9. Торбас О.О. Закриття кримінального провадження за новим кримінальним процесуальним кодексом України: характеристика деяких новел. Теоретичні та практичні проблеми забезпечення сталого розвитку державності та права: матер. Міжнар. наук.-практ. конф., присвяч. 15-річчю Нац. ун-ту «Одес. юрид. акад.» та 165-річчю Одес. шк. Права (Одеса, 30 листопада 2012 р.); відпов. за вип. В.М. Дрьомін. Одеса: Фенікс, 2012. Т. 2. С. 341–343.

10. Литвинов В.В. Класифікація підстав закриття кримінальної справи на стадії досудового розслідування. Право і суспільство. 2011. № 5. С. 196–201.

11. Лапкін А.В. Диференціація форм закінчення досудового розслідування і роль прокурора в їх застосуванні. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. 2016. Вип. 3. С. 87–97.

12. Солтанович А.В. Право подозреваемого на защиту в уголовном процессе Республики Беларусь: автореф. дисс. ... канд. юрид. наук: 12.00.09. Минск, 1992. 22 с.

13. Матюшенко Р.І. Виконання процесуального рішення про закриття кримінальної справи: дис. … канд. юрид. наук: 12.00.09. Київ, 2004. 168 с.

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

УДК 343.34

КІБЕРВАНДАЛІЗМ: ОКРЕМІ СПОСОБИ ВЧИНЕННЯ

Стаття присвячена аналізу одного з видів кібервандалізму – DoS-/DDoS-атаці (Distributed Denial of Service), окремим особливостям розслідування зазначеної категорії справи. Розглянуто проблему кібервандалізму через статичні дані та надано його характеристику. Запропоновано перелік процесуальних дій для розслідування кібервандалізму.

Ключові слова: *кібервандалізм, DoS-/DDoS-атаки, кримінальне провадження, досудове розслідування.*

Статья посвящена анализу одного из видов кибервандализма – DoS-/DDoS-атаке (Distributed Denial of Service) и отдельным особенностям расследования указанной категории дел. Рассмотрена проблема кибервандализма с помощью статических данных и предоставлена его характеристика. Предложен перечень процессуальных действий для расследования кибервандализма.

Ключевые слова: *кибервандализм, DoS-/DDoS-атаки, уголовное производство, досудебное расследование.*

The article is devoted to the analysis of one of the types of cyber vandalism of the DoS-/DDoS-attack (Distributed Denial of Service) and the specific features of the investigation of this category`s cases. The problem of cyber vandalism is considered through static data and its characteristic is given. The list of procedural actions for investigation of cyber vandalism is offered.

Key words: *cyber vandalism, DoS-/DDoS-attacks, criminal proceedings, pre-trial investigation.*

Вступ. В умовах цифрової епохи вандалізм набуває інформаційно-кібернетичного змісту та знаходить своє вираження на теренах Інтернет-простору. Традиційний вандалізм у зв'язку з активним упровадженням інформаційних технологій трансформувався в такий новий підвид, як кібервандалізм.

Окремі аспекти вандалізму досліджувалися в працях Д. Сафонова, Л. Філіппової, Е. Харіної, В. Шурухнова, Е. Бейтс, Б. Вебба, П. Вікстрема, А. Гольдштейна, М. Фелсона, Д. Кантера, С. Коена й ін. Однак стосовно кібервандалізму як окремого підвиду вандалізму, відсутні ґрунтовні криміналістичні дослідження. Проте боротьба з його наслідками лише починає здійснюватися на державному рівні.

Постановка завдання. У межах цієї статті розглянемо саме мережеву DoS-/DDoS-атаку (Distributed Denial of Service), яка здійснюється через віддалений доступ із використанням протоколів міжмережевої взаємодії шляхом віддзеркалення (коли IP-адреса джерела розповсюдження підміняється на IP-адресу потерпілого) і посилення шкідливого трафіку, що спрямовується на такі сервери, як DNS-сервер і NTP-сервер, а також визначимо основні напрями розслідування цього злочину.

Результати дослідження. Кібервандалізм – це вид ірраціональної деструктивної протиправної поведінки в мережі Інтернет, за якої предмету посягання завдається шкода. Серед видів кібервандалізму можна виділити такі: троянська програма, шкідливі та шпіонські програми; DoS-/DDoS-атаки (Distributed Denial of Service): атаки на IP-адреси; drive-by (попутне) завантаження; фішинг (от англ. «fishing» – «ловля риби»), який є видом соціальної інженерії з метою «виуджування» у користувачів Інтернету їх конфіденційних даних [5, с. 47], рекламні системи (adware), ботнети (бот-сети). Тим не менше, цей перелік не є вичерпним з огляду на постійну модернізацію інформаційних технологій.

