DOI: 10.33663/0869-2491-2021-32-245-257
УДК 341.3. 349

Н. Р. МАЛИШЕВА,
доктор юридичних наук, професор
академік НАПрН України[*]
ORCID: 0000-0001-6630-227X

КІБЕРБЕЗПЕКА КОСМІЧНОЇ ДІЯЛЬНОСТІ ТА МОЖЛИВОСТІ ЇЇ ЗАБЕЗПЕЧЕННЯ ЗАСОБАМИ МІЖНАРОДНОГО ПРАВА

Стаття присвячена дослідженню актуальних проблем убезпечення космічної діяльності від кіберзлочинності засобами міжнародного права. Аналізуються чинні правові інструменти, які здатні поставити заслін поширенню кібератак на космічну інфраструктуру. Підкреслюється, що в умовах відсутності комплексного міжнародно-правового акта, предметом спеціального регулювання якого стали б відносини щодо кібербезпеки, необхідно до відповідної сфери з певними застереженнями застосовувати чинні норми традиційних галузей міжнародного права: права збройних конфліктів, космічного, повітряного, морського та ін.

***Ключові слова**: кібербезпека, кіберзлочинність, космічна діяльність, критична космічна інфраструктура, міжнародне право, національне законодавство.*

Малышева Н. Р. **Кибербезопасность космической деятельности и возможности ее обеспечения средствами международного права**

Статья посвящена исследованию актуальных проблем обеспечения безопасности космической деятельности от киберпреступности средствами международного права. Анализируются действующие правовые инструменты, которые способны поставить заслон распространению кибератак на космическую инфраструктуру. Подчеркивается, что в условиях отсутствия комплексного международно-правового акта, предметом специального регулирования которого стали бы отношения по кибербезопасности, необходимо к соответствующей сфере с определенными оговорками применять действующие нормы традиционных отраслей международного права: права вооруженных конфликтов, космического, воздушного, морского и др. Отмечается роль национальных законодательств в соответствующей сфере.

***Ключевые слова**: кибербезопасность, киберпреступность, космическая деятельность, критическая космическая инфраструктура, международное право, национальное законодательство.*

Malysheva Nataliia. **Cybersecurity of space activities and the possibility of ensuring it by means of international law.**

The article is devoted to the study of topical problems of ensuring the space activities safety from cybercrime by means of international law. The current legal instruments which are able to

[*] ***Malysheva Nataliia**, Doctor of Juridical Sciences, Full Professor, Academician of the NALS of Ukraine*

put a barrier to the spread of cyberattacks on space infrastructure are analyzed. It is emphasized that taking into account the absence of a comprehensive international legal act regulating relations on cybersecurity, it is necessary to apply to the relevant area, with certain reservations, the existing norms of traditional braunches of international law: the law of armed conflicts, space, air, sea law, etc. The role of national legislations in the relevant field is noted.

Key words: *cybersecurity, cybercrime, space activities, critical space infrastructure, international law, national legislation.*

Постановка проблеми. Створення нових систем зв'язку, навігації, супутникові телекомунікації, дистанційний моніторинг природних ресурсів з допомогою аерокосмічних засобів, запобігання надзвичайним ситуаціям природного і техногенного походження та інші напрями розвитку космічних технологій уже давно увійшли в повсякденне життя людства, дали підстави для активної уваги світового співтовариства до космічного простору.

Водночас на зламі XX і XXI століть активного освоєння зазнав ще один важливий для людської цивілізації глобальний простір – кібернетичний, доступ до якого тією чи іншою мірою наразі на планеті мають близько 5 млрд людей. Поряд з безумовними стратегічними і тактичними перевагами, які пов'язані з використанням кіберпростору, в останні роки дедалі більшу турботу держав, міждержавних об'єднань, бізнес-структур викликає його вразливість, тобто доступність для різного роду втручань і, як наслідок, – збоїв. В останні роки перед людством постали проблеми, пов'язані з появою та стрімким зростанням нового виду злочинності, що має різні прояви, але отримала узагальнюючу назву «кіберзлочинність». За статистичними підрахунками, кібератаки в усіх сферах зростають з кожним роком. Генеральний секретар ООН Антоніо Гуттереш оцінив щорічні збитки від кіберзлочинності у світі в розмірі 1,5 трлн доларів. За прогнозами експертів з кібербезпеки, у майбутньому кількість злочинів і збитків від кібератак лише зростатиме, адже зазвичай правопорушники йдуть щонайменше на крок попереду механізмів, які впроваджують державні органи та приватні особи щодо запобігання і розкриття таких злочинів.

Кіберзагрози впливають на різні сфери життя суспільства. Особливий вплив вони чинять на космічну діяльність, виводячи з ладу космічні системи як наземної, так і космічної інфраструктури. Забезпечення кібербезпеки космічної діяльності підпадає під загальні засади та принципи здійснення діяльності у відповідній сфері, водночас має суттєві особливості, пов'язані зі специфікою космонавтики, її унікальним характером, суттєвими ознаками вразливості, загальнопланетарними масштабами самої космічної діяльності й використання її наслідків, режимом секретності доступу до космічних технологій тощо.

Метою даної статті є виявлення як можливостей, так і обмежень у вирішенні правовими засобами проблем кіберзлочинності в космічній сфері з врахуванням насамперед міжнародно-правового контексту.

Ступінь розробленості проблеми. До аналізу окремих аспектів даної проблематики під різними кутами зору зверталися вітчизняні та зарубіжні науковці: Д.В. Дубов[1], П. Біленчук і М. Малій[2], Н.Р. Малишева і А.М. Гурова[3], Д. Лівінгстон і П. Левіс[4], С. Себекін[5], П. Дуггал[6], О. Баран-Жені[7], Ф. Шраєр, Б. Вікс, Т. Вінклер[8] та ін.

