УДК 341:34:004.056:347.8
DOI https://doi.org/10.24144/2307-3322.2025.89.4.18

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ У КОСМІЧНІЙ ДІЯЛЬНОСТІ: МІЖНАРОДНО-ПРАВОВИЙ ТА ТЕХНОЛОГІЧНИЙ АСПЕКТИ

Гордеюк А.О.,
кандидат юридичних наук, доцент,
професор «ХАІ», доцент кафедри права
Національного аерокосмічного університету
«Харківський авіаційний інститут»
ORCID: 0000-0001-7423-3673
e-mail: alla.law.gor@gmail.com

Демура Р.І.,
аспірант кафедри комп'ютерних систем, мереж і кібербезпеки
Національного аерокосмічного університету
«Харківський авіаційний інститут»
ORCID: 0009-0003-2248-2565
e-mail: r.i.demura@csn.khai.edu

Гордеюк А.О., Демура Р.І. Проблеми кібербезпеки у космічній діяльності: міжнародно-правовий та технологічний аспекти.

У статті авторами досліджено актуальні проблеми забезпечення правового регулювання кібербезпеки космічної діяльності на міжнародному рівні в умовах зростаючої залежності людства від супутникових технологій. Наведено реальні приклади кібератак, здійснених на космічну інфраструктуру (зокрема інциденти із супутниками Landsat-7, Terra AM-1 та мережею Viasat), негативні наслідки яких зумовлюють необхідність побудови ефективного міжнародно-правового механізму, який здатний сприяти упередженню та протидії кіберзлочинності у космічній галузі.

З метою створення потужної системи технологічного та правового захисту супутникових космічних технологій, проаналізовано сучасні підходи провідних космічних держав (США, ЄС, Франції, Німеччини, Великої Британії) щодо вирішення цієї проблеми. Встановлено, що ці підходи виявляються у розроблені галузевих керівних правил, затверджені практик забезпечення кібербезпеки у космічному сегменті шляхом створення комплексної системи космічної кібербезпеки, яка функціонує, наприклад, у державах ЄС. В межах цієї системи здійснюється аналіз ризиків і загроз, моніторинг інформаційних потоків та технічних параметрів, що дозволяє превентивно виявляти кіберінциденти та вживати заходів кіберзахисту космічної інфраструктури. У державах ЄС достатньо ефективно працюють: Федеральне управління з інформаційної безпеки (BSI) у Німеччині, однієї із опцій якого є управління космічною кібербезпекою; Французьке агентство кібербезпеки (ANSSI), що займається захистом військових супутників, виявленням кібератак і поновленням інфраструктури після спричиненої ними шкоди. Зауважено, що космічні держави з метою укріплення оборони та стримування ворожнечі у космічному просторі співпрацюють у космічній програмі Olympic Defender.

На підставі аналізу досвіду напрацювань космічних держав у правовому регулюванні кібербезпеки космічної діяльності (зокрема супутникових систем), для запровадження ефективного міжнародно-правового механізму забезпечення кібербезпеки у зазначеній сфері з обґрунтуванням доцільності, авторами запропоновано: створення міжнародної конвенції з кібербезпеки космічної діяльності та спеціалізованої міжнародної організації як органу моніторингу і контролю, а також платформи для нормотворчої діяльності; розроблення уніфікованих міжнародних стандартів безпеки космічної діяльності, що включатиме стандарти з кібербезпеки; в умовах активної комерціалізації космічної діяльності встановлення протоколів дотримання заходів кібербезпеки для приватних компаній та передбачення в них алгоритмів та методів тестування супутникових

систем з метою виявлення прогалин та упередження кібератак. Особливу увагу авторами приділено пропозиції використання технології блокчейн та запровадженню концепції bug bounty, як інноваційних інструментів у сфері кіберзахисту.

Ключові слова: космічна кібербезпека, космічні технології, міжнародно-правовий механізм, національний правовий механізм, система кіберзахисту, тестування супутникових систем, технологія блокчейн.

Hordeiuk A.O., Demura R.I. Cybersecurity issues in space activities: international legal and technological aspects.

