ПРАВОВА ОСНОВА КІБЕРБЕЗПЕКИ УКРАЇНИ

Азаренко А.П.
Науковий керівник – канд. юрид. наук, доц. Турута О.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. філософії, тел. (057)702-1-465)
e-mail: artem.azarenko@nure.ua

In this article author opens the question of crimes in the sphere of informative technologies in Ukraine, he defines this kind of crime and gives its features. The legal basis in the sphere of informative technologies in Ukraine is analyzed.

Розвиток інформаційного суспільства призвів до появи інформаційних технологій, які стали невід'ємною частиною нашого життя. Вони дають не тільки можливість для розвитку здібностей, покращення знань та розширення кола інтересів, але й містять у собі реальні загрози. Одна з найсерйозніших загроз – виникнення нового виду злочинності – комп'ютерна злочинність. За наявності великого обсягу персональної та конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки.

Для України комп'ютерна злочинність є відносно новим видом злочинності. На сьогоднішній день в країні є ряд нормативно-правових актів, що описують проблеми забезпечення кібербезпеки держави. За даними Управління боротьби з кіберзлочинністю МВС України, найбільш поширеними видами кіберзлочинів є: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів) та несанкціоновані дії з інформацією, яка ними оброблюється.

Правову основу кібернетичної безпеки України становлять Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», та інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також видані на виконання законів інші нормативно-правові акти.

Загрози національній безпеці України в кібернетичному просторі призвели до створення Стратегії кібербезпеки України, що була введена в дію Указом Президента України від 15 березня 2016 року. Стратегія є важливим кроком на шляху розбудови системи кібербезпеки України та являє собою програму дій, за якою мають слідувати державні органи.

До стратегії було створено Розпорядження Кабінету Міністрів України від 24.06.2016 року «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України», в якій зазначені заходи, забезпечення яких покладається на органи виконавчої влади та окремі військові формування. Ця стратегія базується на положеннях Конвенції

про кіберзлочинність, яка ратифікована Законом України від 7 вересня 2005 року № 2824-IV.

Метою даної стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства, держави. Вона складається з загальних положень, основних загроз кібербезпеці, основних суб'єктів забезпечення кібербезпеки, пріоритетів та напрямів забезпечення кібербезпеки України та прикінцевих положень.

У законі України «Про основи національної безпеки України» та в «Доктрині інформаційної безпеки України» згадуються поняття «комп'ютерна злочинність» та «комп'ютерний тероризм», проте визначення цих термінів в законі немає. В законі «Про боротьбу з тероризмом» поняття «комп'ютерний тероризм» не висвітлюється зовсім, а те що до нього відноситься називається «технологічним тероризмом». Для покращення нормативно-правової бази у сфері кіберзлочинності Верховною Радою України було прийнято закон «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року. В цьому законі визначили терміни «кіберзлочинність» та «кібертероризм».

В Державному центрі кіберзахисту та протидії кіберзагрозам Держспецзв'язку є структурований підрозділ Computer response team of Ukraine (Cert-UA) – команда реагування на комп'ютерні надзвичайні події України. Основна мета Cert-UA – забезпечити захист інформаційних ресурсів та інформаційних та телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності.

Отже, кіберпростір на сьогоднішній день відіграє велику роль у забезпеченні інформаційної безпеки держави. Тому закони України повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Найбільш перспективними напрямами розвитку національної системи кібербезпеки є: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури, створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Не виключено, що саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній.