Кримінальне право і кримінологія; кримінально-виконавче право
УДК 343.592

Тітова Вікторія Ігорівна
студентка міжнародно-правового факультету
Національного юридичного університету імені Ярослава Мудрого

КІБЕРЗЛОЧИНИ, ЇХ ПОНЯТТЯ ТА ПРАВОВА ПРИРОДА

Анотація. *У статті розглядається актуальність кіберзлочинів як нової загрози у багатьох сферах суспільного життя. Було проаналізовано основні ознаки, що властиві злочинам у даній сфері, на основі яких надано визначення поняття кіберзлочину, яке пропонується закріпити законодавчо.*

Ключові слова: *кіберзлочинність, кіберзлочини, комп'ютерний злочин.*

Постановка проблеми. Ми живемо в епоху інформаційного суспільства, коли комп'ютери і телекомунікаційні системи охоплюють всі сфери життєдіяльності людини і держави. Але людство, поставивши собі на службу телекомунікації та глобальні комп'ютерні мережі, не передбачала, які можливості для зловживання створюють ці технології. Сьогодні жертвами злочинців, що діють у віртуальному просторі, можуть стати не тільки люди, а й цілі держави. При цьому безпеку тисяч користувачів може виявитися в залежності від декількох злочинців. Кількість злочинів, скоєних в кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж, і, за оцінками Інтерполу, темпи зростання злочинності, наприклад, в глобальній мережі Інтернет, є найшвидшими на планеті.

Розслідування злочинів, скоєних в кіберпросторі, вимагає, як технічних, так і теоретичних знань. З урахуванням гострого дефіциту останніх виникає необхідність обґрунтування єдиного поняття

кіберзлочину, а також вивчення їх правової природи, що сприятиме поглибленню і розширенню термінології теоретичної бази та допоможе практичному використанню даних нормативних положень.

Аналіз останніх досліджень. Роботи зарубіжних вчених: М. Бреннера і С. Гудман, Ф. Вільямса, Д. Деннинг, У. Зібера, Д. Льюїса, М. Кабе, Б. Коліна, Л. Шеллі, присвячені кіберзлочинності, дають непогане уявлення про це явище, але, на жаль, ці дослідження не охоплюють Україну та українське законодавство в даній сфері. Проте вони дають хороші теоретичні основи для вивчення кіберзлочинності в глобальному аспекті.

Ціль статті. На жаль, в українській науковій літературі практично не висвітлено проблему кіберзлочинності як наслідку глобалізації інформаційних процесів. Цю прогалину ще належить заповнити.

Виклад основного матеріалу. Зростання кіберзлочинності, що сталося в останні роки, відзначають і фахівці правоохоронних органів держав, і співробітники організацій, що займаються дослідженнями за допомогою альтернативних методів збору статистичних даних. При цьому фінансові втрати від кіберзлочинності обчислюються мільйонами доларів.

Кіберзлочинність володіє підвищеною суспільною небезпекою внаслідок можливості заподіяння великої шкоди при мінімальних витратах і невисокому ризику. Крім того, кіберзлочинність характеризується високою латентністю, в результаті чого статистика правоохоронних органів не відображає достовірної картини стану кіберзлочинності як на рівні окремих держав, так і на світовому рівні.

У даний час офіційне законодавче закріплення терміну «кіберзлочин» в українському законодавстві так і не прийнято, не зважаючи на стрімко зростаючу гостроту даного питання. У вітчизняній же науковій літературі поняття «комп'ютерна злочинність» використовується для ідентифікації протиправної діяльності із застосуванням комп'ютерних технологій, однак дане поняття не відображає повною мірою природу зазначеного явища, що

дозволяє мати на увазі набагато більш широке коло діянь, ніж це випливає з його буквального тлумачення.

До інформаційних злочинів зазвичай відносять злочини, скоєні за статтями Кримінального кодексу України, що входять до Розділу 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». До них належать: ст. 361 КК — Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; ст. 361-1 КК — Передбачає покарання за створення та розповсюдження вірусів, незалежно від мети таких дій; ст. 362 КК — 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; ст. 361-2 — Передбачає санкції за зловживання правом доступу до інформації [1].

Кіберзлочинність по своїй семантиці і по суті набагато ширше поняття «комп'ютерна злочинність» і охоплює цілий спектр протиправних діянь. Останнє дає підставу охарактеризувати кіберзлочинами суспільно небезпечним діянням, що здійснюються в кіберпросторі, і посягають, з одного боку, на громадську безпеку, власність, права людини, інші охоронювані законом відносини, а з іншого - необхідним елементом механізму підготовки, вчинення та приховування злочину, відображенням якого є комп'ютерна інформація, яка виступає в ролі предмета або засоба вчиненого злочину [2].

