Секція 4.
ПРАВО

Дрижакова Діна Юріївна,
директор Товариства з обмеженою відповідальністю
«Юридична компанія «Пріма лідер груп»
Аспірант 1 курсу 081 Право Навчально-науковий інститут права,
кафедра кримінально-правової політики та кримінального права
КНУ ім. Тараса Шевченка
м. Київ, Україна

ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ОБ'ЄКТ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ), ЕЛЕКТРОННИХ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ, ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ

Виклики в інформаційному просторі змінюються постійно.

Сучасному періоду інтенсивного розвитку суспільства притаманне зростання ролі інформаційної сфери, що поєднує інформаційний простір та кіберпростір, яка є сукупністю інформації, інформаційної інфраструктури і суб'єктів, що реалізують регулювання інформаційних відносин у суспільстві. Інформаційна сфера постає системо-утворюючим чинником життя суспільства; вона здійснює активний вплив на стан воєнної, економічної, політичної, та інших сфер національної безпеки держави.

Тому різноманітного роду впливи на інформаційну систему країни як зовнішні, так і внутрішні, можуть завдавати їй серйозної шкоди.

Науково-технічна революція початку XXI ст. спричинила в усьому світі глибокі системні перетворення. Стрімкий розвиток інформаційних технологій, інформатизація та комп'ютеризація, створення глобального інформаційного простору сформували принципово нові

субстанції — інформаційне суспільство, інформаційний простір та кіберпростір, які мають невичерпний потенціал і відіграють важливу роль в економічному та соціальному розвитку країн світу. Разом з цим виникли такі нові терміни, як «кібербезпека», «кіберзагрози», «кібертероризм» тощо. Створення інформаційного суспільства призводить до виникнення багатьох інформаційних загроз та кіберзагроз.

Нормативно-правовою основою функціонування інформаційно-телекомунікаційних систем, комп'ютерних мереж та мереж електрозв'язку, технічного захисту оброблюваної в них інформації та кримінальної відповідальності за несанкціоноване втручання в їх роботу є Конституція України, закони України, Кримінальний кодекс України, 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 приводить до неврегульованості більшості злочинів, вчинених на просторах інформаційної інфраструктури, а в певних випадках навіть відсутність відповідальності.

Так, на сьогодні у Кримінальному кодексі України відповідальність за правопорушення у сфері використання комп'ютерних мереж та мереж електрозв'язку передбачена Розділом XVI.

Кримінальний кодекс досить вузько на сьогодні розглядає і описує правопорушення у даній сфері, не визначаючи на що в кінцевому підсумку спрямовуються такі правопорушення.

Стаття 361 КК України передбачає відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж передбачає відповідальність за ст. 361КК України.

Об'єктом аналізованих злочинів можуть бути суспільні відносини у сфері комп'ютерної інформації.

Предметом злочину в класичній теорії кримінального права визнаються речі матеріального світу, діючи на які особа посягає на цінності (блага), що належать суб'єктам суспільних відносин [1].

Протягом останніх років у всьому світі поширилися кібератаки на об'єкти критичної інфраструктури, завдаючи великих збитків економічній системі різних країн. Безліч критичних інфраструктур, зокрема електроенергетика, водопостачання, транспорт, у державі функціонують з використанням комп'ютерних систем диспетчерського управління та збору даних. Ці системи можуть піддаватися кібератаці, спрямованій на порушення їхнього функціонування, і, як наслідок, на заподіяння фізичної шкоди та руйнувань, наприклад, скидання води з дамби, переведення залізничних колій та в подальшому зіткнення поїздів, порушення роботи авіадиспетчерських служб та авіакатастрофи. Велику загрозу критично важливим об'єктам у світі становлять віруси-шифрувальники, зокрема суро, які проникають у мережі стратегічних об'єктів, АЕС, аеропортів, нафтопроводів, оборонних підприємств, великих заводів, викликаючи техногенні катастрофи. Збиток і втрати від таких проникнень у світі обчислюють сотнями мільйонів доларів [2].

Виходячи із кінцевої мети даних злочинів як об'єкт несанкціонованого втручання в роботу комп'ютерних мереж можна розглядати об'єкти критичної інфраструктури.

Критична інфраструктура — це сукупність об'єктів такої інфраструктури. Об'єкти критичної інфраструктури (далі — ОКТІ) — об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво національним інтересам [3].

