УДК 340+35.078.3 DOI https://doi.org/10.26661/2616-9444-2020-4.1-24

Правовий чинник у попередженні кіберзагроз на міжнародному та національному рівнях

Тарасюк А. В.
кандидат юридичних наук,
головний науковий співробітник
Наукової лабораторії забезпечення інформаційної та кібернетичної безпеки
Науково-дослідний інститут інформатики і права
Національної академії правових наук України
вул. Саксаганського, 110-в, Київ, Україна
orcid.org/0000-0002-0479-0666
tarast25@gmail.com

Ключові слова:
кібербезпека, кіберзагрози, правовий чинник.

Досліджено актуальні питання правового забезпечення кібербезпеки на сучасному етапі. Визначено проблеми та загрози кібербезпеці на міжнародному та національному рівнях. Аналіз практики правового регулювання сфери інформаційної, кібернетичної безпеки дає підстави виокремити дві групи проблем, котрі, вважаємо, потребують невідкладного й кардинального розв'язання. Це, по-перше, питання виконання відповідного законодавства. До другої групи належать питання, що стосуються узгодження національного законодавства з міжнародно-правовими нормами й відповідними стандартами правозастосування.
Акцентовано на такій важливій проблемі, як керовані комп'ютерною технікою автоматизовані кібернетичні системи, які стають нині повноцінними суб'єктами інформаційної взаємодії. Крім того, можна стверджувати, що нинішній світоустрій утворено саме за допомогою розумних машин, штучного інтелекту. Отже, серйозну небезпеку може становити можливість шляхом віддаленого управління через вказаних суб'єктів делегувати певні повноваження, реалізовувати, навіть їх перекручувати та спотворювати. Тому нині в умовах тотального поширення інформаційно-телекомунікаційних технологій, використання кіберпростору часом важко визначити справжнє джерело управління й контролю (людина це чи машина) й виявити при цьому якісь відмінності.
Вивчено міжнародний досвід попередження кіберзагроз на сучасному етапі. На цій основі обґрунтована думка, що ідея міжнародної співпраці задля вироблення загальних принципів правового регулювання використання кіберпростору, укладання відповідних угод складна й багатоаспектна, вона потребує ретельного дослідження й опрацювання. Потребу застосування у вказаній сфері міжнародних правових актів і міждержавних угод обґрунтовано потребою уникнення прийняття різними країнами національних норм і законів, які конфліктують між собою, а також необхідністю вироблення універсальних підходів та єдиних стандартів щодо нормативно-правових актів, котрі стосуються інформаційно-телекомунікаційних технологій, користування кіберпростором, мережею Інтернет.

Legal factor in preventing cyber threats at the international and national levels

Tarasyuk A. V.
Candidate of Law,
Chief Researcher at the Scientific Laboratory
for Information and Cyber Security
Research Institute of Informatics and Law
of the National Academy of Sciences of Ukraine
Saksaganskogo str., 110-v, Kyiv, Ukraine
orcid.org/0000-0002-0479-0666
tarast25@gmail.com

Key words:
cybersecurity, cyberthreats, legal factor.

Topical issues of legal support of cybersecurity at the present stage are studied. Problems and threats to cybersecurity at the international and national levels have been identified. The analysis of the practice of legal regulation in the field of information and cyber security gives grounds to single out two groups of problems that, in our opinion, need to be addressed urgently and radically. This is, firstly, a matter of compliance with relevant legislation. The second group includes issues related to the harmonization of national legislation and international law and relevant law enforcement standards.

Emphasis is placed on such an important issue as computer-controlled automated cybernetic systems, which today are becoming full-fledged subjects of information interaction. Moreover, it can be argued that the current world order was formed with the help of intelligent machines, artificial intelligence. Therefore, the possibility of delegating certain powers, exercising, and even distorting and distorting them through remote management through these entities may pose a serious danger. Therefore, today in the conditions of total spread of information and telecommunication technologies, use of cyberspace it is sometimes difficult to define the real source of management and control - it is the person or the car and to reveal at the same time any differences.

