РОЗДІЛ 7
КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343
DOI https://doi.org/10.32782/2524-0374/2022-3/44

ПОНЯТТЯ ТА ОЗНАКИ КІБЕРПРОСТОРУ, ЯКІ РОБЛЯТЬ ЙОГО ПРИВАБЛИВИМ ДЛЯ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В СФЕРІ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

CONCEPTS AND FEATURES OF CYBERSPACE THAT MAKE IT ATTRACTIVE FOR COMMITTING CRIMINAL OFFENSES IN THE FIELD OF COMPUTER INFORMATION

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

Активне використання комп'ютерних технологій практично у всіх сферах суспільного життя, стало невід'ємною частиною сучасності. Можна наголосити, що 21 століття – є століттям цифрових та інформаційних технологій.

Ще декілька десятиліть назад про кримінальні правопорушення які вчиняються у кіберпросторі мало згадок, однак за короткий проміжок часу, вони почали нести не лише окрему загрозу для осіб чи суспільства, а й для держави в цілому. Ведення інформаційних воєн, кібертероризм, поширення ролі кіберзлочинності в житті окремого індивідуума є реаліями сьогодення. Багато правових відносин виникають та реалізуються в специфічному середовищі – кіберпросторі. Наразі як серед вітчизняних науковців так і зарубіжних, немає чіткого консенсусу щодо визначення поняття кіберпростір. Поняття кіберпростір є відносно новим адже фактично корелюється з розвитком інформаційного суспільства. Визначається, що більшість авторів співвідносить поняття кіберпростір з поняттям інтернет мережі. Стаття присвячена визначенню поняття кіберпростір та його основних ознак, на основі яких надано авторське визначення поняттю кіберпростір. Зокрема під кіберпростором на нашу думку варто розуміти своєрідне віртуальне середовище, яке складається з інформаційно-телекомунікаційних мереж, має транснаціональний характер, і не підпорядковується та не належить жодним суб'єктам. Крім того в науковій роботі визначаються та характеризуються основні особливості кіберпростору які роблять його привабливим для вчинення кримінальних правопорушень. Серед основних особливостей кіберпростору, що роблять його привабливим для зловмисників вбачаймо: анонімність як особливість, що забезпечує фактично повну безкарність особи яка вчиняє кримінальне правопорушення у кіберпросторі; дистанційність, тобто можливість особи займатися протиправною діяльністю у будь якій частині світу; транскордонний характер таких правопорушень, означає що для діянь у кіберпросторі немає просторових меж та латентність. Окремо звернули увагу на таку особливість як вік осіб та доступність матеріалів для здійснення протиправної діяльності в кіберпросторі.

Ключові слова: кіберпростір, кримінальне правопорушення у кіберпросторі, інтернет, інтернет мережа.

The active use of computer technology in almost all spheres of public life has become an integral part of modern times. It can be emphasized that the 21st century is the century of digital and information technologies.

Until a few decades ago, there were few mentions of criminal offenses committed in cyberspace, but in a short period of time, they began to pose not only a particular threat to individuals or society, but also to the state as a whole. Waging information wars, cyberterrorism, spreading the role of cybercrime in the life of an individual are the realities of today. Many legal relationships arise and are implemented in a specific environment – cyberspace. Currently, both among domestic and foreign scientists, there is no clear consensus on the definition of cyberspace. The concept of cyberspace is relatively new because it actually correlates with the development of the information society. It is determined that most authors correlate the concept of cyberspace with the concept of the Internet. The article is devoted to the definition of the concept of cyberspace and its main features, based on which the author's definition of the concept of cyberspace. In particular, in our opinion, cyberspace should be understood as a kind of virtual environment, which consists of information and telecommunication networks, has a transnational character, and is not subordinated or owned by any entities. In addition, the scientific work identifies and characterizes the main features of cyberspace that make it attractive for committing criminal offenses. Among the main features of cyberspace that make it attractive to attackers, we see: anonymity as a feature that ensures virtually complete impunity of a person who commits a criminal offense in cyberspace; remoteness, ie the ability of a person to engage in illegal activities in any part of the world; the cross-border nature of such offenses means that there are no spatial boundaries or latency for cyberspace actions. Special attention was paid to such a feature as the age of persons and the availability of materials for illegal activities in cyberspace.