In this article, the authors have examined the current problems of ensuring legal regulation of cybersecurity of space activities on the international level in the minds of the growing dependence of humanity on satellite technologies. Real examples of cyberattacks on space infrastructure are given (in particular, incidents involving Landsat-7, Terra AM-1 satellites and the Viasat network), the negative consequences of which necessitate the construction of an effective international legal mechanism capable of contributing to the prevention and counteraction of cybercrime in the space industry.

In order to create a powerful system of technological and legal protection of satellite space technologies, modern approaches of leading space powers (the USA, the EU, France, Germany, and the UK) to solving this problem were analyzed. It has been established that these approaches are reflected in the development of industry guidelines, approved practices for ensuring cybersecurity in the space segment by creating a comprehensive space cybersecurity system, which operates, for example, in EU countries. Within this system, risk and threat analysis is carried out, information flows and technical parameters are monitored, which allows for preventive detection of cyber incidents and implementation of cyber security measures for space infrastructure. In the EU countries, the following are working quite effectively: the Federal Office for Information Security (BSI) in Germany, one of whose options is to manage space cybersecurity; the French Cybersecurity Agency (ANSSI), which is responsible for protecting military satellites, detecting cyberattacks, and restoring infrastructure after damage caused by them. It is noted that space powers are cooperating in the Olympic Defender space program to strengthen defense and deter hostility in outer space.

Based on the analysis of the experience of space powers in the legal regulation of cybersecurity of space activities (in particular, satellite systems), in order to build an effective international legal mechanism for ensuring cybersecurity in this area with a justification of feasibility, the authors proposed: the creation of an international convention on cybersecurity of space activities and an specialized international organization as a monitoring and control body, as well as a platform for rulemaking activities; the development of unified international space security standards, including cybersecurity standards; in the context of active commercialization of space activities, establishing protocols for compliance with cybersecurity measures for privet companies and providing algorithms and methods for testing satellite systems in order to identify possible gaps and prevent cyberattacks. Particular attention is paid to the proposal to use blockchain technology and the introduction of the bug bounty concept as innovative tools in the field of cyber defense.

Key words: space cybersecurity, space technologies, international legal mechanism, national legal mechanism, cyber defense system, testing of satellite systems, blockchain technology.

Постановка проблеми. У сучасних умовах стрімкого розвитку інформаційних технологій питання забезпечення кібербезпеки у сфері космічної діяльності набуває особливої актуальності. Кіберзагрози щодо космічних об'єктів, систем зв'язку, навігації та дистанційного зондування Землі становлять суттєвий ризик як для окремих держав, так і для міжнародної безпеки в цілому. Особливої уваги потребує інтеграція технологій штучного інтелекту, які, з одного боку, підвищують ефективність обробки космічної інформації, а з іншого – створюють потенціал для складних, високоточних кібератак із мінімальним залученням людських і технічних ресурсів. У такому контексті виникає потреба у формуванні комплексної, багаторівневої системи кіберзахисту, яка б ґрунтувалася як на ефективному правовому регулюванні кібербезпеки в умовах транснаціонального космічного співробітництва, так і на застосуванні передових технологічних рішень у сфері кіберзахисту.

Отже, на сучасному етапі забезпечення кібербезпеки у космічній діяльності постає як пріоритетний напрям у розвитку космічного права щодо розроблення міжнародних стандартів кібер-

захисту, так і пріоритетне завдання фахівців у сфері інформаційних технологій. Вважаємо, що системне розв'язання цієї проблеми можливе лише за умови поєднання міжнародно-правових механізмів превенції кіберзагроз із високотехнологічними методами їх виявлення та нейтралізації.

З урахуванням окресленої проблематики, **метою даного дослідження** є проведення аналітичного огляду матеріалу щодо формування правових засад забезпечення кібербезпеки космічної діяльності у так званих «космічних державах» на національному рівні для визначення оптимальних підходів до структурування норм міжнародного права космічної кібербезпеки та вироблення стратегії боротьби з кіберзагрозами через створення і використання більш досконалих механізмів превентивного захисту інформаційних технологій, які використовуються у космічному просторі.

Стан опрацювання проблематики. Проблематиці розроблення ефективних правових механізмів запобігання та боротьби із кіберзагрозами у сфері космічної діяльності приділяли увагу у своїх роботах Н.Р. Малишева, А.М. Гурова, також вивчали окремі аспекти космічної діяльності та забезпечення її безпеки – Н.Д. Красіліч, Л.В. Сорока, М. Семенчук, О.М. Григоров, О.В. Драган та інші. Але ж, на наш погляд, не можна сказати, що відповідна тематика наразі є вичерпаною та досліджена всебічно. Є багато відкритих питань, які залишаються актуальними, що зумовило дослідницький інтерес авторів до обраної теми.

