DOI: https://doi.org/10.32839/2304-5809/2021-4-92-58
УДК 342.9

**Пахомов В.В., Каріх І.В., Репін Д.А.**
Сумський державний університет

## МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРПРОСТОРУ

**Анотація.** XXI століття ознаменоване стрімким розвитком інформаційних технологій, застосування яких не знає і не дізнається кордонів: на сьогоднішній день вони є інструментом вдосконалення систем управління, продажів, надання послуг у соціальній та кредитно-фінансовій сферах, в освіті, охороні здоров'я, культурі і т.п. Однак, інформаційні технології стали не тільки «помічниками», вони стали «самостійними» учасниками в житті суспільства, а потім і «творцями» особливої соціальної середовища. Ми говоримо про кіберпросторі, як про комп'ютерно-технологічної реальності в якому існує і розвивається соціум: тут є своя законодавча, всі необхідні об'єднання і служби, це суспільство здатне спілкуватися (наприклад, в соціальних мережах), задовольняти свої потреби (духовні, престижні, соціальні, екзистенційні, тобто 4 з 5 груп, відповідно до пірамідою А. Маслоу) здійснювати підприємницьку (на сьогоднішній день можна створювати інтернет-магазини, віртуальні школи і т.п.) або трудову діяльність (людина може стати IT-спеціалістом, фрілансером, онлайн продавцем і ін.). Таким чином, у віртуальній реальності людина може робити практично все, і дане наріччя з кожним роком все менше затребуване в даному контексті.

**Ключові слова:** кіберспорт, кіберспортивна організація, комерційна організація, некомерційна організація, правовий статус, кіберспортивний.

**Pakhomov Volodumyr, Karikh Igor, Repin Danilo**
Sumy State University

## INTERNATIONAL LEGAL REGULATION OF CYBERSPACE

**Summary.** This article attempts to consider various issues of legal regulation of the activities of an e-sports organization (club). The history of the emergence and legal regulation of eSports in Ukraine and abroad is considered. Disclosed the issues of regulation of cybersport activity in Ukraine from the point of view of organizational and legal formation in Ukrainian legislation. Some legal problems related to the regulation of the activities of an e-sports organization (club) as an active unit of a rapidly developing type of activity all over the world have been studied. It is concluded that the considered legal issues are not exhaustive and each of them taken separately may constitute a separate study. However, the beginning of their solution is the creation of a unified international legal framework on cybersport and the organization of a structured system of governing bodies for this sport. The 21st century is marked by the rapid development of information technologies, the use of which does not know and does not recognize boundaries: today they are a tool for improving management systems, sales, provision of services in the social and credit and financial spheres, in education, healthcare, culture, etc. However, information technologies have become not only "helpers", they have become "independent" participants in the life of society, and then the "creators" of a special social environment. We are talking about cyberspace as a computer-technological reality in which society exists and develops: it has its own legislative, all the necessary associations and services, this society is able to communicate (for example, in social networks), satisfy its needs (spiritual, prestigious, social , existential, that is, 4 out of 5 groups, in accordance with A. Maslow's pyramid) carry out entrepreneurial (today you can create online stores, virtual schools, etc.) or work (a person can become an IT specialist, freelancer , online seller, etc.). Thus, in virtual reality, a person can do almost everything, and this adverb is less and less in demand in this context every year. The legal issues discussed are not exhaustive and each of them separately may represent a separate study. However, the beginning of their solution is the creation of a unified international legal framework on e-sports and organization of a structured organ system management of this sport.

**Keywords:** e-sports, e-sports organization, commercial organization, non-profit organization, legal status, esports.

**Постановка проблеми.** Технології, що з'явилися в останнє десятиліття зробили популярним поняття – кіберпростір. Розвиток інформаційного суспільства передбачає впровадження інформаційних технологій в усі сфери життя, але це означає і появу нових загроз безпеки – від витоків інформації до кібертероризму. За оцінками експертів, матеріальна шкода світовій економіці від злочинів, що здійснюються за допомогою інформаційно-комунікаційних технологій, обчислюється трильйонами доларів США. Такі масштаби вимагають ефективних засобів правового регулювання відносин, що складаються в кіберпросторі. У зв'язку з цим міжнародне співтовариство проявляє серйозну зацікавленість в розробці багатосторонньої правової основи співпраці в області кібербезпеки.

