DOI: 10.33498/louu-2023-11-116

СЛОВО МОЛОДИМ ВЧЕНИМ

Діна Дрижакова

директорка ТОВ "Юридична компанія "Пріма лідер груп",
аспірантка кафедри кримінально-правової політики
та кримінального права
Навчально-наукового інституту права
Київського національного університету
імені Тараса Шевченка
(Київ, Україна)
d.dryzhakova@gmail.com

УДК 343.346.8

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ У СФЕРІ ПРОТИДІЇ НЕСАНКЦІОНОВАНИМ ВТРУЧАННЯМ У РОБОТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ЧИ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Анотація. Швидкі темпи розвитку інформаційно-телекомунікаційних технологій, систем і мереж розширюють можливості їх використання у різних видах кримінально-протиправної діяльності. Зростання кількості користувачів кіберпростору сприяє не тільки скоєнню стосовно них кримінальних правопорушень, а й можливості їхньої участі у злочинній діяльності, зокрема і в її організованих формах.

Варто зауважити, що феномен злочинності у кіберпросторі для нашої держави є доволі новим, однак при цьому має значний ступінь суспільної небезпечності та може бути об'єктом посягання багатьох суспільних відносин. Збройна агресія Російської Федерації стала певним каталізатором вироблення нової якісної системи охорони кіберпростору України. Це перш за все стосується вдосконалення існуючої стратегії кібербезпеки України, а також внесення змін у чинний Кримінальний кодекс України щодо питання кримінальної відповідальності за суспільно небезпечні діяння, які вчиняються у кіберпросторі.

Мета статті – аналіз нормативно-правових актів із протидії несанкціонованим втручанням у роботу інформаційно-телекомунікаційних систем, аналіз прогалин у нормативно-правовому регулюванні цієї сфери, огляд нормативно закріпленого понятійного апарату, що використовується під час проведення судових комп'ютерно-технічних і телекомунікаційних експертиз.

Ключові слова: нормативно-правове регулювання; закон; інформаційно-телекомунікаційна система; кібертероризм; кіберзагроза; телекомунікаційна експертиза; комп'ютерно-технічна експертиза.

Мета дослідження – аналіз нормативно-правових актів із протидії несанкціонованим втручанням у роботу інформаційно-телекомунікаційних систем, аналіз прогалин у нормативно-правовому регулюванні цієї сфери, огляд нормативно закріпленого понятійного апарату, що використовується під час проведення судових комп'ютерно-технічних і телекомунікаційних експертиз.

Нормативно-правовою основою функціонування інформаційно-телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку, технічного захисту оброблюваної в них інформації та кримінальної відповідальності за несанкціоноване втручання в їхню роботу є Конституція України, закони України, Кримінальний кодекс України (далі – КК України)[1], акти Президента України, Кабінету Міністрів України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, а також міжнародні договори України, згоду на обов'язковість яких надала Верховна Рада України.

Законодавство не встигає за розвитком зазначеної сфери, що призводить до неврегульованості більшості злочинів, вчинених на просторах інформаційної інфраструктури, а в певних випадках – навіть до відсутності відповідальності.

Перш ніж говорити про Україну, звернемо увагу, що відповідальність користувача за правопорушення при роботі з конфіденційною інформацією, комп'ютерами і комп'ютерною інформацією в розвинених країнах узаконена вже давно. Ось коротко деякі закони, що найбільш яскраво висвітлюють зазначену юридичну сферу:

У США – "Закон про безпеку комп'ютерних систем" – 1987 р., "Акт про зловживання з використанням ЕОМ" – 1986 р., "Закон про свободу інформації", "Закон про захист обчислювальних засобів невеликих фірм і освіти", "Закон про дотримання таємниць" – 1974 р., "Закон про фінансові таємниці", "Закон про авторське право", Конституція США – 1787 р.

У Канаді – "Закон про комп'ютерні й інформаційні злочини" – 1985 р.

У Франції – "Закон про інформаційні технології, бази даних, громадянські свободи" – 1978 р.

У Великій Британії – "Закон про захист інформації" – 1984 р.

У Німеччині – "Закон про подальший розвиток електронної обробки і захисту даних" – 1990 р., "Федеральний закон про охорону даних" – 1978 р.

