ISSN 2078-6670. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Журнал. Серія Право. №3(15), 2017.

КРИМІНАЛЬНЕ ПРАВО, КРИМІНОЛОГІЯ, КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО. КРИМІНАЛЬНИЙ ПРОЦЕС, КРИМІНАЛІСТИКА ТА СУДОВА ЕКСПЕРТИЗА

УДК 343.14:343.345

Басиста Ірина Володимирівна,
доктор юридичних наук, професор,
професор кафедри кримінального права та процесу
Львівського торговельно-економічного університету

ОКРЕМІ АСПЕКТИ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КІБЕРПОЛІЦІЇ ЩОДО ВИЯВЛЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Дана публікація покликана привернути увагу практикуючих юристів, наукової спільноти та інших фахівців до проблематики виявлення кримінальних правопорушень підрозділами Кіберполіції. Адже «кеш-треппінг» (cash trapping), «ransomware», шахрайство за допомогою шкідливого програмного забезпечення, соціальної інженерії і фішингових атак, тощо набувають ледь не глобального поширення, тому протидія їм повинна бути все більш наступальною та ефективною.

Ключові слова: *підрозділи Кіберполіції, кримінальні правопорушення, шахрайство, незаконні дії з документами на переказ, платіжні картки, електронні гроші, захоплення готівки.*

Постановка проблеми. Здавалося б банальна теза про те, що злочинність досить часто випереджує засоби щодо її протидії, вже нікого в юридичних колах, та й пересічних громадян, не дивує. Однак, як на мене, сьогоднішній стан речей у цій царині є надто «стрімким», так як поява нових різновидів протиправних дій дозволяє суб'єктам їх вчинення уникати покарання до того часу, поки правоохоронні органи напрацьовують окремі методи і способи їх виявлення та методики розслідування.

У зв'язку із появою нових різновидів кримінальних правопорушень, що передусім пов'язані із бурхливим розвитком в галузі ІТ та протиправному використанню її можливостей, нагальною постала потреба у фахівцях, які були б здатні дати гідну відсіч таким кримінальним викликам, як «кеш-треппінг» (cash trapping) – в дослівному перекладі означає «захоплення готівки»; «ransomware» – шифрування файлів користувачів, із подальшою пропозицією здійснити переказ грошей зловмисникам за їх розшифровку; шахрайство за допомогою шкідливого програмного забезпечення, соціальної інженерії і фішингових атак тощо.

Аналіз останніх досліджень і публікацій. Окремі аспекти задекларованої проблематики були об'єктом дослідження вітчизняних та зарубіжних науковців й економістів, зокрема І. О. Воронова, С. Ю. Гаврика, С. В. Демедюка, Г. В. Загіки, О. М. Комара, М. Ю. Літвінова, О. В. Манжая, В. П. Поїзда, С. М. Рогозіна, А. В. Тарасюка, Л. Л. Тимченка, К. В. Тітуніної, В. Є. Ткаліча, О. А. Федотова, І. Ф. Харабер'юша, Д. М. Цехана, В. П. Шеломенцева, О. М. Юрченка.

Постановка завдання. Метою та завданням статті є висвітлення окремих аспектів діяльності Кіберполіції щодо виявлення окремих різновидів кримінальних правопорушень, зокрема таких, як «кеш-треппінг» (cash trapping), «ransomware», шахрайство за допомогою шкідливого програмного забезпечення, соціальної інженерії і фішингових атак, тощо.

Виклад основного матеріалу дослідження. Варто підкреслити, що означені при постановці проблеми та інші чинники у своїй сукупності сприяли тому, що на виконання постанови Кабінету Міністрів України № 831 від 13 жовтня 2015 року «Про утворення територіального органу Національної поліції», а також відповідно до наказів МВС від 15 жовтня 2015 року № 1250 «Про проведення позачергового атестування осіб начальницького складу підрозділів боротьби з кіберзлочинністю» та № 1251 від 15 жовтня 2015 року «Про проведення конкурсу на заміщення вакантних посад старших інспекторів, інспекторів і спеціальних агентів інформаційних технологій міжрегіонального територіального органу Департаменту кіберполіції Національної поліції», з метою проведення якісного відбору висококваліфікованих фахівців у підрозділи кіберполіції 15 жовтня 2015 року оголошено про початок реформування підрозділів боротьби з кіберзлочинністю МВС в кіберполіцію Національної поліції та початок конкурсу з відбору кандидатів на заміщення вакантних посад в кіберполіції.