Виклад основного матеріалу. У зв'язку з розвитком космічних технологій, зростанням кількості космічних запусків і новими можливостями використання космічних ресурсів питання безпеки у космічній галузі загострюються та стають дедалі важливими. Безпека в космосі – це багатогранне питання, що охоплює різні аспекти, від запобігання космічним катастрофам до забезпечення ефективного міжнародного співтовариства [1].

Отже, на сьогодні науковці визначають чимало актуальних проблем у системі убезпечення космічної діяльності, серед яких демілітаризація космосу, екологія космосу, безпекова життєдіяльність людини у космосі, комерціалізація космічної діяльності, кібербезпека. Якщо зазначені у переліку перша-четверта проблеми виникли не сьогодні і їх вирішення та правове регулювання було актуальним майже с самого початку розвитку космонавтики та створення її правового забезпечення, то проблема кібербезпеки функціонування космічних технологій є саме сучасним надбанням людства насамперед через активне використання супутників, які відіграють ключову роль у світовій комунікації в сучасному світі. У зв'язку з цим спостерігається процес зростання залежності людства від супутникових технологій, що забезпечують для нього можливість використання кіберпростору, телекомунікації, зв'язок, навігацію та моніторинг із космосу, і водночас виникають нові загрози (кібератаки), які здатні набути глобального негативного характеру, якщо їх ретельно не відслідковувати, своєчасно не упереджувати та не працювати над створенням ефективного правового механізму щодо контролю над ними, протидії та мінімізації.

Перша успішна кібератака на супутниковий зв'язок була зафіксована ще у 1986 році: вона була спрямована проти телевізійної компанії HBO і здійснена американським хакером Джоном Реєм МакДугаллом, який діяв під псевдонімом Captain Midnight (Капітан Міднайт). Під час телетрансляції він провів акцію протесту проти підвищення цін на супутникове телебачення [2]. Але ж на той час це був одноразовий випадок. У сучасних реаліях за даними Центру обміну і аналізу космічної інформації (Space Information Sharing and Analysis Center, Space ISAC) фіксуються понад 100 спроб кібератак на космічні системи щотижня.

Одним із перших задокументованих прикладів кібервтручання у функціонування космічних апаратів стали інциденти, зафіксовані в період 2007-2008 років із супутниками Landsat-7 та Terra AM-1, які належать до систем спостереження за Землею, що функціонують під егідою NASA та Геологічної служби США [3]. Згідно з матеріалами, підготовленими для Комісії з економічного та безпекового огляду США та Китаю, невстановлені хакери чотири рази здійснювали несанкціоноване втручання в роботу цих апаратів через наземну станцію, розташовану в Норвегії.

Супутник Landsat-7 зазнав перешкод двічі – у жовтні 2007 року та липні 2008 року, причому кожне втручання тривало 12 хвилин або більше. У свою чергу, щодо супутника Terra AM-1 несанкціоновані втручання були зафіксовані в червні 2008 року (тривалістю близько двох хвилин) та в жовтні того ж року (приблизно дев'ять хвилин). Хоча в жодному з випадків зловмисники не реалізували деструктивні дії чи не змінили траєкторії супутників, їм вдалося отримати достатній рівень доступу до систем управління, що могло потенційно дозволити перехоплення або модифікацію даних, зміну режиму роботи, а також втручання у системи телеметрії та навігації. Ці інциденти стали предметом уваги оборонних структур США, зокрема ВПС та Міністерства внутріш-

ньої безпеки. Як публічно зазначила тодішній міністр внутрішньої безпеки Джанет Наполітано, хакери кілька разів були близькі до дезактивації елементів критичної інфраструктури країни, що підтверджує масштаб і потенційну загрозу подібних кібероперацій. У контексті космічної діяльності ці інциденти продемонстрували критичну вразливість наземного сегменту супутникового зв'язку, а також виявили брак ефективних міжнародно-правових механізмів для запобігання, виявлення та реагування на подібні втручання, що виходять за межі національної юрисдикції.

