УДК 343.1 (477):65.012.8+004

О. В. МАНЖАЙ
викладач кафедри інформаційної безпеки
навчально-наукового інституту психології, менеджменту,
соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ КІБЕРПРОСТОРУ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

Сьогодні високі технології активно впроваджуються в усі сфери людської діяльності. Майже одразу з появою комп'ютерних технологій з'явилися особи, які почали використовувати ЕОМ з протиправною метою. І якщо раніше це були люди, що мали досить великий обсяг знань та досвід у сфері високих технологій, то зараз є непоодинокими випадки, коли комп'ютерну техніку з протиправною метою використовують пересічні громадяни, що мають лише базові навички роботи з нею.

У зв'язку з наведеними обставинами правоохоронні органи не можуть лишатися осторонь і вже зараз активно протидіють кіберзлочинності.

Саме слово «кіберзлочинність» передбачає використання в процесі злочинної діяльності віртуального простору – кіберпростору. Відповідно і методи боротьби з такими злочинами в рамках здійснення оперативно-розшукової діяльності (далі – ОРД) повинні містити не лише стандартні прийоми, але й використання кіберпростору. Саме визначенню місця кіберпростору в оперативно-розшуковій діяльності присвячено дану статтю.

Уперше термін «кіберпростір» було використано у вжиток письменником В. Гібсоном у 1982 р. у новелі «Спалення Хром» («Burning Chrome»). У 1984 р. це поняття було більш детально розкрито у творі «Нейромант» («Neuromancer»). На думку В. Гібсона, кіберпростір (cyberspace) – це створена галюцинація, під дією якої щодня перебувають мільярди звичайних операторів у всьому світі. Це логічне представлення відомостей, збережених у пам'яті та на магнітних носіях комп'ютерів усього людства, потоки даних у просторі розуму; скупчення та сузір'я інформації [1, с. 32].

Термін «кіберпростір» став синонімом поняття «комп'ютерна віртуальна реальність».

Для того щоб з'ясувати значення слова «кіберпростір» у сучасному його контексті, необхідно дослідити його етимологію.

Як бачимо, термін «кіберпростір» є сполученням двох слів – «кібер» та «простір». Слово «**кібер»** походить від грецького κυβερ та означає *над*. Згідно з одним із визначень великого тлумачного словника сучасної української мови [2, с. 1170] під **простором** розуміють вільний великий обшир; просторінь; територію. Таким чином, буквально кіберпростір – це якась надтериторія. Якщо розглядати кіберпростір як скорочення словосполучення «кібернетичний простір», то кіберпростір – це простір (територія), який створений, працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки інформації) [2, с. 539]. Обидва визначення слова не повною мірою характеризують сутність кіберпростору, тому розглянемо думки різних учених стосовно цього поняття.

Близьким до визначення кіберпростору, наданого вище, є позиція Й. М. Дзялошинського. На його думку, кіберпростір – це сукупність певних структур (індивідів, їх груп і організацій), об'єднаних інформаційними відносинами, тобто відносинами збору, виробництва, поширення і споживання інформації [3].

Очевидно, що кіберпростір є *інформаційним* простором; саме цю його ознаку відзначають В. Д. Гавловський (кіберпростір як комп`ютерний інформаційний простір [4, с. 51]) та В. О. Голубєв, який у статті «Боротьба з комп'ютерними злочинами – проблема транснаціонального масштабу» визначає термін «кіберпростір» як інформаційний простір, що моделюється за допомогою комп'ютера, в якому існують визначені об'єкти або символьне уявлення інформації – місце, де діють комп'ютерні програми й переміщуються дані [5].

Кіберпростір є не лише інформаційним простором, але й *утворюваним за допомогою технічних систем комунікативним середовищем*. Цю його рису визначають О. Шмідтке (царина машинних процесів комунікації, в якій комунікаційні процеси здійснюються настільки незалежно, що комуніканти вільні від необхідності зустрічатися фізично» [6, с. 81]); С. В. Бондаренко (деяке узагальнене визначення

технічних систем, в яких користувачі здійснюють комп'ютерно-опосередковані інтеракції, одержують інформацію у візуальній, слуховій і тактильній формах про середовище, яке існує у формі даних, представлених у цифровому вигляді в комп'ютерних та аналогічних їм пристроях [7, с. 130–131]). В. Недбай узагалі асоціює кіберпростір з новою формою співтовариства [8, с. 157].