Відповідно до Положення про Департамент кіберполіції НП України, затвердженого наказом Національної поліції від 10 листопада 2015 № 85, як міжрегіональний територіальний орган створено Департамент кіберполіції, який є юридичною особою публічного права. Цей міжрегіональний територіальний орган Національної поліції України відповідно до законодавства України забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції.

До складу Департаменту входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковані начальникові Департаменту (Донецьке, Карпатське, Київське, Подільське, Поліське, Придніпровське, Причорноморське та Слобожанське управління кіберполіції, а також управління інформаційних технологій та програмування в західному, південному та східному регіонах). Відповідно до Закону України «Про ратифікацію Конвенції про кіберзлочинність» та з метою забезпечення міжнародної діяльності кіберполіції, у штатній структурі Департаменту кіберполіції створено сектор Національного контактного пункту з реагування на кіберзлочини. На сьогодні, відбувається перетворення колишньої моделі підрозділів боротьби з кіберзлочинністю до новітнього органу правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу миттєвого реагування на кіберзагрози, а також, у відповідності до кращих європейських та світових стандартів проводитиме міжнародну співпрацю по знешкодженню транснаціональних злочинних угрупувань у даній сфері [6].

Серед завдань на Департамент кіберполіції Національної поліції України (скорочена назва – ДКП) покладається участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (сфера протидії кіберзлочинності).

Як на мене, то досить актуальними та персоніфікованими є такі функції ДКП, як вживання передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів, що становлять оперативний інтерес, у тому числі об'єктів

сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень; організація виконання, у межах компетенції, доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях; створення та забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі; забезпечення функціонування локальних експертних лабораторій ДКП та мобільних груп швидкого реагування, призначених для залучення до місць вчинення кримінальних правопорушень, з метою зняття даних з носіїв інформації тощо.

Працівники Департаменту мають право, серед іншого, здійснювати оперативно-розшукову діяльність, спрямовану на виявлення та припинення злочинів у сфері протидії кіберзлочинності, а також комплексне використання джерел оперативної інформації, можливостей оперативних підрозділів та застосування оперативно-технічних засобів під час провадження в оперативно-розшукових справах, контроль за використанням коштів, призначених для проведення цієї роботи; здійснювати оперативно-технічні заходи за оперативно-розшуковими справами, що знаходяться в їх провадженні; в установленому порядку запитувати та отримувати від посадових осіб органів внутрішніх справ і органів державної влади документи, довідкові та інші матеріали (у письмовій або усній формі), необхідні для прийняття рішень з питань забезпечення реалізації державної політики у сфері протидії кіберзлочинності; користуватися в установленому законодавством порядку базами даних Національної поліції України, МВС та інших державних органів з питань, що належать до компетенції Департаменту, а також інші права, передбачені законодавством [3].

Слід відзначити, що ДКП реалізовує і профілактичну діяльність, окремі заходи загальної профілактики можна простежити і на офіційному сайті Департаменту Кіберполіції України. Заходи щодо інформування про виявлені новітні шахрайські схеми є корисними як для правоохоронних органів, так і для пересічних громадян. Для прикладу, такий різновид «кеш-треппінгу», коли шахраї використовують звичайні алюмінієві планки кустарного виробництва (в більшості випадків виготовлені з деталей меблевої фурнітури), які зовні схожі на шторки банкомату, з тильного боку приклеюються злочинцями двосторонньою клейкою стрічкою і закріплюються на отворі видачі готівки. Неуважні люди знімають готівку в банкоматі, не звернувши уваги на його зовнішній вигляд. Після цього думають, що банкомат поламався і йдуть в відділення банку або до іншого банкомату. В цей час, шахраї, які чекали неподалік, знімають встановлену панель і забирають приклеєні до її внутрішньої сторони гроші своєї жертви [7].

Або ж, коли зловмисники розсилали шкідливе програмне забезпечення (ШПЗ) українським державним та приватним підприємствам. Після запуску такого ШПЗ, на комп'ютерах користувачів зашифровувався певний порядок файлів, і далі з'являлось повідомлення про можливість їх розшифровки за певну суму грошових коштів. Задля боротьби з цією загрозою, у липні 2016 року, Національна поліція Нідерландів, Європол та Intel Security, створили проект під назвою «No more Ransom». З моменту запуску, до проекту приєднались десятки партнерів з усього світу. Через дев'ять місяців після запуску постійно зростає кількість співробітників правоохоронних органів і приватних партнерів, котрі приєднались до ініціативи, яка дозволить жертвам шифрування файлів, отримати їх назад, без переказу грошових коштів злочинцям. Платформа: www.nomoreransom.org тепер доступна на 14 мовах, та містить 40 безкоштовних програмних продуктів для розшифровки

файлів. Згідно останнього звіту у грудні 2017 року, більше 100 тисяч жертв із усього світу, змогли розшифрувати свої файли за допомогою безкоштовних продуктів, які доступні на зазначеній онлайн-платформі. Попередньо, проект був доступний англійською, голландською, французькою, італійською, португальською та російською мовами. Наразі, сторінка також переведена на фінську, німецьку, іврит, японську, корейську, словенську, іспанську та українську мови. В даний момент, доступні 15 програмних продуктів для розшифровки файлів постраждалих [5].