Виклад основного матеріалу. Кіберпростір – це віртуальний простір, поява якого пов'язана з глобальною інформатизацією всіх сфер людського життя, бурхливим розвитком інформаційно-комунікаційних технологій. Цей простір

складається з глобального взаємозв'язку комп'ютеризованого цифрового обладнання для обробки даних, інформаційних технологій, телекомунікаційних мереж, інформаційних систем. Інфраструктура відповідного простору – це не лише система Інтернет – відкрита мережа мереж, яка є його епіцентром; це також різного роду приватні, національні, транснаціональні та інші мережі.

Уже стало майже одностайним сприйняття кібернетичного простору, цього принципово нового (негеографічного) простору, як п'ятої сфери протиборства (після землі, повітря, моря та космосу)[9].

Космічний і кібернетичний простори є тісно переплетеними і залежними один від одного. Зокрема, варто зазначити, що життєво необхідні людству космічні технології не можуть створюватися й експлуатуватися без застосування комп'ютерних технологій. А останні стають дедалі вразливішими з боку кіберзлочинців. Найчастішими ураженнями тут є заклинювання (створення перешкод у роботі), спуфінг (узурпація) та злом систем (хакерство)[10]. Кіберзлочини вже продемонстрували можливості несанкціонованого впливу на всі системи і стадії управління супутниками через отримання неправомірного доступу до супутникових інформаційних систем, посягання на недоторканність, цілісність супутникових даних, їх викрадення, перенаправлення масивів сонячних панелей на самознищення та навіть зміни траєкторії супутників, що може викликати їх зіткнення, руйнівнийвплив на різного роду об'єкти критичної космічної інфраструктури[11]. Крім власне програмного забезпечення самих супутників, об'єктом кібератак можуть стати сигнали між супутниками та наземною інфраструктурою (центрами управління), станцією ретрансляції даних, пристроями прийому та оброблення супутникового сигналу тощо.

Саме тому світове співтовариство майже одностайно наразі вважає оцінку кібервразливостей космічних систем та їх подолання важливим викликом людства, що має вирішуватись як на етапі попередження, так і в процесі створення, розроблення, експлуатації таких систем. Це, своєю чергою, вимагає наявності правових засобів для вирішення зазначених завдань.

Як і космічний, кібернетичний простір не може бути взятий під юрисдикцію та контроль жодної окремо взятої держави. Віртуальний, мережевий характер кіберпростору, його багатовимірність, комплексність і нелінійність унеможливлюють створення всеохоплюючої парадигми кіберзахисту космічних систем. Водночас рух у відповідному напрямі триває, а пошук найбільш прийнятних ефективних правових форм протидії кіберзлочинності набирає обертів як на міжнародному рівні, так і на рівні окремих держав світу, на регіональному і навіть на локальному рівнях. Однак, зважаючи на те, що 90% усіх кіберзлочинів мають міжнародний характер[12], найбільш важливим є напрацювання на міждержавному рівні скоординованих «правил гри» у кіберпросторі, які б унеможливили або хоча б знизили загрозу кіберзлочинності.

За оцінками фахівців, наразі існує принаймні 28 ключових міжнародних організацій і програм, до предмета діяльності яких належить, серед іншого, розроблення механізмів управління кіберпростором і забезпечення кібербезпеки. Серед них – Міжнародний союз електрозв'язку (МСЕ), Міжнародна електротехнічна комісія (МЕК), Міжнародна організація з питань стандартизації (ІСО), ООН, Рада Європи (РЄ), Європейський Союз (ЄС), Інтерпол, НАТО та низка інших[13].

З поширенням кіберзагроз у центрі уваги світового співтовариства постало питання визначення можливості та доцільності розроблення самостійних

міжнародних інструментів, які б гарантували безпеку кіберпростору. Для з'ясування цього питання різні міжнародні інституції провели інвентаризацію того, що є сьогодні в активі механізмів міжнародного регулювання протидії кіберзлочинності?

Першим і практично єдиним на цей час міжнародно-правовим актом обов'язкової сили є Конвенція Ради Європи про кіберзлочинність (23.11.2001 р., Будапешт, ратифікована Україною 07.09.2005 р.[14]). Причому Конвенція була відкрита для приєднання не лише державами – членами Ради Європи, а й усіма іншими державами. У результаті, крім членів РЄ, до Конвенції приєдналися Канада, США, Японія, Південна Африка та деякі інші. Сфера регулювання Конвенції охоплює три основні напрями: 1) рекомендації щодо узгодження норм національного законодавства, особливо кримінального, у сфері кіберзлочинності; 2) визначення порядку розслідування відповідних злочинів; 3) напрацювання принципів міжнародної співпраці в протидії кіберзлочинності.

Водночас ні цей, ні жоден інший міжнародно-правовий інструмент не містять детального регулювання відносин, які виникають у сфері кібербезпеки і яке б дало змогу застосовувати міжнародну відповідальність до заподіювачів кіберзлочинів. Більше того, ні в цій Конвенції, ні в жодному іншому акті міжнародного договірного права немає визначення кіберпростору, кібербезпеки, кібератаки та інших базових понять. Спробу надати визначення «кібербезпеки» ми знаходимо в акті «м'якого права» Рекомендаціях МСЕ X.1205МСЕ-Т, де відповідне поняття визначається як набір засобів, стратегій, принципів забезпечення безпеки, заходів щодо забезпечення безпеки, керівних принципів, підходів до управління ризиками, дій, професійної підготовки, практичного досвіду, страхування та технологій, які можуть бути використані для захисту кіберпростору, ресурсів організації та користувача[15]. Вважаємо, однак, це визначення таким, що не має регулівного значення, оскільки не окреслює саму сутність відповідного поняття, а саме «стан захищеності» від кіберзагроз. Водночас як визначення «кібербезпеки» в Рекомендаціях подаються лише засоби та заходи, що характеризують забезпечувальний блок цього явища.