Досить нейтральним є визначення кіберпростору, надане Верховним судом США: унікальний носій, відомий його користувачам як кіберпростір, що не знаходиться на певній території, але доступний кожному в будь-якій точці світу через Інтернет [9].

У рекомендації «Про розвиток та використання багатомовності та загальному доступі до кіберпростору», прийнятій на 32-й сесії Генеральної конференції ЮНЕСКО у 2003 р., кіберпростір визначається як віртуальний світ цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою [10].

У нормативно-правових актах України безпосередньо термін «кіберпростір» зустрічається вкрай рідко, а тлумачення відсутнє. Так, наприклад, у «Типології легалізації (відмивання) доходів, одержаних злочинним шляхом в 2005–2006 роках», затверджені наказом Держфінмоніторингу України від 22 грудня 2006 р. № 265 [11] наголошується, що кількість злочинів у *кіберпросторі* зростає більш швидкими темпами порівняно з усіма іншими видами злочинів. Однак трактування поняття «кіберпростір» не наводиться.

Проаналізувавши наявні нормативно-правові документи та думки різних учених щодо тлумачення поняття «кіберпростір» можна сформулювати його комплексне визначення.

Отже, кіберпростір характеризується трьома основними ознаками:

– *це інформаційний простір;*

– *він є комунікативним середовищем;*

– *він утворюється за допомогою технічних систем.*

Таким чином, ***кіберпростір*** **–** *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.*

Правове регулювання відносин у кіберпросторі має велике значення, особливо в питаннях, що стосуються застосування національного права та компетенції держави (юрисдикції) в цій сфері. Ці питання досліджувалися як вітчизняними, так і зарубіжними спеціалістами, зокрема, В. Наумовим [12, с. 12–13], С. Уілске [13], Т. Лі [14], Д. Менте [15], Дж. Зітрейном [16] та ін.

Для того, щоб з'ясувати питання компетенції в кіберпросторі, перш за все, необхідно визначити зміст поняття «юрисдикція».

Юрисдикція (лат. jurisdictio – судочинство, від jus (juris) – право і dicere – говорити, проголошувати) – це повноваження давати правову оцінку фактам, розв'язувати правові питання [2, с. 1644].

У юридичній енциклопедії зазначено, що юрисдикція (в тому значенні, що нас цікавить) поділяється на *юрисдикцію держави* та *юрисдикцію міжнародну*. Юрисдикція держави поділяється на *територіальну* та *особисту* (національну). Юрисдикція територіальна зумовлюється суверенністю влади держави в межах її території, де вона має абсолютну юрисдикцію, за винятком випадків, коли відповідними міжнародними угодами не передбачається інше. Особиста (національна) юрисдикція держави поширюється на своїх громадян, які перебувають за межами її території (наприклад, у відкритому морі, в Антарктиці, в космічному просторі). В окремих випадках, передбачених національним законодавством, юрисдикція держави поширюється на громадян цієї держави, які перебувають на території іншої держави, однак здійснюватися така юрисдикція може лише на території своєї держави, якщо інше не передбачено міжнародними угодами. Юрисдикція міжнародна – це підсудність певної категорії справ міжнародним органам. Даний вид юрисдикції, на відміну від юрисдикції держави, є певним обмеженням державного суверенітету. Цей фактор зумовлює те, що для визнання юрисдикції будь-якого міжнародного органу необхідна явно виражена згода відповідної держави [17, с. 490].

Одним з основних завдань для визначення юрисдикції у сфері кіберпростору є встановлення факту поширення внутрішньодержавних правових норм на відносини в цьому середовищі.

У ст. 2 Конституції України [18] вказується, що суверенітет України поширюється на всю її територію. Згідно зі ст. 8 Конституції України вона має найвищу юридичну силу. Таким чином, законодавчо стверджується влада України над своєю територією.

На даний момент під територією держави розуміють не лише певну ділянку землі

область (сухопутна територія), але й води (внутрішні та територіальні води), повітряний простір, розташований над сушею і водами (тропосфера, стратосфера, іоносфера, а також значна частина вищерозміщеного простору). Надра, що знаходяться під сухопутною і водною територією, є приналежністю даної держави до технічно доступної глибини [19, с. 509].

Свого часу Г. Кельзен указував на те, що територія – не річ, зокрема, не земля або її частина. Це образний вираз, що позначає певне якісне право, територіальну сферу владитарності, національного юридичного порядку [20, с. 226].

