УДК 004.738.5:343.9.02:341.31
DOI: 10.31733/15-03-2024/2/359-360

Єлизавета КИСЕЛЬОВА
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Володимир ВАРАВА
доцент кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ВОЄННОГО СТАНУ

Під час воєнного стану кібератаки в Україні стали набагато частіше, злочинці використовують інфопростір для завдання шкоди обороноздатності України, та й з боку тих, хто вирішив скористатися ситуацією, коли правоохоронні органи перевантажені. Кіберзлочинність – сукупність злочинів, скоєних у «кіберпросторі» за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору. Ще до початку війни, після кібератак 14 січня на сайти державних органів влади, відчувалася необхідність запровадження невідкладних змін в українському законодавстві для узаконення процедури Bug Bounty [1].

Більшість існуючих злочинів у глобальних комп'ютерних мережах мають такі особливості:

1. Підвищена скритність скоєння злочину.

2. Транскордонний характер мережевих злочинів, при якому злочинець, тобто, об'єкт злочинного посягання та потерпілого може перебувати на територіях різних держав.

3. Особлива підготовленість злочинців, інтелектуальний характер злочинної діяльності.

4. Можливість скоєння злочину в автоматизованому режимі у кількох місцях одночасно [2, с.323].

Сьогодні кіберзлочинність містить у собі великий діапазон протиправних дій – від невирішеного вторгнення до комп'ютерних мереж, крадіжок індивідуальних даних, фінансового шпигунства та відмивання готівки. Останніми роками інтернет-ресурси використовуються у всіх циклах торгівлі людьми та забороненими предметами, а також у подальшій легалізації злочинних доходів.

Кіберзлочинці використовують свій арсенал інформаційної зброї, що являє собою сукупність коштів, призначених для порушення (копіювання, спотворення чи знищення) інформаційних ресурсів на стадії їх створення, обробки, розповсюдження та зберігання.

До основних видів інформаційної зброї відносять такі:

1. Бекдор – даний інструмент передбачає прихований метод системи, що дозволяє отримати доступ до захищеної області.

2. Комп'ютерні віруси – спеціальні програми, які впроваджуються у програмне забезпечення комп'ютерів, знищують, спотворюють чи дезорганізують його функціонування. Вони здатні передаватися лініями зв'язку, мереж передачі даних, виводити з ладу системи керування тощо. Крім того, «віруси» здатні самостійно розмножуватися.

3. Програмне шкідливе забезпечення – програми або утиліти, які після встановлення виконують незаявлені функції в фоновий режим.

4. Нейтралізатори тестових програм, які забезпечують збереження природних та штучних недоліків програмного забезпечення [3].

Поширеність кіберзлочинів у всьому світі зумовлює пошук нових підходів щодо забезпечення інформаційної безпеки та розробки заходів щодо протидії кіберзлочинності. Звісно, ніхто не може забезпечити стовідсоткову захищеність від кібератак. З урахуванням транснаціонального характеру злочинів, що розглядаються, а саме тісна співпраця країн (держав) дозволить своєчасно запобігти таким протиправним діянням, а відповідно, заподіяння майнової шкоди фізичним або юридичним особам у результаті кібератак.

У кримінальному законодавстві держави криміналізація кіберзлочинності яка включає діяння, безпосередньо посягає на інформаційну безпеку (консолідовані з врахуванням тотожності родового об'єкта зазіхання), але й охоплює інші суспільно небезпечні посягання, пов'язані з використанням інформаційно-телекомунікаційних мереж (у яких інформаційна сфера є факультативним об'єктом злочину) [4].

Мета нового Закону 2149-IX

1. Посилення спроможностей та оптимізація національної системи кібербезпеки для протидії кіберзагрозам.

2. Впровадження дієвих кримінально-правових механізмів протидії кіберзлочинності.

3. Забезпечення надійності та безпеки використання цифрових послуг [5].

Таким чином, висока соціальна небезпека кіберзлочинності пояснюється її транснаціональним та організованим характером, тому жодна держава сьогодні не здатна активно протидіяти цій загрозі самостійно, у зв'язку з чим нагальною є потреба активізації міжнародного співробітництва. Ефективна боротьба з кіберзлочинністю потребує колективних зусиль, бо під час воєнного стану боротьба з кіберзлочинністю стала складніша. Для цього необхідно вести постійну роз'яснювальну роботу серед населення. Потрібно тривалий і що важливо, наполегливий виховний процес для того, щоб люди усвідомлювали необхідність запобіжних заходів. Підвищення ефективності боротьби з кіберзлочинністю під час війни та посилення відповідальності за відповідні злочини є давно назрілим кроком. Новий закон розширює межі діяльності правоохоронних органів щодо розслідування кіберзлочинів, передбачених статтями 361, 361-1 ККУ. Посилення санкцій та додаткова криміналізація окремих діянь здатні частково стримати потенційних злочинців від вчинення нових злочинів.

1. Інтернет-шахрайства в умовах воєнного стану: як не потрапити на гачок до аферистів. URL : https://legalaid.gov.ua/publikatsiyi/internet-shahrajstva-v-umovah-voyennogo-stanu-yak-ne-potrapytyna-gachok-do-aferystiv (дата звернення 16.10.2023)

2. Протидія кримінальним правопорушенням в умовах воєнного стану : збірник матеріалів Всеукраїнської науково-практичної конференції в авторській редакції, (м. Кропивницький, 27 жовтня 2022 року). Кропивницький, 2022. 367 с

3. Закон України Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам. URL : https://ips.ligazakon.net/document/view/T222137?an=41 (дата звернення 16.10.2023)

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. N 2163-VIII. База даних «Законодавство України». ВР України. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.10.2023).

5. Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon. Сайт Державної служби спеціального зв'язку та захисту інформації України. URL : https://cip.gov.ua/ua/news/kiberatakana-derzhavni-organizaciyi-ukrayini-z-vikoristannyam-shkidlivoyi-programi-cobalt-strike-beacon (дата звернення: 15.10.2023)