Key words: cyberspace, criminal offense in cyberspace, internet, internet network.

Сьогодні спостерігається стрімке зростання різного типу інцидентів у галузі інформаційної безпеки, які мають загрозливий характер і набувають все більшого поширення не тільки в нашій країні, але і у світі в цілому. Варто зауважити, що багато таких загроз стосуються широкого кола приватних, державних, та корпоративних інтересів.

Інтеграція України у світовий інформаційний простір, розвиток суспільства нашої країни, як суспільства знань призвели до появи нових загроз її національним інтересам, пов'язаних з безпекою у кіберпросторі. Основними тенденціями розвитку загроз є: [1, с. 22].

- збільшення кількості атак, багато з яких призводять до великих збитків;
- підвищення складності атак, які включають кілька етапів і можуть використовувати спеціальні методи захисту від можливих контрзаходів;
- вплив практично на всі електронні (цифрові) пристрої, серед яких останнім часом все більшого значення набувають мобільні пристрої та найбільше піддаються ризикам у сфері інформаційної безпеки;
- дедалі частіші атаки на інформаційну інфраструктуру великих корпорацій, великих промислових підприємств і навіть державних установ;
- використання найбільш передових країн у сфері засобів комп'ютерної техніки та методів кібератак на інші країни.

Не дивлячись на різноманітність дискусій, які присвячені різним аспектам визначення дефініції поняття кіберпростору та характеристики його основних ознак, сам термін кіберпростір на нашу думку змістовного визначення не одержав. Термін кіберпростір на міжнародному рівні фігурує в Окінавській хартії та Конвенції про злочинність у сфері комп'ютерної інформації, однак в них немає дефініції поняття кіберпростір.

В національному законодавстві України поняття кіберпростору визначено в Законі України «про основні засади забезпечення кібербезпеки України» – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [2].

Доктринальне визначення поняття кіберпростір, досліджували як вітчизняні так і зарубіжні науковці, так в літературі часто поняття мережі Інтернет та кіберпростору синонімізуються, хоча ряд авторів відзначає нелогічність ототожнення кіберпростору та Інтернету.

Д. Мент під поняття кіберпростір розуміє певну конкретну точку з'єднання між комп'ютерами, яка перетворилася на глобальне віртуальне місце, а саму мережу Інтернет при цьому визначає виключно з функціональних позицій, передусім як соціальну структуру яка об'єднує різних індивідуумів з усього світу – користувачів мережі, розповсюджувачів інформації, сервіс-провайдерів та інших зацікавлених осіб [3]

Баррі Веллман розглядає кіберпростір як посередника, завдяки якому люди організовують свої справи та заповнюють час між зустрічами. Кіберпростір надає низку безперечних переваг: люди можуть спілкуватися онлайн саме з тими, з ким вони хочуть. Поряд з фізичним простором, що продовжує зберігати своє важливе значення, кіберпростір стає сукупністю кібермісць (cyberplace), завдяки яким індивіди знаходять або створюють нові спільноти, що отримали назву «віртуальні спільноти» [4].

Інформаційний аспект кіберпростору передбачає аналіз кіберпростору як сукупності незліченних інформаційних потоків, якими з неймовірною швидкістю курсує інформація, перекладена цифрову форму.

Д.В. Грибанов пропонує визначати кіберпростір через технічно – інформаційну базу на основі якої він функціонує. До складу цієї бази автор включає сукупність програмного забезпечення, за допомогою яких здійснюються обробка та передача інформації [5, с. 60].

Хилдрет С. А. у докладі Дослідницької служби Конгресу США, навпаки вважає, що оскільки кіберпростір є певним чином віртуальним полем яке може продукуватися в інфраструктурі інтернету, кіберпростір пропонується у значенні інтернет-простору, тобто як юридичний термін, що позначає наявність певної міжнаціональної юрисдикції [6].

