Кобилянська Людмила,
Київський університет імені Бориса Грінченка,
м. Київ, Україна,
l.kobylianska@kubg.edu.ua

ПРАВОВІ ЗАСАДИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

LEGAL BASIS OF INTERNATIONAL COOPERATION IN FIGHT AGAINST CYBERCRIME

Актуальність дослідження. Тотальна комп'ютеризація, мережа Інтернет і цифрові технології стрімко увірвались в усі сфери людської діяльності. Розвиток ІКТ значно спрощує виробничі, управлінські, організаційні процеси та збереження інформації, водночас актуалізуючи такий різновид незаконної діяльності, як кіберзлочинність у віртуальній мережі. Йдеться передусім про порушення прав корпоративної та інтелектуальної власності, безпосередні крадіжки коштів через мережі, моральні втрати, блокування роботи сайтів організацій та державних установ.

Метою роботи є дослідження міжнародного правового досвіду протидії кіберзлочинності та з'ясування можливостей удосконалення чинного законодавства України, а також застосування інших заходів протидії незаконній діяльності у віртуальному просторі.

Виклад основного матеріалу дослідження. Дослідниками явища кіберзлочинів (серед яких Центр стратегічних і міжнародних досліджень (США) та компанія McAfee) з'ясовано, що шпигунство та крадіжки інтелектуальної власності, розголошення конфіденційних даних клієнтів з подальшими виплатами штрафів і компенсаційних виплат постраждалим споживачам, зниження конкурентоспроможності компаній генерують величезні втрати для національної економіки та призводять до деформації відносної економічної ефективності. Найбільше кіберзлочинність поширена у фармацевтичній, біотехнічній та хімічній галузях промисловості, а також у сферах виробництва електроніки та комп'ютерних технологій.

Зазвичай компанії чи корпорації не в змозі оцінити реальні збитки через кіберзлочинну діяльність, тому що незаконне привласнення інте-

лектуальної власності чи важливої ділової інформації важко піддається кількісній оцінці. Також надзвичайно складно визначити у вартісному вимірі втрати ділової репутації банківських установ, адвокатських контор або юридичних компаній. Значними є витрати на страхування суб'єктів господарювання та відновлення їх діяльності у випадку скоєння кіберзлочинів. З року в рік зростають додаткові витрати фізичних осіб, організацій та держав на оновлення операційних систем захисту персональних комп'ютерів, убезпечення діяльності підприємств, банківських установ від несанкціонованого втручання в роботу комп'ютерних систем.

Однак наслідки злочинних дій у віртуальному просторі не зводяться лише до матеріальних втрат. Торгівля підробними ліками та нанесення шкоди здоров'ю, торгівля людьми, розповсюдження порнографії, моральні травми, втручання у роботу державних електронних мереж та комунікацій стратегічних об'єктів, кібертероризм — це далеко не повний перелік проблем, пов'язаних з кіберзлочинами. Окремі терористичні угруповання, такі як "Hezbollah", "Hamas", "The Abu Nidal Organization" використовують комп'ютерні системи, електронні мережі для шифрування та передачі інформації, фінансування та всілякої підтримки злочинної діяльності. Кібертероризм як різновид зброї дедалі активніше застосовується з метою виведення з ладу важливих державних та соціальних об'єктів.

Вирішення питань протидії кіберзлочинності залишається одним із пріоритетів діяльності інституцій Організації Об'єднаних Націй завдяки впровадженню Глобальної програми по боротьбі з кіберзлочинністю.

Правовою основою міжнародного рівня з мінімізації загроз впливу кіберзлочинності є Конвенція Ради Європи про злочинність у кіберпросторі, прийнята 23 листопада 2001 р. у Будапешті [1]. Серед основних питань, висвітлених у даному документі, — криміналізація правопорушень, здійснених завдяки комп'ютерним пристроям з метою втручання у роботу комунікаційних мереж та викрадення даних; вдосконалення національного законодавства у боротьбі з кіберзлочинністю; розвиток міжнародного співробітництва.

Згідно з класифікацією, що прийнята вищезазначеною Конвенцією, кіберзлочини поділяються на п'ять різновидів: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; правопорушення, пов'язані з комп'ютерами; правопорушення,

пов'язані зі змістом інформації; правопорушення, пов'язані з порушенням авторських і суміжних прав; дії расистського і ксенофобського характеру.

У форматі Європейського Союзу узгоджено низку документів з метою боротьби зі злочинністю у віртуальному просторі, серед яких: Директива № 2000/31/ЄС Європейського Парламенту і Ради про деякі правові аспекти послуг інформаційного співтовариства, як-от електронна торгівля на внутрішньому ринку [4]; Директива Європейського Парламенту та Ради ЄС про зберігання зібраних або оброблених даних у зв'язку з наданням суспільно доступних послуг електронного зв'язку або використанням мереж зв'язку загального користування [5]; Директива Європейського Парламенту та Ради ЄС про обробку персональних даних та захист приватного життя в сфері електронних комунікацій [6]; Рамкове рішення Ради ЄС про атаки на інформаційні системи [2]; Рамкове рішення Ради ЄС про боротьбу з шахрайством і підробкою безготівкових платіжних засобів [3].

Ефективність протидії явищу кіберзлочинності вбачається у спільних діях державного і приватного секторів, вдосконаленні міжнародного та національного законодавства, організації міжнародних підрозділів та структур у боротьбі з кіберзлочинами. З цією метою у 2013 р. в ЄС створено Європейський центр боротьби з кіберзлочинністю (Гаага).

