика окремих видів кіберзлочинів. Прикарпатський юридичний вісник. Випуск 1(16), том 2, 2017. с. 196-201.

7. Ставер А. В. Загальні вразливості банківських карт і способи їх усунення. Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 144-147.

8. Русецький А. А. Теоретико-правовий аналіз понять "кіберзлочин" і "кіберзлочинність". Право і безпека. – 2017. – № 1 (64). – С. 74-78.

9. Болгов В. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посіб. / В. М. Болгов, Н. М. Гадіон, О. З. Гладун та ін. Київ: Національна академія прокуратури України, 2015. 202 с.

10. Наказ Міністерства Юстицій України. Про внесення змін до Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки матеріалів та призначення судових експертиз. URL: https://zakon.rada.gov.ua/laws/show/z1393-06#Text

11. Варданян А. В., Грибунов О. П. Судебные экспертизы, назначаемые при расследовании хищений на объектах транспорта. Теория и практика противодействия преступности в азиатско-тихоокеанском регионе: сб. науч. тр. – Хабаровск: Изд-во Дальневост. юрид. ин-та М-ва внутр. дел России, 2016. – С. 274–277.

12. Пилипчук В. Г., Дзьобань О. П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. Стратегічні пріоритети. 2011. № 4 (21). С. 12–17.

13. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. Ресурсний центр ГУРТ: сайт. URL: http://www.gurt.org.ua/articles/34602