УДК: 342.52

ІНФОРМАЦІЙНО-ПРАВОВІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Клімова А.С., 2 курс
Науковий керівник: Нестеренко О.М., викл.
Таврійський державний агротехнологічний університет

Постановка проблеми. В наші дні використання інформаційних технологій не має меж. Віртуальний простір переймає від реального все підряд, у тому числі й злочинність у її нових формах і проявах. Практично кожен чув про кіберзлочинність і,можливо, навіть особисто з нею зіштовхнувся. Кіберзлочинність, включає в себе різні види злочинів, що здійснюються за допомогою комп'ютера і мережі Інтернет. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу і держави в цілому. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні. Дані обставини обумовлюють актуальність теми дослідження.

Аналіз останніх досліджень і публікацій. Проблемі поширення кіберзлочинності, вивченню способів протидії, а також боротьбі з кіберзлочинцями присвячені праці таких науковців як: В. Брижко, В. Бутузов, В. Пилипчук, К. Тітуніна, М. Швець, О. Юрченко та інші.

Метою написання статті є визначення загрози кіберзлочинів та боротьбі з ними. Дослідження інформаційно-правових аспектів протидії кіберзлочинності. Дослідження значення кіберполіції в умовах сучасності.

Виклад основного матеріалу. «Кіберзлочинність», «хакери», «комп'ютерний взлом», «крадіжка машинного часу» − ці терміни вже перестали бути екзотикою для юристів. Проблеми протидії злочинам у сфері використання комп'ютерної техніки активно обговорюється науковцями, досить швидко розвивається практика застосування відповідних норм законодавства про кримінальну відповідальність.

На сьогодні комп'ютерні злочини - це одна з найдинамічніших груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем − це далеко не повний перелік подібних злочинів.

Кіберзлочини – це суспільно-небезпечні діяння, які так чи інакше пов'язані з кіберпростором та комп'ютерною інформацією, що моделюється комп'ютерами. Такі злочини характеризуються наступними особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказу в суді подібних справ, транснаціональною складовою в основному з використанням інформаційної мережі Інтернет, високим збитком навіть від одиничного злочину.

На сьогодні в Україні діє низка законів та нормативних документів різних рівнів, що охоплюють питання кібербезпеки держави. Це, зокрема, Закони України «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України», Указ Президента України «Про Національний координаційний центр кібербезпеки» та інші нормативно-правові акти. Крім того, у вересні 2016 року Верховна Рада України прийняла у першому читанні Закон України «Про основні засади забезпечення кібербезпеки України».[2]

Стратегічними документами у цій сфері є Стратегія кібербезпеки України, Стратегія національної безпеки України, а також ратифікована Верховною Радою України «Конвенція про кіберзлочинність». Чинний Кримінальний кодекс України встановлює (відповідно до

розділу XVI) відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Система злочинів у сфері кіберзлочинності, запропонована національним законодавством України, охоплює кримінальні правопорушення у сфері: використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем); обігу інформації протиправного характеру із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; господарських відносин та приватної власності, яка включає в себе незаконні фінансові операції та заборонені види господарської діяльності, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж.[1]

Так, в чинному Кримінальному кодексі України є розділ XVI, який встановлює відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, до яких віднесено:

Стаття 361 Кримінального кодексу України передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

Стаття 361-[1] Кримінального кодексу України передбачає відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

Стаття 361-[2] Кримінального кодексу України передбачає відповідальність за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

Стаття 362 Кримінального кодексу України передбачає відповідальність за несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї

Стаття 363 Кримінального кодексу України передбачає відповідальність за порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється

Стаття 363-[1] Кримінального кодексу України передбачає відповідальність за перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку. [4]

Кіберполі́ція — структурний підрозділ Національної поліції України, що спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких, передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем.[5]

Основні завдання Кіберполіції:

1. Реалізація державної політики у сфері протидії кіберзлочинності.
2. Завчасне інформування населення про появу новітніх кіберзлочинів.
3. Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.
4. Реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів.
5. Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.

6. Участь у міжнародних операціях та співпраця в режимі реального часу. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.
7. Протидія кіберзлочинам: У сфері використання платіжних систем, у сфері електронної комерції та господарської діяльності, сфері інтелектуальної власності, у сфері інформаційної безпеки.[5]

Висновки. Розуміння інформаційно-правових проблем протидії кіберзлочинності, а також можливостей їх вирішення підвищить ефективність розслідування кіберзлочинів правоохоронними органами України.

Для цього існує необхідність: деталізації законодавства, яке б відображало положення Конвенції про кіберзлочинність, щодо отримання електронних доказів, обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу), специфічних умов проведення обшуку і арешту цифрових (електронних) доказів; закріплення механізмів сприяння правоохоронним органам України операторів, провайдерів щодо забезпечення цілісності та неспростовності електронних даних, обмеження доступу абонентів до інформаційного ресурсу (інформаційного сервісу), адреси мережі Інтернет, веб-сайту, веб-сторінки, через які розповсюджуються злочинний контент тощо; створення у межах державно-приватного партнерства загальнодержавної бази IPадрес для забезпечення негайного розкриття вчинених кіберзлочинів; удосконалення протоколу офіційної правової допомоги з урахуванням норм національного законодавства для ефективного розслідування кіберзлочинів щодо вилученої та збереженої інформації у електронному (цифровому) вигляді; використання правоохоронними органами України механізмів, передбачених Угодою між Україною та Європолом про оперативне та стратегічне співробітництво у напрямку оперативного (через глобальну захищену міжнародну мережу електронного зв'язку) отримання інформації про кіберзлочини і кіберзлочинців. Перспективним напрямком у зв’язку з означеними проблемами є регулярне підвищення кваліфікації слідчих та інших задіяних співробітників правоохоронних органів з метою вивчення актуальних питань тактики проведення слідчих дій для отримання електронних доказів при розслідуванні кіберзлочинів.

Список літератури.

1. Про основні засади забезпечення кібербезпеки України : Закон України. – Режим доступу : http://zakon3.rada.gov.ua
2. Марущак А.І. Пріоритети розвитку інформаційного права України // Інформація і право. – № 1(1)/2011. – С. 20-24.
3. Конвенція про кіберзлочинність від 23.11.01 р. // Офіційний вісник України. – 2007. – № 65. – Ст. 253.
4. Кримінальний процесуальний кодекс України від 13.04.12 р. // Офіційний вісник України. – 2012. – № 37. – Ст. 1370.
5. Про рішення Ради національної безпеки і оборони України від 29.12.16 р. “Про загрози кібербезпеки держави та невідкладні заходи щодо їх нейтралізації” : Указ Президента України від 13.02.17 р. № 32. – Режим доступу : http://zakon3.rada.gov.ua