Серед основних видів кіберзлочинів в Україні — підробка банківських карток, крадіжка конфіденційних даних банківських карт, шахрайство з банкоматами, злочинні дії у банківській системі он-лайн. Дедалі частіше трапляються випадки поширення вірусів з метою незаконного втручання в роботу комп'ютерних мереж через мобільні пристрої користувачів, зокрема: телефони, смартфони, планшети.

Згідно з експертними висновками фахівців компанії "Norton", небезпека криється в тому, що близько 49 % споживачів використовують свої особисті мобільні пристрої водночас як для роботи, так і для гри, таким чином спрощуючи доступ хакерам до конфіденційної інформації. Близько половини смартфонів і планшетних пристроїв не оснащено навіть елементарними запобіжними заходами, йдеться, зокрема, про використання паролів, безпекове програмне забезпечення, резервне копіювання файлів з мобільних пристроїв. Дослідження компанії свідчать про те, що 35 % користувачів мають принаймні один незахищений пристрій, що залишається вразливим для злочинців, шкідливих веб-

сайтів та фішинг-атак, водночас майже 44 % споживачів віртуальних послуг не вважають свою діяльність вартою уваги хакерів [7]

Пріоритетними напрямами створення державної стратегії в Україні у сфері гарантування інформаційної безпеки та протидії кіберзлочинам залишаються поєднання координаційних зусиль та взаємодія правоохоронних органів, спецслужб, судової системи, а також їх матеріально-технічне забезпечення, підготовка необхідної кількості фахівців, узагальнення слідчої та судової практики стосовно кіберзлочинів, розробка чітких рекомендацій щодо їх розслідування, налагодження механізму обміну інформацією правоохоронної системи України з правоохоронними органами інших держав, що здійснюють боротьбу з кіберзлочинністю.

Надзвичайно гостро постає необхідність удосконалення чинного законодавства України у сфері боротьби з кіберзлочинністю. У вітчизняному законодавстві панує невизначеність стосовно термінів «кіберзлочин», «кіберзлочинність», «кібератака», натомість існує лише узагальнене визначення цього типу злочинів, як шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки (стаття 190 Кримінального кодексу України); несанкціонованого 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); несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинених особою, яка має право доступу до неї (стаття 362 КК України); порушень 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 обробляється (стаття 363 КК України); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку за допомогою масового поширення повідомлень електрозв'язку (стаття 363^1 КК України) [8].

Висновки. Наразі в Україні відсутня єдина державна стратегія з кібербезпеки та цифрового суверенітету, виробництва власних про-

грам та сучасної електронної комп'ютерної техніки, а також єдина національна операційна система обміну інформацією. За відсутності власної технічної, програмної бази країна з низьким рівнем обізнаності та інформаційної безпеки й надалі залишатиметься залежною і вкрай вразливою до глобальних загроз. Очевидно також, що існує потреба удосконалення чинного законодавства України шляхом доповнення термінології стосовно незаконної кібердіяльності.

Втручання в роботу телекомунікаційних систем в Україні потребує застосування низки заходів протидії, зокрема: зменшення кількості авторизаційних лімітів, розширення використання чіпових карт, впровадження сучасного мережевого захисту банківських систем, у тому числі систем додаткового підтвердження платежів через одноразові паролі та коди.

Нагадаємо, що небезпечним є одночасне використання браузера для ігор чи спілкування у соціальних мережах та здійснення інтернет-банкінгу. Використання ліцензійного програмного забезпечення, новітні системи мережевого захисту фінансових установ та організацій, роз'яснювальна робота серед клієнтів щодо питань збереження конфіденційності інформації та індивідуальних даних сприятимуть зниженню кількості кіберзлочинів.

Кіберзлочинність щорічно завдає глобальних економічних збитків, які надзвичайно складно визначити у кількісному вираженні. Водночас суб'єкти господарювання та уряди держав недооцінюють реальні виклики та загрози, пов'язані з кіберзлочинами у глобальному вимірі (йдеться про так званий прихований чи тіньовий Інтернет, кібертероризм, промисловий шпіонаж, функціонування бот-мереж та вірусних програм).

Боротьба з кіберзлочинністю у міжнародному форматі актуалізує необхідність координації дій державного і приватного секторів на основі об'єднання фінансових, технічних, комунікаційних і організаційних ресурсів, обмеження анонімності користувачів у всесвітній мережі Інтернет, соціальних мережах та під час проведення банкінгових операцій. Також є потреба у створенні міжнародних підрозділів та структур для боротьби з кіберзлочинністю з наданням права передачі даних про рух інформації, екстрадицію, допомогу, розробку міжнародних чи транскордонних комунікаційних мереж для відстеження в реальному часі і передачі інформації про кіберзлочини.

Джерела

1. Convention on Cybercrime. Budapest, 23.XI.2001 [Електронний ресурс]. — Режим доступу : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561
2. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems [Електронний ресурс]. — Режим доступу : http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32005F0222
3. Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment [Електронний ресурс]. — Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001F0413
4. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [Електронний ресурс]. — Режим доступу : http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031
5. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [Електронний ресурс]. — Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024
6. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [Електронний ресурс]. — Режим доступу : http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX: 32002L0058
7. 2016 Norton Cyber Security Insights Report [Електронний ресурс]. — Режим доступу : https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security- insights-report.pdf
8. Кримінальний кодекс України [Електронний ресурс]. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/2341-14/page