Матвійчук М.П.
Національний університет «Одеська юридична академія»,
студентка судово-адміністративного факультету

КІБЕРЗЛОЧИНИ: ПОНЯТТЯ ТА ВИДИ

Кіберзлочинність – це сукупність злочинів, що вчиняються з використанням комп'ютерної системи, або комп'ютерної мережі, чи мережі електрозв'язку, у межах комп'ютерної системи або комп'ютерної мережі чи мережі електрозв'язку, чи проти комп'ютерної системи або комп'ютерної мережі чи мережі електрозв'язку (Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання. «Питання кримінального права, кримінології та кримінально-виконавчого права». – В.В. Пивоваров, С.Ю. Лисенко, 2016 р.)

В пункті 14 Доповіді Комітету II Десятого Конгресу Організації Об'єднаних Націй по попередженню злочинності і поводженню з правопорушниками, що відбувся в Відні 10-17 квітня 2000 року (далі – Десятий Конгрес ООН), зазначено, що існує дві категорії таких злочинів:

- Кіберзлочин у вузькому сенсі (комп'ютерний злочин): будь-яке протиправне діяння, вчинене за допомогою електронних операцій, метою якого є безпека комп'ютерних систем і оброблюваних ними даних.
- Кіберзлочин у широкому розумінні: (як злочин, пов'язаний з комп'ютерами): будь-яке протиправне діяння, вчинене за допомогою чи пов'язане з комп'ютерами, комп'ютерними системами або мережами, включаючи незаконне володіння і пропозицію або розповсюдження інформації за допомогою комп'ютерних систем або мереж (Волеводз А.Г. Противодействие компьютерным преступлениям: правове основы международного сотрудничества. – М.: ООО Издательство «Юрлитинформ», 2002. – 496 с.).

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 (Кримінальний кодекс України від 05.04.2001 № 2341-III, редакція від 18.04.2018. [Електронний ресурс]: – Режим доступу: http://zakon3.rada.gov.ua/laws/show/ru/2341-14).

Отже, визначення кіберзлочину у законодавстві України є важливим кроком, який спрямований на усунення розбіжностей щодо уявлення про таке явище та ефективну протидію йому, проте таке визначення суперечить окремим положенням кримінального законодавства, положенням міжнародних нормативно-правових актів а також тенденціям розвитку законодавства у сфері кримінальної юстиції. Це свідчить про необхідність подальших досліджень у цій сфері та вдосконалення законодавства.