УДК 343.1
DOI https://doi.org/10.32782/2524-0374/2022-4/65

КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА СПОСОБІВ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ОБІГОМ ПРОТИПРАВНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ

CRIMINAL CHARACTERISTICS OF WAYS OF COMMITTING CRIMINAL OFFENSES RELATED TO THE CIRCULATION OF ILLEGAL CONTENT ON THE INTERNET

Тарасенко О.С., д. ю. н., доцент,
професор кафедри оперативно-розшукової діяльності
Національна академія внутрішніх справ

У статті на основі ретроспективного аналізу еволюції способів учинення корисливих зазіхань у сфері комп'ютерних технологій, узагальнення слідчої й судової практики розкрито зміст способів учинення кримінальних правопорушень, пов'язаних з протиправним контентом в мережі Інтернет, а також технологій злочинної діяльності, що застосовують на етапах підготовки, вчинення та приховування (розповсюдження, збут, завідомо неправдиве повідомлення; публічні заклики), що має значення для встановлення джерел інформації про підозрюваного, обрання тактичних прийомів розслідування. Розповсюдження та збут шкідливих програмних чи технічних засобів можуть вчинятися як особою, що створила шкідливі засоби, так і іншою, яка не брала участі в їх утворенні. Як розповсюдження, так і збут є закінченими складами злочину з моменту передачі шкідливих програмних або технічних засобів, незалежно від того, чи зміг отримувач ними розпорядитися чи ні. До основних способів вчинення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет віднесені ті, що пов'язані з: функціонуванням соціально орієнтованих мереж, діяльність яких заснована на так званій вікі(viki)-технології; функціонуванням технологій електронної комерції, створені для здійснення торгівлі через Інтернет; функціонуванням технології електронної розсилки, IP-телефонії; функціонуванням шкідливого програмного забезпечення. Способи підготовки, пов'язані з завантаженням, пошуком, створенням, зберіганням, редагуванням відповідних текстових, фото-, відеофайлів або інших форм публікації. Способи приховування найчастіше не застосовують, а в окремих випадках для забезпечення анонімності злочинець може використовувати віртуальні приватні мережі (VPN-технології). Наведена група способів може набувати реалізації у формі одиничного кримінального правопорушення або містити багато епізодів кримінальної протиправної діяльності та може мати довготривалий характер. Такі способи не є вичерпними, але на цей час вони найоб'єктивніше відбивають інтерактивний характер кримінальної протиправної діяльності у кіберпросторі.

Ключові слова: протиправний контент, Інтернет, кримінальне правопорушення, спосіб, вчинення, приховування, маскування.

Based on a retrospective analysis of the evolution of ways of committing selfish encroachments in the field of computer technology, generalization of investigative and judicial practice, the article reveals the content of ways of committing criminal offenses related to illegal content on the Internet and criminal technologies used in stages preparation, commission and concealment (dissemination, sale, knowingly false information; public appeals), which is important for establishing sources of information about the suspect, choosing tactics of investigation. The distribution and sale of malicious software or hardware may be committed by the person who created the malicious software or by another who did not participate in its creation. Both distribution and sale are completed corpus delicti since the transfer of malicious software or hardware, regardless of whether the recipient was able to dispose of them or not. The main ways of committing criminal offenses related to the circulation of illegal content on the Internet include those related to: the functioning of socially oriented networks, the activities of which are based on the so-called viki technology; the functioning of e-commerce technologies designed to trade via the Internet; functioning of electronic mailing technology, IP-telephony; malware operation. Preparation methods related to uploading, searching, creating, storing, editing relevant text, photo, video or other forms of publication. Concealment methods are often not used, and in some cases the perpetrator may use virtual private networks (VPN-technologies) to ensure anonymity. This group of methods can be implemented in the form of a single criminal offense or contain many episodes of criminal activity and can be long-term. Such methods are not exhaustive, but at the moment they most objectively reflect the interactive nature of criminal illegal activities in cyberspace.

Key words: illegal content, Internet, criminal offense, method, commission, concealment, disguise.