Виходячи з наведених тверджень та самого визначення терміна «кіберпростір», його можна умовно розглядати як специфічний вид території, що не має геологічної основи, з усіма відповідними правовими наслідками.

Отже, кіберпростір у широкому сенсі можна співвіднести з поняттям «територія», тож необхідно з'ясувати її вид: міжнародна, державна або зі змішаним статусом. Крім того необхідно проаналізувати правові концепції, що можуть застосовуватися до кіберпростору.

Слід зазначити, що досить часто кіберпростір асоціюють зі поняттям «інтернет». Однак це велике узагальнення, яке не враховує окремі випадки. Так, кіберпростір можна розглядати як 1) ***локальне середовище*** при функціонуванні засобу комп'ютерної техніки (далі – ЗКТ), який не підключено до мережі, та як ***розосереджене середовище***, яке виникає в разі підключення ЗКТ до 2) *локальної* або 3) *глобальної мережі* передачі даних (інтернет).

У першому та другому випадках на кіберпростір безумовно має поширюватися відповідна територіальна юрисдикція. Щодо третього випадку, то багато юристів схиляється до думки про необхідність оголошення кіберпростору, який має транскордонні масштаби (інтернет), міжнародною територією на кшталт Антарктиди або космічного простору.

Найбільш обґрунтовану позицію щодо цього питання було викладено в роботі Д. Менте «Юрисдикція в кіберпросторі: теорія міжнародних просторів». У ній Д. Менте пропонує вважати інтернет територією, на яку не поширюється суверенітет окремої держави. Як аналогію автор наводить відносини в Антарктиді, космосі та нейтральних водах.

У той же час у деяких державах спостерігалися спроби встановити власну компетенцію над частиною інтернету [21] або поширити особисту юрисдикцію на окремі сфери діяльності в цьому середовищі [22].

Таким чином, зараз намітилися три шляхи вирішення питання щодо правового режиму інтернету і відповідно визначення компетенції держави в цій сфері:

1) інтернет є міжнародним простором, і його правовий режим має визначатися нормами міжнародного права;

2) інтернет є територією зі змішаним правовим режимом на кшталт континентального шельфу прибережних держав;

3) в окремих випадках інтернет можна віднести до державної території.

Оскільки питання регулювання відносин в інтернеті залишається не вирішеним на міжнародному рівні, Україні з цього питання слід керуватися основними принципами міжнародного права та чинним законодавством.

Після того, як було визначено поняття кіберпростору, його форми та компетенцію держави щодо нього, розглянемо питання застосування оперативно-розшукових повноважень в кіберпросторі.

Згідно зі ст. 8 Закону України «Про оперативно-розшукову діяльність» [23] оперативно-розшукові підрозділи наділено рядом прав, які можуть бути реалізовані в тому числі і в кіберпросторі.

Суб'єктами ОРД органів внутрішніх справ (далі – ОВС), яким найчастіше доводиться використовувати кіберпростір з оперативно-розшуковою метою, є відділ боротьби з кіберзлочинністю у структурі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми МВС України [24], та оперативні підрозділи Управління по боротьбі з правопорушеннями у сфері інтелектуальної власності та високих технологій, яке функціонує у Департаменті ДСБЕЗ МВС України [25].

Застосування оперативно-розшукових повноважень щодо українського сегмента кіберпростору не викликає значних правових питань. У той же час, якщо реалізація цих прав торкається іноземних юрисдикцій, можуть виникати певні правові неузгодженості. Причому швидкість з'єднання та відсутність кордонів, які роблять кіберпростір дуже зручним у користуванні, часто заважають правоохоронцям. Адже вони й самі інколи не можуть визначити, чи перетнули кордон.

Як приклад проблемних ситуацій можна навести потенційну необхідність оперативного огляду поштової скриньки, зареєстрованої на поштовому сервері в іншій країні, використання автентифікаційних даних для доступу до профілю користувача, зареєстрованого на

сервері, розташованого в межах іноземної юрисдикції тощо.

Базовим документом для ОВС у цій сфері є наказ Міністерства внутрішніх справ України від 15 травня 2007 р. № 158 «Про організацію міжнародної діяльності органів внутрішніх справ України» [26]. Зокрема, цим наказом затверджено Інструкцію про порядок організації співробітництва органів внутрішніх справ України з правоохоронними органами іноземних держав з питань попередження, розкриття та розслідування злочинів (далі – Інструкція).