Законодавство України у цій сфері помітно слабкіше західного. Закон України "Про інформацію"[2] декларує загальні принципи одержання, використання, поширення і збереження інформації, закріплює право осо-

[1] Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-ІІІ <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 16.11.2023).

[2] Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 16.11.2023).

бистості на інформацію у всіх сферах життя. Визначає статуси учасників інформаційних відносин, регулює доступ до інформації і забезпечує її охорону, захищає особистість і суспільство від недостовірної інформації. Документ є ідеологічною основою для всіх наступних документів у сфері захисту інформації.

Закон України "Про державну таємницю"[3] регламентує інформаційні відносини, пов'язані з доступом до державної секретної інформації:

– Державну таємницю можуть становити відомості зі сфери оборони, економіки, міждержавних відносин, державної безпеки й охорони правопорядку.

– Забороняється засекречувати в будь-якій формі відомості про стихійні нещастя, катастрофи, екологію, рівні добробуту народу, стани правопорядку, про незаконні дії органів влади, а також будь-які інші зведення, засекречування яких порушує конституційні права і волю громадян.

– Інформацію засекречують державні експерти з питань секретів, якими є президент, спікер парламенту, прем'єр-міністр, а також спеціально призначені президентом посадові особи.

– Недержавні структури, що мають намір працювати з інформацією, що становить державну таємницю, повинні ліцензуватися Державним комітетом з питань держсекретів.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"[4] дає визначення основних термінів у сфері автоматизованих систем (далі – АС), і регламентує відносини між сторонами в процесі обробки інформації в АС, установлює загальні вимоги до захисту інформації в АС, порядок міждержавних відносин у сфері захисту інформації в АС:

– Суб'єктами відносин у процесі обробки інформації в АС є власник інформації, власник АС, користувач інформації, користувач АС.

– Після процесу обробки інформації в АС отриманий продукт є власністю користувача АС, що її обробив, якщо інше не передбачене договором між ним і власником інформації.

– Якщо власником оброблюваної інформації є держава, то власник АС зобов'язаний забезпечити захист інформації відповідно до державних стандартів.

– Власник АС є її адміністратором і організатором роботи користувачів АС. Власник АС зобов'язаний інформувати власника інформації і користувача АС про методи спілкування з АС, а також методи захисту інформації в його системі.

[3] Про державну таємницю: Закон України від 21 січня 1994 р. № 3855-XII <https://zakon.rada.gov.ua/laws/show/3855-12#Text> (дата звернення: 16.11.2023).

[4] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата звернення: 16.11.2023).

– Захист інформації в АС забезпечується програмними, апаратними й іншими засобами, що повинні сертифікуватися, якщо на них планується обробляти державну інформацію секретного характеру.

– Особи, винні у втраті інформації внаслідок неграмотної побудови систем захисту АС, несуть дисциплінарну, адміністративну, кримінальну відповідальність або матеріально компенсують завданий збиток.

На жаль, законодавство України не дає однозначного визначення категорії "несанкціоноване втручання в роботу". У Законі України "Про захист інформації в інформаційно-телекомунікаційних системах" наводиться дефініція поняття "несанкціоновані дії щодо інформації в системі", до яких відносяться такі, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Згідно зі ст. 1 зазначеного Закону доступ до інформації в системі – це отримання користувачем можливості обробляти інформацію в системі. Порядок доступу до інформації в системі – це умови отримання користувачем можливості обробляти інформацію в системі та правила її обробки. Обробка інформації в системі – це виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання, які здійснюються у системі за допомогою технічних і програмних засобів. З огляду на аналіз наведених категорій, можна зробити висновок, що несанкціоноване втручання в роботу – це порушення користувачем умов та правил отримання й обробки інформації[5].

Закон України "Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану"[6] набрав чинності 3 квітня 2022 р.[7]. Його прикінцеві положення вимагають від Кабінету Міністрів України розробити та забезпечити введення в дію у місячний строк з дня ухвалення цього Закону (тобто до 24 квітня 2022 р.) порядку пошуку та виявлення потенційних вразливостей інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Проте лише майже через рік – 16 травня 2023 р. Постанова Кабінету Міністрів України № 497 затвердила Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електрон-

[5] О Курман, 'Криміналістична характеристика несанкціонованого втручання у роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку' [2017] 4 (2) Наук. вісн. Херсон. держ. ун-ту. Серія "Юрид. науки" 127–30.