Актуальність статті. Дії суб'єкта безпосередньо «запускають» механізм кримінального правопорушення, частина якого може згодом протікати незалежно від суб'єкта. Тому в утворенні слідової картини кримінального правопорушення визначальним є спосіб як початкова точка злочинного діяння. З першої дії або утримання від дії (бездіяльності) суб'єкта запускається весь механізм кримінального правопорушення і починається зміна середовища. Тому саме у зв'язку із способом кримінального правопорушення потрібно розглядати характерні його наслідки, зокрема сліди. Цей зв'язок нерозривний і взаємний: спосіб утворює сліди злочину, а сліди дозволяють встановити спосіб.

Інформація про спосіб підготовки, вчинення, приховування (маскування) кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, слугує основою для: розробки характеристики цього виду кримінальних правопорушень; виявлення взаємозв'язку між структурними елементами характеристики (спосіб – особа злочинця, спосіб – сліди, спосіб – предмети посягання тощо); побудови слідчих версій; планування досудового розслідування; розробки конструкції тактики проведення слідчих (розшукових) дій (СРД) та негласних слідчих (розшукових) дій (НСРД); розробки запобігання кримінальним правопорушенням [1, с. 427].

Виклад основного матеріалу. У криміналістичній характеристиці спосіб вчинення досліджується для того, щоб з'ясувати, які сліди залишило кримінальне правопорушення у навколишньому середовищі, де ці сліди потрібно шукати, які вони містять дані щодо особи, яка вчинила кримінальне правопорушення [2, с. 49]. Не варто також змішувати кримінально-правове і криміналістичне значення дій з підготовки та приховування кримінального правопорушення. Кримінально-правове значення мають ті дії з підготовки і приховування кримінального правопорушення, що передбачені як кримінальне каране діяння і вказані в диспозиції статті Особливої частини КК України. На думку А. А. Хмирова, криміналістичне значення мають дії з підготовки і приховування кримінального правопорушення, які становлять єдиний цілеспрямований комплекс дій, що створюють спосіб вчинення кримінального правопорушення [3, с. 53]. Ці положення варто враховувати визначаючи криміналістичне поняття і зміст способу вчинення кримінального правопорушення при проведенні розслідування у конкретному кримінальному провадженні [4].

Знання способів вчинення кримінальних правопорушень дозволяє слідчому (дізнавачу) методично правильно визначати напрями розслідування. Водночас злочинці прагнуть використовувати способи, які істотно утруднили б проведення розслідування, або унеможливили його проведення. З цією метою винаходяться нові, видозмінюються вже відомі способи вчинення кримінального правопорушення та його приховування [5, с. 48].

У ході проведеного дослідження та на основі вивчення матеріалів кримінальних проваджень встановлено способи вчинення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, зокрема:

1) розповсюдження у мережі Інтернет порнографічних предметів і зображень, творів, що пропагують культ насильства та жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 161, 300, 301) (42 %), яке може відбуватися й у формі спілкування в цій мережі (42 %);

2) розповсюдження у мережі Інтернет відомостей, що становлять державну або іншу таємницю, яка охороняється законом (ст. 114, 145, 159, 168, 232, 328, 361-2, 381, 387, 422) – дія, за допомогою якої зазначені об'єкти безпосередньо чи опосередковано пропонуються публіці, зокрема доводяться до відома невизначеного кола осіб таким чином, що особи мають можливість здійснити вільний доступ до цих об'єктів за власним вибором (23 %);

3) розповсюдження у мережі Інтернет шкідливих програмних засобів (ст. 361-1) – це будь-яка дія, безпосередня чи опосередкована пропозиція, за допомогою якої ці об'єкти (зокрема, комп'ютерні віруси) поширюються чи починають автоматично відтворюватись у електронно-обчислювальних машинах, автоматизованих системах, комп'ютерній мережі або комп'ютерних мережах чи мережах електрозв'язку в результаті їх «закладання» в програмне забезпечення, а також створення умов, за яких інші особи можуть здійснити доступ до них або отримати у користування з будь-якого місця і в будь-який час за власним вибором, у тому числі мережею та іншим способом на платній чи безоплатній основі (20 %);

4) завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259) (8 %);

5) публічні заклики, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109), заклики до вчинення дій, що загрожують громадському порядку (ст. 295) (7 %) [6].

Таким чином, *способами вчинення є розповсюдження, збут, розміщення, розголошення предмета протиправного контенту.* Розглянемо детальніше.