Віднесення об'єктів до ОКІ та формування Переліку (реєстру) об'єктів критичної інфраструктури здійснюються відповідно до приписів ст. 8 Закону України «Про критичну інфраструктуру» від 16.11.2021 у порядку, встановленому КМ України, та має здійснюватися за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму.

До об'єктів критичної інфраструктури відносяться: підприємства, установи, організації незалежно від форм власності, які: 1) провадять діяльність та надають послуги у таких галузях: енергетика, хімічна промисловість, транспорт, комунікаційні технології, електронні комунікації, інформаційно-фінансовий сектор; банківський та 2) надають послуги у таких сферах життєзабезпечення населення: централізоване водопостачання, водовідведення, постачання електричної електроенергії і газу, виробництво продуктів харчування, охорона здоров'я; 3) аварійні та рятувальні служби, служби екстреної допомоги населенню; 4) мають стратегічне значення для економіки і безпеки держави; 5) підлягаю охороні та обороні в умовах надзвичайного стану і особливого періоду; 6) є об'єктами потенційно небезпечних технологій і виробництв. Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Водночас поряд з традиційними способами вчинення диверсійних та терористичних актів на ОКТ (вибухи, підпали тощо), терористами широко застосовуються новітні інформаційно-комунікаційні технології для порушення штатних режимів роботи автоматизованих систем управління технологічними процесами. Дедалі більшого розповсюдження у кіберпросторі набуває політично вмотивована діяльність у формі кібератак на державні та корпоративні інформаційні ресурси.

В умовах російської військової агресії та ведення гібридної війни проти України в числі загроз, Стратегія кібербезпеки-2021 виділила: російську гібридну агресію проти України у кіберпросторі; активну реалізацію російської концепції інформаційного протиборства, базованої на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої тривалий час активно застосовуються у гібридній війні проти України; російські кібератаки, спрямовані на інформаційно-комунікаційні системи державних органів України та інші ОКП з метою виведення їх з ладу, отримання прихованого доступу і контролю; вчинення російських актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури України [4].

Аналіз вироків по кримінальних провадженнях за ст. 361 КК України за період 2022 — початку 2023 років, внесених до Єдиного державного реєстру судових рішень, дозволяє стверджувати про відсутність на сьогоднішній день вироків щодо осіб, які здійснили

кібератаки, спрямовані на втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж установ, підприємств та організацій України з метою пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення.

Висновок: на сьогодні з урахуванням збройної агресії на Україну необхідно доповнити статті 361, 361[1] щодо санкцій за заподіяння шкоди через несанкціоноване втручання в комп'ютерні мережі об'єктам критичної інфраструктури, що призвело до тяжких наслідків.

Література

1. Кравцов С.Ф. Предмет злочину: Автореферат дисертації на здобуття наукового ступеня кандидат юридичних наук. 12.00.08. / Ленінградський державний університет ім. А.А. Жданова. — Ленінград, 1976. — С. 9.

2. Панов Н.І. Спосіб скоєння злочину та кримінальна відповідальність. — Харків : Вища школа, 1982. — С. 127–143.

3. Когут Ю.І. Гібридна війна нового типу як загроза національній безпеці держав. 2023/ Консалтингова компанія Сідкон. — С. 224–235.

4. Цього року РФ здійснила понад 550 кібератак на Україну. URL: https://lb.ua/society/2023/02/17/546281_tsogo_roku_rf_zdiysnila_ ponad_550.html

5. Науково-практичний коментар до Кримінального Кодексу України. Під загальною редакцією Потебенька М.О., Гончаренка В.Г. — К., — «ФОРУМ», 2001., у 2-х ч. — Особлива частина. — С 721.

6. Кримінальне право України: Особлива частина: Підруч. для студ. вищ. навч. зал. освіти / М.І. Бажанов, В.Я. Тацій, В.В. Сташис, І.О. Зінченко та ін.; За ред. Професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. — К. : Юрінком Інтер; Х. : Право, 2001. — С. 363.

7. Науково-практичний коментар до Кримінального кодексу України: За станом законодавства і Постанов Пленуму Верховного Суду України на 1 грудня 2001 р. / За ред. С.С. Яценка. — К. : А.С.К., 2002. — С.с. 783–784.