Згідно інформації, оприлюдненої на сайті Департаменту Кіберполіції України на даний час існує досить велика кількість класифікацій атак на інтернет-банки з різними підходами і виходячи з різних цілей. Основна кількість випадків шахрайства в системах інтернет-банкінгу припадає на шахрайство за допомогою шкідливого програмного забезпечення, соціальної інженерії і фішингових атак. Причому, якщо за прогнозом масштаби використання програмного забезпечення (троянів) на комп'ютерах поступово будуть зменшуватися, то використання троянів на платформі Android буде тільки зростати. Одночасно вірусописьменники для комп'ютерів будуть все більше орієнтуватися на західні банки, а фішингові атаки будуть автоматизуватися. Що ж стосується соціальної інженерії і фішингових атак – атак, коли зловмисники намагаються змусити клієнта несвідомо розголосити основні реквізити, що дозволяють аутентифікувати шахрайську операцію, то такі атаки є трендом в інтернет-банку для фізичних осіб. В більшості випадків перелічені атаки є спрямованими (Advanced Persistent Threat, APT), тобто атаками, метою яких стає конкретний інтернет-банк, а іноді і конкретні клієнти. Зловмисники за допомогою різних методів встановлюють на комп'ютер клієнта троян, який замість клієнта формує платіжні доручення або підміняє в ньому реквізити платежу. При відновленні обставин інцидентів в ході криміналістичних досліджень робочих станцій, на яких працювали з ДБО, ретельному аналізу піддаються журнали міжмережевих екранів і проксі, а також інші джерела інформації. Найбільш частий сценарій вчинення злочину складається з трьох основних етапів: отримання інформації для доступу в систему ДБО, проведення шахрайської операції, переведення в готівку грошей [1].

Ведучи мову про такий надзвичайно актуальний напрям діяльності, як виявлення підрозділами Кіберполіції злочинних дій з платіжними картками, варто звернутися до базових понять та категорій.

Зокрема, стаття 200 КК України встановлює кримінальну відповідальність за незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

Так, частина 1 цієї статті передбачає кримінальну відповідальність за підробку документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей, а так само за придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ, платіжних карток або їх використання чи збут, а також неправомірний випуск або використання електронних грошей.

За ті самі дії, вчинені повторно або за попередньою змовою групою осіб встановлює кримінальну відповідальність санкція до частини другої зазначеної статті.

У примітці до статті 200 КК України визначено, що під документами на переказ слід розуміти документ в паперовому або електронному виді, що використовується банками чи їх клієнтами для передачі доручень або інформації на переказ грошових коштів між суб'єктами переказу грошових коштів (розрахункові документи, документи на переказ готівкових коштів, а також ті, що використовуються при проведенні міжбанківського переказу та платіжного повідомлення, інші) [2].

Платіжна картка – електронний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для ініціювання переказу коштів з рахунка платника або з відповідного рахунка банку з метою оплати вартості товарів і послуг, перерахування коштів зі своїх рахунків на рахунки інших осіб, отримання коштів у готівковій формі в касах банків через банківські автомати, а також здійснення інших операцій, передбачених відповідним договором. Вид платіжної картки, що емітується банком, тип її носія ідентифікаційних даних (магнітна смуга, мікросхема тощо), реквізити, що наносяться на неї у графічному вигляді, визначаються платіжною організацією відповідної платіжної системи, у якій ця картка застосовується. Обов'язковими реквізитами, що наносяться на платіжну картку, є реквізити, що дають змогу ідентифікувати платіжну систему та емітента. Платіжні картки внутрішньодержавних платіжних систем повинні містити ідентифікаційний номер емітента, визначений у порядку, встановленому НБУ.