У загальному вигляді *розповсюдження* в мережі Інтернет відомостей, що становлять державну або іншу таємницю, творів, зображень, предметів порнографічного характеру або творів, що пропагують культ насильства та жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію – це будь-яка дія, за допомогою якої зазначені об'єкти безпосередньо чи опосередковано пропонуються публіці, зокрема доводяться до відома невизначеного кола осіб таким чином, що особи мають можливість здійснити вільний доступ до цих об'єктів за власним вибором. Розповсюдження контенту у мережі Інтернет може проводитись у формі його опублікування, дарування, показу, відкриття доступу до свого комп'ютера, сервера чи іншого носія інформації, демонстрації та інших дій, внаслідок яких відомості сприймаються іншими особами [6–8].

Розповсюдження шкідливих програмних засобів – це будь-яка дія, безпосередня чи опосередкована пропозиція, за допомогою якої ці об'єкти (зокрема, комп'ютерні віруси) поширюються чи починають автоматично відтворюватись у ЕОМ, АС або комп'ютерних мережах чи мережах електрозв'язку в результаті їх «закладання» в програмне забезпечення, а також створення умов, за яких інші особи можуть здійснити доступ до них або отримати у користування з будь-якого місця і в будь-який час за власним вибором, у тому числі мережею та іншим способом на платній чи безоплатній основі [6].

За результатами такої діяльності ці об'єкти (шкідливі програмні засоби) поширюються чи починають автоматично відтворюватись у ЕОМ, АС або комп'ютерних мережах чи мережах електрозв'язку в результаті їх «закладання» в програмне забезпечення чи надання доступу до цих об'єктів невизначеному колу осіб на платній чи безоплатній основі [7].

Способи розповсюдження можуть бути різні: самовідтворення; «закладання» в програмне забезпечення; розповсюдження з використанням комп'ютерної мережі, установка (інсталяція) таких засобів у процесі виготовлення, ремонту, реалізації, ознайомлення інших осіб зі змістом програмних і технічних засобів комбінації названих способів [7].

Збут шкідливих програмних засобів – оплатне або безоплатне (продаж, дарування, обмін, сплата боргу, позика тощо) відчуження фізичного носія зі шкідливим програмним засобом іншій особі. Типовим прикладом збуту шкідливих програм є продаж дисків із записаними на них шкідливими програмами. Збут передбачає відчуження зазначених вище предметів, речовин іншій особі, яка може розпоряджатися ними (або їх частиною) як своїм майном. Для настання відповідальності достатньо факту збуту хоча б одного предмета чи речовини хоча б одній особі [7–8].

Збут забороненого контенту вражається *незаконним*, якщо він здійснюється з порушенням норм, які регламентують порядок обігу предметів та речовин, заборонених для вільного обігу.

Під *збутом* відомостей, що становлять державну або іншу таємницю, творів, зображень або предметів порнографічного характеру тощо, розуміють їх оплатне або безоплатне відчуження (продаж, дарування, передача в якості повернення боргу тощо) хоча б одній особі [7].

Збут або розповсюдження забороненого контенту потрібно вважати *несанкціонованим,* якщо ці дії вчинені без дозволу (згоди) власника цього контенту. Несанкціоновані збут або розповсюдження містять ознаки кримінального правопорушення як в тому випадку, коли вони вчинені особою, якій в установленому порядку було надано доступ до відповідної інформації, так і у випадку вчинення їх особою, яка такого доступу не мала [7].

Розповсюдження творів, зображень або предметів через мережу Інтернет може відбуватися й у формі спілкування в цій мережі.

Спілкування в мережі Інтернет – процес обміну електронними повідомленнями між двома та більше комп'ютерними пристроями, що підключені до Інтернету й передають ці повідомлення у вигляді пакетів даних, створюваних та оброблюваних на основі стандартів протоколу IP. Відповідне спілкування може відбуватися як у вигляді безпосереднього обміну повідомленнями між учасниками спілкування, так і опосередковано, через публічні Інтернет-ресурси: сайти, форуми, чати, блоги, дошки повідомлень тощо. Повідомлення можуть бути у вигляді тексту, малюнків, фотозображень, в аудіо- та відеоформаті. Спілкування може бути як в режимі реального часу, так і з відстрочкою отримання повідомлення адресатом (адресатами) [6–9].

Під *розміщенням* контенту треба розуміти процес публікації інформації за допомогою комп'ютерного пристрою, що підключений до мережі Інтернет. Розміщення даних, як правило, відбувається на власних або публічних Інтернет-ресурсах: порталах, сайтах, вебсторінках, форумах, чатах, блогах, дошках повідомлень тощо. Розміщені

дані можуть бути у вигляді тексту, графічних об'єктів, аудіо- та відеофайлів [7].

