Щодо проблеми визначення поняття «кіберзлочини» та «кіберзлочинність»

Атамась Вадим Романович,
студент 2 курсу спеціальності «Право»
ННІ економіки і права
Черкаського національного університету
імені Богдана Хмельницького

Постановка проблеми. Інтернет, комп'ютери, мобільні телефони та інші форми технологій здійснили революцію у всіх аспектах людського життя за останні кілька десятиліть. Це ввібрало в себе те, як ми спілкуємось, робимо покупки, отримуємо новини та розважаємо себе. Ці технологічні досягнення мають і темний бік, адже створили незліченні можливості для правопорушників вчинити різні форми суспільно-небезпечних діянь. Інформаційні правопорушення часто називають кіберзлочинністю і трапляються вони через те, що винний використовує спеціальні знання про кіберпростір. Кіберзлочинність в Україні та світі має швидкі темпи розвитку, а кількість потерпілих від цих правопорушень обчисляється – мільйонами. Тож, кіберзлочинність можна розглядати як великий загальний термін, який охоплює комп'ютерну злочинність та технології. Саме тому питання визначення поняття кіберзлочинності та введення відповідальності за відповідне кримінальне правопорушення є актуальним для України задля забезпечення гідного рівня захисту громадян та недоторканності їхнього особистого життя та даних.

Стан наукового дослідження. Різнорідними концепціями становлення та розвитку інформаційних даних, розробкою предмета та тлумачення поняття "кіберзлочинності" займалися такі науковці як: В. О. Голубєв, М.А. Кравцова, В. С. Сідак, Т. Л. Сироїд, М. О. Будаковим, В. М. Бутузовим, М.М. Галамбою, Р. А. Калюжним, Ю. Є. Максименко, О. В. Орлова Д. Л. Дубов, М.А. Ожеван та інших. Проте необхідність подальших наукових досліджень ґрунтується на прогалинах в кримінальному законодавстві щодо протидії кіберзлочинності. Дослідження передбачає аналіз зарубіжного законодавства та досвіду в сфері боротьби проти кіберзлочинності.

Мета даної роботи полягає у визначені доцільності введення в національне законодавство понять кіберзлочину та кіберзлочинності, відповідно до міжнародних стандартів.

Виклад основного матеріалу. Термін “кіберзлочинність” має як соціально-технічну, так і юридичну забарвленість. Під ним слід розуміти кримінально-протиправну діяльність, яка спрямована на шахрайство, викрадення цінних даних або ж вторгнення в приватне життя. Для досягнення цих цілей використовуються комп’ютери, комп’ютерні мережі або мережеві пристрої.

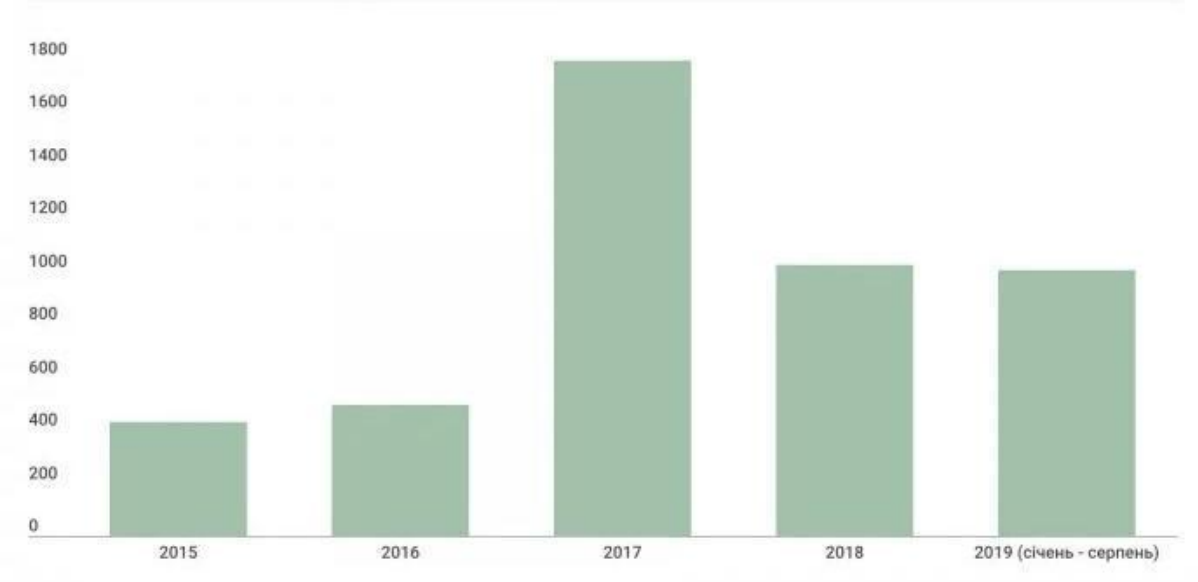
Більшість кіберзлочинів здійснюються кіберзлочинцями або хакерами, які є досить організованими, використовують передові технології та мають високу технічну кваліфікацію. Сенс кіберзлочинів виявляється в нападі на інформацію про приватних осіб, корпорації чи уряди певних країн. Хоча напади не відбуваються на фізичне тіло, вони відбуваються на особистому або корпоративному віртуальному тілі, що є сукупністю інформаційних атрибутів, що визначають людей та установи в Інтернеті. Іншими словами, у цифрову епоху наші віртуальні ідентичності є важливими елементами повсякденного життя: ми являємо собою набір чисел та ідентифікаторів у безлічі комп’ютерних баз даних, якими володіють уряди та корпорації [2, с. 320].