**Аналіз останніх досліджень і публікацій.** Аналіз наукових публікацій В. Гібсона, М. Камчатного, О. Манжая, Л. Бурячка, Б. Толубка, В. Хорошка, С. Гнатюка та ін. щодо розкриття суті та значення поняття «кіберпростір», показав, що всі вони тлумачать це по-різному. Законодавства окремих країн показує також різні підходи до кібербезпеки, яка теж трактується ними по-різному.

Міжнародні реалії свідчать про низку важливих проблем, що заважають ефективно протидіяти загрозам у кіберпросторі.

**Мета статті** полягає у систематизації положень міжнародних нормативно-правових норм, що регламентують функціонування та регулювання кіберпростору. Відповідна систематизація надасть змогу розкрити понятійний

апарат проблематики регулювання кіберпростору як складової інформаційного простору, визначити та оцінити його ключові складові.

**Виклад основного матеріалу дослідження.** Незважаючи на те що, термін «кіберпростір» був введений в науковий обіг відносно недавно, але все частіше його використовують у правовій доктрині та на практиці. Сьогодні зазначене поняття можна зустріти в міжнародно-правових актах, національних джерелах права, а також в доктринальних працях зарубіжних та вітчизняних науковців Науковці зазначають, що вперше дане поняття було використано канадським письменником-фантастом В. Гібсоном в оповіданні «Спалення Хром» в 1982 р. Автор пише про кіберпростір як про середовище «Чуттєвих галюцинацій, які випробовуються щодня мільярдами операторів всіх націй, в тому числі і дітей, які вивчають математичні науки ... Графічне відображення даних комп'ютерів, що належать людям. Немислима складність. Потоки світла, впорядковані людським розумом, скупчення і сузір'я інформації» [1]. Таким чином, завдяки роботам Гібсона, поняття «кіберпростір» міцно зміцнилося в масовій свідомості і багато в чому визначило сучасну культуру сприйняття простору і часу.

За даними американського експерта Ф.Д. Крамера, в західній науковій доктрині налічується близько 28 визначень «кіберпростору». Олександр Войскунський визначає кіберпростір як «наявність якогось світу, що володіє протяжністю і метрикою представленого в свідомості», уточнюючи, що в свідомості різних людей воно представлено, найімовірніше, по-різному. Особливістю світу кіберпростору є зберігання практично необмежених обсягів інформації і розваг, а також надання індивідам «можливостей для незліченних способів самовираження» [2, с. 65]. Французький проф. С.І. Лоран вказує, що «кіберпростір – це соціально-технічна реальність, яка глибоко пов'язана з політичним контекстом» [3]. Баррі Уеллман розглядає кіберпростір як посередника, завдяки якому люди організовують свої справи і заповнюють час між зустрічами [4].

Деякі держави все ж пропонують власне визначення згаданого поняття. Дослідницькою службою Конгресу США було запропоновано визначення кіберпростору як «безліч всеосяжних зв'язків між людьми, створеного на основі комп'ютерів і телекомунікацій незалежно від фізичного та географічного положення» [5]. В той же час Міністерство оборони США вважає, що кіберпростір – це «сфера (область), в якій застосовуються різні РЕЗ (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління і наведення) для прийому, передачі, обробки, зберігання, видозміни (трансформації) інформації і пов'язана з ними інформаційна інфраструктура ВС» [6]. У Німеччині кіберпростір – це вся інформаційна структура, яка доступна через Інтернет поза будь – якими територіальними кордонами [7, с. 62].

В Україні 5 жовтня 2017 року був прийнятий Закон «Про основні засади забезпечення кібербезпеки України», який регламентує кіберпростір, як 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 [8].

В Китаї з 1 червня 2017 року вступив в силу Закон «Про кібербезпеку» , який регламентує дії постачальників мережевих продуктів і послуг зі збирання, зберігання і обробки даних користувача; порядок і специфіку забезпечення безпеки інформаційної інфраструктури в стратегічно важливих галузях. Головною метою прийняття Закону проголошується захист національного «кіберсуверенітета» КНР [9].

Вважається, що проблематика кіберпростору, в цілому, і кібербезпеки, зокрема, актуалізувалася внаслідок війни в Перській затоці 1990–1991 рр., використання новітніх військових технічних досягнень супроводжувалося потужною інформаційною кампанією і освітленням в пресі [10].

