14. Кучер О.Б. Україна та Міжнародний кримінальний суд: еволюція та розвиток взаємовідносин. Науковий вісник Ужгородського національного університету. Серія «Право». 2014. Вип. 27. Т. 3. С. 179–181.

15. Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 р., Першого протоколу та протоколів № № 2, 4, 7 та 11 до Конвенції: Закон України від 17 липня 1997 р. № 475/97-ВР. URL: http://zakon.rada.gov.ua/laws/show/475/97-%D0%B2%D1%80.

16. Про виконання рішень та застосування практики Європейського суду з прав людини: Закон України від 23 лютого 2006 р. № 3477–IV. URL: http://zakon.rada.gov.ua/laws/show/3477-15.

17. Стандарты справедливого правосудия (международные и национальные практики) / кол. авторов; под. ред. Т.Г. Морщаковой. М.: Мысль, 2012. 584 с.

УДК 343.34

ЛАТИШ К.В.

КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КІБЕРВАНДАЛІЗМУ

В умовах цифрової епохи вандалізм набуває нових форм кібервандалізму та нового змісту. Тому важливими є висвітлені в статті проблеми криміналістичної характеристики кібервандалізму. Проаналізовано окремі елементи криміналістичної характеристики вандалізму, як-от предмет злочинного посягання, спосіб злочину, обстановка, час, особа злочинця, особа потерпілого та типові сліди.

Ключові слова: *кібервандалізм, криміналістична характеристика, кібервандал, особа потерпілого.*

В условиях цифровой эпохи вандализм трансформируется в новые формы кибервандализма и приобретает новый смысл. Поэтому важными для исследования являются освещенные в статье проблемы криминалистической характеристики кибервандализма. Проанализированы отдельные элементы криминалистической характеристики вандализма: предмет преступного посягательства, способ преступления, обстановка, время, личность преступника, личность потерпевшего, типичные следы.

Ключевые слова: *кибервандализм, криминалистическая характеристика, кибервандал, личность потерпевшего.*

In the digital era, vandalism is transformed into new forms of cyber vandalism and is gaining new meaning. Therefore, it is quiet significant to analyze issues of the criminalistics description of cyber vandalism. Some elements of forensic characteristics of vandalism are described, such as the subject of a criminal offense, the method of crime, the situation, time, the person of the offender, the victim's personality and typical traces.

Key words: *cyber vandalism, forensic characteristic, cyber vandal, victim's person, information protection, threat of safety.*

Вступ. Інтернет-простір – це не лише віртуальне середовище для обміну інформацією, але й недостатньо контрольоване правоохоронними органами «поле» для злочинів. Кіберзлочинність як негативне явище, з яким ведеться активна боротьба, поширене в усьому світі. В Україні лише останніми роками особливо гостро постала проблема кібербезпеки. У зв'язку із чим у прискореному режимі ухвалено Закон України «Про основні засади забезпечення

© ЛАТИШ К.В. – кандидат юридичних наук, асистент кафедри криміналістики (Національний юридичний університет імені Ярослава Мудрого)

кібербезпеки України», приділено більше уваги реалізації Конвенції про кіберзлочинність, ратифікованій ще 2005 р. Питання інформаційної безпеки перейшло в площину стратегічних завдань кожної держави.

Постановка завдання. Метою статті є проведення аналізу та надання криміналістичної характеристики кібервандалізму, визначення її структури та опис окремих елементів з урахуванням практики сьогодення.

Результати дослідження. Вандалізм спостерігається в різних проявах, які кожного року модернізуються. Кібервандалізм – це несанкціонований доступ до інформації, який здійснюється за допомогою новітніх інформаційно-телекомунікаційних технологій та засобів, які дозволяють отримати такий доступ, а також можливість її викривити або іншим чином внести зміни (блокування, знищення, обмеження в доступі тощо).

Криміналістична характеристика – це система відомостей про криміналістично значущі ознаки цього злочину, що відтворює закономірні зв'язки між ними, слугує побудові й перевірці слідчих версій у розслідуванні вандалізму. Її метою є оптимізація процесу розкриття й розслідування злочину, а також вона сприяє:

1) розробленню окремих криміналістичних методик;

2) побудові типових програм і моделей розслідування злочинів;

3) визначенню напряму розслідування конкретного злочину [4, с. 888].

