УДК 343
DOI https://doi.org/10.32782/2524-0374/2023-5/69

НЕПРАВОМІРНИЙ ВПЛИВ НА ІНФОРМАЦІЙНУ ІНФРАСТРУКТУРУ УКРАЇНИ

IMPROPER INFLUENCE ON THE INFORMATION INFRASTRUCTURE OF UKRAINE

Думчиков М.О., к.ю.н.,
старший викладач кафедри кримінально-правових дисциплін та судочинства
Навчально-науковий інститут права Сумського державного університету

Каріх І.В., к.п.н.,
старший викладач кафедри адміністративного, господарського права та фінансово-економічної безпеки
Навчально-науковий інститут права Сумського державного університету

Архішвидкі темпи розвитку інформаційно-телекомунікаційних технологій, систем та 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, у тому числі в її організованих формах. Відсутність фізичних кордонів кіберпростору дозволяє використовувати його з метою скоєння транснаціональних кримінальних правопорушень. Аналіз актуальності проблем, що розглядаються в статі, показує, що суттєвим профілактичним заходом поліпшення ситуації, за аналогією з розвитком подібних структур у розвинутих країнах, є об'єднання сил і засобів спеціальних служб з метою комплексного забезпечення необхідного рівня захищеності інформаційної критичної інфраструктури.

Масштабне захоплення кіберпростору простору представниками різних кримінальних кіл, лавиноподібне поширення заборонених контентів та активне паразитування на соціальних хворобах суспільства вимагають від кримінальної політики більш уважного та своєчасного реагування на подібні тенденції. В роботі наголошено на необхідності протидії злочинності у кіберпросторі шляхом попередження зазначених суспільно небезпечних діянь шляхом цілеспрямованого впливу на інформаційні потоки.

Зазначено, що незважаючи на нормативне регулювання питання встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі обмежується лише окремими суспільно небезпечними діяннями, оминаючи при цьому загрози інформаційній безпеці, зокрема посягання на інформаційно-телекомунікаційні технології, системи та мережі критичної інфраструктури держави, а також цифрової інформації, яка в них зберігається.

Наголошено на необхідності введення окремих ознак, які б обтяжували вчинення кримінальних правопорушень, об'єктами яких виступають інформаційно-телекомунікаційні технології, системи та мережі, які мають ознаки критичної інфраструктури.

Ключові слова: кримінальні правопорушення у кіберпросторі, кібертероризм, кібератака, кіберзлочин, кіберпростір.

The extremely fast 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. The absence of physical borders of cyberspace allows it to be used for the purpose of committing transnational criminal offenses. The analysis of the relevance of the problems considered in the article shows that an essential preventive measure to improve the situation, by analogy with the development of similar structures in developed countries, is the unification of the forces and means of special services in order to comprehensively ensure the required level of security of critical information infrastructure.

The large-scale takeover of cyberspace by representatives of various criminal circles, the avalanche-like spread of prohibited content and the active parasitism of social diseases in society require a more careful and timely response to such trends from criminal policy. The work emphasizes the need to combat crime in cyberspace by preventing the specified socially dangerous acts through purposeful influence on information flows.

It is noted that, despite the normative regulation, the issue of establishing criminal responsibility for committing criminal offenses in cyberspace is limited only to certain socially dangerous acts, bypassing threats to information security, in particular encroachment on information and telecommunication technologies, systems and networks of the state's critical infrastructure, as well as digital information , which is stored in them.

It is emphasized the need to introduce separate features that would aggravate the commission of criminal offenses, the objects of which are information and telecommunication technologies, systems and networks that have features of critical infrastructure.

Key words: criminal offenses in cyberspace, cyberterrorism, cyberattack, cybercrime, cyberspace.

Сьогодні однією з найважливіших завдань нашої держави виступає протидія злочинності у сфері інформаційно-телекомунікаційних технологій. Цифровізація, діджиталізація та стрімкий розвиток інформаційно-телекомунікаційних технологій, систем та мереж загалом , призводить до того, що злочинність у кіберпросторі породжує все нові методи та простори для здійснення протиправних суспільно небезпечних дій. Варто зауважити, що феномен злочинності у кіберпросторі для нашої держави є доволі новим, однак при цьому має значний ступінь суспільної небезпечності є 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 в існуючий Кримінальний кодекс України, щодо питання кримінальної відповідальності за суспільно небезпечні діяння, які вчиняються у кіберпросторі.

Інновації у сфері інформаційно-телекомунікаційних технологій сприяють не лише прогресивному економічному розвитку, а й призводять до появи нових форм кримінально-протиправних посягань на інформаційні інфраструктури критично важливих об'єктів. В нинішніх умовах інформаційно-телекомунікаційні технології можуть бути використані як засоби терору, війни та зброї.