Іншим показовим прикладом масштабної кібератаки на космічну інфраструктуру стала атака на супутникову мережу компанії Viasat у 2022 році, яка призвела до суттєвих порушень у функціонуванні телекомунікаційних систем на території Європи [4]. Унаслідок деструктивного втручання раптово втратили зв'язок тисячі користувачів, зокрема було зафіксовано відключення понад п'яти тисяч вітрових турбін у Німеччині, які втратили з'єднання зі своїм центральним вузлом керування.

Однак справжнім об'єктом атаки був інший сегмент користувачів – українські військові, які використовував супутникові канали для забезпечення захищеного зв'язку та управління критичними процесами. Зловмисники скористалися вразливістю в мережевій адміністративній інфраструктурі провайдера, яка дозволила їм отримати контроль над системами віддаленого керування модемами. В результаті була запущена деструктивна команда, що перезаписала флеш-пам'ять великої кількості терміналів, вивівши їх із ладу без можливості відновлення. Компанія Viasat була змушена замінити понад 30 000 пристроїв, що підтверджує масштаб і глибину інциденту. Заступник голови Держспецзв'язку Віктор Жора пізніше визнав, що «це була справді величезна втрата зв'язку на початку війни» [5].

Враховуючи надані приклади, можна уявити наскільки велика шкода, може бути спричинена кіберзлочинцями, тому світова спільнота має приймати виклики часу, та будувати міжнародне право забезпечення кібербезпеки. При створенні системи міжнародної космічної кібербезпеки вважаємо, що доцільним було б використання досвіду напрацювання спеціальних правових механізмів убезпечення космічної діяльності від кіберзагроз космічними державами, які звісно не могли ігнорувати можливість виникнення катастрофічних наслідків «нових загроз» та розглядають створення відповідної системи забезпечення безпеки як складову національної безпеки. Зокрема США є найпершою у світі державою, що напрацювала зазначені механізми, які б шляхом рецепції мало сенс запозичити для правового регулювання кібербезпеки на міжнародному рівні.

Так, правове регулювання забезпечення кібербезпеки у США почалось зі створення законодавства про захист критичної інфраструктури, у наслідок терористичного акту від 2001 року. Насамперед був прийнятий Закон «Про захист критичної інфраструктури» від 2001 року, в якому визначається, що політика кібербезпеки має здійснюватися на засадах публічно-правового партнерства, а також на засадах, згідно з якими будь-яке порушення в роботі фізичної чи віртуальної інфраструктури мають бути рідкісними, короткими, обмеженими географічно, керованими та мінімально згубними для економіки, людини, урядових сервісів та національної безпеки США [6]. З даного положення виходить, що наслідки будь-яких посягань на об'єкти критичної інфраструктури мають бути нейтралізовані у найкоротші строки і відповідно для цього має бути попереднім чином ретельно підготовлений ресурс.

Наступним важливим етапом у формуванні міжнародної політики кібербезпеки, що має безпосередній вплив на захист критичної інфраструктури, зокрема космічної, стало прийняття у США закону «Cybersecurity Enhancement Act of 2014» (Публічний закон № 113–274) [7]. Цей нормативний акт закріпив офіційний мандат для Національного інституту стандартів і технологій (NIST) на розробку та оновлення рамкових документів із кібербезпеки для державних і приватних суб'єктів, зокрема у ньому надано поняття кібернетичного ризику, який визначений як: «загроза або вразливість інформації чи інформаційних систем і будь-які пов'язані з ним обставини, спричинені або ті, що виникли внаслідок недозволеного доступу, використання, розкриття, пошкодження, зміни чи знищення інформації та інформаційних систем, що спричинені актом тероризму». Визначення поняття «кібернетичного ризику» у даному контексті надає можливість ідентифікувати певну загрозу як саме кіберзагрозу і відповідно бути готовими реагувати на неї та протистояти їй. А також визначається поняття інциденту як «випадку, який дійсно або неминуче без законних підстав загрожує цілісності, конфіденційності або доступності інформації в інформаційній системі чи становить порушення або неминучу загрозу порушення закону, політики безпеки, процедур безпеки або прийнятих правил використання».

