Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Кіберпростір як складова інформаційної сфери: проблема правової інституалізації

Яременко О.І.
кандидат наук з державного управління, доцент
завідувач кафедри правових наук та філософії
Вінницького державного педагогічного університету ім. М. Коцюбинського

Ключову роль у розвитку сучасної інформаційної сфери соціуму відіграють комп'ютерні технології, завдяки яким виникають широкі можливості для інформаційної діяльності, створення електронних моделей різноманітних соціальних інститутів та явищ, ефективно здійснюються соціальні комунікації. Як наслідок, паралельно з об'єктивним фізичним світом та суб'єктивними уявленнями про нього, виникає нова реальність, яка отримала назву віртуальної. Науковцями, ще в 1995 році, було відзначено тенденцію домінування віртуальної реальності над фізичною і здійснено прогноз щодо майбутнього перетворення її на основну форму існування соціального середовища [1, с. 17]. У зв'язку з цим актуалізуються наукові дослідження окремих складових віртуальної реальності, зокрема, поняття «кіберпростір».

Правові аспекти кіберпростору є предметом дослідження О.В. Арістової., О.А. Баранова, К.І., Бєлякова, В.М. Брижка, Д.В.Дубова, Р.А. Калюжного, О.В.Копана, В.К Конах, Б.А. Кормича, О.В. Кохановської, О.В. Марущака, Н.А. Савінової, В.С. Цимбалюка, М.Я.

Метою даної статті є аналіз проблеми правової інституалізації кіберпростору як складової інформаційної сфери.

В праці одного із перших дослідників проблем кіберпростору Кетша Е. зазначається, що концептуально це поняття пов'язано з розвиненою електронною культурою, яка дозволяє обробляти та працювати з інформацією в електронній формі, з використанням складних комп'ютерів, які зберігають та аналізують дані та дозволяють здійснювати комунікації незалежно від місця знаходження [2, с. 414].

В сучасній науці спостерігається поліваріантність підходів до кіберпростору. Дубов Д.В. трактує його як середовище, створене організованою сукупністю інформаційних процесів на підставі об'єднаних загальними принципами та правилами інформаційних, телекомунікаційних та інформаційно- телекомунікаційних систем незалежно від форми власності [3, с. 314].

На думку Рибки С.В., кіберпростір - це середовище, утворене організованою сукупністю інформаційних процесів (створення інформації, передача, використання) за участю людини, зокрема, на об'єктах критичної інфраструктури держави із застосуванням ресурсів складових частин національної інформаційно-комунікаційної інфраструктури [4, с. 128].

Фурашев В.М. розглядає кіберпростір як форму співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на породження, сприйняття, запам'ятовування, переробку та обмін інформацією. Науковець підкреслює, що кіберпростір є дуже складним явищем, що об'єднує в собі реальність і віртуальність, матеріальне і нематеріальне, абстрактність і дійсність і має наступні властивості: протяжність; єдність дискретності та неперервності; матеріальність та нематеріальність; абстрактність і дійсність; реальність загальнодіючого впливу [5, с. 164].

Гаков С.О., аналізуючи кібернетичний простір з точки зору сферу соціальної діяльності, зазначає, що його зміст складають суспільні відносини між володільцями інформаційних систем, власниками інформації, споживачами (користувачами), спеціально уповноваженими державними органами, роботодавцями, працівниками, юридичними та фізичними особами – виробниками ІТ-продукції та ІТ-послуг тощо; правові норми, які регулюють відповідні суспільні відносини, визначають правові режими інформації, інформаційних систем (їх компонентів) та технологій, юридичну відповідальність тощо; практична діяльність людини щодо створення кіберпростору, реалізації інформаційної технології та її підтримання у працездатному стані, забезпечення кібербезпеки особи, суспільства та держав тощо [6, с. 55].