Крім предмета посягання, криміналістична характеристика передбачає наявність системи таких елементів, як: спосіб злочину, час, місце, обстановка його скоєння, особа злочинця, типові сліди злочину. Криміналістична характеристика – це типова інформаційна модель криміналістично значущих особливостей злочину, заснована на науково зібраних та узагальнених даних [5, с. 67].

Під час вчинення вандалізму злочинець взаємодіє із предметами навколошнього середовища, але предметом злочинного посягання буде лише той, на який особа безпосередньо злочинно вплинула: наругалася, обмалювала, пошкодила, знищила, та (або) яким вона заволоділа без спеціальних на це повноважень. Взаємодія злочинця із предметом посягання пов'язана з появою різних змін предмета. «Ці зміни локалізуються: 1) на місці злочинної події; 2) на самому предметі і його частинах; 3) у місцях подальшого його знаходження, приховування, реалізації; 4) на злочинці (його комп'ютерних пристроях, інших носіях тощо); 5) на знаряддях злочину, технічних засобах, що використовувалися злочинцем» [8, с. 21].

Взаємозв'язок інформаційних технологій та безпеки останнім часом є дуже щільним, шкідливі комп'ютерні програми застосовують як зброю для вирішення деяких проблем. Усі стратегічні об'єкти мають автоматизовані системи управління, які можуть бути уражені комп'ютерними вірусами через певні мотиви (хуліганські, корисливі, політичні).

Спосіб злочину дозволяє зорієнтуватися в сутності того, що відбувається загалом, та в окремих обставинах правопорушення для ефективного розслідування злочину. Із криміналістичного погляду спосіб злочину є образом дій злочинця, що виражається у взаємозалежній системі операцій і прийомів підготовки, вчинення й приховування злочинів [6, с. 22]. Спосіб злочину відбивається в слідах-наслідках [9, с. 48–50].

Спосіб кібервандалізму може бути представлений тричленною системою: підготовчі дії, вчинення та приховування, однак зміст дій дещо відрізняється від традиційного. Так, підготовчі дії в разі кібервандалізму передбачають вивчення електронної системи, діагностики наявних ступенів захисту, визначення переліку необхідних для доступу технічних засобів [4, с. 886]. Зазначимо такі способи кібервандалізму:

– здійснення термінації трафіку (рефайл) із країн усього світу;

– незаконна маршрутизація трафіку на тимчасово окуповані території Луганської області з інших регіонів та території Російської Федерації, а також маршрутизація у зворотному напрямку, що полягає в телефонних дзвінках міжнародних операторів із порушенням встановленого порядку маршрутизації, підміні оригінального телефонного номера абонента закордонного оператора на номер абонента внутрішньої мережі [2];

– спам;

– несанкціонований доступ до реєстрів та інформації: крадіжка особистих даних, грошей через крадіжку даних карти тощо. Так, постійно спостерігаються несанкціоновані реєстраційні дії в Державному реєстрі прав на нерухоме майно;

– мережева DoS-атака (DDoS-атака) (Distributed Denial of Service), скоєна через віддалений доступ із використанням протоколів міжмережевої взаємодії шляхом віддзеркалення (коли

IP-адреса джерела поширення підміняється на IP-адресу потерпілого) та посилення шкідливого трафіку, що спрямовується, зокрема, на такі сервери, як DNS-сервер та NTP-сервер.

Для створення окремого вірусу можуть використовуватися вкрадені офіційні сертифікати відомих виробників комп'ютерної техніки. Для ідентифікації вірусу необхідне вивчення його вихідного коду та мотивів застосування.

Водночас, як свідчить практика, усі вразливості, які вдалося ідентифікувати через кібервандалізм, намагаються оперативно ліквідувати для унеможливлення їх використання в майбутньому, тому зазвичай окремий вид вірус застосовується один раз.

Також для вчинення кібервандалізму можуть розроблятися різні стратегії, які полегшують подолання систем захисту для отримання доступу, серед них:

– соціальний інжиніринг (фішинг);

– претекстінг;

– несанкціоноване проникнення слідом за авторизованим користувачем;

– цілеспрямована стійка загроза (комплексна атака на носія інформації) [4, с. 886].