Прикладом використання кіберпростору з неправомірною метою є кібератака, безпосередньо спрямована проти національної безпеки Естонії 2007 р. Передумовою такого втручання вважається рішення уряду Естонії про переміщення пам'ятника радянським воїнам часів Другої світової війни із центру Таллінна на його околиці. Це рішення спровокувало хвилю атак на численні інтернет – сайти Естонії. У результаті втручання хакерів протягом декількох тижнів були неспроможні функціонувати в нормальному режимі урядові, банківські сайти й інформаційні системи, сайти багатьох засобів масової інформації, громадських організацій. Хакерам вдалося навіть ненадовго вимкнути сервіс невідкладної допомоги, який функціонував завдяки мережі Інтернет. Відновлення повноцінного функціонування інформаційної інфраструктури потребувало певного часу та значних фінансових потреб [11, с. 16].

Дж. Карр стверджує, що кібервійна не повинна спричинити реальних фізичних наслідків, тобто це «боротьба без крові». Д. Дубов зазначає, що кібервійна буде вважатися такою виключно якщо буде завдано певної сукупності кібератак.

Протягом тривалого періоду часу в науковому співтоваристві триває дискусія щодо питання: чи можливо застосовувати існуючі міжнародно-правові норми до кіберпростору або необхідно зробити нові правила регулювання цієї сфери відносин?

Припущення про те, що міжнародно-правові зобов'язання держав, включаючи зобов'язання, що випливають з міжнародних договорів, які не застосовні до кіберпростору, привело б нас до висновку про відсутність правового регулювання і свободи держав від яких-небудь міжнародно-правових зобов'язань в цій сфері. Іншими словами, ми б зіткнулися з правовою прогалиною, наявність якого дозволило б поставити під сумнів державний суверенітет в кіберпросторі, а поряд з цим, викликало б необхідність прийняти для кіберпростору нових норм, які не грунтуються на принципах Статуту ООН. З цієї причини для нас є неприпустимим припущен-

ня про відсутність правового регулювання кіберпростору нормами сучасного міжнародного права. У цьому контексті виникає питання: які з існуючих норм сучасного міжнародного права застосовні до кіберпростору?

На думку науковців, «основними джерелами права в цій галузі є Статут ООН, міжнародні договори, укладені в розвиток положень Статуту ООН щодо забезпечення міжнародного миру і безпеки, міжнародні договори з гуманітарних аспектів ведення війни, рішення Міжнародного Суду, що містять трактування положень міжнародного права використання сили» [12].

Якщо ж звернутися до питання створення нових норм для регулювання кіберпростору, то в даний час зусилля держав, нажаль, сконцентровані на вузькій сфері питань, що стосуються прав людини, конфіденційності даних і ін. Більш того, не всі держави зацікавлені в створенні сучасного і ефективного механізму співпраці, відкрито виступаючи проти розробки нових міжнародно-правових інструментів. З цієї причини в даний час відсутня всеосяжна міжнародно-правова база в сфері кіберпростору.

Єдиним багатостороннім договором, що стосується злочинної діяльності в сфері інформаційних технологій, є Конвенція про злочинність у сфері комп'ютерної інформації, прийнята 23 листопада 2001 року в Будапешті [13].

Конвенція спочатку поділяла кіберзлочини на чотири групи (згодом був прийнятий додатковий протокол, зараз груп – п'ять), виділяючи першу групу «комп'ютерні злочини» та називаючи їх злочинами проти конфіденційності, цілісності і доступності комп'ютерних даних і системи:

– Незаконний доступ – ст. 2 (протиправний умисний доступ до комп'ютерної системи або її частини);

– Незаконне перехоплення – ст. 3 (протиправне умисне перехоплення не призначені для суспільства передач комп'ютерних даних на комп'ютерну систему);

– Втручання в дані – ст. 4 (навмисне пошкодження, видалення, порушення, зміна комп'ютерних даних);

– Втручання до системи – ст. 5 (серйозне протиправне перешкоджання функціонування комп'ютерної системи шляхом введення, передачі, пошкодження, видалення, порушення, зміна комп'ютерних даних).