З питань можливості наразі розробити міжнародно-правовий договірний інструмент, який би убезпечив космічну діяльність та й інші сфери функціонування людської цивілізації від кіберзагроз, позиція юристів-міжнародників є майже одностайною: напрацювати відповідний самостійний інструмент за нинішньої міри розробленості проблеми практично неможливо, а дехто вважає, що й недоцільно. Тому на рівні різних міжнародних організацій робились неодноразові спроби пристосувати до нової реальності (кіберпростору) вже існуючі інструменти міжнародного права, за умови доповнення їх нормами національних законодавств.

Найбільш успішною стала в цьому напрямі діяльність Робочої комісії, що об'єднала два десятки експертів під егідою Центру кіберзахисту НАТО (CCD-CoE), розміщеного в Таллінні (Естонія). Комісія протягом трьох років провела дослідження можливості пристосування існуючих норм міжнародного права до кіберзлочинів. При цьому насамперед аналізувались норми щодо збройних конфліктів, космічного, морського, повітряного та інших галузей міжнародного права під кутом зору застосовності відповідних норм до кібератак. Результатом роботи Комісії став виданий у 2013 р. документ, який отримав назву «Талліннський посібник щодо міжнародного права, що може бути застосоване до кібервійни»

(далі – Талліннський посібник, посібник), друга, переглянута, уточнена й доповнена версія якого побачила світ 2017 р. і в назві якої «кібервійна» була змінена на «кібероперації», що свідчило про розширення сфери застосування посібника[16]. І хоча даний документ не має обов'язкової юридичної сили, в умовах відсутності міжнародно-правового регулювання відповідних відносин його слід вважати першою доволі вдалою спробою надати певні реперні точки застосування міжнародно-правових норм у випадках кіберінцидентів міжнародного характеру, в тому числі у сфері космічної діяльності. І сьогодні з цим документом звіряють свої дії з забезпечення кібербезпеки в космічній сфері 50 держав світу[17].

Необхідність розроблення посібника базувалася на трьох основних цілях: тлумачення існуючих міжнародно-правових норм і з'ясування їх застосовності до кібернетичних атак; поєднання кібертехнічного та правового просторів у їх спільному розумінні ознак предметної сфери; оцінка здатності держав знаходити консенсус щодо етичних і правових лімітів у віртуальному просторі, особливо щодо можливості тлумачення кібератак як збройної агресії або застосування сили.

Одна з основних труднощів, з якою стикнулись експерти при підготовці цього посібника, стосувалася термінологічних відмінностей, що існують, з одного боку, між юристами та операторами комп'ютерних систем, а з другого – між різними національними законодавствами і доктринами, які використовують різні визначення кіберпростору та пов'язаних термінів. Водночас розробникам все ж вдалося напрацювати узгоджене визначення «кібератаки», яке на сьогодні в міжнародному праві є єдиним, що застосовується при кваліфікації кіберзлочинів, у тому числі в космічній сфері. Відповідно до ст. 30 Талліннського посібника кібератака – це кібероперація, як наступальна, так і оборонна, яка за обгрунтованими очікуваннями може спричинити тілесне ушкодження або смерть людини, пошкодження або знищення матеріальних об'єктів. До речі, таке визначення повністю кореспондує поняттю шкоди за Конвенцією про міжнародну відповідальність за шкоду, завдану космічними об'єктами (далі – Конвенція про відповідальність), п. «а» ст. 1 якої декларує, що термін «"шкода" означає позбавлення життя, тілесне ушкодження або інше ушкодження здоров'я; чи знищення або пошкодження майна держав, або фізичних чи юридичних осіб, або майна міжнародних міжурядових організацій».

Найбільш детально у Талліннському посібнику опрацьовано питання права на військові дії у кіберпросторі, регламентації відносин щодо застосування сили, засобів законної самооборони, виокремлення військової мети в кіберпосяганнях. При цьому робиться спроба пристосування міжнародного права до міждержавних відносин у кібернетичному операційному контексті.

Чи можна вважати військовими діями атаки в кіберпросторі, що впливають на космічну діяльність? Якщо застосовувати stricto sensu норми міжнародного права до кібератак у космосі, слід брати до уваги, що держава є суверенною і відповідальною за кіберінфраструктуру на своїй території, а це означає, що саме держава, відповідно до своєї юрисдикції, відповідальна за запобігання кібератак зі своєї території; саме вона може переслідувати авторів шкідливих кіберакцій, а також забороняти використання відповідних інфраструктур (за наявності інформації) для вчинення зловмисних дій.

Стосовно космічної діяльності дане положення конкретизується ст. VI Договору ООН про принципи, що регулюють діяльність держав з дослідження та використання космічного простору, включаючи Місяць та інші небесні тіла

(далі – Договір про космос), де декларується, що держави несуть міжнародну відповідальність за всю національну діяльність у космічному просторі, в тому числі на Місяці та інших небесних тілах, незалежно від того, чи здійснюється така діяльність урядовими установами чи неурядовими організаціями. Саме держава через дозвільні механізми, державне регулювання та нагляд, у тому числі за недержавними структурами, забезпечує здійснення національної діяльності відповідно до норм міжнародного права.