Наступним кроком у створенні ефективного правового регулювання кібербезпеки у США можна вважати підписання 19.02.2019 року Президентом США Директиви щодо космічної політики № 4, відповідно до якої в структурі Департаменту оборони створюється окремий підрозділ – Департамент космічних військ, у склад якого входить департамент кібербезпеки. Відповідно до стратегії цифрової модернізації до 2023 року у США було передбачено досягнення цілей, які пов'язані із захистом від кіберзагроз космічної галузі, в першу чергу мілітарі-діяльності держави у космосі.

Більш системні завдання щодо убезпечення критичної космічної інфраструктури від кібернетичних інцидентів визначила Директива з космічної політики № 5 від 04.09.2020 року, яка передбачає, що «принципи та практики кібербезпеки мають застосовуватись до космічних систем, з особливим урахуванням віддаленого оновлення та реагування на інциденти, що вимагає інтегрованості їх в конструкцію космічного корабля перед запуском, оскільки в цей час фізичний доступ до більшості космічних апаратів на орбіті неможливий. До власників та операторів космічних систем висувається вимога розробляти та реалізовувати плани кібербезпеки, які містять: захист від несанкціонованого доступу до критичних функцій; заходи фізичного захисту систем управління та телеметричного приймача; захист зв'язку за допомогою захищених передавачів приймання, шифрування, моніторингу, потужності сигналу; захист наземних систем з метою зменшення ризику зараження шкідливим програмним забезпеченням та зловмисного доступу до систем, в тому числі від інсайдерських загроз; прийняття практики гігієни кібербезпеки, фізичної безпеки автоматизованих інформаційних систем та методів виявлення вторгнень до елементів системи, таких як інформаційні системи, антени, термінали, приймачі, маршрутизатори, пов'язані локальні та глобальні мережі і джерела живлення; управління ризиками всього ланцюга поставок; оцінка інших доступних заходів зменшення ризику» [8].

На думку фахівців у галузі міжнародного космічного права, зокрема Н.Р. Малишевої «вказаний документ та визначені у ньому правила містять лише загальні норми, але вони поклали початок поглибленому галузевому регулюванню кібербезпеки в космічній сфері, розробленню галузевих керівних правил, затвердженню практик та рекомендацій, стандартів тощо» [6]. Окрім того, О. Григоров вважає, що «в рамках сучасного законодавства США ми можемо спостерігати спробу правового вирішення однієї з найважливіших проблем у сфері космічної кібербезпеки – використання космічних систем подвійного призначення (як цивільних, так і військових), що ще більше ускладнює розробку міжнародно-правових стандартів у космічній галузі»[9, с. 128].

Окрім заходів забезпечення кібербезпеки космічних систем, що здійснюються у США, інші космічні держави також намагаються системно протистояти космічній кіберзлочинності. Для захисту космічних активів Європейського Союзу створюється комплексна система кібербезпеки, яка функціонує як розподілена мережа безпеки. У її межах здійснюється аналіз ризиків і загроз, провадиться безперервний моніторинг інформаційних потоків та технічних параметрів, що дозволяє своєчасно виявляти інциденти та вживати заходів кіберзахисту в контексті космічної інфраструктури. Декілька центрів Європейського космічного агентства (ЄКА) (European Space Agency (ESA)), що розташовані у різних країнах ЄС, відповідають за різні аспекти кібербезпеки. Наприклад, Бельгія відповідає за безпеку космічних систем, Італія проводить аналіз інцидентів та управління ризиками, Німеччина здійснює моніторинг безпеки місій і виявлення загроз. Також у Німеччині працює Федеральне управління з інформаційної безпеки (BSI), яке відповідає за укріплення кібербезпеки космічної інфраструктури та забезпечує стабільний доступ до захищених послуг зв'язку через супутники, курує питання зберігання таємної інформації у військових та цивільних супутникових системах, таких як Державна служба європейської системи Galileo.

У Франції на рівні національного органу працює Французьке агентство кібербезпеки (ANSSI). Це агентство координує французькі та європейські дослідження, займається захистом військових супутників, відповідає за виявлення кібератак і поновлення інфраструктури після спричиненої ними шкоди. До того ж у 2024 році Франція та Німеччина приєдналися до космічної програми Olympic Defender, яку було розроблено за ініціативою США з метою укріплення оборони та стримання ворожнечі в космічному просторі. У Великій Британії захист глобальних супутникових служб здійснюють Національні кіберсили (National Cyber Force, NCF), в цю структуру входять оборонні та розвідувальні агентства [10].