Реклама контенту, що містить ознаки порнографії або пропаганди культу насильства і жорстокості, – це інформація про такий контент, призначена для формування або підтримання обізнаності споживачів реклами та їх інтересу щодо такого контенту. Розповсюдження цієї реклами може здійснюватися, зокрема, через мережу Інтернет [7].

Розголошення відомостей, що становлять державну або іншу таємницю, яка охороняється законом, – розміщення цих відомостей в мережі Інтернет без згоди їх власника, внаслідок чого з цими відомостями безпосередньо чи опосередковано можуть ознайомлюватись певні особи чи невизначене коло осіб. Обсяг розголошених відомостей для кваліфікації кримінального правопорушення значення не має [10, с. 792].

Основними способами вчинення кримінальних правопорушень, вчинених з використанням шкідливих програмних чи технічних засобів, є: створення шкідливих програмних засобів; створення шкідливих технічних засобів; використання шкідливого технічного засобу; використання шкідливого програмного засобу; збут шкідливого програмного засобу; збут шкідливого технічного засобу; розповсюдження шкідливого програмного засобу; розповсюдження шкідливого технічного засобу [7, с. 11].

Найпоширенішими різновидами шкідливих програмних засобів є: комп'ютерні віруси, автономні агенти, «троянський кінь», засоби перехоплення трафіку (сніффери), програми-шпигуни [11, с. 363].

Створення шкідливих програмних засобів – це дії, в результаті яких відбувається фізична матеріалізація (факт створення) шкідливого програмного засобу на носії інформації або в просторових формах. Під створенням шкідливої програми необхідно розуміти творчу діяльність суб'єкта, спрямовану на створення якісно нової програми, завідомо наділеної функціями, виконання яких спричиняє протиправний вплив на комп'ютерну інформацію, процеси її автоматизованої обробки та електронно-обчислювальні засоби [6].

Створення шкідливих програмних засобів включає в себе написання алгоритму шкідливої програми для ЕОМ з наступним (обов'язковим) перетворенням його у машинну мову. Причому внесення змін до вже існуючої комп'ютерної програми, внаслідок чого вона набуває ознак шкідливості, або якщо у неї додалися нові шкідливі функції, чи у результаті подібних змін було створено якісно нову шкідливу програму для ЕОМ, також потрібно вважати створенням. Характер змін, що вносяться в існуючу програму, може бути різним: додавання, вилучення, дублювання частини машинного коду та інші можливі модифікації програми, які можуть стосуватися і шкідливих функцій.

Обов'язковою умовою доказування під час досудового розслідування має бути визначення мети створення програмного засобу, а саме, його використання, розповсюдження або збут для несанкціонованого втручання. Тобто, якщо вказане забезпечення було створене, наприклад, виключно з дослідницькою метою, то таке діяння не повинно вважатися караним. Якщо ж мала місце злочинна ціль (будь-яка з перелічених), кримінальна відповідальність повинна наставати за сам факт створення, незалежно від реалізації такої мети.

Так, на початку квітня 2010 року ОСОБА_2, діючи умисно з корисливих мотивів, перебуваючи у себе вдома, а саме на орендованій квартирі у м. Києві, використовуючи власний ноутбук торгової марки "DELL", моделі "Vostro3700", серійний номер № 2FH87L1, можливість доступу до мережі Інтернет, а також власний досвід у сфері створення програмного забезпечення, на мові програмування «С++» шляхом написання вихідних кодів розпочав створення шкідливого програмного засобу – шкідливої комп'ютерної програми під назвою «ІНФОРМАЦІЯ_11», призначеної для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), якій у подальшому ним було надано умовну назву «ІНФОРМАЦІЯ_12», з метою його збуту через мережу Інтернет [12].

Створення шкідливих технічних засобів полягає у виготовленні будь-яким способом відповідного пристрою, обладнання чи устаткування. Причому, зважаючи на специфічність такого устаткування, виготовлення може полягати не лише у його фізичному збиранні, а й, наприклад, у розробці чи налагодженні устаткування відповідним чином або його програмуванні (перепрограмуванні), після чого пристрій набуватиме ознак шкідливості.