Враховуючи основні принципи міжнародного права, міжнародний досвід [27], положення даної Інструкції, можна окреслити загальні правила поведінки українських правоохоронців у кіберпросторі. Оперативні працівники повинні докласти достатніх зусиль для з'ясування питання щодо розташування комп'ютерної системи, даних, очевидців (свідків) чи суб'єктів, причетних до злочину, в межах іноземної юрисдикції. Для визначення місця розташування об'єкта можуть використовуватися різні способи. Наприклад, можна перевірити загальнодоступну інформацію про розташування Інтернет-провайдера, який надає відповідні послуги (сервіс Whois).

Якщо виявиться, що один із вищеназваних об'єктів знаходиться за межами України, то в загальному випадку оперативники повинні діяти за Інструкцією, тобто через інститут співробітництва і лише через структурні підрозділи центрального апарату МВС України за напрямами службової діяльності, Управління міжнародних зв'язків та робочий апарат Національного центрального бюро Інтерполу в Україні [28, п. 3.2]. Ігнорування цієї вимоги може призвести до настання небажаних міжнародних наслідків, оскільки мова йде про порушення суверенітету іншої держави. Така ж процедура застосовується для отримання електронних доказів, які зберігаються за кордоном.

Слід зазначити, що збирання інформації з відкритих джерел шляхом використання кіберпростору не потребує залучення інституту співробітництва. Також в окремих випадках отримати доступ до відповідних електронних ресурсів, що знаходяться за кордоном, можна за дозволом адміністратора, який супроводжує даний ресурс.

Складними є випадки, коли оперативним працівникам необхідно через кіберпростір спілкуватися з очевидцями злочину або особами, що становлять оперативний інтерес, з інших країн. Такі дії можуть викликати занепокоєння інших держав щодо контактів їх громадян з іноземцями, особливо якщо правоохоронці працюватимуть під вигаданими іменами. Тому перед учиненням таких дій необхідно ретельно зважити всі ризики та вигоди. У разі виникнення ускладнень необхідно провести консультації з особою, відповідальною за організацію та координацію міжнародної діяльності у складі свого підрозділу. Таким же чином слід діяти в разі використання кіберпростору для спонукання особи, що становить оперативний інтерес, до прибуття в Україну.

Підбиваючи підсумки, необхідно зазначити, що на даний момент у правоохоронних органів України існує гостра необхідність у розробці наказу та методичних рекомендацій щодо здійснення оперативно-розшукових заходів шляхом використання кіберпростору. Впровадження таких документів у практичну діяльність дозволить заповнити наявні прогалини в цій сфері.

Література

1. Gibson W. Neuromancer / W. Gibson. – London : HarperCollins, 1994. – 271 p.
2. Великий тлумачний словник сучасної української мови (з дод. і допов.) / [уклад. і голов. ред. В.Т. Бусел]. – К. ; Ірпінь : Перун, 2005. – 1728 с.
3. Дзялошинский, И. Права человека в киберпространстве [Електронний ресурс] / И. Дзялошинский. – Режим доступу : http://www.dzyalosh.ru/02-dostup/pravo/2003_83_84%2811_12%29/dz_11_12.html.
4. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) / В. Гавловський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2000. – С. 50–53.
5. Голубєв В. О. Боротьба з комп'ютерними злочинами – проблема транснаціонального масштабу [Електронний ресурс] / В. О. Голубєв. – Режим доступу : http://www.crime-research.ru/library/Cybercr.htm.
6. Schmidtke O. Berlin in the Net: Prospects for Cyberdemocracy From Above and From Below / O. Schmidtke ; in R. Tsagarousianou D. Tambini & C. Brya (Eds.), Cyberdemocracy: Technology, Cities and Civic Networks. – London : Routledge, 1998. –P. 60–83.
7. Бондаренко С. В. К вопросу о таксономии киберпространства / С. В. Бондаренко // Рационализм и культура на пороге третьего тысячелетия : материалы Третьего российского философского конгресса

(16–20 сентября 2002 г.). Т. 4. – Ростов-н/Д : Изд-во СКНЦ ВШ, 2002. – С. 130–131.

8. Недбай, В. Віртуальні співтовариства як нова форма суспільної самоорганізації [Електронний ресурс] / В. Недбай // Освіта регіону. Політологія, психологія, комунікації. – 2008. – № 1–2. – С. 154–157. – Режим доступу : www.nbuv.gov.ua/portal/Soc_Gum/Or/2008_1_2.pdf.