У реалізації цих міжнародно-правових положень уже виявилось два проблемних питання. По-перше, це пов'язано з визначенням території відповідальності держави, де кібероперація готується. А по-друге, проблемною є кваліфікація кібероперації як такої, що порушує державний суверенітет[18]. Пункт 4 ст. 2 Статуту ООН декларує, що всі члени Організації Об'єднаних Націй утримуються в їх міжнародних відносинах від загрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, *так і будь-яким іншим чином, несумісним з Цілями Об'єднаних Націй*[19]. Для поширення конструкції «загроза силою або її застосування» на відносини в кіберпросторі Талліннський посібник пропонує керуватися як якісними, так і кількісними критеріями, які, однак, докладно в посібнику не прописані внаслідок багатоаспектності й залежності від різного роду чинників. Однак, виходячи з системної оцінки рекомендацій, що містяться в посібнику, можна дійти узагальнюючого висновку, що кібератака на об'єкт критичної космічної інфраструктури тоді може бути віднесена до «застосування сили», коли її рівень (ступінь / поріг інтенсивності) та її ефекти зіставні з традиційною (не кібернетичною) операцією, яка за наслідками (реальними чи потенційними) досягає відповідного рівня застосування традиційної сили.

Ще складніше застосувати до кібероперації поняття «загрози застосування сили», оскільки в міжнародному праві відсутні критерії для визначення цього поняття. Однак у будь-якому разі аналіз з метою з'ясування можливості кваліфікувати кібероперацію як «застосування сили» чи «загроза силою» завжди має бути інтерпретаційним і керуватися поєднаною оцінкою суми факторів: тяжкість збитків; прямий причинно-наслідковий зв'язок; ступінь вторгнення-проникнення в комп'ютерну систему космічної інфраструктури (з урахуванням рівня захищеності системи втручання); оцінка всіх наслідків (чи були людські жертви, їх кількість); військовий характер атаки; участь держави в кібератаці; презумпція законності та ін.

Оцінюючи процесуальні моменти, пов'язані з віднесенням кібератак до таких, що підпадають під чинні норми міжнародного права і можуть зумовити міжнародну відповідальність, фахівці з міжнародного права вважають, що необхідно, по-перше, «авторизувати» комп'ютерну атаку, тобто з'ясувати, чи не походила вона від певного самостійного індивіда, а була інспірована і підтримувана саме державою, по-друге, визначити природу такої атаки (вважати її актом агресії чи ізольованої дії, здебільшого фінансово-економічного характеру)[20].

Для космічної діяльності, яка в питаннях відповідальності традиційно керувалась Конвенцією про відповідальність, важливо визначитись, чи інформаційно-технологічні космічні системи та програмне забезпечення космічних об'єктів можна вважати їх «складовими частинами», які Конвенція охоплює поняттям «космічний об'єкт» (п. «d» ст. 1). Думки дослідників з цього питання не є одностайними. Однак вважаю, що нинішній рівень розвитку космічних технологій

настільки залежить від інформаційних систем управління, що виносити їх за дужки поняття «космічного об'єкта» немає жодного сенсу. Тому на шкоду, заподіяну космічними об'єктами, мають поширюватись усі положення Конвенції про відповідальність, як у частині абсолютної відповідальності держав(и) запуску (за шкоду, заподіяну на поверхні Землі або повітряному судну в польоті), так і в частині відповідальності за винну поведінку (за шкоду, заподіяну у космічному просторі).

Загалом Талліннський посібник, так само, як і інші доктринальні джерела відповідного напряму, пройняті ідеєю можливості застосування кваліфікації «збройної агресії» до дій у кіберпросторі. У цьому ж напрямі йдуть стратегічні документи регіональних інтеграційних об'єднань, а також національне законодавство провідних космічних держав.

Важливим аспектом дослідницької уваги як наукових, так і методичних джерел є також питання легітимності та меж *дій у відповідь* з боку держави, що постраждала; визначення всіх нюансів з точки зору дотримання міжнародно-правових принципів пропорційності та необхідності відповідних дій. Переважна позиція в цьому контексті зводиться до того, що третя держава, що зазнала побічної шкоди в результаті кібератаки між двома іншими державами, може застосовувати легітимний самозахист, якщо ефекти від кібератаки, яких вона зазнала, за інтенсивністю та наслідками можуть бути прирівняні до збройного нападу. Йдеться про доцільність зацікавити кожну державу в наданні відповіді на кіберакцію, яка може вважатися збройним нападом. Усі можливі випадки надання державам права на дії у відповідь, а також суворого обмеження такого права, зокрема, розглядаються в Талліннському посібнику. При цьому підкреслюється, що застосування сили є далеко не ексклюзивним і єдиним засобом реагування на кібератаку. Розглядаються також дипломатичні, економічні та інші дії у відповідь. Але в усіх випадках зустрічні дії повинні мати миттєвий, не віддалений у часі характер.

Для диференціації кібератаки на космічну інфраструктуру як військової (на відміну від цивільної) слід керуватися чотирма основними критеріями:

1) природа об'єкта посягання: чи є він за своєю сутністю та призначенням військовим (кібервійськова інфраструктура);

2) локалізація: традиційно йдеться про географічний критерій, про зону, акції в якій дають змогу сприяти військовим діям;

3) сфера застосування: якщо будь-який об'єкт використовується у військових цілях, він має трактуватися як військовий об'єкт. Так, мережа комп'ютерів, що використовуються у військових цілях, стає військовим об'єктом, навіть якщо вона створена для виконання цивільних завдань;

4) мета: для космічної інфраструктури важливою є диференціація належності в кіберконтексті об'єкта подвійного призначення. Щодо цього посібник надає однозначну відповідь: такий об'єкт має тлумачитись як військовий. Загалом оцінка за цим критерієм є складним завданням, оскільки відповідна військова мета має бути чітко викристалізованою. А от жодних критеріїв визначення «військових намірів» посібник не надає, тому відповідне питання повністю належить до оціночних.