До другої групи входять злочини, пов'язані з використанням комп'ютерних засобів. Конвенція визначає як введення, зміна, знищення, або блокування комп'ютерних даних, що тягнуть за собою порушення автентичності даних з наміром, щоб вони розглядалися , або використовувались в юридичних цілях в якості автентичних, незалежно від того чи піддаються ці дані безпосередньому читанню і чи є вони зрозумілими. Шахрайство в кіберпросторі, згідно Конвенції – це позбавлення іншої особи його власності шляхом різного введення, зміни, видалення, блокування комп'ютерних даних і різного виду втручання в функціонування комп'ютерної системи, з шахрайськими намірами отримання неправомірної економічної вигоди для себе або третіх осіб.

Третю групу складають злочини , пов'язанні з контентом (вмістом даних), розміщених в комп'ютерних мережах. Найпоширеніший вид цих кіберзлочинів – злочин пов'язаний з дитячою порнографією.

В четверту групу входять злочини пов'язані з порушенням авторського права і суміжних прав. Види таких злочинів в Конвенції не передбачені: встановлення таких правопорушень відноситься до компетенції національних законодавчих органів держав.

П'ята група – злочини, що посягають на суспільну безпеку. До цієї групи відносяться такі діяння, як кібертероризм із використанням кіберпростору в терористичних цілях (наприклад, залучення до злочину терористичного характеру, або інше сприяння їх вчиненню).

Слід враховувати, що дана конвенція розроблялася в той час, коли рівень розвитку інформаційно-комунікаційних технологій був невисокий і багато видів мережевих загроз ще не були відомі. З цієї причини ст. 1 Конвенції, яка містить визначення, і наступні статті Конвенції навіть не згадують про використовування зловмисниками «ботнетах»,«фішинг», «спам» і ін.

Науковцями з Росії було розроблено і поширено для ознайомлення на профільних міжнародних платформах проект Конвенції Організації Об'єднаних Націй «Про співпрацю в сфері протидії інформаційній злочинності» [14].

Конвенція передбачає широкий понятійний апарат: «бот-мережу», «шкідлива програма», «дитяча порнографія», «інформаційно-комунікаційні технології» (ІКТ), Інформація», «об'єкти критичної інфраструктури», «спам», «пристрій ІКТ» та ін. Так, наприклад, згідно з Конвенцією, «бот-мережа» означає два і більше пристрою ІКТ, на які встановлено шкідлива програма, керована централізовано і прихована від користувачів. Під «інформаційно-комунікаційними технологіями» (ІКТ) розуміється сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою формування, перетворення, передачі, використання і зберігання інформації ».

Проект Конвенції був поширений на різних міжнародних майданчиках, в тому числі 28 грудня 2017 року він був розповсюджений як офіційний документ Генеральної Асамблеї ООН. Даний документ був переведений з російської мови на всі офіційні мови Організації Об'єднаних Націй і в електронному вигляді розміщено на офіційних веб-сайтах ООН.

Однак деякі делегації відкрито виступають проти даного проекту Конвенції, а також проти розробки будь-яких нових міжнародно-правових інструментів в цій сфері, наполягаючи на тому, що існуючий міжнародно-правовий механізм, під яким зазвичай розуміється згадувана раніше Конвенція про злочинність у сфері комп'ютерної інформації, є достатнім для успішної боротьби зі злочинністю в кіберпросторі.

З цієї причини, в світі відсутня повноцінна універсальна міжнародно-правова база співробітництва в сфері кіберпростору.