9. Reno V. ACLU / 117 S.Ct. 2329, 2334–35.

10. Рекомендация о развитии и использовании многоязычия и всеобщем доступе к киберпространству [Електронний ресурс]. – Режим доступу : http://www.unesco.ru/docs/multilingv-ciberspace-recom-rus.pdf.

11. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом в 2005–2006 роках, затверджені наказом Держфінмоніторингу України від 22 груд. 2006 р. № 265 // Українська інвестиційна газета. – 2007. – № 44.

12. Наумов В. Б. Право и Интернет: очерки теории и практики / В. Б. Наумов. – М., 2002. – 432 с. : ил.

13. Wilske S. International Jurisdiction in Cyberspace: Which States May Regulate the Internet? [Електронний ресурс] / S. Wilske, T. Schiller. – Режим доступу : http://www.law.indiana.edu/fclj/pubs/v50/no1/wilske.html.

14. Lee T. In Rem Jurisdiction in Cyberspace [Електронний ресурс] / T. Lee // Wash. L. Rev. – 1997. – № 75. – Режим доступу : http://cyber.law.harvard.edu/property00/jurisdiction/lee.html.

15. Menthe D. Jurisdiction In Cyberspace: A Theory of International Spaces [Електронний ресурс] / D. Menthe // Mich. Telecomm. Tech. L. Rev. – Режим доступу : http://www.mttlr.org/volfour/menthe.html.

16. Zittrain J Jurisdiction in Cyberspace [Електронний ресурс] / J. Zittrain. – Режим доступу : http://cyber.law.harvard.edu/ilaw/mexico_2006_module_9_jurisdiction.

17. Юридична енциклопедія : в 6 т. Т. 6 Т–Я / [редкол. : Ю. С. Шемшученко (голова редкол.) та ін.]. – К. : Укр. енцикл., 2004. – 768 с. : іл.

18. Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

19. Большая советская энциклопедия : в 30 т. Т. 25. Струнино – Тихорецк / [гл. ред. А.М. Прохоров]. – Изд. 3-е. – М. : Советская энциклопедия, 1976. – 600 с. : с илл.

20. Kelsen H. Principles of International Law / Hans Kelsen. – New York : Rinehart & Company Inc., 1952. – 461 p.

21. Великий китайский фаервол [Електронний ресурс]. – Режим доступу : http://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%B8%D0%B9_%D0%BA%D0%B8%D1%82%D0%B0%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%84%D0%B0%D0%B9%D1%80%D0%B2%D0%BE%D0%BB.

22. Minnesota v. Granite Gate Resorts, Inc., 1996 WL 767431 (Minn. Dist. Ct. 1996) [Електронний ресурс] / Court File No. C6-95-7227. – Режим доступу : http://www.loundy.com/CASES/Minn_v_Granite_Gate.html.

23. Про оперативно-розшукову діяльність : закон України від 18 лют. 1992 р. // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303.

24. У Міністерстві внутрішніх справ України створено відділ боротьби з кіберзлочинністю [Електронний ресурс]. – Режим доступу : http://www.mvs.gov.ua/mvs/control/main/uk/publish/article/243867.

25. Про створення у структурі ДСБЕЗ підрозділів по боротьбі з правопорушеннями у сфері інтелектуальної власності та високих технологій : наказ МВС України від 31 трав. 2001 р. № 429.

26. Про організацію міжнародної діяльності органів внутрішніх справ України : наказ МВС України від 15 трав. 2007 № 158.

27. Перепелиця М. М. Провадження оперативно-розшукових заходів у Великій Британії, Росії, США та Україні : монографія / М. М. Перепелиця, О. В. Манжай. – Х. : Друкарня № 13, 2008. – 248 с. : іл.

28. Інструкція про порядок організації співробітництва органів внутрішніх справ України з правоохоронними органами іноземних держав з питань попередження, розкриття та розслідування злочинів, затверджена наказом МВС України «Про організацію міжнародної діяльності органів внутрішніх справ України» від 15 трав. 2007 р. № 158.

Надійшла до редколегії 12.11.2009

Анотації

Досліджено питання визначення поняття «кіберпростір», його форми, питання юрисдикції в кіберпросторі та повноваження правоохоронних органів щодо його використання.

Исследованы вопросы определения понятия «киберпространство», его формы, вопросы юрисдикции в киберпространстве, а также полномочия правоохранительных органов по его использованию.

The problems of the notion determination «cyberspace», its forms, jurisdiction problems in cyberspace and also authorities of law enforcement agencies of its use are researched.