[6] Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24 березня 2022 р. № 2149-IX <https://zakon.rada.gov.ua/laws/show/2149-20#Text> (дата звернення: 16.11.2023).

[7] Детальніше див.: Микола Хавронюк, 'Втручання в роботу інформаційно-комунікаційних систем: кримінальна відповідальність' *(Центр політико-правових реформ,* 29.04.2022) <https://pravo.org.ua/blogs/vtruchannya-v-robotu-informatsijno-komunikatsijnyh-system-kryminalna-vidpovidalnist> (дата звернення: 16.11.2023).

них комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж[8], який визначає механізм здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (далі – пошук потенційної вразливості системи).

Однак дія цього Порядку є досить обмеженою. Він не поширюється на інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі, в яких обробляється службова інформація та/або інформація, що становить державну таємницю, розвідувальну таємницю, банківську таємницю.

Відповідно, виявити вразливості в системах службової інформації та/або інформації, що становить державну таємницю, розвідувальну таємницю, банківську таємницю, складно.

Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку караються згідно з КК України, а саме:

– несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – згідно зі ст. 361;

– створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут – згідно зі ст. 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 – згідно зі ст. 361^2 КК України;

– 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 – згідно зі ст. 362 КК України;

– порушення 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 оброблюється, – згідно зі ст. 363 КК України;

– перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електро-

[8] Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затверджений постановою Кабінету Міністрів України від 16 травня 2023 р. № 497 <https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text> (дата звернення: 16.11.2023).

зв'язку через масове розповсюдження повідомлень електрозв'язку – згідно зі ст. 363[1] КК України.

Одним із основоположних міжнародних документів щодо узгодження боротьби з комп'ютерними злочинами є Конвенція про кіберзлочинність, ратифікована Україною 7 вересня 2005 р.[9].

Саме собою несанкціоноване втручання в роботу згаданих систем чи мереж не є кримінальним правопорушенням, оскільки не створює жодних наслідків, які можна було б охопити поняттям "істотна шкода" (див. ст. 11 КК України).

Тут має місце помилка законодавця, оскільки передбачене у ч. 1 ст. 361 КК України несанкціоноване втручання в роботу вказаних систем чи мереж – без витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації – не здатне спричинити жодного зі згаданих наслідків.

Так, згідно зі статтями 361 та 361[1] КК України шкідливі програмні засоби – це програмні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що може призвести до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.

Водночас низка інших нормативних документів містить визначення окремих різновидів програмного забезпечення, яке за багатьма ознаками може вважатися шкідливим, без зазначення співвідношення цих визначень із визначенням загального поняття "шкідливий програмний засіб", який наведений у КК України.

Як приклад можна навести ситуацію, яка виникла 23 грудня 2015 р., коли за допомогою шкідливого програмного забезпечення *"BlackEnergy"* було відключено близько 30 підстанцій Прикарпаття-обленерго[10].

За даними Департаменту кібербезпеки Служби безпеки України, за 2022 р. було нейтралізовано понад 4,5 тис. кібератак, а на перший квартал 2023 р. – 550. Також було зазначено, що здебільшого Російська Федерація атакує об'єкти логістики, енергетики, транспорту, військові об'єкти[11].

Розрізняють такі види шкідливого забезпечення: комп'ютерний вірус, програмна закладка, люк (бекдор), троянський кінь.

[9] Конвенція про кіберзлочинність від 23 листопада 2001 р. <http://zakon5.rada.gov.ua/laws/show/994_575> (дата звернення: 16.11.2023).

[10] 'Українські обленерго атакували вірусом BlackEnergy – США' (*Мультимедійна платформа іномовлення України,* 31.01.2016) <https://www.ukrinform.ua/rubric-society/1944263-ukrajinski-oblenergo-atakuvali-virusom-blackenergy-ssha.html> (дата звернення: 16.11.2023).

[11] 'Україна не готова до сучасних кібератак – експерт' (*Радіо свобода,* 14.12.2016) <https://www.radiosvoboda.org/a/28176636.html> (дата звернення: 16.11.2023).

Аналізуючи зазначені визначення, нескладно дійти висновку, що без їх упорядкування до єдиної системи проблематично розраховувати на однозначне об'єктивне тлумачення усіма працівниками, задіяними у цій сфері.