Так, гр-н К. у м. Ірпінь, з корисливих мотивів, придбав у невстановленої особи чисту картку-емулятор (тобто здатну імітувати дію іншого пристрою) та коди KI та IMSI сім-картки китайського оператора мобільного зв'язку. Надалі він вставив у свій мобільний телефон картку-емулятор і ввів у неї отримані коди KI та IMSI, внаслідок чого зазначена картка стала клоном оригінальної сім-картки, за допомогою якої стало можливо здійснювати емуляцію її роботи. Таким чином, даний громадянин створив шкідливий технічний засіб, призначений для несанкціонованого втручання в роботу мереж електрозв'язку, після чого активував означену сім-картку в своєму власному телефоні та здійснював дзвінки на свій телефон, у якому знаходилась сім картка оператора мобільного зв'язку «Білайн», унаслідок чого отримав грошовий бонус на вказаний номер [13].

Оскільки у своєму первинному вигляді картка-емулятор не мала шкідливих функцій, що також характеризує і окремо взяті коди зв'язку, то можна вважати, що здатність впливати на процес роботи мереж електрозв'язку технічний засіб отримав унаслідок його відповідного налагодження (програмування).

Таким чином, створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів пропонується вважати закінченим з моменту набуття створюваної програми або пристрою ознак шкідливості (тобто їх властивості негативно впливати на встановлений порядок обробки інформації).

Розповсюдження шкідливих програмних засобів – це будь-яка дія, безпосередня чи опосередкована пропозиція, за допомогою якої ці об'єкти (зокрема, комп'ютерні віруси) поширюються чи починають автоматично відтворюватись у ЕОМ, АС або комп'ютерних мережах чи мережах електрозв'язку в результаті їх «закладання» в програмне забезпечення, а також створення умов, за яких інші особи можуть здійснити доступ до них або отримати у користування з будь-якого місця і в будь-який час за власним вибором, у тому числі мережею та іншим способом на платній чи безоплатній основі [6].

За результатами такої діяльності ці об'єкти (шкідливі програмні засоби) поширюються чи починають автоматично відтворюватись у ЕОМ, АС або комп'ютерних мережах чи мережах електрозв'язку в результаті їх «закладання» в програмне забезпечення чи надання доступу до цих об'єктів невизначеному колу осіб на платній чи безоплатній основі.

Способи розповсюдження можуть бути різні: самовідтворення; «закладання» в програмне забезпечення; розповсюдження з використанням комп'ютерної мережі, установка (інсталяція) таких засобів у процесі виготовлення, ремонту, реалізації, ознайомлення інших осіб зі змістом програмних і технічних засобів комбінації названих способів.

Спосіб *«закладання» шкідливих програмних засобів у* програмне забезпечення полягає в тому, що особа, яка розповсюджує ці засоби, включає шкідливу програму до складу використовуваного програмного забезпечення. Один із таких способів розповсюдження шкідливих про-

грам одержав назву «троянський кінь». Суть його полягає в тому, що винний розповсюджує якесь корисне програмне забезпечення, наприклад, текстовий редактор, перекладач або навчальну програму, однак, крім корисних функцій, програма містить і приховані, призначені для порушення права власності на інформацію [6].

Розповсюдження шляхом *використання комп'ютерних мереж* полягає, як правило, у наданні доступу до шкідливих програм шляхом їх розміщення на мережевих носіях інформації або в розсиланні електронною поштою копій шкідливих програм.

Так, Кіровським районним судом м. Кіровограда засуджено А. у вчиненні злочину, передбаченого частиною першою ст. 361-1 КК України, який, користуючись локальною комп'ютерною мережею гуртожитків, діючи умисно, завантажив у власний комп'ютер програмні засоби. Ці засоби пізніше під час експертизи було визнано програмами для віддаленого зчитування паролів або нейтралізації засобів захисту комп'ютерних програм чи інформації, які після встановлення паролів та їх нейтралізації дають можливість доступу до певної комп'ютерної інформації, комп'ютерної програми, комп'ютерної мережі, операційної системи та здійснення непомітно для власника чи законного користувача несанкціонованої передачі інформації сторонній особі. Після цього А. надав вільний доступ до свого комп'ютера всім абонентам локальної мережі [14].

Розповсюдження шкідливих технічних засобів – є їх установлення в оплатній або безоплатній формі в ЕОМ, АС або комп'ютерних мереж чи мереж електрозв'язку, які продаються або передаються на іншій основі, наприклад, здаються в оренду.

