DOI: 10.36695/2219-5521.3.2020.59

УДК 34.096

Н.Р. МАЛИШЕВА, А.М. ГУРОВА

*Наталія Рафаелівна Малишева, доктор юридичних наук, професор, академік НАПрН України, завідувач відділу Інституту держави і права імені В.М. Корецького НАН України**

ORCID: 0000-0001-6630-227X

*Анна Михайлівна Гурова, кандидат юридичних наук, науковий співробітник Інституту держави і права імені В.М. Корецького НАН України***

ORCID: 0000-0003-4134-761X

ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ КОСМІЧНОЇ ДІЯЛЬНОСТІ В США: ДОСВІД ДЛЯ УКРАЇНИ

Постановка проблеми. Кіберпростір, тобто віртуальний простір, який складається з глобального взаємозв'язку комп'ютеризованого цифрового обладнання для обробки даних, інформаційних технологій, телекомунікаційних мереж та інформаційних систем, швидко проникає в усі аспекти нашого життя, породжуючи, з одного боку, значну залежність від нього суспільства, а з іншого, – небезпеки, що супроводжує його використання. Це повною мірою стосується й космічних послуг (телекомунікації, навігації, медичного забезпечення тощо), які за допомогою ІТ-технологій стають все більш доступними для широкого кола суб'єктів, однак водночас все більш вразливими. З огляду на критичну залежність космічної діяльності від кібербезпеки, необхідним стає розроблення ефективних правових механізмів запобігання та боротьби із вказаними загрозами.

Аналіз останніх досліджень і публікацій. Актуальність вказаної проблеми стала підставою для її широкого обговорення в межах таких міжнародних організацій, як UNOOSA¹, UNIDIR², Secure World Foundation³. Не обійшли увагою питання використання кіберпростору в злочинних цілях, в тому числі й під час реалізації космічної діяльності, і вітчизняні науковці, зокрема П. Біленчук та М. Малій⁴. Проте відповідні дослідження були зосереджені на технічних і політичних аспектах проблеми та не вдавалися до детального аналізу інституційних і правових підходів до її вирішення.

Формулювання мети дослідження. Метою цієї статті є розкриття сучасного стану та перспектив розвитку правових та організаційних засад кібербезпеки у США як держави, що першою в світі й найбільш успішно напрацювала спеціальні правові механізми убезпечення космічної діяльності від кіберзагроз, а також порівняння з рівнем розвитку відповідного регулювання в Україні, зважаючи на те, що наша держава перебуває на початковому етапі формування відповідних механізмів. Вказане порівняльне дослідження не слід розцінювати як модель для прямого запозичення досвіду США для України. Це скоріше ілюстрація загальних підходів до правового та організаційного забезпечення кібербезпеки як у державі в цілому, так і в її космічній сфері зокрема. Коротка характеристика процесу нормотворення у відповідній сфері в Україні покликана виявити реперні точки, на яких варто зосередити увагу, щоб актуалізувати вітчизняну космічну діяльність відповідно до новітніх вимог безпеки та сталості.

Виклад основного матеріалу. Історію розвитку законодавства США у сфері кібербезпеки можна поділити на 2 періоди: 1) початок 2000-х рр. – 2014 роки. Цей період був пов'язаний з домінуванням ідеї необхідності протистояння терористичним атакам, причому актуальність проблеми на порядок посилилась після

© Н.Р. Малишева, А.М. Гурова, 2020

* *Nataliia Malysheva, Dr. hab in Law, Professor, academician of NALS of Ukraine, Head of the Department of V.M. Koretsky Institute of State and Law of the NAS of Ukraine*

** *Anna Hurova, Ph.D. in Law, Research fellow of V.M. Koretsky Institute of State and Law of the NAS of Ukraine*

теракту 11 вересня 2001 р. Саме в цей період були сформовані ключові державні органи кібербезпеки; 2) після 2014 р. донині: у відповідь на численні кібератаки формується законодавство, покликане протистояти новітнім загрозам, які ще не набули гостроти на початку тисячоліття. Законодавство щодо захисту інфраструктури від кіберзагроз розвивалось поступово, від обмеження кола адресатів лише федеральними органами⁵ до розбудови широкої мережі публічно-приватного партнерства в цій сфері.