Слід зазначити, що Талліннський посібник надає чимало корисних орієнтирів і щодо інших важливих питань, які постають у зв'язку з кваліфікацією кіберзлочинів у космічній сфері та можливістю реагування на них.

Низка стратегічних, у т. ч. нормативних рішень у сучасний період ухвалено на рівні Європейського Союзу. Насамперед слід наголосити на прийнятті у

грудні 2020 р. нової Стратегії кібербезпеки Євросоюзу на наступні 10 років[21]. Показовою у визначенні спрямованості цієї Стратегії і на підтвердження сучасного підходу до організації кібербезпеки є заява заступника голови Європейської комісії з захисту європейського способу життя Маргаритіса Схінаса: «Ми повинні *відмовитися від різних підходів до фізичної та кібернетичної безпеки інфраструктури* і використовувати запропонований у даній стратегії комплексний підхід». Важливою новацією даної Стратегії ЄС є й положення про те, що створення нових технічних та інформаційних систем кібербезпеки, так само як і проєкти з підготовки кадрів для цієї сфери, будуть розглядатися як *проєкти військового значення*, що можуть розвиватися в рамках європейської програми Постійного структурованого співробітництва в сфері оборони та безпеки (PESCO).

На рівні ЄС діють кілька директив, регламентів і рішень, присвячених забезпеченню кібербезпеки: Директива 2002/21/ЄС Європейського Парламенту та Ради від 7 березня 2002 р. про спільну нормативну базу для електронних комунікаційних мереж та послуг (Рамкова директива)[22], Директива ЄС щодо заходів із забезпечення високого загального рівня безпеки мережевих та інформаційних систем у ЄС[23], Регламент (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 р. про електронну ідентифікацію та послуги довіри для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС[24], Рішення Ради 2013/488/ЄС від 23 вересня 2013 р. про правила безпеки для захисту секретної інформації ЄС[25] та деякі інші. Планується розроблення нових актів ЄС, які мають надати правове значення базовим положенням, закладеним у нову Стратегію кібербезпеки ЄС. І Україна, що адаптує свою правову систему до європейської, насамперед у межах Угоди про асоціацію, повинна тримати в полі зору спрямованість політики ЄС щодо убезпечення кіберпростору.

Певна правотворча робота, метою якої є убезпечення кіберпростору від злочинних посягань, ведеться також під егідою інших міжнародних організацій. Значний регулюючий сегмент у відповідній сфері припадає й на національне законодавство. У сфері космічної діяльності найбільш успішною є ця робота в США, де за останнє десятиліття створено потужну інституційну базу запобігання кіберпосяганням на космічну сферу, а також прийнято достатньо деталізоване законодавство щодо кібербезпеки космічної інфраструктури[26].

В Україні законодавство про кібербезпеку почало створюватись лише в останнє десятиліття, в основному у зв'язку з виявленою вразливістю кіберпростору і необхідністю посилення протидії зовнішній агресії. У 2016 р. було затверджено Стратегію кібербезпеки України[27]. На базі цієї Стратегії 05.10.2017 р. було прийнято Закон України «Про основні засади забезпечення кібербезпеки України»[28], регулівний вплив якого поширюється й на кіберсферу космічної діяльності. Для міжнародного співробітництва України, зокрема, важливими є пп. 1, 2, 20 частини 3 ст. 8 цього Закону щодо вироблення і оперативної адаптації державної політики у сфері кібербезпеки на досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО і гармонізації з ними нормативно-правової та термінологічної бази предметної сфери; підтримки міжнародних ініціатив щодо захисту кіберпростору, які походять від цих інтеграційних об'єднань, а також від ОБСЄ. А згідно зі ст. 14 Закону Україна здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

На розвиток базового Закону в сфері кібербезпеки прийнята низка норм підзаконного регулювання. Це, зокрема, Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19 червня 2019 р. № 518[29], постанова Кабінету Міністрів України від 9.10.2020 р. «Деякі питання об'єктів критичної інформаційної інфраструктури»[30]. А у Верховній Раді України зареєстрований законопроєкт «Про критичну інфраструктуру та її захист» (реєстраційний № 10328 від 27.05.2019 р.)[31].

Водночас у сфері визначення та захисту критичної інфраструктури космічної галузі залишається ще чимало проблем, пов'язаних, по-перше, з певною термінологічною неузгодженістю як різних актів відповідного законодавства України між собою, так і з їх неуніфікованістю з міжнародною термінологією, а також з термінологією, що вживається в актах ЄС, НАТО та ОБСЄ. В космічному законодавстві, зокрема, у чинній редакції Закону України «Про космічну діяльність», немає жодної згадки про належність кіберзагроз до сфери його регулювання. Не набули до цього часу відображення засади кібербезпеки космічної діяльності і в затвердженій 13.01.2021 р. Розпорядженням № 15-р Кабінету Міністрів України Концепції Загальнодержавної цільової науково-технічної космічної програми України на 2021–2025 рр. А необхідність відповідного фокусу регулювання особливо гостро постає у зв'язку з одним із передбачених Концепцією очікуваних результатів реалізації Космічної програми – створення та розвиток супутникового угруповання космічного спостереження на основі вітчизняних платформ і сканерів середнього та високого розрізнення з метою задоволення національних потреб і забезпечення спільної роботи з європейською системою COPERNICUS. Немає до цього часу чіткого розуміння і єдиного підходу до визначення об'єктів критичної інфраструктури в контексті кіберзахисту, а також передбаченого Законом Переліку таких об'єктів в Україні. Є й чимало інших проблем національного законодавства України, яке мало б розвинути й доповнити міжнародно-правове регулювання протидії кіберзлочинності в космічній сфері.