Вітчизняні науковці, досліджуючи поняття кіберпростору, працюють переважно у загальнофілософському або ж у юридичному дискурсі. Так, у студіях щодо значення терміна «кіберпростір» О. Манжай пропонує таке визначення: «Це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами» [7, с. 145].

У свою чергу, А. Погорецький та В. Шеломенцев пропонують під «кіберпростором» розуміти – штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління й оброблення інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг ведення електронної комерції тощо)» [8, с. 80].

Для формування конкретної дефініції поняття кіберпростір, а також визначення його сутності спробуємо визначити його специфічні ознаки. На думку І. Рассолова кіберпростір має наступні ознаки:

1) об'єднує глобальні комп'ютерні мережі та інформаційні ресурси, що не мають чітко визначеного власника та забезпечують інтерактивну комунікацію фізичних і юридичних осіб;

2) взагалі не обмежений жодними кордонами;

3) має децентралізований статус, яким повністю не володіє та не управляє жодна держава, об'єднання держав, жодна міжнародна організація, а також жоден оператор зв'язку;

4) є простором, у якому будь-яка особа може вільно діяти, висловлюватися та навіть працювати [9, с. 116].

На нашу думку серед основних ознак кіберпростору варто виділити:

1) інформаційна складова (кіберпростір складається з інформаційно-телекомунікаційних мереж, інформаційних ресурсів та ЕОМ).

2) віртуальна складова (існування поряд з реальним світом).

3) транснаціональна складова (відсутність просторових меж).

4) нематеріальна складова (відсутність чіткого матеріального виміру);

5) децентралізованість (кіберпростір не може належати і бути повністю контрольованим окремим суб'єктом чи суб'єктами).

Таким чином можна визначити кіберпростір як своєрідне віртуальне середовище, яке складається з інформаційно-телекомунікаційних мереж, має транснаціональний характер, і не підпорядковується та не належить жодним суб'єктам.

Разом с тим вважаємо за необхідне визначити ознаки які роблять кіберпростір привабливим для вчинення зловмисниками кримінальних правопорушень, серед найбільш значущих можна виділити:

1. Відсутність географічних кордонів. Найхарактерніший атрибут Інтернету виявляється у тому, що географічні межі тут не відіграють жодної ролі. Кіберпростір – це електронний інформаційний простір комунікацій, що перевищує локальні межі, тобто Інтернет не є просто багато територіальним, а має між територіальний, загальний та глобальний характер. Тому при розслідуванні кримінальних правопорушень вчинених в кіберпросторі та наступної можливості покарання суб'єктів правопорушень, суттєво обмежені необхідністю їхньої реальної ідентифікації та іншими вимогами національного законодавства (обов'язкова фіксація необхідних доказів, виявлення самого юридичного факту – правопорушення, скоєного у «матеріальній формі» тощо).

2. Анонімність. Зловмисник може здійснювати протиправну діяльність з будь – якої точки світу. Джерело походження такої діяльності може бути прихованим або закодованим. Зловмисник може мати псевдонім або певну електронну ідентифікацію повністю відмінну від його реального ідентифікування. Як правило така протиправна діяльність у кіберпросторі дозволяє уникати відповідальності за таку кримінально протиправну діяльність. Сьогодні це помітно щодо зловживань авторськими правами, поширення наклепів, порнографії та ведення так званих інформаційних воєн.

3. Дистанційність кримінальних правопорушень які вчиняються у кіберпросторі. Зловмисники які мають спе-

ціальні знання про комп'ютерні мережі можуть викрасти декілька мільйонів у банківському секторі, розвернути супутник на 180 градусів, відключити в лікарні систему життєзабезпечення пацієнтів і при цьому знаходитися в будь якому куточку світу залишаючись непоміченим.