Початок першого періоду ознаменувало рішення Президента США № 63 1998 р., згідно з яким у межах Федерального бюро розслідувань було утворене Управління захисту об'єктів критичної інфраструктури (National Infrastructure Protection Center); при цьому в кожному департаменті засновувались посади співробітників із контролю за критичною інфраструктурою, що згодом об'єдналися у відповідний центр у межах Департаменту торгівлі (Critical Infrastructure Assurance Office (CIAO) of Department of Commerce)⁶. Крім того, Законом про захист критичної інфраструктури 2001 р. було визначене базове для відповідного законодавства поняття «критичної інфраструктури» як фізичних чи віртуальних систем та активів, які є настільки необхідними для США, що їх виведення з ладу або знищення могло б мати послаблюючий вплив на безпеку, національну економіку, національне публічне здоров'я або будь-яке їх поєднання. Цим актом також позначені сфери критичної інфраструктури: транспорт, енергетика, телекомунікації, фінансові сервіси та вода. Пізніше до цих сфер були додатково включені сектори: критичного виробництва, надзвичайних сервісів, базової оборонної індустрії, дамб, хімічний, комерційного устаткування, урядового устаткування, продовольства та сільського господарства, охорони здоров'я, інформаційних технологій та ядерних реакторів, матеріалів та сміття (усього 16)⁷. Крім того, в цьому Законі зазначалось, що політика кібербезпеки має здійснюватись на засадах публічно-приватного партнерства, а також на засадах, згідно з якими будь-які порушення в роботі фізичної чи віртуальної інфраструктури мають бути рідкісними, короткими, обмеженими географічно, керованими та мінімально глибокими для економіки, людини, урядових сервісів та національної безпеки США. Вказаним законом було створено Національний центр моделювання та аналізу інфраструктури (National Infrastructure Simulation and Analysis Center (NISAC)), який отримував для цілей своєї діяльності дані як з державних, так і з приватних джерел та забезпечував роботу федеральних і локальних інституцій, відповідальних за захист критичної інфраструктури⁸.

Іншим важливим для сфери аналізу актом першого етапу слід визнати Закон США про Департамент національної безпеки 2002 р., згідно з яким на вказаний Департамент покладено обов'язок запобігати, мінімізувати та боротися з наслідками тероризму, для чого йому було надано широкі повноваження із захисту критичної інфраструктури, в тому числі й від кіберзагроз. У структурі Департаменту було виділено Агенцію кібербезпеки та безпеки інфраструктури, а також почала реалізовуватися програма щодо моделювання та аналізу інфраструктури. До повноважень Департаменту належить розробка національного плану забезпечення основних ресурсів та критичної інфраструктури в США⁹. Донині було розроблено два відповідних плани (так звані National Infrastructure Protection Plan (NIPP): 1) Партнерство для безпеки та стійкості критичної інфраструктури (2013 р.); 2) Прийняття викликів для розробки та впровадження (2018 р.)¹⁰.

Ще однією важливою функцією, закріпленою за Департаментом національної безпеки, є проведення всеохоплюючої оцінки вразливості ключових ресурсів та критичної інфраструктури США, який втілюється у формі підготовки Списку найпріоритетнішої критичної інфраструктури (National Critical Infrastructure Prioritization Program (NCIPP) list of the nation's highest-priority critical infrastructure (CI)). Підхід до віднесення об'єктів до критичної інфраструктури є дуже гнучким і базується на критеріях, розроблених самим Департаментом національної безпеки¹¹. У деяких дослідженнях підкреслюється, що не слід плутати Національну базу даних про активи з переліком критичних активів, оскільки перший є всеохоплюючим каталогом, що серед іншого включає й національну критичну інфраструктуру та ключові ресурси^{12,13}.

Ще одним вагомим нормативним актом першого етапу розвитку відповідного законодавства США став Закон про управління федеральною інформаційною безпекою 2002 р. (Federal Information Security Management Act of 2002 (FISMA)). Не зважаючи на те, що наразі діє його оновлена редакція 2014 р., в його первісній редакції закладені деякі важливі норми, які становлять основу сучасної моделі захисту інформації від кіберзагроз в США. По-перше, ним встановлено засади захисту чутливої інформації, створеної федеральними агентствами, тому навіть зараз якщо НАСА оголошує конкурс на реалізацію певного проєкту приватними суб'єктами, вказаний закон передбачає необхідність дотримання контрагентами цього федерального агентства вимог щодо убезпечення чутливої інформації. По-друге, урядові агенції зобов'язуються щорічно, а також в міру необхідності звітувати перед Конгресом про інциденти порушення інформаційної безпеки. По-третє, Національний інститут стандартів та технологій при Департаменті торгівлі був уповноважений на розробку стандартів та керівних принципів стосовно захисту інформаційних систем держави, які урядові структури мають імплементувати в свою діяльність¹⁴. Відповідно до вимог цього закону було прийнято низку стандартів: FIPS 199 «Стандарти для категоризації безпеки федеральних інформаційних систем»¹⁵ та FIPS 200 «Мінімальні вимоги безпеки для федеральних інформаційних систем»¹⁶ в комплексі з NIST 800-53 «Рекомендований контроль безпеки для федеральних інформаційних систем»¹⁷. Згідно з цими стандартами План безпеки таких систем підлягає сертифікації та акредитації відповідно до стандартів NIST SP 800-18¹⁸ та 800-37¹⁹. Зазначена система захисту в дещо зміненому вигляді функціонує й зараз.