Одним зі способів дії вірусу є Diskcoder.C (ExPetr, PetrWrap, Petya, NotPetya), який вразив сервери та комп'ютерні пристрої на території всієї країни 2017 р. Так, здійснено несанкціонований доступ до персонального комп'ютера одного з розробників із метою отримання вихідних кодів програми "M.E.Doc", в які вбудовано бекдор (backdoor), за допомогою якого надалі встановлювався несанкціонований віддалений доступ під час оновлення зазначеної програми.

"M.E.Doc" – це комп'ютерна програма, призначена для бухгалтерського документообігу. Вимагання викупу зашифрованих даних було нічим іншим як маскуванням для прикриття слідів злочинної діяльності (backdoor).

Розглянемо на прикладі несанкціоноване втручання в роботу мереж електрозв'язку, а саме створення та налаштування програмно-технічного обладнання, за допомогою якого можна несанкціоновано змінювати напрям голосового трафіку з мережі Інтернет у мережу GSM (GSM-рефайл).

Так, група осіб, які порушили вимоги п. 4 ч. 1 ст. 33, ч. 2 ст. 42, п. 9 ст. 58, ч. 1 ст. 63 Закону України «Про телекомунікації» від 18 листопада 2003 р., п. 32 р. 1 та п. 230 р. IV «Правил надання та отримання телекомунікаційних послуг», затверджених постановою Кабінету Міністрів України № 720 від 9 серпня 2005 р., п. 4.8 «Положення про діяльність операторів міжміського, міжнародного зв'язку телефонної мережі загального користування України та їх взаємодію між собою», затвердженого наказом Державного комітету зв'язку та інформатизації України № 19 від 14 лютого 2001 р., п. п. 1.1, 1.2, 1.3 наказу Державного комітету зв'язку та інформатизації України «Про порядок маршрутизації вхідного міжнародного телефонного трафіку» № 33 від 22 лютого 2000 р., за допомогою виготовленого обладнання міжнародний телефонний трафік, отриманий із мережі Інтернет, спрямовувала в телекомунікаційну мережу загального користування України шляхом підміни оригінальних номерів ініціаторів міжнародних телефонних викликів на мобільні телефонні номери операторів мобільного зв'язку України. Тобто наявне несанкціоноване втручання в роботу мереж електрозв'язку, що призвело до спотворення процесу оброблення інформації щодо міжнародного телефонного трафіку та до порушення встановленого порядку її маршрутизації.

Функції та завдання були чітко розподілені між учасниками групи: один займався білінгом; другий – налагоджував програмно-технічні засоби, збирав обладнання, а третій – розробляв запчастини для обладнання, адміністрував систему.

Двоє із цих осіб були співробітниками IT-компанії, що мала офіційний доступ до програмних продуктів, які потім використовувалися в їхній злочинній діяльності. Так, вони, використавши несанкціоновано скопійовані програмні продукти, виготовили та налаштували програмно-технічне обладнання для GSM-рефайлу.

Запчастини для вказаного обладнання замовляли через Інтернет, отримували їх через філії фірм-перевізників («Автолюкс», «Нічний Експрес», «Міст Експрес». Так само замовлялися й одержувалися стартові пакети операторів мобільного зв'язку України, картки поповнення рахунків SIM-карт.

Для отримання голосового телефонного трафіку з мережі Інтернет орендовано сервер, для цього укладено договір про надання послуг. Після закінчення всіх підготовчих дій укладено договори про оплатне надання послуг із маршрутизації міжнародного телефонного трафіку в мережі операторів мобільного зв'язку України з окремими закордонними компаніями.

Отже, за допомогою виготовленого, розміщеного та підключеного обладнання для GSM-рефайлу маршрутизовано в мережу оператора мобільного зв'язку України ТОВ «Астеліт» понад 1 432 381 сек. голосового міжнародного трафіку [1].

Знаряддям вчинення кібервандалізму є спеціальне телекомунікаційне обладнання, програмне й апаратне забезпечення, комп'ютери, мобільні та комп'ютерні мережі.