Висновки. Кібербезпека космічної діяльності є тим напрямом правового регулювання, який постав на порядку денному світового співтовариства лише кілька десятиліть тому, але внаслідок бурхливого розвитку засобів негативного впливу на кіберпростір космічної сфери впевнено виходить на перший план у пошуку шляхів убезпечення космічної інфраструктури від знищення чи пошкодження.

Зважаючи на те, що як космічний простір, так і кіберпростір не знають державних кордонів, а за масштабами впливів є транснаціональними, то й шляхи запобігання кіберзлочинності в космічній сфері мають насамперед структуруватись на міжнародному рівні. Наразі десятки міжнародних організацій включили питання забезпечення безпеки кіберпростору до сфери своїх досліджень. При цьому практично всі дослідження, що здійснювались під егідою різних міжнародних організацій, дійшли одностайної думки: на сучасному етапі розробити всеохопний міжнародно-правовий договірний інструмент у сфері кібербезпеки немає жодних можливостей.

Найбільш дієвим і результативним у сенсі орієнтації держав на застосування тих чи інших засобів протидії кіберзлочинності, у тому числі в космічній сфері, став т. зв. Талліннський посібник щодо міжнародного права, що може бути застосоване до кібероперацій, розроблений під егідою Центру кіберзахисту НАТО. Не ставлячи собі за мету розроблення нового інструменту міжнародного права, фокус уваги в посібнику зосереджений на рекомендаціях

щодо можливості застосування до кібератак міжнародної відповідальності, передбаченої іншими галузями міжнародного права, а саме міжнародним правом збройних конфліктів, космічним, морським, повітряним та іншими.

Водночас важливо усвідомлювати, що проблема правового забезпечення протидії кіберзлочинності в космічній сфері на сучасному етапі не може бути вирішена виключно засобами міжнародного права. Оскільки кіберзагрози є різноплановими, розрізненими, важкими для ідентифікації, з часом неконтрольованими наслідками, міжнародне співробітництво та обмін інформацією мають поєднуватися з національним регулюванням кібербезпеки. Саме держава є відповідальною за кіберінфраструктуру на своїй території і за запобігання кібератак зі своєї території; саме вона може переслідувати заподіювачів шкідливих кіберакцій, а також забороняти використання відповідних інфраструктур для вчинення протиправних дій. Тому дуже важливо на державному рівні напрацювати законодавство щодо державного регулювання, дозвільної діяльності, державного нагляду і відповідальності за кібератаки, що здійснюються з території відповідної держави.

При цьому розроблення спільних наукових доктрин, що базуються на сучасних потребах кіберзахисту та виявлених проблемах, напрацювання кодексів кращої практики, дипломатичні та політичні спільні дії держав повинні продовжуватися.

1. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ, 2014. 328 с. **2.** Біленчук П., Малій М. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття. URL: https://lexinform.com.ua/dumka-eksperta/kosmichna-j-elektronna-kiberzlochynnist-zagrozy-i-vyklyky-novogo-tysyacholittya-2/ **3.** Малишева Н. Р., Гурова А. М. Правові засади кібербезпеки космічної діяльності в США: досвід для України. *Часопис Київського університету права*. 2020. № 3. С. 325–332. **4.** David Livingstone, Patricia Lewis. *Space, the Final Frontier for Cybersecurity*. URL: https://www.chathamhouse.org/2016/09/space-final-frontier-cybersecurity#technical-aspects-of-cyberthreats-to-satellites **5.** Себекин С. Кибербезопасность космической инфраструктуры: векторы развития международного сотрудничества. URL: http://www.pircenter.org/blog/view/id/423 **6.** Pavan Duggal. Cyber security law, its regulation and relevance for outer space. URL: https://www.unoosa.org/documents/pdf/hlf/HLF2017/presentations/Day2/Session_7b/Presentation5.pdf **7.** Oriane Barat-Ginies. Existe-il un droit international de ciberespace? *Herodote*. 2014/1 № 152–153. P. 201–220. URL: https://www.cairn.info/revue-herodote-2014-1 **8.** Шрайер Ф., Викс Б., Винклер Т.Х. Кибербезопасность: дорога, которую предстоит пройти. URL: https://docplayer.ru/37995058-Zhenevskiy-centr-demokraticheskogo-kontrolya-nad-vooruzhennymi-silami-dcaf-kiberbezopasnost-doroga-kotoruyu-predstoit-proyti.html **9.** Cyberwar: War in the Fifth Domain. *Economist*, July 1, 2010. **10.** Espace et cyberattaques: une équation sensible. URL: https://gouvernance.news/2019/07/12/espace-et-cyberattaques-une-equation-sensible. **11.** Pavan Duggal. Cybersecurity law, its regulation and relevance for outer space. URL: http://www.unoosa.org/documents/pdf/hlf/HLF2017/presentations/Day2/Session_7b/Presentation5.pdf **12.** Oriane Barat-Ginies. Existe-il un droit international de ciberespace? *Herodote*. 2014/1 № 152–153. P. 201–220. P. 218. URL: https://www.cairn.info/revue-herodote-2014-1 **13.** Шрайер Ф., Викс Б., Винклер Т.Х. Кибербезопасность: дорога, которую предстоит пройти. Женевский центр демократического контроля над вооруженными силами (DCAF). DCAF Horizon 2015 Working paper № 4 ru. С. 38. **14.** Конвенція про кіберзлочинність, ратифікована Україною із застереженнями і заявами. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text **15.** МСЭ-Т X 1205 (04/2008). Сектор стандартизации электросвязи МСЭ. Серия X: Сети передачи данных, взаимосвязь открытых систем и безопасность. Обзор кибербезопасности. **16.** Tallinn Manual on the International Law applicable to Ciber Operation. 2017. URL: https://ccdcoe.org/research/