Тут слід зробити ремарку: проаналізовані вище положення законодавства США не поширюються на інформаційну систему національної безпеки, яка використовується для розвідувальної, крипологічної діяльності та управління військами²⁰, оскільки за безпеку цієї інформації відповідає Головний інформаційний

офіс Департаменту безпеки США²¹. І хоча механізми забезпечення урядової інформації в цивільній і безпечній сфері є певним чином схожими, але компетенційно вони розділені.

Другий етап в законодавчому забезпеченні кібербезпеки інформаційних та інших активів США почався з 2014 р, коли було прийнято спеціальний Закон про національну кібербезпеку. Відповідно до цього Закону було надано визначення базових для цієї сфери понять. «Кібернетичний ризик» тут визначається як загроза або вразливість інформації чи інформаційних систем і будь-які пов'язані з ними обставини, спричинені або ті, що виникли внаслідок недозволеного доступу, використання, розкриття, пошкодження, зміни чи знищення інформації та інформаційних систем, включаючи такі, що спричинені актом тероризму. «Інцидент» визначається як випадок, 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 використання²².

Згідно з цим Законом, до Національного інтеграційного центру із кібербезпеки та комунікацій Департаменту національної безпеки (The National Cybersecurity and Communications Integration Center (NCCIC)) увійшли як представники урядових структур, в тому числі розвідки, так і приватних компаній. Він став центральним хабом по виявленню кібернебезпек, уповноваженим на багатовекторне та міжсекторальне поширення інформації між урядовими структурами та приватним сектором, а також надання на вимогу технічної допомоги, сприяння управлінню ризиками і відповіді на інциденти. Крім того, цей орган виступає національним центром інформації про кібер- та комунікаційну техніку, проводить технічну експертизу та оперативну інтеграцію, а також керує 24/7 центром розвідування ситуацій, аналізу та реагування на інциденти, проводить глобальний обмін інформацією про кібер- та комунікаційні послуги²³. Крім цього, відповідно до вказаного Закону федеральним центром, який забезпечує інформацію від інцидентів, є United States Computer Emergency Readiness Team (US-CERT). Інформація про інцидент подається за спеціальними критеріями, які максимально допомагають виявити джерело загрози та масштаби шкоди. Отримана інформація оцінюється спільно US-CERT та NCCIC задля визначення ступеня небезпеки інциденту, а звіт про великі або значні кібернетичні інциденти відповідно до Директиви Президента № 41²⁴, подається в 7-денний строк до Конгресу²⁵. Ступінь відповідного інциденту оцінюється на підставі Системи оцінки кіберінцидентів (стандарт NIST 800-61)²⁶ та Схеми серйозності кіберінцидентів, відповідно до яких передбачено шість рівнів серйозності інцидентів. Якщо одночасно буде виявлено кілька інцидентів одного рівня щодо одного і той самого об'єкта, то оцінка небезпеки рівня інциденту піднімається на один порядок²⁷. Наразі відповідна система функціонує в межах Агенції з кібербезпеки та безпеки інфраструктури, заснованої відповідно до однойменного Закону 2018 р.²⁸

19 лютого 2019 р. Президентом США була підписана Директива щодо космічної політики № 4, відповідно до якої в межах Департаменту оборони створюється окремий підрозділ – Департамент космічних військ, задля забезпечення таких цілей: 1) захисту національних інтересів США в космосі і мирного використання космосу для всіх відповідальних суб'єктів, згідно із застосовним правом, в тому числі міжнародним; 2) забезпечення безперешкодного використання космосу США для цілей національної безпеки, економіки, громадян, партнерів та союзників; 3) стримування агресії та захисту націй та союзників від ворожих дій в / та / з космосу; 4) інтеграції космічних можливостей до всіх підрозділів військ; 5) побудови військових сил в / до космосу задля забезпечення національних інтересів тощо. Крім того, інші департаменти в складі Департаменту оборони, серед яких і департамент кібербезпеки, мають забезпечувати діяльність Департаменту космічних військ²⁹. Відповідно до стратегії цифрової модернізації до 2023 р. у США передбачається досягнення цілей, які стосуються безпеки космічної діяльності від кіберзагроз, а саме: 1) модернізувати управління, контроль, зв'язок та комп'ютеризацію інфраструктури та системи військових сил; 2) зміцнити співпрацю з міжнародними партнерами та союзниками за допомогою координації зусиль у рамках Міністерств оборони держав НАТО, союзників для просування оперативної сумісності та операційної коаліції, поглибити можливості обміну інформацією, надання партнерам доступу до набору основних послуг та оперативних інструментів для модернізованого виконання місії, зокрема послуг, інфраструктури та стандартів військового супутникового зв'язку (MILSATCOM); 3) покращити функціонування та захист позиціонування, навігації та хронометражу, що забезпечить точність удару та мережеву синхронізацію, поліпшить спроможності Об'єднаних сил діяти в умовах, що відрізняються від GPS або погіршених GPS; 4) забезпечити передачу даних про системи передачі сигналу, розвідку, нагляд та спостереження процесів, необхідних для розміщення даних з повітряних платформ до споживачів даних у момент потреби, що реалізовуватиметься за допомогою глобальних супутникових шлюзів для прямого зв'язку³⁰.

