УДК 341.4
DOI.ORG/10.32703/2663-6352/2024-1-15-170-175
ORCID.ORG/0000-0001-8127-457X
Тацієнко Валерій Вікторович,
кандидат юридичних наук,
доцент кафедри економічної безпеки та фінансових розслідувань Національної академії внутрішніх справ, доцент

НОВІТНІ СПОСОБИ І ТЕХНОЛОГІЇ ВЧИНЕННЯ ТРАНСНАЦІОНАЛЬНИХ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ У СФЕРІ ЕКОНОМІКИ (ЗГІДНО З ДОСЛІДЖЕННЯМИ ЗАРУБІЖНИХ ВЧЕНИХ)

Анотація. *Статтю присвячено дослідженню новітніх способів і технологій вчинення транснаціональних комп'ютерних злочинів у сфері економіки. Вивчення цих способів і технологій є необхідним для вдосконалення національного та міжнародного законодавства щодо запобігання транснаціональній комп'ютерній злочинності. У статті розкриваються головні характеристики транснаціональних комп'ютерних злочинів. Підкреслюється, що такі злочини завжди вчиняються зі злочинним умислом, носять транснаціональний характер та є неможливими без застосування мережі Інтернет – або ж їхнє здійснення в таких масштабах без застосування мережі Інтернет значно ускладнюється. В статті докладно розглядаються два способи вчинення транснаціональних комп'ютерних злочинів – за допомогою застосування вірусів та за допомогою застосування хробаків (worms). Даються відмінності між цими двома видами шкідливих комп'ютерних програм. Розповідається, як за допомогою цих програм здійснюються масовані DDoS-атаки на сервери банків, крупних компаній тощо.*

Окремо розглядається створення і функціонування ботнетів, як окремий вид злочину, підкреслюється, що в сучасному світі створення ботнетів є окремим, дуже прибутковим злочинним бізнесом, який становить неабияку небезпеку для міжнародної спільноти.

Ключові слова: транснаціональна економічна злочинність, транснаціональна злочинність, кіберзлочини, комп'ютерні злочини, транснаціональна комп'ютерна злочинність.

Annotation. *The article is devoted to the scientific research of the latest methods and technologies of committing economical transnational computer crimes in the. The researching of these methods and technologies is necessary for the improvement of national and international law in the sphere of prevention of transnational cybercrime. The article reveals the main characteristics of transnational computer crimes. It is emphasized that such crimes are always committed with criminal intent, are transnational in nature and are impossible without the use of the Internet - or their execution on such a scale without the use of the Internet is significantly more difficult. The article examines in detail two ways of committing transnational cybercrimes - using viruses and using worms. The differences between these two types of malicious computer programs are given. It tells how these programs are used to carry out massive DDoS attacks on the servers of banks, large companies, etc. The creation and functioning of botnets is considered separately as a separate type of crime. It is emphasized that in today's world, the creation of botnets is a separate, very profitable criminal business, which poses a considerable danger to the international community.*

Keywords: transnational economic crime, transnational crime, cybercrime, computer crime, transnational computer crime.

Актуальність теми дослідження. В сучасному світі кібертехнології постійно вдосконалюються і змінюються. Транснаціональна злочинність з метою наживи користується

найновішими способами і технологіями вчинення злочинів, тож недивно, що комп'ютерні технології стали засобами скоєння злочинів. Сучасна західна наука знаходиться на передовій боротьби з найновішими видами кіберзлочинів, в той час як в Україні науковці, на жаль, продовжують писати в статтях про способи і методи здійснення кіберзлочинів, які вже є застарілими (наприклад, перебирання телефонних номерів з метою отримання доступу до стаціонарного комп'ютеру). Задля вдосконалення вітчизняного законодавства щодо боротьби з транснаціональними економічними кіберзлочинами потрібно вивчати міжнародний досвід і адаптувати його під вітчизняні потреби.