## Список літератури:


1. Norbert Wiener. Cybernetics or Control and Communication in the Animal and the Machine. Hermann & Cie Editeurs. Paris : The Technology Press, Cambridge: Mass., John Wiley & Sons Inc., New York, 1948.
2. Войскунский А.Е. Метафоры интернета. *Вопросы философии*. 2001. № 11. С. 64–79. URL: http://www.relarn.ru/human/cyberspace.html
3. Киберпространство как стратегический инструмент социальной инженерии. URL: https://whatisgood.ru/theory/analytics/kiberprostranstvokak-strategicheskiy-instrument/ (дата звернення: 21.04.2021).
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.
5. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сете-центрических войнах начала XXI века. Санкт-Петербург : Наукоемкие технологии, 2017. С. 237.
6. AFDD 3-13. Information Operations. USAF, 2011. 65 p. ULR: https://fas.org/irp/doddir/usaf/afpd10-7.pdf (дата звернення: 21.04.2021).
7. Присяжнюк М., Цифра Є. Особливості забезпечення кібербезпеки. Експертні системи та підтримка прийняття рішенн. 2017. С. 61–68.
8. Про основні засади забезпечення кібербезпеки України відомості ВРУ. 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 21.04.2021).
9. 中华人民共和国网络安全法 Чжунхуа жэньминь гунхэго ванло аньцюань фа [Закон о кибербезопасности КНР]. URL: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (дата звернення: 21.04.2021).
10. Warden J.A. The Enemy as a System. *Airpower Journal.* 1995. Vol. 9. № 1.
11. Камчатний М. Основні ознаки поняття «кібервійна» в сучасному міжнародному праві. *Альманах міжнародного права*. 2017. Вип. 15. С. 12–22.
12. Стрельцов А. О проблемах адаптации международного права к информационным конфликтам. URL: https://digital.report/problemyi-adaptatsii-mezhdunarodnogoprava-k-informatsionnyim-konfliktam (дата звернення: 21.04.2021).
13. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23ноября 2001 г.). URL: https://base.garant.ru/4089723/ (дата звернення: 21.04.2021).
14. Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности. URL: https://www.mid.ru/documents/ (дата звернення: 21.04.2021).


## References:


1. Norbert Wiener (1948). Cybernetics or Control and Communication in the Animal and the Machine. Hermann & Cie Editeurs. Paris: The Technology Press, Cambridge: Mass., John Wiley & Sons Inc., New York.
2. Vojskunskij A.E. (2001). Metafory interneta [Internet metaphors]. *Voprosy fil*osofii, no. 11, pp. 64–79. URL: http://www.relarn.ru/human/cyberspace.html
3. Kiberprostranstvo kak strategicheskij instrument social'noj inzhenerii [Cyberspace as a strategic tool for social engineering]. URL: https://whatisgood.ru/theory/analytics/kiberprostranstvokak-strategicheskiy-instrument/ (accessed 21 April 2021).
4. Wellman B. (2001). Physical place and cyberplace: the rise of personalized networking. *International Journal of Urban and Regional Research*, vol. 25 (2), pp. 247.
5. Makarenko S.I. (2017). Informacionnoe protivoborstvo i radioelektronnaya bor'ba v sete-centricheskih voĭnah nachala XXI veka [Information confrontation and electronic warfare in network-centric wars of the beginning of the XXI century]. *Naukoemkie tekhnologii*.
6. AFDD 3-13 (2011). Information Operations. USAF, p. 65. ULR: https://fas.org/irp/doddir/usaf/afpd10-7.pdf (accessed 21 April 2021).
7. Prisyazhnyuk M., Cifra E. (2017). Osoblivosti zabezpechennya kiberbezpeki [Features of cybersecurity]. *Ekspertni sistemi ta pidtrimka prrijnyattya rishenn'*.
8. Pro osnovni zasadi zabezpechennya kiberbezpeki Ukraïni vidomosti VRU [On the basic principles of cybersecurity in Ukraine]. 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (accessed 21 April 2021).
9. Zakon o kiberbezopasnosti KNR [PRC Cyber Security Act]. URL: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (accessed 21 April 2021).
10. Warden J.A. (1995). The Enemy as a System. *Airpower Journal*, vol. 9, no. 1.
11. Kamchatnij M. (2017). Osnovni oznaki ponyattya «kibervijna» v suchasnomu mizhnarodnomu pravi [The main features of the concept of "cyberwar" in modern international law]. *Al'manah mizhnarodnogo prava*, vol. 15, pp. 12–22.
12. Strel'cov A. O problemah adaptacii mezhdunarodnogo prava k informacionnym konfliktam [On the problems of adaptation of international law to information conflicts]. URL: https://digital.report/problemyi-adaptatsii-mezhdunarodnogoprava-k-informatsionnyim-konfliktam (accessed 21 April 2021).
13. Konvenciya o prestupnosti v sfere komp'yuternoj informacii ETS № 185 (2001) [ETS Computer Crime Convention № 185]. URL: https://base.garant.ru/4089723/ (accessed 21 April 2021).
14. Proekt Konvencii Organizacii Ob"edinennyh Nacij o sotrudnichestve v sfere protivodejstviya informacionnoj prestupnosti [Draft United Nations Convention on Cooperation in Countering Cybercrime]. URL: https://www.mid.ru/documents/ (accessed 21 April 2021).