УДК 343.98
DOI: 10.31733/15-03-2024/2/89-90

Данило КРИВОРОТ
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

ДІЯЛЬНІСТЬ СПЕЦІАЛЬНИХ ОПЕРАТИВНИХ ГРУП У СПРАВАХ КІБЕРЗЛОЧИНІВ ТА ІНШИХ КІБЕРЗАГРОЗ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖ І ІНФОРМАЦІЇ

З появою мережі Інтернет та настанням епохи великих даних залежність людей від Інтернету постійно зростає. Останній став обов'язковим інструментом для життя та роботи людей, будучи необхідною річчю у суспільстві; галузей, які створює Інтернет, стає дедалі більше, тим самим надаючи нові простори для розвитку кіберзлочинності. В останні роки кіберзлочинність має тенденцію до постійного зростання, тому проблема пошуку методів та прийомів ефективної боротьби з кіберзлочинністю залишається однією з найактуальніших.

Під кіберзлочинністю розуміють «застосування комп'ютерних технологій правопорушниками, використання Інтернету для атак і псування комп'ютерних систем або носіїв інформації». Також цей термін «використовується для шахрайств, крадіжки особистої інформації у користувачів Інтернету. До них належать злочини, скоєні правопорушниками, які застосовують програмування комп'ютера, шифрування, методи декодування або інструменти в мережі, також включають злочини, скоєні правопорушниками, які використовують інструкції програмного забезпечення. Одним словом, кіберзлочинність – це злочин стосовно мережі та її використання, її суть полягає у руйнуванні мережі та її інформаційної безпеки та порядку» [1].

Варіацій скоєних злочинів безліч. Від крадіжки коштів із банківських карт пенсіонерів до створення шкідливих програм, що становлять загрозу цифровій безпеці цілих держав. Більшість діянь пов'язане, зрозуміло, з банківськими рахунками, але водночас дедалі частішають випадки злому акаунтів порталу державних послуг. У деяких випадках фактично відбувається крадіжка «цифрової» особистості людини.

Варто сказати, що одною з ключових переваг кіберзлочинності є анонімність. Для того, щоб приховати свою особистість, зловмисники можуть використовувати комп'ютери та Інтернет-мережі вільного доступу. Також необхідно враховувати, що є безліч програм, які дозволяють замаскувати IP-адресу комп'ютера [2].

На даний момент існують кілька міжнародних організацій з протидії кіберзлочинам:

1) Організація Об'єднаних Націй (ООН) з ІКТ – Міжнародна спілка електрозв'язку (МСЕ);

2) Міжнародне багатостороннє партнерство проти кіберзагроз (IMPACT). Є виконавчим органом МСЕ у сфері кібербезпеки. IMPACT – це перший у світі міждержавний союз урядів, найкращих експертів у галузі цифрових технологій та організацій боротьби з кіберзлочинністю. Велика заслуга IMPACT полягає у створенні засобів та ресурсів для протидії кібератакам. Всі держави-члени отримують доступ до накопичених знань;

3) Міжнародний альянс забезпечення кібербезпеки (ICSPA) – ще одне об'єднання урядів різних країн, правоохоронних органів та міжнародного бізнесу для відсічі кіберзлочинності.

Діяльність зазначених організацій по суті на даний момент зводиться до вирішення кількох першочергових завдань. Якщо узагальнити, можна представити їх так:

А) створення єдиних загальносвітових ознак кібердіянь, які необхідно криміналізувати;

Б) оформлення загальних понять та термінології;

В) консультація держав під час запровадження відповідних кримінальних норм у своє законодавство [3, с. 147].

В Україні також активно ведеться боротьба з кіберзлочинністю. Серед загальних суб'єктів реалізації інформаційної функції держави слід виокремити такі, як: Верховна Рада України, Президент України, Кабінет Міністрів України, Конституційний Суд України, міністерства, інші центральні і місцеві органи державної виконавчої влади, органи судової влади тощо.

Суб'єктами спеціальної компетенції реалізації інформаційної функції є: Національна рада України з питань телебачення і радіомовлення, Рада Національної безпеки і оборони України, Міністерство інфраструктури України, Служба безпеки України, Державна архівна служба України, Державна служба статистики, Державний комітет телебачення і радіомовлення України тощо [4].

Міністерство внутрішніх справ України також активно залучено до розкриття та розслідування кіберзлочинів. Підрозділи слідства та дізнання на всіх рівнях формують спеціальні підрозділи боротьби з кіберзлочинністю. Складність процесу формування зазначених підрозділів обумовлена мізерною матеріально-технічною базою, складністю специфіки розкриття кіберзлочинів. Окрім іншого, негативний вплив має недостатньо сформоване нормативне регулювання даної сфери.

Таким чином, кіберзлочинність є найважливішою проблемою для законодавця та суспільства загалом. Не можна недооцінювати її суспільну небезпеку. З такими темпами технологічного розвитку, а також переходу життя громадян та процесів держави у віртуальне середовище під загрозою виявляється дедалі більше суспільних відносин. Нові злочини виникають з неймовірною швидкістю: кібершахрайство, тероризм, кібершпигунство, неправомірний доступ до акаунтів у соціальних мережах, транслювання екстремістських ідей, поширення наркотиків та інших психоактивних речовин.

1. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навч.-метод. посібник. Одеса : Національний університет «Одеська юридична академія», 2020. 112 с.

2. Самойленко О. А. Діяльність правоохоронних органів у протидії кіберзлочинності : навч.-метод. посібник. Одеса, 2020. 133 с.

3. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія : Право.* 2021. Вип. 64. С. 386–391.

4. Золотоверха Д. О. Кіберполіція України як суб'єкт забезпечення інформаційної безпеки України. URL : https://elar.naiau.kiev.ua/server/api/core/bitstreams/02c25189-1b98-49b5-91cd-f8795697eb94/content.

УДК 343.982
DOI: 10.31733/15-03-2024/2/90-92

Вікторія КРИСЬКО
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Віталій ТЕЛІЙЧУК
професор кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник, доцент

ЩОДО ОРГАНІЗАЦІЇ І ТАКТИКИ ПРОВЕДЕННЯ ОПЕРАТИВНО-ТЕХНІЧНИХ ЗАХОДІВ

Важливість організації та тактики проведення оперативно-технічних заходів полягає в тому, що вони дозволяють ефективно боротися зі злочинністю та забезпечують безпеку громадян, крім того, сприяють протидії тероризму та іншим загрозам для національної