Ступінь дослідженості. Способи і технології вчинення транснаціональних комп'ютерних злочинів у сфері економіки вивчали такі експерти, як Александра Перлофф-Джилс, Сем Себін, Ліїс Віхул, Крістіан Чоссек, Катаріна Жіолковські, Гевін Вільде, Емма Ланді, Вікторія Вулластон та ін. Проте у зв'язку зі стрімким розвитком технологій і відповідних міжнародних зв'язків, якими користуються міжнародні економічні злочинці, ці дослідження дуже часто стають застарілими і потребують нових поглядів.

Метою статті є вивчення та аналіз проблем, пов'язаних із способами та технологіями вчинення транснаціональних комп'ютерних злочинів у сфері економіки.

Виклад основного матеріалу. Сучасна кіберзлочинність розвивається стрімкими темпами. Як зауважує Рада національної безпеки США, деякі оцінки вказують на те, що онлайн-шахрайство, вчинене центральноєвропейськими кіберзлочинними мережами, завдає збитків громадянам або організаціям США на суму приблизно 1 мільярд доларів США за один рік. За даними Секретної служби США, яка займається розслідуванням кіберзлочинів через свою 31 оперативну групу з боротьби з електронними злочинами, фінансові злочини, яким сприяють анонімні кримінальні онлайн-форуми, призводять до збитків фінансовій інфраструктурі США на мільярди доларів [5].

З точки зору доходу, 2023 рік стане рекордним для програм-вимагачів, коли хакерам буде виплачено понад мільярд доларів [3]. Крім цього, Федеральне бюро розслідувань США (ФБР) повідомляє про рекордні 12,5 мільярдів доларів, втрачених протягом 2023 року через кіберзлочинність у цілому [4]. Оскільки кількість постраждалих користувачів і організацій, суми виплат, критично важливих послуг і вкрадених конфіденційних даних продовжує зростати, провідні країни в останні роки стали розглядати транснаціональну кіберзлочинність як серйозну проблему національної безпеки [7].

Транснаціональні кіберзлочини діють зсередини: вони використовують мову коду для проникнення в системи, переривання обслуговування та компрометації даних.

Наразі транснаціональні кіберзлочини можна розділити на два різновиди: такі, що мають відповідні аналоги в матеріальному світі (наприклад, торгівля наркотиками, розповсюдження дитячої порнографії тощо), й такі, що існують виключно в віртуальній реальності. Ми зосередимося на останніх, оскільки вони наразі є дуже загрозливими як для держав і великих транснаціональних корпорацій, так і для звичайних користувачів мережі Інтернет.

На думку Александри Перлофф-Джилс, транснаціональні кіберзлочини мають три визначальні риси. По-перше, це навмисні злочини: вони вимагають певної умисної дії, щодо якої можна розумно передбачити, що її результат обов'язково завдасть шкоди. Навмисність є кваліфікуючою ознакою: можуть виникнути обставини, за яких необережне невжиття розумних заходів кібербезпеки може призвести до відповідальності, але комп'ютерний технік, який ненавмисно тимчасово порушує роботу мережі своєї компанії, не вчиняє транснаціонального кіберзлочину.

По-друге, транснаціональні кіберзлочини є квінтесенцією кіберзлочинів: вони використовують переваги структурних характеристик Інтернету. Вчена не вважає транснаціональними злочини, вчинені одним злочинцем проти однієї жертви лише за допомогою використання цифрових інструментів (наприклад, крадій особистих даних, який

зламує комп'ютер людини, щоб викрасти дані кредитної картки, або корпорація, яка бере участь у промисловому кібершпигунстві проти конкурента). На думку вченої, не є кіберзлочинами випадки, в яких всі ці злочини можуть існувати в кінетичному світі: злодій, який вкраде кредитну картку нічого не підозрюючої жертви, корпоративний шпигун, який пробирається, щоб отримати комерційну таємницю тощо. Так само, на думку вченої, такі злочини, як відмивання грошей і дитяча порнографія, можуть використовувати Інтернет, але вони також можуть існувати без Інтернету; у них нічого не залежить від мережевої архітектури. Транснаціональні кіберзлочини, навпаки, характерні виключно для кіберпростору: вони використовують децентралізовану, мережеву природу Інтернету, щоб завдати шкоди, яка не має еквіваленту в кінетичному світі [2, с.195-196].