Важливим аспектом кіберзлочинності є його множинно-локальний характер: дії можуть відбуватися в межах, розділених величезною відстанню. Це створює серйозні проблеми для правоохоронних органів, оскільки місцеві чи національні кримінальні правопорушення зараз потребують міжнародної співпраці. Цим самим, кіберзлочинність охоплює різні сфери діяльності. Ними є кримінальні правопорушення, які передбачають грубі порушення особистої або корпоративної конфіденційності, такі як: посягання на цілісність інформації, що зберігається в цифрових репозитаріях, та використання незаконно отриманої цифрової інформації для шантажу фірми чи фізичної особи. На наше переконання, зростає й спектр щодо викрадення особистих даних, засновані на транзакціях, такі як шахрайство, цифрове піратство, відмивання грошей, підробка та їм подібні.

Оскільки кіберзлочинність впливає на безпеку держав, розуміння контексту, в якому відбуваються політика та міжнародні справи, є ключовим, оскільки інтереси країн щодо національної безпеки зазвичай дуже різняться. Це, мабуть, встановило б межі для міжнародної угоди про створення спільного міжнародного закону про кібербезпеку. Крім того, зростання кібератак з роками проливає світло на загрози та серйозність цієї зростаючої кримінальної поведінки, яка потребує термінової міжнародної реакції.

Кіберзлочинність – це п’ятий за значимістю вид економічної протиправності в Україні, слідом за незаконним привласненням майна, незаконним збагаченням і корупцією, практикою підриву конкуренції і маніпуляцією з фінансовою звітністю [1].

За останні п’ять років в Україні кількість інформаційних правопорушень зросла щонайменше у 2,5 рази. Як повідомляється, стрибок кількості всіх кіберзлочинів відбувся у 2017 році. Після цього кількість кримінальних правопорушень почала зростати. Так в 2017 було зафіксовано 1795 справ, в 2018 - 1023, а в період з 2019 по 2020 – 1005:



Статистика поширення кіберзлочинів з 2015 по 2019-20 рр.

Нині в українському законодавстві відсутнє визначення поняття «кіберзлочин» або «кіберзлочинність», є лише узагальнене поняття кримінальних правопорушень, які вчиняються з використанням комп’ютерів, комп’ютерних систем та мереж електрозв’язку, зокрема:

- несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку (стаття 361 КК України);

- створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361-1 КК України);

- 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 361-2 КК України).

Крім того, діяльність кіберзлочинців кваліфікується за статтею 200 КК України – незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима обладнанням для їх виготовлення [3].

Основними проблемами, що ускладнюють боротьбу проти кримінальних правопорушень в інформаційній сфері є:

- відсутність ключових термінів та понять, таких як: "кіберпростір", "кібербезпека", "кіберзахист", "кібератака", "кібервійна", "кібертероризм", "кіберзброя", "кіберінфраструктура", "критична кіберінфаструктура" та ін. Очевидно, що кримінальні правопорушення у кіберсфері неможливо кваліфікувати без назв цих самих правопорушень. КК України повинен бути готовим до тих інноваційних змін, які відповідають сучасним стандартам у сфері інформаційних технологій. З цього, зокрема випливає наступна проблема:

- застарілість чинного кримінального законодавства. КК України є досить архаїчним і відповідальність за кіберзлочини передбачена й узагальнена поняттям "правопорушення, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку". Кримінальний закон повинен надавати конкретизацію відповідних понять та розкривати їхню значимість для національного законодавства [4].

Висновки. Враховуючи вищевикладене, слід по-новому підійти до питання оновлення нормативно-правової бази для боротьби з кіберзлочинністю та ввести до кримінального законодавства поняття «кіберзлочину» та «кіберзлочинності». Рівень інформаційних технологій в Україні вимагає належного нормативного забезпечення, враховуючи міжнародний досвід в цій сфері. Спротив кіберзлочинності зобов'язує правоохоронні органи ще більш активно та на належному компетентному рівні протидіяти кіберзлочинності.

Список використаних джерел:

1. Всесвітній огляд економічних злочинів [Електронний ресурс]. – Режим доступу : https://www.pwc.com/ua/uk/ Україна].

2. Кравцова М. А. Понятие киберпреступности и ее признаки / М.А. Кравцова // Часопис Київського університету права. 2015. № 2. С. 320.

3. Кримінальний кодекс України : Закон : від 05.04.2001 № 2341-III [Електронний ресурс] //Сайт Верховної Ради України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2341-14.

4. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : аналітична записка / Д. Дубов, М. Ожеван [Електронний ресурс]. – Режим доступу: http://www.nis.gov.ua/articles/454.

Науковий керівник:
***Сокуренко Олександр Михайлович*,**
кандидат юридичних наук, доцент,
доцент кафедри державно-правових дисциплін
Черкаського національного університету
імені Богдана Хмельницького