4. Вік осіб які вчиняють кримінальні правопорушення в кіберпросторі. Внаслідок того, що кримінальні правопорушення які зловмисники вчиняють у кіберпросторі є дуже прибутковою формою зайнятості, а сама інформація певні методичні вказівки щодо скоєння кримінальних правопорушень у кіберпросторі знаходиться у вільному доступі, спостерігається знижений вік суб'єктів таких кримінальних правопорушень.

5. Латентність. Кримінально-протиправні діяння які вчиняються у кіберпросторі наразі є найбільш латентним видом з поміж усіх сфер кримінально-противоправної діяльності. Це зумовлене тим, що особи які стали жертвами зловмисників, дуже часто не звертаються до органів до підслідності яких належить розслідування зазначених кримінальних правопорушень з причини недовіри до них. Часто самі суб'єкти онлайн електронної комерції не повідомляють те, що вони стали жертвами таких кримінальних правопорушень, щоб уберегти свою репутацію.

6. Доступність та велика кількість навчальних матеріалів за допомогою яких вчиняються протиправні дії у кіберпросторі. Наразі стати фахівцем який провадить свою протиправну діяльність у кіберпросторі дуже легко. На тернах інтернету в цілому та окремих хакерських форумах зокрема, можна отримати як безоплатне навчання за допомогою якого в подальшому можна здійснювати протиправну діяльність в кіберпросторі, так і пройти платне навчання. Різницю становить тільки якість навчання і подальша можливість заробляти за такий вид діяльності.

Як підсумок можна визначити, що кіберпростір – це новий життєвий простір сучасної людини незалежно від волі та свідомості кожного. Особистість є частиною цього середовища, оскільки більшість соціальних взаємодій у світі відбувається за допомогою інформаційно-комунікаційних технологій, продуктом яких є ця всеохоплююча цифрова реальність. Незважаючи на чисельні наукові дискусії щодо визначення поняття кіберпростір, спостерігається значні відмінності в підходах до його розуміння і залишається в край розмитим. Але пропонуємо визначати кіберпростір на основі визначення його основних ознак: інформаційність, віртуальність, транснаціональність та децентралізованість. Окрім того було визначено основні характеристики кіберпростору, які роблять його привабливим для скоєння кримінальних та інших правопорушень, зокрема анонімність, латентність, просторову межу та дистанційність. Перспективою дослідження теми вважаємо подальше вивчення природи кіберпростору та співвідношення з інформаційним інтернет простором.

ЛІТЕРАТУРА

1. Безкоровайний М.М., Татузов А.Л. Кібербезпека – підходи до визначення поняття. *Питання кібербезпеки*. 2014. № 1 (2). С. 22-27.
2. Закон України «Про основні засади забезпечення кібербезпеки України» від. 05.10.2017 № 2163-VIII.
3. Menthe D. C. Jurisdiction in cyberspace: A theory of international spaces. Michigan Telecommunications and Technology Law Review. 1998. Vol. 4. Pp. 69– 103. URL: http://www.mttlr.org/volfour/menthe.pdf (дата звернення 19.03.2022)
4. Wellman B. Physical place and cyberplace: the rise of personalized networking. *International Journal of Urban and Regional Research*. 2001. Vol. 25 (2). P. 247. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2427.00309 (дата звернення 19.03.2022)
5. Грибанов Д. В. К вопросу о правовой теории кибернетического пространства. *Государство и право*. 2010. № 4. С. 57–62.
6. Хілдрет С. А. Кібертероризм. Матеріали Дослідницької служби Конгресу. Доповідь Дослідницької служби Конгресу. URL: http://www.infousa.ru/information/bt-1028.htm. (дата звернення 19.03.2022)
7. Манжай О. В. Використання кіберпростору в оперативнорозшуковій діяльності. *Право і безпека. Науковий* журнал. 2009. № 4. С. 142–149.
8. Погорецький М., Шеломенцев В. Поняття кіберпростору як середовища вчинення злочинів. *Інформаційна безпека людини, суспільства, держави*. 2009. № 2. С. 77–81.
9. Рассолов И. М. Право и Интернет. Теоретические проблемы: монография, «Норма», 2009. 384 с.