Збут шкідливих програмних чи технічних засобів – оплатне або безоплатне (продаж, дарування, обмін, сплата боргу, позика тощо) відчуження фізичного носія зі шкідливим програмним засобом іншій особі. Типовим прикладом збуту шкідливих програм є продаж дисків із записаними на них шкідливими програмами.

Збут шкідливих програмних або технічних засобів відрізняється від розповсюдження тим, що він пов'язаний з відчуженням предмета. Так, якщо при розповсюдженні предмет залишається в особи (шкідливе програмне забезпечення продовжує знаходитися на мережевому ресурсі, з якого розповсюджується, повертається шкідливий технічний засіб, що передавався для використання), то в результаті збуту він відчужується, тобто не залишається в особи, яка його збуває [15].

Розповсюдження та збут шкідливих програмних чи технічних засобів можуть вчинятися як особою, що створила шкідливі засоби, так і іншою, яка не брала участі в їх утворенні. Як розповсюдження, так і збут є закінченими складами злочину з моменту передачі шкідливих програмних або технічних засобів, незалежно від того, чи зміг отримувач ними розпорядитися чи ні.

У разі збуту таких засобів злочин є закінченим з моменту передачі іншій особі хоча б однієї програми, яка є шкідливим програмним засобом, чи шкідливого технічного засобу.

Диспозицією частини першої ст. 361-1 КК України передбачено кримінальну відповідальність за *створення шкідливих програмних чи технічних засобів з* метою їх використання, але не криміналізовано використання, як таке, що є нелогічним, оскільки безпосереднє використання, вочевидь, має більшу суспільну небезпечність, ніж створення з метою використання, тому що при використанні шкідливої програми настає шкідливий наслідок або створюється небезпека його настання.

ОСОБА_1 у березні 2012 р. незаконно збув шкідливий програмний засіб "KGB Keylogger 4.2", призначений для несанкціонованого втручання в роботу електронно-обчислювальних машин, оскільки в лютому 2012 р. ОСОБА_1, маючи знання в сфері користування мережею Інтернет, перебуваючи в невстановленому в ході досудового розслідування місці, з метою подальшого незаконного збуту, скачав на власний флеш-накопичувач з невстановленого в ході досудового розслідування Інтернет-сайту шкідливий програмний засіб "KGB Keylogger 4.2", основним функціональним призначенням якого є несанкціоноване та приховане копіювання інформації, яка обробляється на комп'ютері, з послідуючим її відправленням на конкретну електронну скриньку. 16 березня 2012 р. ОСОБА_1, реалізовуючи свій злочинний умисел, перебуваючи у м. Умань на вулиці Радянській, приблизно о 16 годині, незаконно збула шкідливий програмний засіб "KGB Keylogger 4.2" ОСОБА_3. При цьому, ОСОБА_1 особисто скопіювала зазначений програмний засіб із вказаного флеш-накопичувача на оптичний диск CD-R фірми "PATRON", серійний номер C0102R_MB1_80UG, продемонструвавши при цьому ОСОБА_3 на комп'ютері типу «ноутбук» hp Pavillion dv6 принцип роботи шкідливого програмного засобу "KGB Keylogger 4.2" [16].

Разом з тим під використанням шкідливих програмних засобів потрібно розуміти реалізацію будь-яких шкідливих функцій (наприклад, активування та початок функціонування вірусу відповідно до своїх властивостей) щодо здатності даного пристрою впливати на встановлений процес обробки інформації в ЕОМ, АС, комп'ютерних мережах чи мережах електрозв'язку.

Під використанням шкідливого технічного засобу варто розуміти реалізацію будь-яких шкідливих функцій щодо здатності даного пристрою впливати на встановлений процес обробки інформації в ЕОМ, АС, комп'ютерних мережах чи мережах електрозв'язку.

Використання шкідливого технічного засобу треба вважати закінченим з моменту надання доступу такого засобу до ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку іншим особам, або ж дій, після яких починається його автоматичне відтворення і поширення.