The international experience of cyber threat prevention at the present stage is studied. On this basis, it is reasonable to believe that the idea of international cooperation to develop general principles of legal regulation of the use of cyberspace, the conclusion of relevant agreements is complex and multifaceted, it requires careful study and elaboration. The need for application of international legal acts and interstate agreements in this area is justified by the need to avoid the adoption of different countries and conflicting national laws and laws, as well as the need to develop universal approaches and uniform standards for regulations relating to information and telecommunications technologies. cyberspace, the Internet.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Тотальна інформатизація, створення глобальних інформаційно-телекомунікаційних мереж торкнулися усіх сфер людської життєдіяльності. Насамперед, на нашу думку, відповідні юридичні лакуни спричинили проблеми у таких галузях, як комп'ютерні правопорушення, захист таємниці, власність, фінанси і банківська справа, авторське право, безпека даних, транскордонні інформаційні потоки, безпека даних, захист особистої інформації й персональних даних та ін.

Низька ефективність усталених юридичних інструментів у регулюванні актуальних суспільних відносин, особливо у сферах, де найбільше застосовуються новітні інформаційні технології, зводить нанівець спроби влити молоде вино нової культури у старі міхи чинного правопорядку. Так, радикальних змін зазнають такі, здавалося б, довершені правові галузі, як конституційне, авторське, патентне, контрактне право. Оскільки раніше не існувало юридичних норм стосовно злочинів, здійснюваних за допомогою високих технологій, серйозних змін зазнає кримінальне і кримінальне процесуальне право. І цей перелік можна продовжувати.

Аналіз практики правового регулювання сфери інформаційної, кібернетичної безпеки дає підстави виокремити дві групи проблем, котрі, вважаємо, потребують невідкладного й кардинального розв'язання. Це, по-перше, питання виконання відповідного законодавства. Так, ледь не всі фахівці зазначають, що недосконалим є саме це законодавство, зокрема щодо кваліфікації комп'ютерних злочинів і призначення покарання, а також труднощі його застосування [1].

До другої групи належать питання, що стосуються узгодження національного законодавства з міжнародно-правовими нормами й відповідними стандартами правозастосування. Транскордонність і транснаціональність глобальної мережі серйозно утруднює реалізацію приписів національного законодавства й контроль за його дотриманням, спричиняє юрисдикційні суперечності в процесі розв'язання багатьох питань – технологічних, технічних, економічних, культурологічних та інших, які виникають під час використання кіберпростору. Саме функціонування Інтернету зумовлює кардинальні зміни в міждержавних стосунках, потребує переведення співпраці держав і міжнародних структур на більш високий, якісно новий рівень.

Аналіз останніх досліджень і публікацій. В основу написання цієї публікації покладено творчий доробок таких вчених, як Дж. Зітрен, Д. Пост, Ж. Еріксон, Т. Фрохліч, Рю Маєр та ін.

Постановка завдання (формулювання цілей статті). Мета – на основі теоретичного аналізу визначити основні тенденції правового чиннику в процесах забезпечення кібернетичної безпеки на міжнародному та національному рівнях.

Виклад основного матеріалу дослідження з обґрунтуванням отриманих наукових результатів. Нові реалії інформаційного суспільства зумовлюють виникнення перед світовою спільнотою сукупності проблем і завдань, розв'язання яких лежить у міжнародно-правовій площині. Варто при цьому зазначити, що всі ці питання тісно переплетені та взаємозалежні. Приміром, на міжнародну правозастосовну практику негативно впливають недосконаліть національного законодавства, неузгодженість його норм із міжнародними. Водночас національне правове регулювання наштовхується на певні міжнародно-правові обмеження.

Характерно, що до потреби правого регулювання використання кіберпростору останнім часом дедалі більше схиляються навіть ті адепти Інтернету, котрі раніше палко обстоювали його вільності. У цьому контексті нерідко йдеться про певне специфічне регулювання, виходячи з особливостей Інтернету й кіберсередовища загалом [2]. У дискусіях із цього приводу з'явився термін «Інтернет-контроль», який передбачає такі рівні: доступ до електронної мережі; операторність (функціональність) мережі; діяльність у кіберпросторі [3, с. 31].

На нашу думку, проблеми, якими має опікуватися вказаний контроль, стосуються здебільшого соціальної й морально-етичної сфер. Це, скажімо, комп'ютерні шахрайства й крадіжки, спостереження (зокрема за приватним життям), пропаганда расизму, ксенофобії, практичні рекомендації щодо створення вибухівки, зброї та набоїв, інформація, котра ганьбить людську честь і гідність, суспільну мораль тощо. Зазначимо також, що ухвалення рішення стосовно особливого контролю за використанням кіберпростору знаменує собою усвідомлення суспільством потреби державно-правового регулювання суспільних відносин, які виникають у сфері застосування інформаційно-комунікаційних технологій.