В українському законодавстві немає чіткого визначення таких понять, як "кібертероризм" і "кібердиверсія". Низкою законопроєктів планувалось доповнити цими поняттями КК України, проте вони так і не були реалізовані.

Наслідком стрімкого розвитку інформаційно-комунікаційних технологій та мережі Інтернет є поява нових видів міжнародних конфліктів та інформаційні війни, тому міжнародно-правове регулювання правовідносин, що виникають у цій сфері, є вкрай важливим.

Однак, станом на сьогодні, у кримінальному законодавстві України немає спеціалізованої статті, яка б передбачала кримінальну відповідальність за неправомірний або несанкціонований вплив на об'єкти критичної інформаційної інфраструктури, навмисне вживлення в програмне забезпечення закладок або люків (бекдорів), за відсутність тестування програмного забезпечення, що створює певні перешкоди під час досудового розслідування та, в майбутньому, формулюванні обвинувального акту та направлення його до суду. Зокрема, без відповідної нормативно-правової бази виникають проблеми з кваліфікацією відповідних злочинів та доведення їх вчинення.

Слід зазначити, що українська нормативно-правова база містить доволі багато документів, які певним чином регламентують питання протидії несанкціонованим втручанням у роботу інформаційно-телекомунікаційних систем країни. Однак таке розмаїття нормативно-правових актів породжує низку проблем, пов'язаних насамперед з неузгодженістю окремих положень цих актів.

Висновки. Підсумовуючи, вважаємо, що Україні необхідно структурувати понятійний апарат у сфері несанкціонованого втручання в роботу телекомунікаційних і комп'ютерних мереж, ввести відповідальність за кібертероризм.

REFERENCES

Bibliography

Journal articles

1. Kurman O, 'Kryminalistychna kharakterystyka nesanktsionovanoho vtruchannia u robotu elektronno-obchysliuvanykh mashyn (komp'iuteriv), avtomatyzovanykh system, komp'iuternykh merezh chy merezh elektrozv'iazku' [2017] 4 (2) Nauk. visn. Kherson. derzh. un-tu. Seriia "Iuryd. nauky" 127–30 (in Ukrainian).

Websites

2. Khavroniuk M, 'Vtruchannia v robotu informatsiino-komunikatsiinykh system: kryminalna vidpovidalnist' (*Tsentr polityko-pravovykh reform,* 29.04.2022) <https://pravo.org.ua/blogs/vtruchannya-v-robotu-informatsijno-komunikatsijnyh-system-kryminalna-vidpovidalnist> (accessed: 16.11.2023) (in Ukrainian).
3. 'Ukraina ne hotova do suchasnykh kiberatak – ekspert' (*Radio svoboda,* 14.12.2016) <https://www.radiosvoboda.org/a/28176636.html> (accessed: 16.11.2023) (in Ukrainian).
4. 'Ukrainski oblenerho atakuvaly virusom BlackEnergy – SShA' (*Multymediina platforma inomovlennia Ukrainy,* 31.01.2016) <https://www.ukrinform.ua/rubric-society/1944263-ukrajinski-oblenergo-atakuvali-virusom-blackenergy-ssha.html> (accessed: 16.11.2023) (in Ukrainian).

Dina Dryzhakova

LEGAL REGULATION IN THE FIELD OF COMBATING UNAUTHORIZED INTERFERENCE IN THE OPERATION OF INFORMATION AND TELECOMMUNICATION SYSTEMS, COMPUTER NETWORKS OR ELECTRICAL LANGUAGE NETWORKS

Abstract. The rapid pace of development of information and telecommunication technologies, systems and networks expands the possibilities of their use in various types of criminal and illegal activities. The increase in the number of cyberspace users contributes not only to the commission of criminal offenses against them, but also to the possibility of their participation in criminal activity, including in its organized forms.

It is worth noting that the phenomenon of crime in cyberspace is quite new for our country, but at the same time it has a significant degree of social danger and can be the object of encroachment on many social relations. The armed aggression of the Russian Federation became a certain catalyst for the development of a new high-quality system of cyberspace protection of Ukraine. This primarily concerns the improvement of the existing cyber security strategy of Ukraine, as well as the introduction of changes to the existing Criminal Code of Ukraine, regarding the issue of criminal liability for socially dangerous acts committed in cyberspace.

Keywords: regulatory and legal regulation; law; information and telecommunication system; cyber terrorism; cyber threat; telecommunications expertise; computer and technical expertise.