Ще більш рішучі дії щодо забезпечення критичної космічної інфраструктури від кібернетичних інцидентів ілюструє текст Директиви з космічної політики № 5 від 4 вересня 2020 р., в якій визначено, що принципи та практики кібербезпеки мають застосовуватись також до космічних систем, з особливим врахуванням віддаленого оновлення та реагування на інциденти, що вимагає інтегрованості їх в конструкцію космічного корабля перед запуском, оскільки в даний час фізичний доступ до більшості космічних апаратів на орбіті неможливий. Цікаво, що зазначена директива визнає необхідність захищати космічні системи від кіберінцидентів, не відносячи їх напряму до критичної інфраструктури, а з формулюванням їх функціоналу як запобігання порушенням їх здатності надавати надійну та ефективну підтримку в роботі критичної інфраструктури країни. Нею визначено і базовий термінологічний апарат, а саме: поняття «космічної системи», що поділяється на три сегменти: мережу наземного управління, космічний апарат та мережу користувача або місії.

Останні своєю чергою включають урядові космічні системи національної безпеки, урядові системи цивільного простору та приватні космічні системи. До «космічного механізму» Директива відносить супутники, космічні станції, ракети-носії, компоненти верхніх ступенів ракет-носіїв та космічні кораблі. Визначаються також поняття «позитивного контролю» та «критичних функцій» (збій або компрометація останніх може призвести до того, що космічний апарат не реагуватиме на санкціоновані команди, втрачатиме критичну здатність або відповідатиме на несанкціоновані команди).

До власників та операторів космічних систем пред'являється вимога розробляти та реалізовувати плани кібербезпеки, які серед іншого мають містити: а) захист від несанкціонованого доступу до критичних функцій, б) заходи фізичного захисту систем управління та телеметричного приймача, в) захист зв'язку за допомогою захищених передавачів приймання, шифрування, моніторингу потужності сигналу, г) захист наземних систем з метою зменшення ризику зараження шкідливим програмним забезпеченням та зловмисного доступу до систем, у тому числі від інсайдерських загроз, д) прийняття практик гігієни кібербезпеки, фізичної безпеки автоматизованих інформаційних систем та методологій виявлення вторгнень до елементів системи, таких як інформаційні системи, антени, термінали, приймачі, маршрутизатори, пов'язані локальні та глобальні мережі і джерела живлення, е) управління ризиками всього ланцюга поставок; оцінка інших доступних заходів зменшення ризику³¹. 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, затвердження кращих практик, стандартів тощо.

Переходячи до аналізу відповідної правової ситуації в Україні, насамперед зазначимо, що усвідомлення кіберзагроз, а отже, й нормотворення у відповідній сфері тут розпочалось значно пізніше, головним чином у зв'язку з виявленням вразливості критичної інфраструктури до кібератак, джерела яких походили від держави-агресора. Однак розвиток відповідного законодавства в Україні також можна поділити на два етапи, причому другий наразі тільки розпочався.

Указом Президента України № 96/2016 було введено в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України», на підставі якої було прийнято Закон України «Про основні засади забезпечення кібербезпеки України». На виконання положень цього Закону було ухвалено постанову КМУ № 563 від 23 серпня 2016 р. «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» та постанову КМУ № 518 від 19 січня 2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». Вказані акти сьогодні становлять основу законодавства про кібербезпеку в Україні, яке планувалось застосовувати в комплексі із законодавством щодо національної безпеки та захисту інформації в інформаційно-телекомунікаційних системах, а також підзаконними актами Державної служби спеціального зв'язку та захисту інформації України.