Підвищення рівня суспільної небезпечності діянь, що вчиняються в інформаційній сфері, обумовлює необхідність підвищення захищеності критично важливих об'єктів інформаційної інфраструктури та одночасного посилення протидії загрозі розповсюдження злочинності у кіберпросторі. Здається, що руйнація інформаційної інфраструктури критично важливих і потенційно небезпечних об'єктів України шляхом неправомірного або несанкціонованого доступу до цифрової інформації з подальшим зараженням їх шкідливим програмним забезпеченням може завдати значної шкоди національній безпеці, а також призвести до екологічної катастрофи, людських жертв та інших тяжких і особливо тяжких наслідків.

Сьогодні спостерігається широка робота різних держав щодо створення кіберзброї, зокрема вірусів, шкідливого програмного забезпечення та поштових бомб. Перелі-

чену кіберзброю можна завчасно інсталювати на цифрові пристрої, або закласти в інформаційно-телекомунікаційні технології з наступним приведенням їх в дію через інформаційно-телекомунікаційні мережі або системи. Звичайно в теорії це виглядає доволі скептично, адже на практиці такі дії не призведуть до знищення критичної інфраструктурі у загальному розумінні, однак, нанести пошкодження інформаційно-телекомунікаційним технологіям інших держав, проникнути в їх критичну інформаційно-телекомунікаційну систему цілком реально. Результатом таких дій може буди паралізування військової комунікаційної інфраструктури держави.

Загалом, коли ми говоримо про кібертероризм, варто розуміти, що руйнівний характер вчинених дій безпосередньо пов'язаний саме з застосуванням інформаційно-телекомунікаційних технологій, систем та мереж. При цьому неважливо, чи спрямований він на порушення функціонування інформаційних об'єктів чи інших систем, що впливають на життєдіяльність суспільства.

Так, Ю. І. Когут, зазначає, що сьогодні кібертероризм є одним із найнебезпечніших видів тероризму в цілому, а його наслідки можуть бути катастрофічними. Терористичні акти в Сполучених Штатах Америки 11 вересня 2001 року та аварія в енергетичній системі в серпні 2003 року – наочні приклади [1, с. 255].

Сьогодні особи, які спеціалізуються на скоєнні кримінальних правопорушень з використанням інформаційно-телекомунікаційних технологій, дедалі частіше атакують державні, комерційні та інші інформаційно-телекомунікаційні мережі. Як приклад, можна навести ситуацію, яка склалася в сфері енергозабезпечення держави, зокрема, 23 грудня 2015 року за допомогою шкідливого програмного забезпечення «BlackEnergy», яке мало ознаки троянської програми було відключено близько 30 підстанцій Прикарпаття-обленерго, в зв'язку з чим більш 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п'яти годин [2].

Але напевно наймасштабнішою кібератакою яка була здійсненна на критичну державну інфраструктуру можна вважати 6 грудня 2016 року коли була здійсненна кібератака на системи та мережі Міністерства фінансів України, Державну казначейську службу України та Пенсійний фонд України. Особливістю цієї атаки було не просто було не просто блокування інформаційно-телекомунікаційних технологій, систем та мереж зазначених органів, алей й часткове видалення цифрової інформації, яка містилася у них [3].

Ще одним прикладом неправомірного впливу на критичну інфраструктуру України є випадок, коли внаслідок поширення шкідливого програмного забезпечення типу «Petya» була фактично заблокована діяльність таких державних компаній, як Укрпошта, Укртелеком та аеропорт Бориспіль. В даному конкретному випадку кібератака була спрямована на блокування комп'ютерів зазначених секторів інфраструктурних об'єктів держави [4].

За даними Департаменту кібербезпеки Служби безпеки України за 2022 рік було нейтралізовано понад 4.5 тисячі кібератак, а на перший квартал 2023 року 550. Також було зазначено, що здебільшого Російська Федерація атакує об'єкти логістики, енергетики, транспорту, військові об'єкти [5].

Варто зауважити, що на відміну від традиційних кримінальних правопорушень у кіберпросторі таких, як кіберхашрайство, кардинг, скімінг та фішинг, які займають 90% серед усіх вчинених суспільно небезпечних діянь у кіберпросторі і виконавцями яких виступають звичайні користувачі віртуального простору, кримінальні правопорушення, які націлені на об'єкти критичної інформаційної інфраструктури України вчиняються з кадрових співробітників розвідних управлінь, які здійснюють всі найсерйозніші атаки і мають необмежене фінансування.