Варто торкнутися ще однієї важливої проблеми. Керовані комп'ютерною технікою автоматизовані кібернетичні системи стають нині повноцінними суб'єктами інформаційної взаємодії. Крім того, можна стверджувати, що нинішній світоустрій утворено саме за допомогою розумних машин, штучного інтелекту. Отже, серйозну небезпеку може становити можливість шляхом віддаленого управління через вказаних суб'єктів делегувати певні повноваження, реалізовувати, навіть їх перекручувати та спотворювати. Тому нині в умовах тотального поширення інформаційно-телекомунікаційних технологій, використання кіберпростору часом важко визначити справжнє джерело управління й контролю (людина це чи машина) й виявити при цьому якісь відмінності. «*...Нові машини двадцятого століття,* – писала ще кількадесят років тому одна із засновниць так званого кіберфемінізму, професорка Каліфорнійського університету Дона Харавей*, – зробили неоднозначним розмежування природного і штучного розуму й тіла... Потенції наших машин усе зростають, натомість ми самі лишаємося страхітливо інертними*» [4].

З огляду на це, аналізуючи проблеми використання кіберпростору, роботу глобальної електронної мережі, котра є своєрідною технологічною картою, вважаємо за доцільне особливу увагу приділити можливостям кіберсистем, мікрочіпів, гібридів, нанотехнологій. У глобальному інформаційному суспільстві впровадження таких недержавних суб'єктів в інформаційну взаємодію, управлінські процеси, життєдіяльність «цифрової» людини й соціуму видається неминучим. Крім того, цілком імовірно, що сама держава й громадянське суспільство як такі втратять свою актуальність, позаяк штучний інтелект і подібні кіборги непомітно, поволі, але ефективно перебе-руть до своїх рук управління. Тому актуальність

проблем щодо влади, впливу, контролю в контексті використання кіберсередовища не викликає сумнівів, а особливо правовий чинник, який має стати надійним регулятором таких процесів.

Отже, на нашу думку, глобальне проникнення Інтернету в усі сфери життєдіяльності аж ніяк не означає, що держава втрачає здатність контролювати суспільство, що відбувається зумовлена інформаційними технологіями трансформація влади, її глобалізація у віртуальному просторі. Навпаки, як і в «реалі», у кіберпросторі, окрім комп'ютерних технологій, національні закони, традиції та звичаї не менш важливі. Саме на спроможність впливати та стежити за дотриманням законів у глобальному просторі спираються зорієнтовані на державу підходи до розв'язання багатьох зазначених вище питань. На обстоювання інтересів людини й суспільства, забезпечення їхньої інформаційної, кібернетичної безпеки спрямоване осягнення процесу управління цифровим середовищем, котре передбачає таку триєдність: *незалежність – дисципліна – право* [3].

Важливим напрямом, галуззю законодавства у сфері інформаційної безпеки стає боротьба зі здійснюваними за допомогою глобальної мережі Інтернет кібернетичними (інформаційними, комп'ютерними) злочинами, котрі завдають серйозної шкоди, але вельми непросто встановити навіть сам факт їх скоєння. Традиційні кримінологічні й криміналістичні підходи, засоби й методи практично безсилі у віртуальному світі, котрий живе за своїми власними законами і правилами. Тому отримати хоча б орієнтовну статистику кіберзлочинів не видається можливим, позаяк відсутні будь-які свідчення.

Ще одним непростим для кваліфікації та визначення складу злочину є несанкціонований доступ до баз секретної інформації, коли інформація не копіювалася, не змінювалася й не використовувалася. Це, приміром, бажання «хакера» продемонструвати свої «видатні» здібності зламувати будь-який захист. Цілком можливо, що в процесі кваліфікації злочину й визначенні покарання відповідь буде знайдена у площині ретельного аналізу кримінально караної «комп'ютерної поведінки». Ще раз підкреслимо, що при визначенні покарання за різні види кібернетичних (комп'ютерних) злочинів, у тому числі й згаданий вище несанкціонований доступ, питання стосовно матеріальності, «речовинності» об'єкта викрадення та ознак володіння ним (які в разі «традиційних» крадіжок є істотними) не розглядаються.

У цьому контексті корисно звернутися до міжнародного законодавства, виокремивши окремі особливості кваліфікації розглядуваних нами злочинів.