Обґрунтування юридичною наукою теоретичних основ кіберпростору та нормативне закріплення цього поняття ускладняється багатьма факторами, зокрема, його нематеріальною природою. Ключовою характеристикою кіберпростору є належність його до інформаційної сфери, яка розуміється як глобальне системо утворююче явище життєдіяльності суспільства та держави, що складається із сукупності впорядкованої та стихійної соціоприродної інформації, а також системи індивідуумів та інституцій, які забезпечують її обіг, соціальні комунікації та спілкування [7, с. 12]. Вважаємо, що в процесі наукової ідентифікації поняття «кіберпростір», важливе методологічне значення має введення Арістовою О.В. та Чернадчук Т.О. у науковий обіг категорії "інтегративна інформаційна сфера", яка за інформаційним критерієм (тобто за циркуляцією інформації) об'єднує усі

сфери суспільного життя, у тому числі й інформаційну [8, с. 49]. При цьому, кіберпростір є своєрідним «провідником» інформаційних процесів і домінуючою частиною інформаційної сфери сучасного соціуму.

Аналіз зарубіжного досвіду правової інституалізації кіберпростору свідчить про те, що характерною рисою цього процесу є прив'язка до проблем інформаційної безпеки. Так, в доповіді Міністерства оборони США "Операції в кіберпросторі", кіберпростір визначається як глобальний домен в інформаційному середовищі, що складається з взаємозалежної мережі інформаційних технологій, інфраструктури та резидентних даних, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори та контролери. Аналогічна дефініція кіберпростору застосовується в об'єднаній оборонній доктрині Міністерства оборони Великобританії [9, с. 5].

В Україні кіберпростір також розглядається, перш за все, з точки зору інформаційної безпеки держави. Так, в Стратегії кібербезпеки зазначається, що кіберпростір поступово перетворюється на окрему, поряд із традиційними "Земля", "Повітря", "Море" та "Космос", сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу [10].

Слід відзначити, що універсальність та глобальність кіберпростору обумовлює необхідність встановлення міжнародних стандартів щодо його захисту. При цьому, перед міжнародним співтовариством виникають проблеми, які виникала при впорядкуванні використання та захисту морського та космічного простору, а також Антарктиди [11].

Важливе значення для України має прийняття Закону «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки. Він містить легітимне визначення кіберпростору як середовища (віртуального простору), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утвореного в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечує електронні комунікації з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [12]. Аналіз цієї дефініції свідчить, що в її основу покладено функціональну сутність кіберпростору. Водночас, кіберпростір є більш багатогранним явищем і містить в собі технічні, енергетичні, інтелектуальні, контентні складові, сутність а зміст яких може бути предметом подальших досліджень з метою вдосконалення нормативно – правової бази в цій сфері.

Література:

1. Biocca F., Levy M. Virtual reality as a communication system / F. Biocca, M Levy // Communication in the Age of Virtual reality. – Hillsdale. – Lawrence Erlbaum Associates. – 1995. – 395 p. – p. 15 - 31.
2. Katsh E. Law in a Digital World: Computer Networks and Cyberspace / E. Katsh // Villanova Law Review. – 1993. – Vol. – 38. – Iss 2. – p. 403 – 486.
3. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д.В. Дубов. – К. : НІСД, 2014. – 328 с.

The ransomware "Petya" as a challenge to the cybersecurity of Ukraine, main factors of spreading this virus in the focus of Ukraine, the steps taken by the authorities to combat this phenomenon and suggest ways to improve such activities using experience of other countries

Victor Zhoghov
Deputy Chief of information systems administration
Department of information and analytical support
The main Department of the National police in Vinnytsia region
Senior lieutenant of police

Formulation of the problem

On June 27, a large-scale cyber attack was recorded in Ukraine using a new modification of the Petya ransomware, which partially affected companies in Russia, the United States, India, and Australia. A preliminary investigation showed that the pro-state Black Energy group that had previously attacked energy and financial organizations in Ukraine was behind the attack.

According to preliminary estimates, about 80 companies have been attacked, with the majority of them located in Ukraine. The list of victims includes large Ukrainian banks and enterprises, namely, Oschadbank, Ukrgasbank, Pivdenny Bank, OTP Bank, TASKombank, The Epicenter chain store, Kovalska industrial and