Систему органів, на які покладено функції з кіберзахисту в державі, наразі становлять:

- Національний координаційний центр кібербезпеки³² при Раді національної безпеки і оборони України, що здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки.

- Кабінет Міністрів України (далі – КМУ), який забезпечує формування та реалізацію державної політики у сфері кібербезпеки та ряд дотичних функцій.

- Адміністрація Державної служби спеціального зв'язку та захисту інформації України – центральний орган виконавчої влади із спеціальним статусом, до повноважень якого належить, зокрема, формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, державний контроль за станом захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, координація діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту, забезпечення впровадження організаційно-технічної моделі кіберзахисту та функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA³³.

- Кіберполіція в структурі Національної поліції України, до повноважень якої належать: реалізація державної політики в сфері протидії кіберзлочинності, завчасне інформування населення про появу нових кіберзлочинців, впровадження програмних засобів для систематизації кіберінцидентів, реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної цілодобової мережі контактних пунктів³⁴.

- Управління інформаційних технологій Міноборони, до повноважень якого належить забезпечення організації та координація діяльності структурних підрозділів Міністерства оборони у сфері інформаційної безпеки, кібербезпеки та інформатизації, участь у формуванні переліку критичної інфраструктури, участь у моніторингу інформаційного середовища, виявленні потенційних та реальних інформаційних і кібернетичних загроз національній безпеці України в сфері оборони; участь відповідно до компетенції в оцінці рівня воєнної загрози національній безпеці України, проведення інформаційно-аналітичної діяльності та прогнозування розвитку подій, пов'язаних з реалізацією кіберзагроз, здійснення відповідних інформаційних заходів³⁵. Примітні, що саме на це Управління покладено повноваження стосовно провадження, відповідно до закону, космічної діяльності у сфері оборони та національної безпеки України.

До системи протидії кіберрозвідкам іноземних держав, боротьбу з кібертероризмом і кібершпигунством тощо відносять і Ситуаційний центр забезпечення кібербезпеки Служби безпеки України, хоча ця обслуговуюча допоміжна структура до органів держави, звісно, віднесена бути не може³⁶.

Склад органів кіберзахисту в Україні в цілому належить до сектору безпеки і оборони в розумінні ч. 2 ст. 12 Закону України (далі – ЗУ) Про «Про національну безпеку України», що є цілком логічним з огляду на те, що кібербезпека є складовою національної безпеки і оборони³⁷. Водночас слід зазначити, що відповідні органи створюють базу для розвитку спеціальної системи кіберзахисту у всіх галузях господарювання, де є об'єкти критичної інфраструктури. І перші спроби створення таких механізмів уже зроблено в фінансовій сфері.

Так, команда реагування на кіберінциденти в банківській системі (CSIRT-NBU) Центру кіберзахисту Національного банку України³⁸ проводить раннє оповіщення, обмінюється інформацією, технічними стандартами та навіть проводить спільні навчання з Державною службою спеціального зв'язку та захисту інформації України відповідно до Меморандуму про взаємодію та співробітництво в сфері кібербезпеки та кіберзахисту від 2 серпня 2019 р.³⁹ Водночас вважаємо, що такий інструмент, як меморандум про співробітництво між державними органами, не є адаптованим для відповідних відносин інструментом, його юридична сила чітко не визначена. На нашу думку, взаємодія між державними та приватними суб'єктами у сфері забезпечення кібербезпеки доцільно було б регламентувати в окремому законі або принаймні у постанові КМУ. Крім того, слід брати до уваги, що механізми кіберзахисту не обмежуються національними кордонами, а тому в правовому порядку мають бути враховані вимоги щодо інтероперабельності.

Слід зазначити, що аналізуючи перші кроки реалізації чинної моделі кіберзахисту в Україні, можна вже констатувати низку проблем. Насамперед впадає в очі наявне дублювання, а подекуди й суперечливість базових термінів «кібератака», «об'єкти критичної інфраструктури» та деякі інші, що використовуються в різних нормативних актах. Не сприяє ефективному розвитку правовідносин у відповідній сфері й те, що досі не існує затвердженого переліку об'єктів критичної інфраструктури та чітких вимог до проведення незалежного аудиту інформаційної безпеки. Підзаконні акти Державної служби спеціального зв'язку та захисту інформації України спрямовані головним чином на захист державних інформаційних ресурсів і не враховують вимог щодо взаємодії державного та приватного секторів у питаннях захисту критичної інфраструктури незалежно від належності її до тієї чи іншої форми власності.