У Конвенції про кіберзлочинність, відкритої для підписання в м. Будапешті, яка набрала чинності 1 липня 2004 року кіберзлочинами визначаються діяння, спрямовані проти конфіденційності, цілісності та

доступності комп'ютерних систем, мереж і комп'ютерних даних, а так само зловживання такими системами, мережами і даними [3].

Кирбят'єв О. О. у своїй науковій праці зазначає, що під терміном «кіберзлочини» слід розуміти соціальне явище, що являє собою навмисну мотивовану атаку з використанням мережі Інтернет на інформацію в комп'ютерній системі, програми або дані, що чиниться окремою особою або угрупуваннями, яке має суспільну небезпеку для суспільного ладу України, його політичної й економічної системи, власності, особи, політичних, трудових, майнових та інших прав і свобод громадян [4]. А. В. Юрасов, у свою чергу, розглядає кібезлочин як злочин у традиційному сенсі, але у мережі Інтернет [5].

На нашу думку, аби надати коректне визначення кіберзлочину, необхідно розглянути його основні ознаки, через які виявляється правова природа даного виду злочинів.

Розглядаючи ознаки кіберзлочинів, дослідниками називається кілька характерних рис.

По-перше, кіберзлочини здійснюються з використанням засобів комп'ютерної техніки і щодо інформації, що знаходиться (використовуваної і оброблюваної) в мережі Інтернет. Використання комп'ютерних пристроїв і інформаційно-телекомунікаційних мереж виступає в ролі засобів скоєння злочину, а використання шкідливих програм - як знаряддя скоєння злочину.

По-друге, в таких злочинах присутні два об'єкти посягання: суспільні відносини у сфері безпеки поводження комп'ютерної інформації та суспільні відносини, пов'язані з нею, що мають взаємозв'язок з реальним світом, наприклад, відносини власності.

По-третє, для кіберзлочинів характерно використання спеціальних знань в комп'ютерній сфері або спеціальних програмних комплексів для здійснення злочинних діянь.

По-четверте, такі злочини не є очевидними, вони відбуваються приховано і можуть мати як триваючий, так і разовий, одномоментний характер, а тривалість атак може тривати від декількох секунд до багатьох діб і навіть місяців.

По-п'яте, докази, що стосуються таких злочинів, в основному передаються і зберігаються в електронних мережах (саме цим і обумовлюється складність збирання доказів і здійснення процесуальних дій).

Важливою ознакою для даного виду злочинів стає наявність зростаючої і стійкої тенденції до «організованості» кіберзлочинності, груповий характер вчинення таких правопорушень. У зв'язку з тим, що кіберзлочинність має транскордонний характер, для ефективної протидії таким злочинам необхідна організація ефективної взаємодії різних держав.

Висновки. В результаті аналізу наведених ознак «кіберзлочину», можна сформулювати загальне визначення, яке пропонується закріпити на нормативному рівні.

Кіберзлочини - це сукупність злочинів, передбачених Кримінальним кодексом України, що здійснюються в кіберпросторі, де основними безпосередніми об'єктами злочинного посягання виступають конституційні права і свободи людини і громадянина, суспільні відносини у сфері комп'ютерної інформації та інформаційних технологій, суспільні відносини у сфері економіки і економічної діяльності, суспільні відносини у сфері державної влади, суспільні відносини у сфері охорони здоров'я населення і суспільної моралі та інші охоронювані кримінальним законом об'єкти.

Література

1. Кримінальний кодекс України. URL: http://zakon4.rada.gov.ua/laws/show/2341-14

2. Кравцова М. А. Поняття кіберзлочинності і її ознаки / М. А. Кравцова // Часопис Київського університету права. 2015. № 2. С. 320-324.
3. Про ратифікацію Конвенції про кіберзлочинність: закон України від 7 верес. 2005 р. № 2824-IV // Відомості Верховної Ради України. 2006. № 5-6. Ст. 71
4. Кирбят'єв О. О. Комп'ютерні злочини: реалії сучасності, проблеми боротьби з ними та ймовірні шляхи їх вирішення / О. О. Кирбят'єв // Вісник Запорізького національного університету. 2010. № 1. С. 165–170. URL: http://web.znu.edu.ua/herald/issues/2010/Ur-1-2010/165-170.pdf
5. Юрасов А. В. Основи електронної коммерції: навч. / А. В. Юрасов. М.: Горячая лінія-Телком, 2008. С. 165.
6. Кравцова М. А. Поняття кіберзлочинності і її ознаки / М. А. Кравцова // Часопис Київського університету права. 2015. № 2. С. 320-324.