tallinn-manual/ **17.** Over 50 states consult Tallinn Manual. URL: https://ccdcoe.org/over-50-states-consult-tallinn-manual-20.html **18.** Oriane Barat-Ginies. Existe-il un droit international de ciberespace? *Herodote.* 2014/1. № 152–153. P. 201–220. P. 206–207. https://www.cairn.info/revue-herodote-2014-1 **19.** Статут ООН. URL: https://zakon.rada.gov.ua/laws/show/995_010#Text **20.** Oriane Barat-Ginies. Existe-il un droit international de ciberespace ? *Herodote.* 2014/1. № 152–153. P. 201–220. P. 201–202. URL: https://www.cairn.info/revue-herodote-2014-1 **21.** Еврокомиссия представила стратегію кибербезопасности Евросоюза на 10 лет. URL: https://tass.ru/mezhdunarodnaya-panorama/10270263 **22.** Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). OJ L 108, 24.4.2002, p. 33. **23.** Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG **24.** Regulation (EU) № 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73. **25.** Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information. OJ L 274, 15.10.2013, p. 1. **26.** Малишева Н.Р., Гурова А.М. Правові засади кібербезпеки космічної діяльності в США: досвід для України. *Часопис Київського університету права*. 2020. № 3. С. 325–332. **27.** Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836 **28.** Про основні засади забезпечення кібербезпеки України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text **29.** Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. *Офіційний вісник України*. 2019. № 50. Ст. 1697. **30.** Деякі питання критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text **31.** Проект Закону про критичну інфраструктуру та її захист. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996

References

1. Dubov D.V. Kiberprostir yak novyi vymir heopolitychnoho supernytstva. Monohrafiia. Kyiv, 2014. 328 s. [ukr]. **2.** Bilenchuk P., Malii M. Kosmichna y elektronna kiberzlochynnist: zahrozy i vyklyky novoho tysiacholittia: https://lexinform.com.ua/dumka-eksperta/kosmichna-j-elektronna-kiberzlochynnist-zagrozy-i-vyklyky-novogo-tysyacholittya-2/ [ukr]. **3.** Malysheva N. R., Hurova A.M. Pravovi zasady kiberbezpeky kosmichnoi diialnosti v SShA: dosvid dlia Ukrainy. *Chasopys Kyivskoho universytetu prava*. 2020. № 3. S. 325–332 [ukr]. **4.** David Livingstone, Patricia Lewis. Space, the Final Frontier for Cybersecurity. URL: https://www.chathamhouse.org/2016/09/space-final-frontier-cybersecurity#technical-aspects-of-cyberthreats-to-satellites. **5.** Serhei Sebekyn. Kyberbezopasnost kosmycheskoi ynfrastrukturы: vektorы razvytyia mezhdunarodnoho sotrudnychestva. URL: http://www.pircenter.org/blog/view/id/423 [rus]. **6.** Pavan Duggal. Cyber security law, its regulation and relevance for outer space. URL : https://www.unoosa.org/documents/pdf/hlf/HLF2017/presentations/Day2/Session_7b/Presentation5.pdf. **7.** Oriane Barat-Ginies. Existe-il un droit international de ciberespace ? Herodote. 2014/1 № 152–153. P. 201–220. URL: https://www.cairn.info/revue-herodote-2014-1. **8.** Shraier F., Vyks B., Vynkler T.Kh. Kyberbezopasnost: doroha, kotoruiu predstoyt proity. URL: https://docplayer.ru/37995058-Zhenevskiy-centr-demokraticheskogo-kontrolya-nad-vooruzhennymi-silami-dcaf-kiberbezopasnost-doroga-kotoruyu-predstoit-proyti.html [rus]. **9.** Cyberwar: War in the Fifth Domain. Economist, July 1, 2010. **10.** Espace et cyberattaques : une équation sensible. URL: https://gouvernance.news/2019/07/12/espace-et-cyberattaques-une-equation-sensible