Так, гр-н Д., використовуючи технічний пристрій, що емулює (імітує) роботу єдиної таксофонної карти ВАТ «Укртелеком», здійснив 579 незаконних безоплатних телефонних дзвінків, чим спричинив ВАТ «Укртелеком» збитки на суму 12 525 грн. Злочин було кваліфіковано судом за ч. 1 ст. 361 КК України. А гр-н Л. за допомогою шкідливих програмних засобів вчинив втручання в роботу комп'ютерної мережі Інтернет-провайдера ТОВ «Вокар-Телеком», що призвело до блокування інформації і порушення встановленого порядку її маршрутизації. У результаті даного втручання гр-н Л. підробив «агр» таблицю на шлюзі сервера компанії ТОВ «Вокар-Телеком», у зв'язку з чим у нього з'явилася можливість сканувати і контролювати інформацію в локальній та Інтернет-мережі, керувати вилученими комп'ютерами, контролювати комп'ютери інших користувачів, здійснювати збір IP і MAC адрес комп'ютерів інших користувачів, що було кваліфіковано за сукупністю ст. 361, 361-1 КК України [17].

Способи приховування (маскування) кримінальних протиправних дій можна розділити на три групи:

1. Загальні способи: а) способи відволікання уваги від основної злочинної дії: «бухінг» (електронне блокування) – комп'ютерна система блокується одночасною атакою великої кількості зловмисних користувачів з різних місць; паралельне впровадження шкідливої програми, боротьба з наслідками дії якої відволікає увагу;

б) способи приховування процесів або комп'ютерної інформації: використання ремейлерів (Remailers) – комп'ютерів, що отримують електронне повідомлення і переправляють його за адресою, вказаною відправником. В процесі переадресації вся інформація про первинного відправника знищується, через що кінцевий одержувач не має можливості визначити істинного автора повідомлення. Сучасні можливості ремейлерів дозволяють відправляти повідомлення як від фіктивного відправника, так і анонімно; використання анонімізаторів

і спеціальних Proxy-серверів – служб, що дозволяють змінювати початкову IP-адресу комп'ютера користувача даної інформаційної послуги. При цьому призначена IP-адреса є динамічною (такою, що періодично змінюється) і приховує істинне місце знаходження комп'ютера зловмисника. Змінена IP-адреса може використовуватися як для реєстрації на Інтернет-серверах, так і для відправки електронних повідомлень; дотримання значних часових затримок між моментом впровадження програмної закладки та моментом вчинення злочинних дій, або настройка таких засобів на активацію тільки за певних умов (при запуску якої-небудь програми) або в певний момент, день тощо;

в) способи відключення засобів активного захисту (аудиту): використання штатних засобів настройки системи захисту ОС Windows; використання спеціальних програм (наприклад, auditpol.exe з комплекту W2RK).

2. Способи зачистки. Використовуються на заключному етапі злочину:

а) способи видалення змін у системі: використання програм віддаленого адміністрування комп'ютерної системи (наприклад, троянської програми NetBus); використання виявлених під час підготовки та вчинення злочину «потайних ходів» в системі для доступу до необхідних ресурсів;

б) способи руйнації комп'ютерної інформації: використання руйнівних програмних вірусів; використання програм форматування носіїв інформації.

3. Універсальні способи. Такі способи засновані на відновленні первинного стану інформаційного середовища вчинення злочину, що дозволяє практично повністю видалити його сліди, але, водночас, вимагає наявності дуже глибоких професіональних знань у зловмисників. Ці способи знаходять своє втілення в так званих «руткитах» (rootkit) – наборах, що включають всі необхідні програми, які застосовуються на будь-якому етапі вчинення злочину.

Таким чином, визначено способи вчинення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, саме: розповсюдження у мережі Інтернет порнографічних предметів і зображень, творів, що пропагують культ насильства та жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 161, 300, 301), яке може відбуватися й у формі спілкування в цій мережі; – розповсюдження у мережі Інтернет відомостей, що становлять державну або іншу таємницю, яка охороняється законом (ст. 114, 145, 159, 168, 232, 328, 361-2, 381, 387, 422) – дія, за допомогою якої зазначені об'єкти безпосередньо чи опосередковано пропонуються публіці, зокрема доводяться до відома невизначеного кола осіб таким чином, що особи мають можливість здійснити вільний доступ до цих об'єктів за власним вибором; розповсюдження у мережі Інтернет шкідливих програмних засобів (ст. 361-1) – це будь-яка дія, безпосередня чи опосередкована пропозиція, за допомогою якої ці об'єкти (зокрема, комп'ютерні віруси) поширюються чи починають автоматично відтворюватись у електронно-обчислювальних машинах, автоматизованих системах, комп'ютерні мережі або комп'ютерних мережах чи мережах електрозв'язку в результаті їх «закладання» в програмне забезпечення, а також створення умов, за яких інші особи можуть здійснити доступ до них або отримати у користування з будь-якого місця і в будь-який час за власним вибором, у тому числі мережею та іншим способом на платній чи безоплатній основі; – завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259); публічні заклики, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109), заклики до вчинення дій, що загрожують громадському порядку (ст. 295).