У результаті дослідження з'ясовано, що кібервандалізм зумовлений такими чинниками:

– безконтрольність, хаос, безкарність, що стало наслідком реалізації принципів, закріплених у «Декларації незалежності кіберпростору», яку створив Джон Перрі Барлоу. Така неконтрольована свобода в Мережі спричинила поширення кібервандалізму, який із реальної царини перейшов у віртуальну. Тому вважаємо, що на цей віртуальний простір також поширюється «Теорія розбитих вікон» (Джеймс Вілсон і Джордж Келлінг);

– наявність слабкого контролю та/або неналежний захист комп'ютерної програми, сайту або іншого предмета злочинного посягання, унаслідок чого такий предмет має багато вразливостей. Зазначену тезу підтверджує наукова концепція "routine activity theory", розробниками якої є Маркус Фелсон та Лоренс Коен;

– момент вчинення кібервандалізму обирається таким чином, щоби безпосередні протиправні дії були недоступними для зовнішнього спостереження, проте наслідки таких дій мають бути відкритими та доступними для споглядання широкому загалу (підтвердженням цього є принцип «економіки громадської уваги», як назвав його Брігенто).

Особу злочинця можна охарактеризувати як «віртуального вандала» (спамери, хакери, автори вірусів, кіберпанки, кібербулери, кібертролери), дії якого спрямовані на деструктивну діяльність у мережі Інтернет. До них можуть належати особи, які мають відповідну технічну освіту в галузі комп'ютерної техніки й інформаційних технологій, навіть школярі, які відвідують приватні школи із програмування, студенти профільних навчальних закладів, професійні розробники програмного забезпечення та інших продуктів, системні адміністратори, налаштувачі програмного забезпечення, тобто особи, які володіють спеціальними знаннями в галузі програмування. Тип характеру особистості неважливий. Для українського правозастосовувача такий вид особи злочинця є досить новим.

За допомогою інтернет-простору можна «створити себе» заново: придумати яскравий нік, створити імідж у Мережі, «грати» різні соціальні ролі, недосяжні в реальному житті, залишати образливі коментарі та вчиняти інші протиправні дії, які в реальному житті підпадають під кваліфікацію згідно із законодавством.

Зазвичай кібервандали безпосередньо очно не знайомі.

Спостерігається взаємозв'язок віку кібервандала з мотивом та способом вчинення злочину: якщо мотив та спосіб не завдають значної шкоди, а, наприклад, мають за мету самоствердження, то кібервандалом є особа віком від 14 до 22 років; чим старший за віком індивід, тим більша суспільна небезпечність його дій. Крім того, у «віртуального вандала» можна знайти значну кількість спеціалізованої літератури, зокрема з «хакінгу», захисту комп'ютерної інформації. Також є деякі особливості зовнішності такої особи, як-от специфічна зачіска, невибагливість в одязі та вживання жаргонізмів (наприклад, «крута мати» – материнська плата) [7, с. 30].

Кібервандалізм все частіше вчиняють цілі компанії й об'єднання, які самоідентифікуються. Серед них достатньо відомими є такі: «Незамітна рись» (Китай), «Бюро 121» (Пхеньян, Північна Корея), «Аксіома» (Китай), «Підрозділ 61398» («Коментаторська команда», «Панда із клюшкою»), (Китай), «Група безпеки Аякс» (Іран), «Індивідальні операції доступу» (Сполучені Штати Америки). Також варто зазначити такі:

– «Сірійська електронна армія» (Сірія), організована 2011 р., складається здебільшого зі студентів. Їхня протиправна діяльність характеризується традиційним вчиненням «зломів», атаками та неправомірним розміщенням неправдивої інформації на сайтах відомих інформаційних агентств, як-от New York Times, CNN, Washington Post, Time. Після завершення кібервандалізму на екрані з'являється надпис, яким кібервандали самоідентифікуються;

– "Tarsh Andishan" (на фарсі «Мислителі», або «Новатори») – хакерська група, яка фінансується державою та застосовує найсучасніші технології, наприклад, SQL-ін'єкції, нові експлойти, бекдори тощо. Частина цієї групи перебуває в Тегерані;

– «Стрекоза», або «Енергетичний ведмідь» (Східна Європа). Ця група створила власний шпіонський «троян» під назвою Backdoor.Oldrea, Trojan.Karagany. Визначним є те, що зараження таким вірусом можливе й через встановлення легального програмного забезпечення, під час використання спеціальних інтернет-сайтів, на яких серії редиректів використовуються таку кількість разів, доки Backdoor.Oldrea чи Trojan.Karagany не заразять системи потерпілого [10].