Водночас слід констатувати, що увага до цієї проблематики в державі зростає. Зокрема, Український інститут майбутнього у 2020 р. представив доповідь «Кібербезпека. Новий підхід в Україні», в якій вказав на застарілість стратегії кібербезпеки, відсутність єдиної національної системи захисту критичної інфраструктури, необхідність розроблення законодавчих актів, що реалізують положення Конвенції Ради Європи про кіберзлочинність, а також зміни інституційної моделі побудови системи кібербезпеки України за секторальним принципом з огляду на прийняття закону про критичну інфраструктуру⁴⁰.

Розробленням проекту закону «Про критичну інфраструктуру», на нашу думку, було розпочато 2-й етап розвитку вітчизняного законодавства про кібербезпеку. У відповідному законопроекті визначається досить розгалужена державна система захисту критичної інфраструктури з розподілом на режими функціонування, критерії віднесення об'єктів до критичної інфраструктури, їх категоризація й паспортизація, контроль за рівнем безпеки об'єктів критичної інфраструктури шляхом оцінки захищеності об'єктів критичної інфраструктури⁴¹. Водночас пропонується у вказаному проекті модель має низку недоліків, серед яких: 1) нечітка інституційна система забезпечення кібербезпеки (РНБО не включена до відповідної системи, центральні органи виконавчої влади розподіляються без чітких та зрозумілих підстав паралельно на спеціальні, інші та органи виконавчої влади, які визначені відповідальними за відповідні сектори критичної інфраструктури; при цьому взаємодія між органами влади визначається як за посередництвом затвердженого КМУ Регламенту обміну інформацією, так і відповідно до планів взаємодії з суб'єктами державної системи захисту, який погоджується у встановленому законодавством порядку; 2) критерії віднесення до об'єктів критичної інфраструктури не є чіткими, вони включають об'єкти загальнодержавного значення, що становлять підвищену небезпеку, мають стратегічне значення, підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду тощо, що цілком може не підпадати під ознаки об'єкта критичної інфраструктури, яким визначається підприємство, установа, організація, а не природний ресурс чи інший об'єкт матеріального світу; 3) режими функціонування державної системи кіберзахисту не відображають ключової характеристики взаємодії із кіберзагрозами – оперативності, адже у вказаному проекті зазначається, що уповноважений орган у сфері захисту критичної інфраструктури надає пропозиції щодо оголошення зміни режимів функціонування державної системи захисту критичної інфраструктури КМУ, що може зайняти дні чи тижні, коли рахунок буде йти на секунди і хвилини. Це стосується й паспортизації об'єктів критичної інфраструктури, адже стрімкий розвиток кіберзагроз може виявити недієвість громіздкої системи паспортизації; 4) передбачену систему контролю за рівнем безпеки об'єктів критичної інфраструктури без визначення механізмів реагування на виявлення порушень також не можна визнати адекватним засобом.

Висновки. Наразі в Україні базове законодавство про кібербезпеку знаходиться на стадії формування, тому розроблення спеціального правового забезпечення цих відносин у космічній сфері може зіштовхнутися зі значними проблемами. Внаслідок дублювань та прогалин в розмежуванні повноважень між МЕРТ, а сьогодні вже Мінстратегпромом⁴², та ДКА України, яке виникло на підставі постанови КМУ № 1072 від 4 грудня 2019 р.⁴³, не зрозуміло, який із цих органів має бути відповідальним у сфері космічної діяльності за вказаний сектор критичної інфраструктури. На нашу думку, вказану функцію мало б взяти на себе ДКА України.

Як в чинному законодавстві про кібербезпеку, так і в проекті ЗУ «Про критичну інфраструктуру», відсутні будь-які згадки про необхідність формування спеціальних правових норм із забезпечення кібербезпеки космічної діяльності. Виняток може становити хіба що декларативна вказівка в Стратегії кібербезпеки

України на необхідність розвитку інфраструктури електронних комунікацій, включаючи широкосмуговий доступ до мережі Інтернет, цифрове та інтерактивне телебачення⁴⁴, яка так і не знайшла свого практичного втілення. Відповідно до ЗУ «Про основні засади забезпечення кібербезпеки України» до об'єктів критичної інфраструктури можуть бути віднесені, а в проєкті ЗУ «Про критичну інфраструктуру» – відповідно «відносяться» підприємства, установи, організації незалежно від форми власності, які включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави. Навіть за умов включення усіх 14 об'єктів авіаційної та ракетно-космічної промисловості⁴⁵ до переліку об'єктів критичної інфраструктури, невизначеними залишається, по-перше, який режим кіберзахисту буде забезпечено для приватних суб'єктів космічної діяльності, яких після внесення змін до ЗУ «Про космічну діяльність», що набули чинності у січні 2020 р., стає дедалі більше; по-друге, як буде співвідноситись кіберзахист підприємства з конкретними видами космічної діяльності, кожен з яких вимагає своїх специфічних засобів захисту. На нашу думку, принципи та основні вимоги кіберзахисту космічної діяльності мають бути закріплені в базовому для галузі ЗУ «Про космічну діяльність». А плани убезпечення від кіберзагроз (кібератак чи кіберінцидентів) та оперативного реагування на них мають стати одним із необхідних документів для отримання дозволу на провадження окремих видів космічної діяльності⁴⁶.