Кібервандалізм є найбільш поширеною формою кіберконфлікту, що отримує суспільний резонанс. Зазвичай він містить зміни чи знищення змісту веб-сайту, відключення чи перезавантаження серверу, як це, наприклад, відбулося, коли закрили відомий український файлообмінник, «впали» урядові сайти, зокрема й МВС. Однак, незважаючи на свій шкідливий характер, наслідки таких інцидентів обмежені в часі та відносно незначні [2, с. 51].

На думку М. Каветлі, кібервандалізм містить зміни чи знищення змісту, наприклад, веб-сайту, відключення чи перевантаження сервера; це найбільш поширена форма кіберконфлікту, що отримує значний суспільний резонанс, але наслідки є незначними [4, с. 27].

З огляду на викладене, ірраціональність (від лат. irrationalis – нерозумність, нелогічність) поведінки особи злочинця має об'єктивне вираження, тобто для суспільства дії вандала є безглуздими. Проте суб'єктивний зміст, тобто ставлення злочинця-вандала до вчинюваного ним діяння, може мати різні мотиви. Крім того, має місце несвідомий потяг до агресії, що стримується вихованням і трансформується в більш-менш прийнятні форми (за З. Фрейдом – сублімація). При цьому підґрунтям вандалізму є психологічний механізм заміщення агресії, за якого агресія спрямовується не проти джерела стресу, а на інший об'єкт, впливаючи на який особа виміщає свій гнів. Також у якості ознак, що властиві кібервандалізму як підвиду вандалізму, можна навести бажання самоствердитися шляхом приниження в різних формах того, що має цінність для інших, особливо зневажливим способом, нездатність до самореалізації, що призвела до активного цинічного протесту проти суспільства [7, с. 324].

Найбільш розповсюдженою є класифікація кіберзлочинів на агресивні та неагресивні. До першої групи належить кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кібersталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них). Друга група включає кіберкрадіжку, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм [6, с. 215]. Такий вид злочинності набуває все більшої популярності через свою специфіку. Ці злочини є доступними, їх можна вчиняти на великій відстані від об'єкта, а найголовнішим є те, що

під час проведення слідчих (розшукових) дій доволі важко виявити та вилучити інформацію, яку можна розцінювати в якості доказу [9].

За результатами аналізу статистики DDoS-атак із використанням ботнетів у першому кварталі 2015 року, який проводив Kaspersky Lab, Україна опинилася серед топ-15 країн, в яких спостерігається найбільша кількість DDoS-атак [11]. Якщо у 2001 році було всього лише 2 атаки, то у 2016 – 138. Пік припав на 2012 рік, тоді нападів із боку хакерів було понад 180, тобто кожні два дні невідомі атакували один сайт. Було зламано 62 державні сайти та проведено 7 DDoS-атак на сайти з доменним ім'ям gov.ua. Це більше, ніж за аналогічний період 2016 року. Загалом атак зазнали 500 сайтів. Якщо порівнювати з 2016 роком, то фіксується зростання на 12,6%. Тоді було атаковано 444 сайти [12]. Цей підвид кібервандалізму полягає в протиправній діяльності бот-мережі, яка складається зі значної кількості комп'ютерних пристроїв, спрямованої на виведення конкретно визначеної комп'ютерної системи з ладу, унаслідок чого система некоректно працює, а правомірні користувачі позбавляються можливості доступу до неї. Такі дії не потребують ґрунтовних обчислювальних знань від особи злочинця та є достатньо проінструктованими (описаними) у мережі Інтернет на відповідних форумах. При цьому масові атаки можна здійснювати й без використання великих ресурсів шляхом генерації значної кількості відповідей, що в багато разів перевищує кількість запитів. На підтвердження зазначеної тези наведемо такий приклад. Особа, вирішивши зайнятися здійсненням DDoS-атак, завантажила та скопіювала на жорсткий диск свого комп'ютера зі всесвітньої мережі Інтернет програмне забезпечення, необхідне для організації та проведення DDoS-атак на вибрані ним сервери, IP-адреси та ресурси під назвою «Black Energy». Провівши тестування зазначеного програмного продукту, злочинець, спілкуючись у мережі Інтернет на сторінках форуму «xakerok.org», отримав додатковий спеціальний «файл динамічної бібліотеки» «*.dll», після чого програмний продукт «Black Energy» був повністю придатний для здійснення DDos-атак. Крім цього, особа розмістила зазначену програму на серверах «www.psugalaxy.com» та «www.cxim.inattack.ru/www2/www»; для доступу до неї спочатку використовувався ftp-доступ, а в подальшому – файл запуску програми у вигляді EXE-файлу. На цьому зазначена особа не зупинилася й отримала на спеціалізованому форумі так званий «Botnet» (файл управління комп'ютерами, зараженими вірусами), який надавав можливість одночасно з 1000 комп'ютерів здійснити звернення на той чи інший сервер, IP-адресу чи ресурс у мережі Інтернет і таким чином паралізувати його роботу [1].