Варто зауважити, що до вразливих місць інформаційно-телекомунікаційних технологій, систем та мереж кожного інформаційного об'єкта можна віднести: 1) протоколи передачі цифрової інформації; 2) закордонне комунікаційне обладнання; 3) програмне забезпечення в інформаційно – телекомунікаційному обладнанні; 4) сховища та бази даних з віддаленим доступом.

Варто наголосити на тому, що лише декілька країн у світі займаються підготовкою спеціалістів для здійснення кібератак, зокрема це Сполучені Штати Америки, Російська Федерація та Китайська Демократична Народна Республіка. Відповідно до даних голови компанії McAfee Дейва Ді Велта, всі перелічені країни активно займаються кібершпигунством та здійснюють інформаційні атаки щодо потенційних супротивників.

Звичайно, що сучасні загрози та виклики в рамках охорони кіберпростору нагально потребують підготовки спеціалістів з зазначеної сфери. Для прикладу в Китайській Народній Республіці військові відомства часто влаштовують олімпіади для майбутніх «хакерів». Так, Тан Дейлін, який був переможцем подібної олімпіади, потім здійснював кібератаки проти американських урядових відомств, результатом яких був витік більше тисячі секретних документів.

Слід зазначити, що в Європейському Союзі вже давно організовуються та проводяться великомасштабні національні, міжнародні та транснаціональні навчання з кібербезпеки. Такі навчання сприяють підвищенню рівня спеціальної підготовки керівного складу та підлеглих органів управління, сил та засобів кібербезпеки для належного забезпечення стійкого функціонування критично важливих об'єктів національної інфраструктури в умовах інформаційно-технічних впливів ймовірного супротивника [6].

Сьогодні в нашій державі питанням підготовки спеціалістів в рамках кібербезпеки відводиться багато часу. Відповідно до Стратегії кібербезпеки України від 26 серпня 2021 року утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України. Викладено, що інформаційно-телекомунікаційні технології можуть бути використані і як різновид зброї [7].

У багатьох країнах розробляються стратегії ведення віртуальної війни, між ними йде гонка кіберозброєнь, які створюються з метою виведення з ладу державних комп'ютерних мереж та об'єктів життєзабезпечення [8].

Питаннями протидії таким кримінальним правопорушенням стурбована вся світова спільнота, адже атаки проти об'єктів життєзабезпечення та оборони країни можуть призвести до глобальних жертв та руйнувань [9].

Одним із негативних наслідків бурхливого розвитку інформаційно-комунікаційних технологій та мережі Інтернет є поява нових форм міжнародних конфліктів, включаючи інформаційні та мережеві війни.

Виходячи з того факту, що кіберпростір все частіше становиться ареною протистояння, критично важливим є міжнародно-правове регулювання правовідносин, які виникають у ньому. На наше переконання, з метою удосконалення міжнародно-правового регулювання протидії тероризму, нагальним є потреба у розробці спеціальних міжнародних договорів, які повинні бути направлені на протидію новим терористичним викликам. Зокрема, потребує окремої міжнародної регламентації протидії кібертероризму, тобто тероризму з використанням можливостей кіберпростору, де інформаційно-телекомунікаційні технології, системи та мережі можуть виступати, як об'єкти посягання або засоби вчинення суспільно небезпечного діяння.

Зауважимо, що на нашу думку забезпечення міжнародної безпеки в рамках кіберпростору повинно базуватися

на розширенні зав'язків між країнами з метою вироблення спільних зусиль по боротьбі з суспільно небезпечними діяннями у кіберпросторі.

Варто відзначити, що міжнародне законодавство в сфері боротьби з кримінальними правопорушеннями у кіберпросторі має не досконалий стан. Фактично єдиним міжнародним актом, який наразі вважається еталонним, щодо питань встановлення кримінальної відповідальності за суспільно небезпечні діяння вчинені у кіберпросторі є Конвенція «Про кіберзлочинність». Однак, конвенція надає перелік обмеженій кількості правопорушень, які вчиняються шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж, залишаючи при цьому кібертероризм поза увагою [10].

Також, варто відмітити, що на дванадцятому зібранні Конгресу Організації Об'єднаних Націй по попередженню злочинності та кримінального правосуддя було поставлено питання протидії кіберзлочинності, і як результат була прийнята резолюцію в пункті 31 якої визначено, що законодавство щодо встановлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі в нинішній час формується в рамках національних та регіональних умов [11, с. 240].

Провідним способом боротьби з цією формою злочинності слід вважати використання норм національного кримінального права, яке найбільшою мірою відповідає поточному стану злочинності у цій сфері, а також інтересам держави та суспільства.

На відміну від більшості країн де законодавчо не визначений перелік об'єктів критичної інформаційної інфраструктури, Законом України від 16.11.2021 «Про критичну інфраструктуру» статтею 9 визначені основні сектори критичної інфраструктури https://zakon.rada.gov.ua/laws/show/1882-20#Text.

Нажаль, сьогодні в кримінальному законодавстві України немає спеціалізованої статті яка б передбачала кримінальну відповідальність за неправомірний або несанкціонований вплив на об'єкти критичної інформаційної інфраструктури держави. Загалом всі такі дії будуть кваліфікуватися за відповідними статтями XVI Особливої частини Кримінального кодексу України, залежно від наслідків, які були спричинені. На нашу думку виходячи із специфічного об'єкта аналізованих суспільно небезпечних діянь, немає нагальної потреби введення нових статей до Особливої частини Кримінального кодексу України, які б регулювали зазначені суспільно небезпечні діяння, однак при цьому вважаємо за необхідне ввести в рамках кваліфікуючих ознак, до відповідних статей XVI розділу Особливої частини Кримінального кодексу України наступне: 1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж критичної інфраструктури держави; 2) створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних засобів, щодо інформаційно-телекомунікаційних технологій, систем або мереж, що мають ознаки об'єктів критичної інфраструктури держави.

Особлива увага з боку держави має бути зосереджена на запобіганні діям, спрямованим на розв'язання проти неї інформаційних воєн, націлених на дестабілізацію системи національної безпеки.

Як інформаційна зброя можуть виступати абсолютно різні засоби: високоточна зброя для ураження органів управління або окремих радіоелектронних засобів, засоби радіоелектронної боротьби, джерела потужного електромагнітного імпульсу, програмні віруси та ін. Як критерій віднесення до розряду інформаційної зброї може розглядатися тільки ефективність того чи іншого пристрою під час вирішення завдань інформаційної війни.

Загалом ми вважаємо, що основними причинами, що породжують таку кримінальну ситуацію та сприяють зростанню кримінальних правопорушень, що посягають на інформаційні інфраструктури критично важливих та потенційно небезпечних об'єктів України, є: 1) поширення в засобах масової інформації матеріалів, які пропагують безкарність кібертерористів; 2) слабка готовність правоохоронних органів та спеціальних служб протистояти зазначеним суспільно небезпечним діянням; 3) відсутність необхідної профілактики у сфері боротьби з кримінальними правопорушеннями, які посягають на інформаційні інфраструктури критично важливих та потенційно небезпечних об'єктів.

Підсумовуючи вище зазначене хочемо акцентувати увагу та тому, що світовий кіберпростір є метою добре організованих кібератак. Методи та засоби, які використовуються для їх підготовки, постійно вдосконалюються. Такі кібератаки можуть бути спрямовані проти різних об'єктів критичної інформаційної інфраструктури не лише своєї, а й зарубіжних держав. Ефективна протидія кібератакам можлива лише в рамках спільних зусиль усіх заінтересованих країн, насамперед національних уповноважених органів у галузі виявлення та попередження комп'ютерних атак, та уніфікації міжнародного законодавства у сфері забезпечення безпеки критичної інформаційної інфраструктури.

ЛІТЕРАТУРА

1. Ю. І. Когут. Кібертероризм (історія, цілі, об'єкти). Практичний посібник. Київ : Консалтингова компанія «СІДКОН». 2021. 304 с.
2. Українські обленерго атакували вірусом BlackEnergy – США. Мультимедійна платформа іномовлення України. URL: https://www.ukrinform.ua/rubric-society/1944263-ukrajinski-oblenergo-atakuvali-virusom-blackenergy-ssha.html
3. Україна не готова до сучасних кібератак – експерт. Радіо свобода. URL: https://www.radiosvoboda.org/a/28176636.html
4. Як заражалася Україна: хронологія найбільшої в історії кібератаки. Економічна правда. URL: https://www.epravda.com.ua/publications/2017/07/20/627290/
5. 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
6. Міністри оборони країн ЄС проводять кібернавчання в Таллінні. Радіо свобода. URL: https://www.radiosvoboda.org/a/news/28722239.html
7. Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013
8. English, R. (Ed.). The Cambridge History of Terrorism. Cambridge University Press.https://doi.org/10.1017/9781139540902.
9. Havlíček, J. (2012). Threat of Cyberterrosim. Association for International Affairs Prague NATO Summit.https://www.amo.cz/wp-content/uploads/2016/01/PSS-Threat-of-Cyberterrorism-NATO.pdf
10. Конвенція «Про кіберзлочинність» від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
11. Голіна В. В. 12-й конгрес ООН із запобігання злочинності і кримінального правосуддя: комплексні стратегії на глобальні виклики. *Вісник Академії правових наук України* : зб. наук. пр. Харків. 2011. № 1. С. 238–244.