Проаналізований вище досвід у розвитку законодавства США щодо забезпечення правового режиму кіберзахисту космічної сфери, ретельність відповідного регулювання в сучасних умовах, його опрацьованість як з нормативно-інституційної, так і з технічної точок зору, демонструє поступове, але неухильно зростаюче усвідомлення на державному рівні в США важливості відповідної проблеми для безперешкодного, ефективного функціонування космічної діяльності. Увага, яка в останні роки почала приділятися відповідній проблематиці в Україні, є обнадійливою ознакою можливих змін на краще і в нашому національному законодавстві щодо кібербезпеки. А проаналізований досвід США може надати певний орієнтир для напрямів його подальшого вдосконалення.

¹ Cyber Security Law, its Regulation and Relevance for Outer Space. URL: <https://www.unoosa.org/documents/pdf/hlf/HLF2017/presentations/Day2/Session7b/Presentation5.pdf>

² Electronic and Cyber Warfare in Outer Space, May 2019 – Space Dossier 3. URL: <https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf>

³ Global Counterspace Capabilities, 2020 Report. URL: <https://swfound.org/counterspace/>

⁴ 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/>

⁵ [H.R. 4577] PUBLIC LAW 106-554—APPENDIX C, title V, DEC. 21, 2000. URL: <https://www.govinfo.gov/content/pkg/PLAW-106publ554/pdf/PLAW-106publ554.pdf>

⁶ PRESIDENTIAL DECISION DIRECTIVE/NSC-63, May 22, 1998. URL: <https://fas.org/irp/offdocs/pdd/pdd-63.htm>

⁷ National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience

⁸ 42 U.S. Code § 5195c. Critical infrastructures protection. URL: <https://www.law.cornell.edu/uscode/text/42/5195c> ; <https://www.congress.gov/bill/107th-congress/senate-bill/1407/text>

⁹ H.R.5005 - Homeland Security Act of 2002. URL: <https://www.congress.gov/bill/107th-congress/house-bill/5005/text>

¹⁰ National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge is managed by the National Protection and Programs Directorate (NPPD), National Risk Management Center (NRMC), within the Department of Homeland Security (DHS), and in partnership with the National Institute for Hometown Security (NIHS). URL: <https://www.thenihs.org/>

¹¹ Critical Infrastructure Protection. DHS List of Priority Assets Needs to Be Validated and Reported to Congress, March 2013. URL: <https://www.gao.gov/assets/660/653300.pdf>

¹² John Moteff Critical Infrastructure: The National Asset Database CRS Report for Congress, Updated July 16, 2007. 19 p. (P. 8–9). URL: <https://fas.org/sfp/crs/homesec/RL33648.pdf>

¹³ DOD Dictionary of Military and Associated Terms. January 2020. URL: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>

¹⁴ H.R.3844 Federal Information Security Management Act of 2002. URL: <https://www.congress.gov/bill/107th-congress/house-bill/2458/text>

¹⁵ FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems: Federal information processing standards publication, 2004. URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>

¹⁶ FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems: Federal information processing standards publication, 2006. URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>

¹⁷ NIST SP 800-53 Revision 4 Recommended Security Controls for Federal Information Systems and Organizations. URL: <https://nvd.nist.gov/800-53>

¹⁸ SP 800-18 Rev. 1 Guide for Developing Security Plans for Federal Information Systems. URL: <https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final>

¹⁹ SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. URL: <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>

²⁰ US Code Title 44 - PUBLIC PRINTING AND DOCUMENTS CHAPTER 35 - COORDINATION OF FEDERAL INFORMATION POLICY SUBCHAPTER III - INFORMATION SECURITY Sec. 3542 – Definitions. URL: <https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title44-chapter35-subchapter2&edition=prelim>

²¹ DoD Digital Modernization Strategy, 5 June 2019, 72 p. P. 63. URL: <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>

²² S.2519 - National Cybersecurity Protection Act of 2014. URL: <https://www.congress.gov/bill/113th-congress/senate-bill/2519/text?q=%7B%22search%22%3A%5B%22cyber+act%22%5D%7D&r=38&s=2>