Так, із середини 1980-х років правозастосовна практика США поділяє комп'ютерні делікти на злочини проти інтелектуальної власності та несанкціоноване використання інформаційних технологій. Відповідно до федерального закону Австралійського Союзу, несанкціонований доступ до комп'ютерів, насамперед тих, що задіяні в галузях зв'язку й транспорту, вважається кримінальним злочином. Два різновиди комп'ютерних злочинів передбачає законодавство КНР, а саме: поширення неліцензійних програм й умисне зараження системи комп'ютерним вірусом. Низку нормативно-правових актів, спрямованих на запобігання комп'ютерним злочинам і боротьбу з ними, ухвалено в Гонконзі. До кримінально караних правопорушень ці документи зараховують злам комп'ютерної системи з корисливою метою чи для заподіяння шкоди, а також несанкціоноване проникнення в ЕОМ через інформаційно-комунікаційні мережі.

Як бачимо, національні кримінальні законодавства у сфері кібернетичної злочинності мають істотні відмінності як у кваліфікації таких злочинів, так і в питаннях відповідальності за їх скоєння. При цьому зрозуміло, що мета й завдання боротьби з комп'ютерними злочинами, проблеми, які виникають у зв'язку з ними, є ідентичними, зокрема проблема реалізації у глобальному інформаційному середовищі власної нормативно-правової бази. Ще більші законодавчі ускладнення виникають у країнах із федеративним устроєм, позаяк закони, чинні на певній території, втрачають свою силу у випадку транскордонних інформаційних потоків у кіберпросторі.

Тому недивно, що на шляху розв'язання зазначених проблем міжнародно-правового регулювання використання кіберпростору й функціонування Інтернету багато фахівців визнають за доцільне налагодити загальне технічне координування, запровадити універсальну стандартизацію в цій сфері. Дійшовши висновку, що глобальна мережа є передовсім утворенням технічним, дослідники запропонували новий підхід до керування. Зокрема, професор права Стенфордського університету (США) Л. Лессіг вважає, що *специфічною правовою базою – регулятором вільної поведінки користувачів Інтернету має бути архітектоніка мережі, котру становлять технічні протоколи і програмне забезпечення, що виступають певними правилами контролю* [5]. Саме архітектоніка, будова Інтернету зумовлює характер й особливості майбутньої мережі й, відповідно, свобод, гарантованих людині в процесі користування нею. У цьому сенсі універсальні мережеві технічні протоколи, як влучно висловився шведський політолог Ю. Еріксон, значать не менше, ніж генетичний код для людини [3].

Важливо також, що оформлені як комунікаційні протоколи технічні характеристики підвищують ефективність інформаційно-комп'ютерної комунікації та знижують її вартість. Скажімо,

низка оцінювальних специфікацій і стандартів, які розкривають понятєвий апарат, регламентує основні технічні аспекти та пропонує безпекові заходи стосовно функціонування комп'ютерних систем тощо, вони зробили вагомий внесок у створення науково-методологічного підґрунтя у сфері інформаційної та кібернетичної безпеки. Утім, технічними аспектами зовсім не вичерпується кібербезпекова проблематика, тим паче, як засвідчила практика, стандартизовані комп'ютерні системи більш уразливі до зловмисних проникнень.

У цьому контексті дослідники правових аспектів глобалізаційних процесів називають низку актуальних питань, які потребують свого розв'язання, Так, Т. Фрейліх ставить, зокрема, питання про суб'єктність інтернет-контролера контенту, програмного забезпечення тощо, які надходять із різних країн, про можливість адекватно реагувати на сучасні виклики й загрози в кібернетичному просторі країн, обмежених своїми державними кордонами та національними юрисдикціями [6]. Цим пояснюються проблеми щодо, приміром, належності змісту інтернет-контенту до юрисдикції держави, котра його створила, чи країни-отримувача інформації, компетентісних меж стосовно інформації, «спільної» для кількох країн, тощо.

Отже, сучасна наукова думка дедалі більшим пріоритетом вважає питання узгодження використання кіберпростору з міжнародно-правовими нормами поряд із дослідженням інших численних проблем правового регулювання у сфері інформаційних технологій. Цікавою у цьому сенсі є праця П. Маєра, в якій він, дослідивши міжнародно-правові обмеження, виділив ключові напрями розв'язання згаданих вище питань. Це, зокрема, формування загальних принципів діяльності, загальне міжнародне договірне право, загальні міжнародні та міждержавні угоди у сфері користування кіберпростором, координування діяльності всесвітньої мережі Інтернет тощо [7].