Ми, однак, можемо погодитися з цим твердженням лише частково. Так, подібні злочини можуть існувати без Інтернету, проте їхні масштаби неспівставні з подібними злочинами, що відбуваються за допомогою мережі Інтернет. Перш за все, це стосується торгівлі порнографічними матеріалами, особливо дитячою порнографією. Сайт, який знаходиться в одній країні, може приймати відео з іншої країни і продавати його користувачам в третій країні. Відтак, дитяча порнографія розповсюджується такими темпами і в такій кількості, в якій ніколи не могла б розповсюджуватися на матеріальних носіях (відеокасетах, кіноплівках тощо), які потребують фізичного перевезення з однієї країни в іншу. Так само, торговці особистими даними можуть зламати оцифровані державні архіви даних іншої країни та передати ці відомості покупцям в третій країні. Специфічність, яка, на нашу думку, дозволяє віднести такі злочини до кіберзлочинів, полягає саме в активному використанні комп'ютерної мережі Інтернет задля здійснення злочинів, які інакше було б значно складніше здійснити.

По-третє, ці кіберзлочини є саме транснаціональними. Подібно до інших транснаціональних правопорушень, таких як екологічні злочини чи незаконний обіг наркотиків і зброї, транснаціональні кіберзлочини від початку/задуму, безпосередньо вчинення та/або настання прямих чи непрямих наслідків здійснюються більш ніж в одній державі. Вони можуть здійснюватися урядом або недержавними суб'єктами та впливати на окремих осіб, державні установи, корпорації, неурядові організації чи інші групи. Однак найважливіше те, що вони створюють виклики, які виходять за рамки кордонів і які з низки причин не можуть бути вирішені жодною окремою нацією [2, с.195-196].

Атаки можуть бути здійснені з будь-якого місця, де є доступ до Інтернету; зловмисники можуть приховати своє місцезнаходження за допомогою анонімних служб; а Інтернет зменшує трансакційні витрати транскордонної співпраці в плануванні та виконанні атак. Тож кіберзлочинці часто діють із третіх країн, де судове переслідування чи екстрадиція малоймовірні [7]. Крім того, Інтернет-трафік, призначений для проходження найшвидшим маршрутом, не завжди може проходити найбільш географічно прямим маршрутом: один фрагмент шкідливого коду може проходити через кілька країн. Ба більше: завдяки пакетній системі, за якою різні пакети можуть проходити різними маршрутами, потенціал інформації для проходження різних юрисдикцій збільшується в рази. Структура мережі Інтернет ускладнює для користувачів розуміння територіальної юрисдикції сторінки, якою вони потенційно користуються.

Нарешті, транснаціональні кіберзлочини часто мають широке охоплення, тож вплив кібератаки можна відчути далеко від початкової точки запуску або першої цілі. Конфігурація кіберпростору дозволяє програмам, якими користуються злочинці виникати, пересуватися кіберпростором і впливати на свої цілі способами, які є саме транснаціональними [2, с.196-197].

Інфекційне шкідливе програмне забезпечення та відмова в обслуговуванні є двома типовими прикладами транснаціональних кіберзлочинів. Зловмисне (шкідливе) програмне забезпечення – це код, призначений для завдання шкоди даним, хостам або мережам.

Зловмисне програмне забезпечення зазвичай заражає комп'ютерну систему, коли користувач

отримує доступ до пошкодженого веб-сайту або завантажує вкладення електронної пошти. Дві найвідоміші форми шкідливих програм — віруси та хробаки (worms) — легко поширюються з одного комп'ютера на інший. Віруси вставляються у виконуваний файл або програму, залишаючись бездіяльними, доки користувач не запустить заражену програму; потім вони передаються, коли програму передають на інший комп'ютер електронною поштою, компакт-диском, USB-накопичувачем чи іншою системою обміну файлами. Хробаки, навпаки, є автономним програмним забезпеченням: вони можуть самостійно відтворюватися всередині головного комп'ютера та переміщатися без сторонньої допомоги до інших комп'ютерних систем, під'єднаних мережею чи Інтернетом. Таким чином, обидві форми зловмисного програмного забезпечення використовують особливості кіберпространства, взаємодію користувачів/апаратури чи підключення до Інтернету, для поширення загроз потенційно невідомим жертвам [2, с.197].

Дедалі поширенішим варіантом зловмисного програмного забезпечення є програмне забезпечення-вимагач — комп'ютерне шкідливе програмне забезпечення, яке таємно поширюється та блокує комп'ютерні дані жертв, блокуючи їхні екрани («програмне забезпечення-вимагач – локер») або шифруючи їхні файли («крипто-вимагач»). Потрапивши в систему, крипто-вимагач створює зашифровані копії файлів, які можна відкрити лише за допомогою ключа розшифровки, видаляє оригінальні файли та залишає інструкції з вимогою викупу за доступ до ключа. Згідно з деякими оцінками, майже сорок відсотків компаній у всьому світі стали жертвами атак програм-вимагачів [8].

Програми-вимагачі можуть інфікувати пристрої-жертви (такі як комп'ютери, телефони чи сервери), які знаходяться поза межами держави, використовуючи цілу мережу пристроїв (таких як комп'ютери, сервери чи маршрутизатори) або веб-сайти, розташовані та розміщені в кількох різних країнах [6]. Часто ані жертви, ані пристрої-порушники не можуть бути повністю каталогізовані чи ідентифіковані. Жертви часто не знають, що їхні пристрої були заражені або використані для незаконних цілей. Кіберзлочинці часто орендують пристрої у сторонніх постачальників і використовують інструменти анонімізації, щоб приховати свій географічний слід [7].

Другим поширеним транснаціональним кіберзлочином є так звана «відмова в обслуговуванні» (denial-of-service, або DoS). Під час DoS-атаки зловмисник запускає шквал фальшивих запитів з одного джерела, переповнюючи цільову комп'ютерну систему, сервер або мережу. На відміну від шкідливих програм, які змінюють функціональність цільової системи, DoS-атаки тимчасово блокують доступ до цільової системи. Зловмисне програмне забезпечення та DoS-атаку можна об'єднати для створення розподіленої відмови в обслуговуванні (DDoS). Зловмисники під час скоєння DDoS-атак використовують зловмисне програмне забезпечення для викрадення даних та подальшого використання у своїх цілях численних комп'ютерів, які називаються «зомбі», що переповнюють цільові мережі трафіком. Фальшиві запити, надіслані мережею зомбі-комп'ютерів або пристроїв, відомих як «ботнет», можуть вимкнути цільові системи на кілька годин або навіть днів. Використання величезної кількості зомбі-комп'ютерів або «багаторівневих» ботнетів дозволяє хакерам здійснювати атаки через багато різних, географічно рознесених комп'ютерних серверів, а не з єдиної командної точки. У багатьох випадках зловмисник може дистанційно керувати зомбі-пристроями, справжні володільці яких навіть не підозрюють, що його або її пристрій зламали.

Вінт Серф, один із батьків Інтернету, одного разу підрахував, що до однієї чверті всіх мережевих комп'ютерів можуть бути частиною ботнетів [2, с.198].