За результатами узагальнення матеріалів кримінальних проваджень установлено, що для обстановки вчинення кібервандалізму є характерними такі риси:

– безконтрольність, безлад, безкарність; науковим підґрунтям зазначеного слугує «Теорія розбитих вікон», авторами якої є Джеймс Вілсон і Джордж Келлінг,

– відсутність належного контролю й охорони предмета злочинного посягання; зазначену тезу підтверджує наукова концепція «routine activity theory», розробниками якої є Маркус Фелсон і Лоренс Коен;

– час учинення кібервандалізму обирається таким чином, що самі безпосередні протиправні дії є недоступними для зовнішнього спостереження, але наслідки цих дій мають бути відкритими для споглядання широкого загалу; підтвердженням цього є принцип «економіки громадської уваги», як його назвав Брігенто [8, с. 39].

Особу злочинця можна охарактеризувати як «віртуального вандала» (спамери, хакери, автори вірусів), дії якого спрямовані на деструктивну діяльність у мережі Інтернет. Це можуть бути навіть школярі, які відвідують приватні школи з програмування, студенти профільних навчальних закладів, професійні розробники програмного забезпечення й інших продуктів, системні адміністратори, налаштувальники програмного забезпечення, тобто особи, які володіють спеціальними знаннями в галузі програмування. Тип характеру, особистості при цьому не є важливим. Для українського правозастосовувача такий вид особи злочинця є досить новим, тому необхідно звернутися до практики країн, де цей вид злочинців є більш дослідженим. Наприклад, такі особи мають вищу або незакінчену вищу технічну

освіту (52,9%); іншу вищу чи незакінчену вищу освіту мають 20% суб'єктів комп'ютерних злочинів, середньоспеціальну технічну освіту – 11,4%, іншу освіту – 15,7% [3]. Наявним є взаємозв'язок віку кібервандала з мотивом і способом учинення злочину: якщо мотив і спосіб не завдають значної шкоди, а, наприклад, мають на меті самоствердження, то це кібервандал віком від 14 до 22 років; чим старший за віком є індивід, тим більше прогресує суспільна небезпечність, що ним учиняється. Крім того, у «віртуального вандала» можна знайти велику кількість спеціалізованої літератури, зокрема, з «хакінгу», захисту комп'ютерної інформації. Також мають місце певні особливості зовнішності такої особи (специфічна зачіска, невибагливість в одязі та вживання жаргонів (наприклад, «крута мати» – материнська плата)) [10].

Із метою ідентифікації особи злочинця потрібно здійснити перевірку лог-файлів на наявність аномалій, які свідчать про DDoS-атаку; проаналізувати протоколи, які можуть бути використані для реалізації DDoS-атаки; визначити основні параметри з'єднання, які є достатніми для ідентифікації DDoS-атак, і прибрані записи мережевих образів, які не належать до обраного типу шкідливого впливу.

Так, не встановлені органом досудового розслідування особи, діючи за попередньою змовою, здійснили несанкціоноване втручання в роботу зовнішнього сайту Міністерства фінансів України (minfin.gov.ua) у вигляді DDOS-атаки, основна хвиля якої припала на нічний час з 20:00 30 грудня 2016 р. до 09:00 01 січня 2017 р., що підтверджено провайдером ТОВ «Інфоком», з яким укладено договір про надання послуг із захищеного доступу до Інтернету.