ЛІТЕРАТУРА

1. Пясковський В. В., Чорноус Ю. М., Самодін А. В. та ін. Криміналістика : *підручник* / за заг. ред. В. В. Пясковського. 2-ге вид., перероб. і допов. Харків : Право, 2020. 752 с.
2. Зуйков Г. Г. Развитие криминалистического учения о способе совершения преступления и проблема способа сокрытия преступления. Иркутск : Изд-во Ирк.ГУ, 1986. С. 47–59.
3. Хмыров А. А. Криминалистическая характеристика преступления и предмет доказывания. *Криминалистическая характеристика преступлений*. М., 1984. С. 53–54.
4. Способы совершения краж на водном транспорте как один из основных элементов криминалистической характеристики. URL: https://pravo.bobrodobro.ru/62685
5. Юхно О. О., Коршенко В. А., Гнусов Ю. В. та ін. Особливості розслідування злочинів, пов'язаних із незаконним обігом наркотичних засобів чи психотропних речовин із використанням сучасних телекомунікаційних та інших технологій : наук.-метод. рек. Х. : ХНУВС, 2019. 84 с.
6. Тарасенко О. С., Вакуленко О. Ф., Стрільців О. М. та ін. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів : *метод. рек.* Київ, 2016. 55 с.
7. Тарасенко О. С., Стрільців О. М., Волков О. О. та ін. Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням в мережі Інтернет забороненого контенту : *метод. рек.* за заг. ред. Ю. Ю. Орлова. К. : ГСУ, Нац. акад. внутр. справ, 2016. 78 с.
8. Стрільців О. М., Крижна В. В., Максименко О. В. та ін. Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту : *метод. рек.* / за заг. ред. Ю. Ю. Орлова. К. : Нац. акад. внутр. справ, 2014. 80 с.
9. Тарасенко О. С. Теорія та практика протидії кримінальним правопорушенням, пов'язаних з обігом протиправного контенту в мережі Інтернет : *монографія*. Одеса : Видавничий дім «Гельветика», 2021. 432 с.
10. Науково-практичний коментар Кримінального кодексу України / за заг. ред. О. М. Джужі, А. В. Савченка, В. В. Чернєя. 2-ге вид., перероб. і допов. Київ : Юрінком Інтер, 2018. 1104 с.
11. Тарасенко О. С. Інтернет контент як предмет вчинення злочину. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2015. № 2 (35). С. 361–365.
12. Вирок Дарницького районного суду м. Києва від 28 груд. 2015 р. Справа № 753/23764/15-к. *Єдиний державний реєстр судових рішень :* сайт. URL: http://reyestr.court.gov.ua/Review/54799070
13. Вирок Ірпінського міськрайонного суду Київської області від 30 серп. 2013 р. Справа № 373/2151/13-к. *Єдиний державний реєстр судових рішень* : сайт. URL: http://reyestr.court.gov.ua/Review/33209010
14. Вирок Кіровського районного суду м. Кіровограда від 15 лип. 2016 р. Справа № 404/3962/16-к. *Єдиний державний реєстр судових рішень :* сайт. URL: http://reyestr.court.gov.ua/ Review/59029350
15. Кримінальне право. URL: https://pidru4niki.com/1280031560071/pravo/nezakonni_diyi_shkidlivimi_programnimi_abo_tehnichnimi_zasobami
16. Вирок Солом'янського районного суду м. Києва від 28 листоп. 2014 р. Справа № 1-кп/760/715/14. *Єдиний державний реєстр судових рішень :* сайт. URL: http://reyestr.court.gov.ua/ Review/41620960
17. Вирок Білоцерківського міськрайонного суду Київської області від 5 жовт. 2010 р. Справа № 1-7/2010. *Єдиний державний реєстр судових рішень :* сайт. URL: http://reyestr.court.gov.ua/ Review/63156830