Зокрема, у травні 2017 року, атака програми-вимагача WannaCry заразила приблизно 230 000 комп'ютерів у понад 150 країнах. Ця програма заразила телекомунікаційні та комунальні компанії, банки, університети, державні установи, електронні платіжні автомати на АЗС і залізничних компаніях тощо [8].

У березні 2024 року прокуратура Німеччини та співробітники федеральної кримінальної поліції вилучили та закрили нелегальний ринок даркнету, доступний через мережу Tor під назвою Nemesis Market. Німецькі та литовські правоохоронці співпрацювали за допомогою офіційних осіб США, щоб захопити сервери хостингу. Маючи 150 000 користувачів і понад 1100 продавців по всьому світу на момент конфіскації, Nemesis Market з моменту свого створення в 2021році, серед іншого, сприяв продажу наркотиків, викрадених даних і послуг кіберзлочинності для програм-вимагачів, фішингу та DDoS-атак [1].

Окремо слід розглянути так звані «ботнети», створення яких саме по собі вважається транснаціональним кримінальним злочином.

«Ботнет» — термін, що походить від слів «робот» і «мережа», — це мережа взаємопов'язаних дистанційно керованих комп'ютерів, зазвичай заражених шкідливим програмним забезпеченням, яке перетворює заражені системи на так званих «ботів», «роботів» або «зомбі».

Боти дистанційно керуються одним або декількома зловмисниками, яких зазвичай називають «ботоводи» або «ботмайстри». Маючи повний контроль над ботами, ботмайстер може виконувати будь-яку дію, яку може виконати законний власник комп'ютера.

Бот-мережі здебільшого виконують такі команди:

1. Знаходження та зараження інших інформаційних систем шкідливим програмним забезпеченням. Ця функція, зокрема, дозволяє ботмайстрам підтримувати та нарощувати запас нових ботів, щоб вони могли виконувати, серед іншого, наведені нижче функції.

2. Проведення DDoS-атак.

3. Переміщення IP-адрес під одним або декількома доменними іменами з метою збільшення довговічності шахрайських веб-сайтів, які використовуються, наприклад, для розміщення фішингових та/або шкідливих сайтів або серверів керування та контролю (C&C) ботнетів.

4. Надсилання спаму, який, у свою чергу, може поширювати ще більше шкідливого програмного забезпечення.

5. Викрадення конфіденційної інформації зі зламаних комп'ютерів, які належать до ботнету.

6. Розміщення самого шкідливого фішингового сайту, часто на комп'ютерах, що належать до ботнету, щоб забезпечити резервування.

У більшості випадків цілі зловмисників, як правило, зосереджені на фінансовій вигоді, тож цей злочин цілком можна вважати таким, що належить до транснаціональних економічних злочинів. За різними оцінками, ботнети приносять дохід від 10 000 до 10 000 000 доларів США на місяць від однієї мережі ботнет [6]. Так, зокрема, у 2023 році Міністерство юстиції США оголосило про успішну багатонаціональну кібероперацію зі зриву ботнету Qakbot, який заразив понад 700 000 комп'ютерів у всьому світі та використовувався для викрадення понад 8 мільйонів доларів незаконного прибутку [7].

Перегляд цих цифр допомагає зрозуміти, чому зловмисне програмне забезпечення зараз є глобальною кримінальною індустрією, а також дає вказівку на те, скільки ресурсів можна інвестувати в розробку нового, складнішого зловмисного програмного забезпечення, яке більш стійке до виявлення чи протистояння йому. У результаті виник цілий підпільний ботнет-бізнес, у якому ботнети використовуються як послуга, яку можна купити, налаштувати або взяти в оренду [6].

Так, у 2021 році Трансатлантична коаліція правоохоронців оголосила про успішну операцію Сполучених Штатів, Канади, Франції, Німеччини, Нідерландів і Великої Британії з ліквідації ботнету Emotet, який був націлений на банківський сектор, електронну комерцію, охорону здоров'я та державний сектор шляхом зараження пристрої через фішинг електронною поштою. Європол назвав Emotet «найнебезпечнішим шкідливим програмним забезпеченням у світі» та «одним із найзначніших ботнетів останнього десятиліття». Як тільки Emotet заражав

пристрій, його можна було продавати як опору для інших кіберзлочинців, щоб установлювати інші форми шкідливого програмного забезпечення або викрадати фінансові облікові дані [7].