Під іншими засобами доступу до банківських рахунків, електронних грошей слід розуміти інші носії інформації (крім документів на переказ і платіжних карток), що зберігають ідентифікаційну інформацію і за допомогою яких особа може одержати доступ до певного банківського рахунку, електронних грошей, наприклад, мобільний платіжний інструмент, тобто електронний платіжний засіб, реалізований в апаратно-програмному середовищі мобільного телефону або іншого бездротового пристрою користувача; дорожні та іменні чеки в іноземній валюті, які емітовані за кордоном і пред'являються для сплати на території України.

Підробленими документами на переказ та платіжними картками за статтею 200 КК визнаються лише такі повністю чи частково фальсифіковані предмети, які мають схожість зі справжніми предметами за основними реквізитами та функціонально-цільову придатність справжніх предметів, що встановлюється з урахуванням всієї сукупності ознак та властивостей цих предметів. Зокрема, йдеться про придатність предмета для отримання доступу до банківських рахунків та ініціювання переказу коштів, здійснення операцій. Разом з тим не є предметом цього злочину такий предмет, який хоч і надає можливість доступу до банківського рахунку, однак не має схожості зі справжнім документом чи платіжною карткою за основними реквізитами. Створення такого предмета може кваліфікуватися як створення шкідливого програмного чи технічного засобу, призначеного для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [4].

Висновки. Варто констатувати, що виявлення підрозділами Кіберполіції злочинних дій з платіжними картками, а також інших протиправних дій у цій сфері та подальше ефективне розслідування таких кримінальних правопорушень потребують напрацювання алгоритмів та методики такої діяльності, вироблення науково-обгрунтованих методичних рекомендацій в рамках вимог чинного КПК, що є спільним нагальним завданням як науковців, так і практичних працівників правоохоронних органів.

Список використаних джерел

1. Атаки на системи Дистанційного банківського обслуговування (ДБО) // Сайт Департаменту Кіберполіції України [Електронний ресурс]. – Режим доступу: https://www.cybercrime.gov.ua/16-novosti/215-ataki-na-sistemi-distantsijnogo-bankivskogo-obslugovuvannya-dbo#news.
2. Кримінальний кодекс України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/.

3. Наказ Національної поліції України від 10.11.2015 № 85 «Про затвердження Положення про Департамент кіберполіції Національної поліції України» [Електронний ресурс]. – Режим доступу: https://www.cybercrime.gov.ua.
4. Науково-практичний коментар Кримінального кодексу України / за ред. М.І. Мельника, М.І. Хавронюка. – 9-те вид., перероб. та допов. – К.: Юридична думка, 2012. – С. 573-575 [Електронний ресурс]. – Режим доступу: http://mego.info/матеріал/стаття-200-незаконні-дії-з-документами-на-переказ-платіжними-картками-та-іншими-засобами.
5. Проект «No more Ransom» // Сайт Департаменту Кіберполіції України [Електронний ресурс]. – Режим доступу: https://www.cybercrime.gov.ua/no-more-ransom#news.
6. Сайт Департаменту Кіберполіції України [Електронний ресурс]. – Режим доступу: https://www.cybercrime.gov.ua.
7. Що робити щоб не стати жертвою «кеш-треппінгу» // Сайт Департаменту Кіберполіції України [Електронний ресурс]. – Режим доступу: https://www.cybercrime.gov.ua/16-novosti/214-shcho-robiti-shchob-ne-stati-zhertvoyu-kesh-treppingu#news.

Басистая И. В. Отдельные аспекты деятельности подразделений киберполиции по выявлению уголовных правонарушений

Данная публикация призвана привлечь внимание практикующих юристов, научного сообщества и других специалистов к проблематике выявления уголовных правонарушений подразделениями Киберполиции. Ведь «кэш-треппинг» (cash trapping), «ransomware», мошенничество с помощью вредоносного программного обеспечения, социальной инженерии и фишинговых атак и т.д. приобретают чуть ли не глобальное распространение, поэтому противодействие им должно быть все более наступательным и эффективным.

Ключевые слова: *подразделения Киберполиции, уголовные правонарушения, мошенничество, незаконные действия с документами на перевод, платежные карточки, электронные деньги, хищение наличных.*

Basysta I. V. Separate aspects of the activities of the units of the cyberpolicy on the detection of criminal offenses

This publication is designed to draw the attention of practicing lawyers, the scientific community and other professionals to the problem of identifying criminal offenses by units of the Cyberpolicy. After all, «cash trapping», «ransomware», fraud with the help of malicious software, social engineering and phishing attacks, etc. Acquire almost a global spread, so their opposition must be increasingly offensive and effective.

Key words: *subdivisions of Cyberpolicy, criminal offenses, fraud, illegal actions with documents for transfer, payment cards, electronic money, cash theft.*

Надійшла до редакції 1 березня 2017 р.