Багато організацій мають право відстежувати IP-адреси користувачів та їхню життєдіяльність в Інтернеті з метою подальшого таргетування реклами. Відкриваючи ту чи іншу веб-сто-

рінку, браузер надсилає тисячі запитів на різноманітні сервери для подальшого показу цільової реклами, статистичних даних тощо. Але в складі таких компаній є співробітники, які також мають доступ до цих персональних даних і можуть використовувати ці дані в злочинних цілях.

За рівнем кваліфікації кібервандалів диференціюють на осіб із розвиненими спеціальними навичками, а також скрипт-кідді, що діють за приписом, виконують послідовний список команд і фактично не розуміють складу здійснюваних дій. Окрему групу становлять хактивісти – особи, що використовують окремі спеціальні навички зі збирання інформації на користь правозахисної, природоохоронної або політичної діяльності. Специфіка знань, необхідних для роботи із програмним та апаратним забезпеченням, а також постійне вдосконалення електронних засобів спричиняють спеціалізацію кібервандалів. Крекери здійснюють зворотний інжиніринг та злам програмного забезпечення. Фрікери володіють прийомами порушення маршрутизації трафіку телефонних дзвінків [4, с. 886–887].

Усе вищезазначене щодо особи кібервандала стосується здебільшого саме виконавця, але встановити замовника, за його наявності у цій схемі, досить складно.

Найбільше кібервандалів зафіксовано в Китаї, Індонезії, Турції, Індії та Тайвані [3, с. 129–130].

До потерпілих належать державні структури, приватні компанії, а також пересічні громадяни, сайти, комп'ютерні програми яких зазвичай найменш захищені з різних причин (незнання, небажання використовувати сучасні методи захисту інформації тощо).

Сліди кібервандалізму досить важко ідентифікувати у зв'язку з тим, що кібервандали використовують спеціальні сервіси, за допомогою яких сліди маскуються або взагалі не залишаються, наприклад, такі, як VPN та Tor, а також через використання різних видів криптовалют для оплати замовлених кіберпослуг.

Висновки. Отже, вищезазначена криміналістична характеристика кібервандалізму є своєрідною прагматичною, інформаційною моделлю, складники якої змінюють свої головні ролі на другорядні залежно від конкретної слідчої ситуації. Елементи криміналістичної характеристики тісно пов'язані між собою та мають відповідні кореляційні взаємозв'язки.

Список використаних джерел:

1. Справа №1/2506/232/11 // Архів Деснянського районного суду м. Чернігова. 2011.

2. В Одесі кіберполіція припинила термінацію мобільного трафіку до РФ та українських окупованих територій. URL: http://mvs.gov.ua/ua/news/12724_V_Odesi_kiberpoliciya_pripinila_determinaciyu_mobilnogo_trafiku_do_RF_ta_ukrainskih_okupovanih_teritoriy_FOTO.htm.

3. Валиахметова Г. Проблемы информационной безопасности в Азии. Известия Уральского федерального университета. Сер. 3 «Общественные науки». 2015. № 1 (137). С. 128–136.

4. Велика українська юридична енциклопедія: у 20 т. / Нац. акад. прав. наук України, Ін-т держави і права ім. В.М. Корецького, Нац. юрид. ун-т ім. Ярослава Мудрого; за ред. В. Тація та ін. Харків: Право, 2016. Т. 17: Кримінальне право / гол. редкол. В. Тацій. 2017. 1064 с.

5. Головин А. Частные криминалистические методики: проблемы структуры и качества. Криміналіст першодрукований (Криминалистъ первопечатный): міжнар. наук.-практ. юрид. журн. 2013. № 7. С. 67–74.

6. Колесниченко А., Коновалова В. Криминалистическая характеристика преступлений: учеб. пособие. Х.: Юрид. ин-т, 1985. 93 с.

7. Менжега М. Методика расследования создания и использования вредоносных программ для ЭВМ. М.: Юрлитинформ, 2009. С. 28–30.

8. Шевчук В. Методика розслідування контрабанди: проблеми теорії та практики: моногр. Х.: Гриф, 2003. 280 с.

9. Яблоков Н. Криминалистика: учебник для вузов. М.: БЕК, 1996. 318 с.

10. 9 современных хакерских групп, финансируемых государствами. URL: https://www.factroom.ru/kriminal/hackers-government.