УДК 343.(043.2)

Лапаєнко В.С., студент,
Навчально-науковий Юридичний інститут,
Національний авіаційний університет, м. Київ
Науковий керівник: Малярчук Н.В., к.ю.н.

ТЕОРЕТИКО-ПРАВОВІ ПРОБЛЕМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

У зв'язку із поширенням інформаційних технологій відбувається ускладнення відносин щодо регулювання їх діяльності та протидії кіберзлочинності не тільки на технічному рівні, а й на правовому, оскільки чинна нормативно-правова база у сфері протидії кіберзлочинам не задовольняє потреби часу та лише частково охоплює ключові елементи протидії кіберзлочинності.

У Кримінальному кодексі України присвячено окремий розділ – XVI Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, та комп'ютерних мереж і мереж електрозв'язку. Але на нашу думку сама назва розділу не висвітлює всієї сутності такого типу злочинів, та їх проблематики, також відсутнє визначення понять «комп'ютерна мережа» та «комп'ютерна система».

У «Конвенції про кіберзлочинність» (набрала чинності 01.07.2007) є визначення цих понять і на разі це – єдиний документ, який містить визначення цих термінів. Також слід зазначити, що у вітчизняному законодавстві досі відсутні визначення понять із префіксом кібер-.

Незважаючи на це, спостерігається вільне використання значної кількості термінів (та їх синонімів), що часто не узгоджені між собою. Так у Законі України «Про основи національної безпеки України» згадуються «комп'ютерна злочинність» та «комп'ютерний тероризм», при чому жоден з цих термінів не має свого визначення а ні в цьому, а ні в інших нормативних документах. В Законі України «Про боротьбу з тероризмом» поняття «комп'ютерний тероризм» не згадується взагалі, а ті елементи, що можуть до нього відноситись прописані як складова частина поняття «технологічний тероризм». У «Стратегії національної безпеки України» (в редакції від 12 лютого 2007 року № 105/2007) комп'ютерні загрози не згадуються, а «кібербезпека» – лише в контексті необхідності «розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність». Однак, нова оприлюднена редакція «Стратегії національної безпеки» (2011 року) вже використовує термін «кібербезпека». В «Доктрині інформаційної безпеки України» також

згадуються «комп'ютерна злочинність» та «комп'ютерний тероризм», знову ж таки – без жодних пояснень чи посилання на такі пояснення. Крім того, в Доктрині згадуються і «кібератаки» без визначення терміну. Отже можна констатувати, що в більшості своїй вітчизняне нормативно-правове поле в сфері інформаційної (кібернетичної) безпеки оперує термінами, визначення яких фактично відсутні [3].

Запропоновані визначення ключових термінів в сфері кібербезпеки профільними відомствами та науковими установами:

— кіберпростір – метафорична абстракція, яка використовується у філософії та у сфері інформаційних технологій, що є (віртуальною) реальністю або окремим світом як «всередині» комп'ютерів, так і в комп'ютерних мережах. (Служба зовнішньої розвідки).

— кіберпростір – це віртуальний простір, сформований інформаційними, телекомунікаційними та інформаційно-телекомунікаційними системами (локальними комп'ютерами, локальними та глобальними мережами), у яких здійснюється виготовлення, зберігання, обробка, обмін та знищення інформації в електронному вигляді. (Служба безпеки України).

Також нагальною стає проблема координації діяльності правоохоронних структур та правового унормування зон відповідальності відомств, процедур взаємодії та засобів комплексного реагування на загрози кібербезпеці держави, а також значної роботи із попередження таких злочинів. Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» (ДССЗЗІ) на ДССЗЗІ покладено функцію участі у «формуванні та реалізація державної політики у сфері захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації». Обмеженість суто захистом (технічним) державних інформаційних ресурсів не відповідає сучасним тенденціям в сфері боротьби із кіберзлочинністю, що потребує додаткового розширення зон уваги правоохоронних органів в тому числі на приватні комп'ютерні мережі та окремі ПК. Крім того, ДССЗЗІ не має повноважень проводити оперативно-розшукову діяльність, чим займаються профільні відділи, управління та департаменти СБУ та МВС України. Діяльність цих трьох відомств у сфері боротьби із кіберзлочинністю є ключовою. Інтернаціональний характер загроз цілком може змусити долучати до такої діяльності та інші відомства, що можуть відноситись до військової організації держави – Головне управління розвідки Міністерства оборони України та Служба зовнішньої розвідки [3].

Тож у висновку, перед законодавцем постає дві основні, першочергові задачі:

1. Дефініціювати на законодавчому рівні ключові поняття у сфері

кібербезпеки: «кіберпростір», «кібербезпека», «кіберзахист», «кібер-атака», «кібервійна», «кібертероризм», «кіберзброя», «кіберінфра-структура», «критична кіберінфраструктура».

2. Правове унормування діяльності структур, робочих груп та відомств по боротьбі з кіберзлочинністю, визначення зон відповідальності та процедур взаємодії.

Література

1. Кримінальний кодекс України: чинне законодавство зі змінами і доповненнями станом на 16.04.2017 [Електронний ресурс]: офіційний сайт Верховної Ради України. – Режим доступу: http://zakon0.rada.gov.ua/ laws/ show/ 2341-14/page14

2. Конвенція про кіберзлочинність від 07.09.2005 [Електронний ресурс]: офіційний сайт Верховної Ради України. – Режим доступу: http://zakon2. rada. gov. ua/ laws/show/994_575

3. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка. Відділ досліджень інформаційного суспільства та інформаційних стратегій / Д. Дубов, М. Ожеван [Електронний ресурс]: офіційний сайт Інституту стратегічних досліджень. – Режим доступу: http://www.niss.gov.ua/articles/454/

УДК 343

Лахай Є.С., студентка,
Навчально-науковий Юридичний інститут,
Національний авіаційний університет, м. Київ
Науковий керівник: Логвиненко А.О., асистент

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ЕКОЛОГІЧНОЇ ЗЛОЧИННОСТІ

Екологічна злочинність є один з найбільш небезпечних та розповсюджених видів злочинності, оскільки створює реальну загрозу національній безпеці країни.

Екологічні злочини - це передбачені кримінальним законом суспільно небезпечні діяння, які посягають на навколишнє середовище та його окремі компоненти. Тобто йдеться про протиправне використання природних об’єктів або шкідливий вплив на них, що призводить до їх негативних змін.

Природоохоронна діяльність та її охорона ґрунтується на правових засадах. Стаття 50 Конституції України проголошує право кожного на безпечне для життя і здоров’я довкілля та на відшкодування завданої порушенням цього права шкоди. Кожному гарантується право вільного