Насамперед потрібно допитати в якості свідка особу, уповноважену здійснювати системний супровід ІТ-систем Міністерства (як керівника відділу, так і другорядних працівників). Під час допиту такої особи необхідно встановити його посаду, коло обов'язків і деталі того, яким чином було виявлено кібервандалізм. Отже, було допитано начальника відділу системного супроводження Міністерства фінансів України, який пояснив, що 31 грудня 2016 р. о 07:30 ранку, намагаючись зайти на сайт Міністерства фінансів України за адресою minfin.gov.ua, він виявив, що сайт недоступний, при цьому було визначено конкретну IP-адресу. Після виявлення цього факту було прийняте рішення поїхати на роботу для виявлення й усунення проблеми. Близько 9:00, прибувши на роботу, він виявив, що навантаження на сервер Міністерства фінансів України було 100%, інших ознак відхилення роботи сервера від норми не було виявлено. Після перезавантаження веб-сервера навантаження на сервер відновилося. Ураховуючи обставини, у начальника відділу виникла підозра, що на Міністерство фінансів України за Інтернет-адресою minfin.gov.ua за IP-адресою здійснюється Ddos-атака на http-порт 80. Після цього, зателефонувавши до провайдера надання послуг доступу до глобальної мережі Інтернет, ТОВ «Інфоком», він отримав інформацію, яка підтверджувала його підозри, що в запитуваний період часу здійснювалася потужна Ddos-атака (за класифікацією моделі OSI – рівень 4), а саме Ddos-атака великою кількістю запитів. Згідно з відомостями, отриманими від провайдера, інтенсивність такої атаки була близько 1 000 000 запитів на секунду, проте на час надання інформації надвеликої інтенсивності запитів на сайт Міністерства фінансів України не спостерігалося. Тим не менше, завантаження ресурсів сервера все одно залишалося 100%. Задля відновлення роботи веб-сайту Міністерства було прийняте рішення перенести сайт на іншу IP-адресу з подальшим внесенням змін у налаштування сервера імен. Через декілька хвилин веб-сайт став доступний за новою IP-адресою, подальших Ddos-атак на нову адресу не було.

Для встановлення обставин, які мають значення доказів у кримінальному провадженні, органом досудового розслідування в порядку ст. 93 КПК України витребувано з Міністерства фінансів України відомості щодо лог-файлів атаки на офіційний сайт Міністерства фінансів України. У ході аналізу вказаних відомостей установлено IP-адреси, з яких здійснювалися такі Ddos-атаки, що належать провайдеру Інтернет-послуг ТОВ «ЛАНГЕЙТ».

У зв'язку із цим необхідно встановити таке:

1) анкетні дані осіб, які зі встановленої IP-адреси здійснювали Ddos-атаки на офіційний сайт Міністерства фінансів України,

2) відомості щодо місця знаходження комп'ютерного обладнання, з якого здійснювалася така протиправна діяльність, його місце знаходження,

3) відомості щодо електронної інформації, обмін якою здійснювався за допомогою мережі Інтернет із вищезазначеної IP-адреси за період із 00:00 29 грудня 2016 р. до 24:00 01 січня 2017 р.

Слід зауважити, що такі відомості містять охоронювану законом таємницю, а саме відомості щодо персональних даних осіб, яким надаються Інтернет-послуги з використанням установленої IP-адреси, а також відомості, що становлять комерційну таємницю (у частині умов надання Інтернет-послуг таким особам). Тому необхідним є звернення з відповідним клопотанням про надання дозволу на тимчасовий доступ до речей і документів із можливістю вилучення (виїмки) їх копій, серед яких є такі документи:

– належним чином посвідчена копія договору на надання Інтернет-послуг користувачеві мережі Інтернет, якому в період із 00:00 29 грудня 2016 р. до 24:00 01 січня 2017 р. включно для виходу до мережі Інтернет було надано IP-адресу;

– відомості щодо прізвища, імені та по батькові особи, місця проживання, адреси, за якою надаються провайдером Інтернет-послуги кінцевому споживачеві з IP-адресою,

– належним чином посвідчені копії документів, які посвідчують особу підозрюваного, якому в період із 00:00 29 грудня 2016 р. до 24:00 01 січня 2017 р. надано для користування та виходу до мережі Інтернет IP-адресу;

– відомості щодо mac-адреси всього комп'ютерного обладнання кінцевого споживача Інтернет-послуг, якому в період із 00:00 29 грудня 2016 р. до 24:00 01 січня 2017 р. надано для користування IP-адресу;

– відомості щодо актуального користувача IP-адреси;

– відомості щодо всіх URL-даних, на які здійснювалися запити з кінцевого комп'ютерного обладнання користувача IP-адреси в період із 00:00 29 грудня 2016 р. до 24:00 01 січня 2017 р.;

– відомості щодо нешифрованих протоколів передачі даних, що відбувалася між користувачем Інтернет-послуг з IP-адреси й іншими IP-адресами в період із 00:00 29 грудня 2017 р. до 24:00 01 січня 2017 р.;

– відомості щодо прикладних протоколів для передачі інформації у вигляді гіпертекстових документів у форматі HTML (HTTP – HyperText Transfer Protocol), що здійснювалася користувачами Інтернет-послуг з IP-адреси в мережі Інтернет за період часу із 00:00 29 грудня 2017 р. до 24:00 01 січня 2017 р.;

– відомості щодо передачі електронних даних по захищеному протоколу HTTPS, що відбувалася між клієнтом (отримувачем Інтернет-послуг з IP-адреси) та сервером (надавачем таких послуг) за період із 00:00 29 грудня 2017 р. до 24:00 01 січня 2017 р.;

– відомості щодо електронних даних, програмного забезпечення й інших електронних відомостей щодо їх обсягу й інтенсивності передачі у період із 00:00 29 грудня 2017 р. до 24:00 01 січня 2017 р. із першої IP-адреси на другу IP-адресу;

– відомості щодо всіх IP-адрес, між якими здійснювався обмін електронною інформацією з IP-адреси за період із 00:00 29 грудня 2017 р. до 24:00 01 січня 2017 р.

Висновки. Кібервандалізм як підвид вандалізму набуває все більшого поширення на теренах України через необізнаність правоохоронних органів із можливостями використання інформаційних технологій під час розслідування цієї категорії злочинів. Важливим є розуміння поняття й ознак кібервандалізму задля ефективного пошуку та фіксації електронних слідів, а також для подальшого здійснення слідчих (розшукових) дій.

Список використаних джерел:

1. Архів Білоцерківського міськрайонного суду Київської області за 2010 р. Справа № 1-7/2010.

2. Богучарова О., Комісаров С. Безпека кібернетичного простору як екологічного середовища та осередку вчинення злочинів. Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2015. № 3. С. 49–52.

3. Головин А. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации. Центр исследования проблем компьютерной преступности.

4. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки. Політичний менеджмент. 2010. № 5. С. 19–30.

5. Карпова Д. Киберпреступность: глобальная проблема и ее решение. Власть. 2014. № 8. С. 45–50.

6. Кримінологія: Загальна та Особлива частини. Навчальний посібник. Х.: Право, 2014. 513 с.

7. Латиш К. Вандалізм: предмет і способи його вчинення. Проблеми законності 2013. № 123. С. 323–330.

8. Латыш Е. Обстановка совершения вандализма как элемент криминалистической характеристики преступления. Legea si Viata. 2014. № 4. С. 38–44.

9. Марків С. Кіберзлочинність. Нова кримінальна загроза. URL: http://dspace.tneu.edu.ua/bitstream/316497/21460/1/360-362.pdf.

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

11. Украина вошла в топ-15 стран по количеству DDoS-атак. URL: https://zn.ua/TECHNOLOGIES/ukraina-voshla-v-top-15-stran-po-kolichestvu-ddos-atak-178761_.html.

12. Статистика: скільки державних сайтів України зламано хакерами за 16 років. URL: https://tokar.ua/read/22540.

МАМКА Г. М.,
кандидат юридичних наук,
професор кафедри кримінального права
та кримінології
(Національний університет державної фіскальної служби України)

УДК 343.131

ПРО ДЖЕРЕЛА КРИМІНАЛЬНОГО ПРОЦЕСУАЛЬНОГО ПРАВА УКРАЇНИ У КОНТЕКСТІ РЕАЛІЗАЦІЇ РІВНОСТІ ЯК ПРИНЦИПУ ЮРИДИЧНОГО ПРОЦЕСУ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

У статті проаналізовано реалізацію рівності як принципу юридичного процесу у кримінальному провадженні. Вказано на необхідність її дотримання під час формулювання системи джерел кримінального процесуального права України.

Ключові слова: *кримінальне провадження, принципи юридичного процесу у кримінальному провадженні, рівність як принцип юридичного процесу, джерела кримінального процесуального права.*