Висновки. В сучасному світі кіберзлочинці вдало поєднують більш «традиційні» злочини (шахрайство за допомогою мережі Інтернет, розповсюдження порнографії, наркобізнес тощо) із злочинами, які можливі виключно в кіберпросторі (розповсюдження шкідливих програм, створення ботнетів тощо). Величезні прибутки, отримувані злочинцями, дозволяють припустити, що комп'ютерні злочини і в подальшому становитимуть значну загрозу суспільству.

Сучасна комп'ютерна злочинність є переважно транснаціональною, оскільки завдяки мережі Інтернет злочинці легко можуть скоювати злочини поза зоною юрисдикції країни, в якій вони мешкають, тож дуже часто переселяються в країни, які не мають відповідних угод про видачу кіберзлочинців. Кіберзлочини, скоювані в мережі Інтернет, більшою частиною здійснюються за допомогою шкідливих програм, і DDoS-атак, що підтримуються мережами ботнетів. Злочинці створюють ці мережі, і в подальшому здійснюють їхню купівлю/продаж або здачу/взяття в оренду.

Перспективи подальших досліджень. Подальші дослідження, на нашу думку, мають бути зосереджені на докладному вивченні способів та методик, а також технологій, за допомогою яких злочинці здійснюють транснаціональні економічні злочини в кіберпросторі, а також на створенні, по-перше, глобального міжнародного законодавства з протидії таким злочинам, а по-друге, на практичних засобах викриття цих злочинів та запобігання їм.

ЛІТЕРАТУРА

1. Illegal Darknet Marketplace 'Nemesis Market' Shut Down. Federal Criminal Police Office of Germany, 2024, March 21st. URL.: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240321_PM_Nemesis_Market.htm
2. Perloff-Giles, Alexandra. Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. The Yale Journal of International Law, 2018. Vol.43. P.p. 191-227.
3. Sabin, Sam. Ransomware Gangs Collected Record $1.1 Billion from Attacks in 2023. *Axios*, 2024, February 10th. URL.: https://www.axios.com/2024/02/09/ransomware-earnings-2023-chart
4. Toulas, Bill. FBI: U.S. Lost Record $12.5 Billion to Online Crime in 2023. Bleeping Computer, 2024, March 7th. URL.: https://www.bleepingcomputer.com/news/security/fbi-us-lost-record-125-billion-to-online-crime-in-2023
5. Transnational Organized Crime: A Growing Threat to National and International Security. National Security Council. URL.: https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat
6. Vihul, Liis; Czosseck, Christian; Dr. Ziolkowski, Katharina; Aasmann, Lauri; Ivanov, Ivo A.; Dr. Brüggemann, Sebastian. Legal Implications of Countering Botnets: Joint report from the NATO Cooperative Cyber Defence Centre of Excellence and the European Network and Information Security Agency (ENISA). 2012, March. URL.: https://bpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2018/02/191_Transnational-Cyber-Offenses-2i9mpg2.pdf
7. Wilde, Gavin; Landi, Emma. Exploring Law Enforcement Hacking as a Tool Against Transnational Cyber Crime. Carnegie Endowment for International Peace, 2024, April 23rd. URL.: https://carnegieendowment.org/2024/04/23/exploring-law-enforcement-hacking-as-tool-against-transnational-cyber-crime-pub-92263
8. Woollaston, Victoria. WannaCry Ransomware: What It Is and How To Protect Yourself. WIRED, 2017, May 22nd. URL.: http://www.wired.co.uk/article/wannacry-ransomware-virus-patch