Отже, після аналізу напрацювань космічних держав певного досвіду національного та регіонального (в межах ЄС) правового регулювання забезпечення кібербезпеки космічної діяльності

вважаємо доцільним запропонувати використання цього досвіду для побудови ефективних правових механізмів убезпечення кібербезпеки космічної діяльності (зокрема супутникових систем) у певних напрямах.

По-перше, розроблення та прийняття міжнародної конвенції щодо правової регламентації убезпечення кібербезпеки у космічній діяльності. Визначити у цій конвенції базові поняття, ризики, прописати необхідні превентивні заходи, правові алгоритми реагування на кібератаки та ліквідації їх наслідків, визначити відповідальність за кіберзлочини на міжнародному рівні.

По-друге, створення та запровадження системи стандартів убезпечення космічної кібербезпеки та запропонування рекомендовану практику протидії кібератакам на зразок Міжнародних стандартів і рекомендованої практики (SARPs), розроблених ICAO як додатків до Чиказької конвенції з міжнародної цивільної авіації, які спрямовані на системне забезпечення безпеки в авіаційній сфері на міжнародному рівні [11].

По-третє, для ефективного функціонування правового механізму убезпечення кібербезпеки у космосі необхідним є створення спеціалізованої міжнародної організації як органу моніторингу та контролю, а також надійної платформи для нормотворчої діяльності у зазначеній сфері.

По-четверте, на думку науковців (Малишева Н.Р., Гурова А.М.): «технологія блокчейн може відіграти суттєву роль у формуванні правових та технічних механізмів протидії кіберзагрозам у космічній сфері». На наш погляд дослідники мають рацію. Тому що завдяки своїй децентралізованій, криптографічно захищеній і незмінній природі, блокчейн здатен забезпечити високий рівень довіри до передачі та обробки телеметричних даних, підтвердження автентичності команд управління супутниками, а також прозорість логів доступу до критичних систем. Практичний інтерес до цього підходу вже демонструють окремі національні та приватні ініціативи. Зокрема, NASA розглядала можливість використання блокчейну для автоматизованої координації дронів та космічних апаратів через проєкт ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry). Європейське космічне агентство (ESA), зі свого боку, профінансувало низку досліджень, присвячених інтеграції блокчейн-рішень для управління правами доступу до супутникових даних. Крім того, приватні компанії, зокрема SpaceChain та Blockstream, вже проводили експерименти з розміщення блокчейн-вузлів на орбіті для забезпечення незалежної, геополітично нейтральної інфраструктури передачі даних [6; 12].

По-п'яте, з урахуванням активних процесів комерціалізації космічної діяльності має сенс у площині міжнародних приватноправових відносин визначити протоколи дотримання заходів кібербезпеки при здійсненні космічних програм приватними компаніями різних держав. Корисним може бути досвід США щодо використання положень Директиви космічної політики № 5, де визначаються вимоги до юридичних осіб стосовно створення поточних систем кібербезпеки та ефективного тестування, яке може бути засновано на приватних ініціативах та заохочувальному підході та спрямоване на виявлення системних прогалин та упередження кібератак.

Так, доцільною видається ініціатива впровадження міжнародно узгоджених програм незалежного тестування кіберстійкості супутникових систем за принципом концепції «bug bounty», що вже зарекомендувала себе як ефективний інструмент в IT-галузі. Суть такої моделі полягає в організації офіційно санкціонованого процесу пошуку вразливостей третіми сторонами – етичними хакерами, дослідниками безпеки, спеціалізованими компаніями – із подальшим правовим і матеріальним стимулюванням за виявлені недоліки. Такий підхід не лише сприяє виявленню системних прогалин до того, як ними скористаються зловмисники, але й формує спільноту залучених фахівців, які діють у рамках правових механізмів і в інтересах глобальної кіберстабільності.

Інституціоналізація подібної моделі в межах міжнародного правового простору може бути реалізована шляхом створення відповідного регламенту (протоколу) з добровільного тестування супутникових систем, у межах якого визначатимуться права та обов'язки учасників, обсяг дозволених дій, механізми звітності та способи реагування на виявлені вразливості. Такий інструмент дозволив би ефективно поєднати профілактичні заходи із прозорістю та відповідальністю, водночас не створюючи надмірного регуляторного тиску на комерційних операторів.