11. Pavan Duggal. Cybersecurity law, its regulation and relevance for outer space. URL: http://www.unoosa.org/documents/pdf/hlf/HLF2017/presentations/Day2/Session_7b/Presentation5.pdf **12.** Oriane Barat-Ginies. Existe-il un droit international de ciberespace? Herodote. 2014/1 № 152–153. P. 201–220. URL: https://www.cairn.info/revue-herodote-2014-1. P. 218. **13.** Shraier F., Vyks B., Vynkler T.Kh. Kyberbezopasnost: doroha, kotoruiu predstoyt proity. Zhenevskyi tsentr demokratycheskoho kontrolia nad vooruzhennыmy sylamy (DCAF). DCAF Horizon 2015 Working paper № 4 ru. C. 38. [rus]. **14.** Konventsiia pro kiberzlochynnist, ratyfikovana Ukrainoiu iz zasterezhenniamy i zaiavamy. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text [ukr]. **15.** MSЭ-T Kh 1205 (04/2008). Sektor standartizacii elektrosvyazi MSE. Seriya H: Seti peredachi dannyh, vzaimosvyaz' otkrytyh sistem i bezopasnost'. Obzor kiberbezopasnosti. [ukr]. **16.** Tallinn Manual on the International Law applicable to Ciber Operation. 2017. URL: https://ccdcoe.org/research/tallinn-manual/ **17.** Over 50 states consult Tallinn Manual. – URL: https://ccdcoe.org/over-50-states-consult-tallinn-manual-20.html **18.** Oriane Barat-Ginies. Existe-il un droit international de ciberespace? *Herodote*. 2014/1. № 152–153. P. 201–220. URL: https://www.cairn.info/revue-herodote-2014-1. P. 206–207. **19.** Statut OON. URL: https://zakon.rada.gov.ua/laws/show/995_010#Text [ukr]. **20.** Oriane Barat-Ginies. Existe-il un droit international de ciberespace? *Herodote.* 2014/1. № 152–153. P. 201–220. URL: https://www.cairn.info/revue-herodote-2014-1. P. 201–202. **21.** Evrokomyssyia predstavyla stratehiiu kyberbezopasnosty Evrosoiuza na 10 let. URL: https://tass.ru/mezhdunarodnaya-panorama/10270263 [rus]. **22.** Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). OJ L 108, 24.4.2002, p. 33. **23.** Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG **24.** Regulation (EU) № 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73. **25.** Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information. OJ L 274, 15.10.2013, p. 1. **26.** Malysheva N.R., Hurova A.M. Pravovi zasady kiberbezpeky kosmichnoi diialnosti v SShA: dosvid dlia Ukrainy. *Chasopys Kyivskoho universytetu prava.* 2020. № 3. S. 325–332 [ukr]. **27.** Ukaz Prezydenta Ukrainy № 96/2016 «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy"». URL: https://www.president.gov.ua/documents/962016-19836 [ukr]. **28.** Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [ukr]. **29.** Zahalni vymohy do kiberzakhystu obiektiv krytychnoi infrastruktury, zatverdzheni postanovoiu Kabinetu Ministriv Ukrainy vid 19 chervnia 2019 r. № 518. *Ofitsiinyi visnyk Ukrainy*, 2019, № 50, st. 1697. [ukr]. **30.** Deiaki pytannia krytychnoi informatsiinoi infrastruktury. Postanova Kabinetu Ministriv Ukrainy vid 09.10.2020 r. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text [uk]. **31.** Proekt Zakonu pro krytychnu infrastrukturu ta yii zakhyst. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996. [ukr].

Malysheva Nataliia. **Cybersecurity of space activities and the possibility of ensuring it by means of international law**

Introduction. *Cybersecurity of space activities is the area of legal regulation that appeared on the agenda only a few decades ago, but due to the rapid development of negative impact on the cyber infrastructure of the space sector confidently comes to the fore in finding ways to protect space activities from destruction or damage.*

The aim of the article. *The purpose of this article is to identify both opportunities and limitations in solving problems of cybercrime in outer space by legal means, taking into account primarily the context of international law.*

Results. *Both outer space and cyberspace know no national borders, and are multinational in terms of their scale of influence, so the ways to prevent cybercrime in outer space must firstly be structured at the international level. Dozens of international organizations have so far included cyberspace security in their field of activities. At the same time, almost all researches conducted under the auspices of various international organizations have reached a unanimous opinion: at the present stage, there is no possibility to develop a comprehensive international legal instrument in the field of cybersecurity. The most effective and efficient in terms of the orientation for states to the use of certain means of combating cybercrime, including in outer space field, was the so-called Tallinn Manual on International Law Applicable to Cyber Operations, elaborated under the auspices of the NATO Cyber Security Center. The focus of the Manual is on recommendations on the possibility of applying to cyberattacks the international responsibility provisions provided by other branches of international law, namely the international law of armed conflicts, space, sea, air laws and others. At the same time, it is important to realize that the problem of legal regulation of cybersecurity of outer space presently cannot be solved exclusively by means of international law. Because cyber threats are diverse, fragmented, difficult to identify, and sometimes with uncontrolled consequences, international cooperation and information exchange must be combined with national legislation.*

Conclusions. *With the progressive growth of cyberattacks, which pose a risk of damage or even destruction of critical space infrastructure, the focus of increased attention of the world community is the development of legal means that would prevent or at least reduce cyber threats to this important area. Given that 90% of cybercrimes are international by nature, international organizations and researchers have focused primarily on finding ways to prevent cyber attacks and eliminate their consequences, including international responsibility, through international law. Taking into account the limitations of direct treaty international legal regulation in the relevant field, today's level of legal understanding focuses mainly on the application to the cybersphere of the current rules and disposals of traditional branches of international law. At the same time, the national legislation of each state, built in accordance with the national cybersecurity strategy taking into account its own needs, the specifics of critical infrastructure, its protection priorities, etc., should play an extraordinary role in regulating the relevant sphere.*

Key words: *cybersecurity, cybercrime, space activities, critical space infrastructure, international law, national legislation.*

DOI: 10.33663/0869-2491-2021-32-257-267
УДК 349.41

П. Ф КУЛИНИЧ,
доктор юридичних наук, професор,
член-кореспондент НАПрН України[*]
ORCID: 0000-0001-8716-0661

ЦИФРОВІЗАЦІЯ ЗЕМЕЛЬНИХ ВІДНОСИН І ПРАВО В УКРАЇНІ: МЕТОДОЛОГІЧНІ І ТЕОРЕТИЧНІ АСПЕКТИ

У статті досліджуються методологічні і теоретичні питання формування правового забезпечення цифровізації земельних відносин в Україні. Доводиться, що правові норми, які регламентують цифровізацію суспільних відносин, є складовою частиною адміністративного, цивільного, земельного та інших галузей права. Обґрунтовується висновок, що правова інфраструктура цифровізації земельних відносин включає правове

[*] ***Kulynych Pavlo****, Doctor of Juridical Sciences, Full Professor, Corresponding Member of the NALS of Ukraine*