Важко не погодитися з дослідником, що протидіяти безлічі конкретних актуальних безпекових викликів і загроз у кібернетичному просторі (кіберзлочинність, загрози критичній інфраструктурі країн тощо) можна значно ефективніше на основі вироблення й дотримання загальних принципів регуляторної діяльності в глобальному інформаційному середовищі. Так, підтриманню положень міжнародних конвенцій про права і основні свободи людини в інформаційну епоху вельми вагомо може посприяти застосування норм договірного права. Основою вироблення міжнародного інструментарію вдосконалення роботи у сфері передання інформації та іншої взаємодії в кіберпросторі можуть стати міжнародні та міждержавні угоди, договори міжнародних спілок. Доцільним видається також вироблення й ухвалення компетенції різноманітних міжнародних структур щодо координування широкого спектра питань: функціонування ринків телекомунікаційного обладнання, розроблення технічних стандартів, інтернет-адміністрування та ін.

Експертка ЮНЕСКО із Нової Зеландії Е. Лонгворт, підтримуючи ідею укладення вказаної міжнародної угоди, вважає, що вона має передбачати основні положення правового режиму й порядку врегулювання спірних питань у міжнародних судових установах. Дослідниця також пише про необхідність створення розгалуженої децентралізованої структури керування глобальною мережею Інтернет для продовження конструктивного міжнародного діалогу із зазначених питань, що потребує значних спільних зусиль усіх членів світової спільноти. Приєднуються до цієї думки й американські правники, професори Гарвардського й Колумбійського університетів Д. Голдсміт і Т. Ву, котрі впевнені, що ефективне децентралізоване керування значно ліпше стимулює свободу, самовизначення й різноманіття [8]. Наводячи за взірець договір про міжнародні води Антарктики, особливі перспективи Е. Лонгворт убачає в реалізації ідеї міжнародного інформаційного, кібернетичного простору [9]. Своєю чергою застосувати положення про навколоземний простір задля розв'язання юридичних проблем кібернетичного простору, мережі Інтернет пропонує Е.М. Бальсано [9].

Висновки з дослідження і перспективи подальших розробок у цьому напрямі. Як бачимо, ідея міжнародної співпраці задля вироблення загальних принципів правового регулювання використання кіберпростору, укладання відповідних угод складна й багатоаспектна, вона потребує ретельного дослідження й опрацювання. Утім є всі підстави вважати, що вона буде реалізована.

Крім того, потребу застосування у вказаній сфері міжнародних правових актів і міждержавних угод можна, на нашу думку, обґрунтувати потребою уникнення прийняття різними країнами національних норм і законів, які конфліктують між собою, а також необхідністю вироблення універсальних підходів та єдиних стандартів щодо нормативно-правових актів, котрі стосуються інформаційно-телекомунікаційних технологій, користування кіберпростором, мережею Інтернет.

Наявна практика державного регулювання Інтернету, як засвідчило комплексне дослідження перспектив його застосування, потребує серйозного подальшого наукового пошуку. Вважаємо, що віднайти дійові форми та методи регулювання соціальних відносин, що виникають у процесі використання кіберпростору, можна лише на шляху всебічного вивчення проблеми, в тому

числі культурних, етичних, морально-психологічних та інших її складників. Отже, нагальним завданням сучасного суспільства в умовах перманентного підвищення національних і міжнародних безпекових вимог видається дотримання прийнятих положень.

Література

1. Zittrain J. Internet Points of Control. In The Emergent Global Information Policy Regime, edited by Sandra Braman. Houndmills : Palgrave, 2004.
2. Post D., Johnson D. The Great Debate – Law in the Virtual World. *First Monday.* 2006. Vol. 11(2). P. 1230.
3. Eriksson J., Giacomello G. Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State. *International Studies Review.* 2009. Vol. 11(1). P. 20.
4. Haraway D.J. Simians, Cyborgs and Women: The Reinvention of Nature. New York : Routledge, 1991. P. 225.
5. Lessig L. Code and Other Laws of Cyberspace. New York : Basic Books, 1999. P. 61.
6. Froehlich T.J. Survey and analysis of legal and ethical issues for library and information services, UNESCO Report (Contract № 401.723.4), for the International Federation of Library Associations. IFLA Professional Series. Munich : G.K. Saur, 1997.
7. Mayer P. Das Internet im offentlichen Recht. Unter Berucksichtigung europarechtlicher und volkerrechtlicher Vorgaben. Berlin : Duncker & Humblot, 1999.
8. Goldsmith J., Wu T. Who Controls the Internet?: Illusions of a Borderless World. New York : Oxford University Press, 2006.
9. Les dimensions internationales du droit du cyberspace. Publio sous la direction de Teresa Fuentes-Camacho. Editions UNESCO. 2000. P. 11.