Висновки. Проведене дослідження підтвердило, що кібербезпека у сфері космічної діяльності є критично важливим і водночас недостатньо врегульованим напрямом міжнародної безпеки. Зростаюча кількість кібератак на космічну інфраструктуру, як державну, так і комерційну, свідчить про необхідність формування комплексної системи реагування, що включає правові, організаційні та технологічні інструменти. Досвід провідних космічних держав – США, країн ЄС,

Великої Британії – демонструє можливість ефективного поєднання нормативного регулювання, інституційного забезпечення та сучасних технологій, зокрема блокчейну та концепції bug bounty. Водночас існує потреба у створенні універсальної міжнародної конвенції щодо кібербезпеки в космосі, яка б узгодила термінологію, визначила відповідальність за кіберзлочини та передбачила механізми незалежного моніторингу і реагування на загрози. Подальші дослідження повинні зосереджуватись на розробці міжнародно-правових механізмів у сфері захисту космічних систем та на аналізі технічних засобів забезпечення стійкості до кібератак з урахуванням швидкої комерціалізації космічної галузі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кібербезпека космічної діяльності та можливість її забезпечення засобами міжнародного права. *Правова держава*. Вип. 32. 2021. С. 245–257. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001262694.
2. Boyer P. J. HBO Piracy Incident Stuns Other Sattellite Users. Нью-Йорк таймс. URL: https://www.nytimes.com/1986/04/29/arts/hbo-piracy-incident-stuns-other-satellite-users.html (date of access: 08.06.2025).
3. Report: Hackers Interfered with Landsat-7, Terra AM-1 in 2007 and 2008. Via Satellite. URL: https://www.satellitetoday.com/government-military/2011/10/31/report-hackers-interfered-with-landsat-7-terra-am-1-in-2007-and-2008/ (date of access: 08.06.2025).
4. Hackers, Spies and Contract Killers: How Putin's Agents Are Infiltrating Germany / M. Baumgärtner et al. DER SPIEGEL | Online-Nachrichten. URL: https://www.spiegel.de/international/germany/hackers-spies-and-contract-killers-how-putin-s-agents-are-infiltrating-germany-a-2cc6c24c-16ac-43d4-97fa-103081414acc (date of access: 08.06.2025).
5. Борисіхіна К. Що відомо про злом Viasat – найбільшу кібератаку нашого часу. https://techno.nv.ua. URL: https://techno.nv.ua/ukr/it-industry/zlom-viasat-50229704.html (дата звернення: 08.06.2025).
6. Малишева Н.Р. Гурова А.М. Правові засади кібербезпеки космічної діяльності в США: досвід для України.URL.http://C/users/alla/Downloads/406-Text%20статті-784-1-10-20210207.pdf.
7. Cybersecurity Enhancement Act of 2014 № 113-274. Congress.gov. URL: https://www.congress.gov/bill/113th-congress/senate-bill/1353 (date of access: 08.06.2025).
8. Memorandum on Space Policy Directive-5/Cybersecurity Principles for Space Systems. Issued on: September 4, 2020. URL :https//www.whitehouse.gov/wp-content/uploads/ 2020/09/2020SPD5.mem.pdf (date acces: 06.06.2025).
9. Григоров О. Міжнародне космічне право: підручник/ О. Григоров; Київ. нац. ун-т ім. Т. Шевченко. – Київ; Одеса: Фенікс, 2023. 130 с.
10. Поляков М. Кібервійни переміщуються у космос: супутники потребують захисту від кібератак.URL.http://maxpolykov.com/ua/kiberviini-peremishuyutsa-v-kosmos-suputnici-potrebuyut-zakhistu-vid-kiberatac.
11. Standards and Recommended Practices (SARPS). URL:https://icao.int/safety/Safety Management/pages/sarps.aspx (date of access: 05.06.2025).
12. Blockchain fail-safes in space: SpaceChain, Blockstream and Cryptosat. cointelegraph.com. URL: https://cointelegraph.com/magazine/blockchain-fail-safes-in-space-spacechain-blockstream-cryptosat (date of access: 11.06.2025).