- ²³ NCCIC Services for Federal Agencies. URL: <https://us-cert.cisa.gov/sites/default/files/publications/NCCIC%20Service%20Menu%20-%20Federal.pdf>
- ²⁴ Presidential Policy Directive – United States Cyber Incident Coordination: Presidential policy directive/PPD-41, July 26, 2016. URL: <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>
- ²⁵ S. 2521 An Act To amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security. Dec. 18, 2014. URL: <https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf>
- ²⁶ SP 800-61 Rev. 2. Computer Security Incident Handling Guide. URL: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>
- ²⁷ US-CERT Federal Incident Notification Guidelines. URL: https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf
- ²⁸ Cybersecurity and Infrastructure Security Agency Act of 2018. URL: <https://www.congress.gov/bill/115th-congress/house-bill/3359>
- ²⁹ Establishment of the United States Space Force: Space Policy Directive-4, February 19, 2019. URL: <https://www.spaceforce.mil/About-Us/SPD-4>
- ³⁰ DoD Digital Modernization Strategy, 5 June 2019, 72 p. P. 16-22. URL: <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>
- ³¹ 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>
- ³² Національний координаційний центр кібербезпеки посилює співпрацю із міжнародними виробниками кібер-технологій / сайт РНБО. URL: <https://www.rnbo.gov.ua/ua/Diialnist/4658.html> (дата звернення : 07.08.2020).
- ³³ Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України: постанова КМУ від 3.09.2014 р. № 411. URL: <https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#Text>
- ³⁴ Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 року. URL: <https://cyberpolice.gov.ua/strategy-2020/>
- ³⁵ Про управління інформаційних технологій: наказ Міністерства оборони України № 426 від 5.08.2019 р. URL: https://www.mil.gov.ua/content/mou_orders/mou_426_05082019.pdf
- ³⁶ Ситуаційний центр забезпечення кібербезпеки / Сайт СБУ. URL: <https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky>
- ³⁷ Про Національну безпеку України: Закон України № 2469-VIII від 21.06.2018 р. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
- ³⁸ Національний банк України посилює вимоги до інформаційної безпеки та кіберзахисту в банках України / Сайт НБУ, 04.10.2017. URL: https://old.bank.gov.ua/control/uk/publish/article?art_id=55564890
- ³⁹ Національний банк та Державний центр кіберзахисту співпрацюватимуть у сфері кібербезпеки / Сайт НБУ від 02.08.2019. URL: <https://bank.gov.ua/ua/news/all/natsionalniy-bank-ta-derjavniy-tsentr-kiberzahistu-spivpratsyuvatimut-u-sferi-kiberbezpeki>
- ⁴⁰ Кібербезпека. Новий підхід в Україні від UIFuture, 24.07.2020. URL: <https://uifuture.org/publications/kiberbezpechna-ukrayina-novyj-pidhid/>
- ⁴¹ Проект Закону про критичну інфраструктуру та її захист № 10328 від 27.05.2019 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996
- ⁴² Деякі питання Міністерства з питань стратегічних галузей промисловості України: постанова КМУ від 7.09.2020 р. № 819. URL: <https://www.kmu.gov.ua/nras/deyaki-pitannya-ministerstva-z-pitan-a819>
- ⁴³ Про внесення змін та визнання такими, що втратили чинність, деяких актів Кабінету Міністрів України: постанова КМУ № 1072 від 04.12.2019 р. URL: <https://zakon.rada.gov.ua/laws/show/1072-2019-%D0%BF#n166>
- ⁴⁴ Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15.03.2016 р. URL: <https://zakon.rada.gov.ua/laws/show/96/2016#Text>
- ⁴⁵ Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави: постанова КМУ від 4.03.2015 р. № 83. URL: <https://zakon.rada.gov.ua/laws/show/83-2015-%D0%BF#Text>
- ⁴⁶ Про затвердження Порядку видачі (відмови у видачі, анулювання) дозволів на провадження окремих видів космічної діяльності: постанова КМУ від 26.02.2020 р. № 197. URL: <https://zakon.rada.gov.ua/laws/show/197-2020-%D0%BF#Text>

Резюме

Малишева Н.Р., Гурова А.М. Правові засади кібербезпеки космічної діяльності в США: досвід для України.

У статті досліджується розвиток правових засад та інституційної структури, що лежать в основі кібербезпеки США. Особлива увага приділяється принципам та керівним нормам, які створюють умови для кібербезпеки космічної діяльності, що є взірцевими не лише для американських суб'єктів господарювання, а й становлять кращу практику нормотворення в цій сфері для інших космічних держав, зокрема для України. Проаналізовано також чинне законодавство України у сфері кібербезпеки та проект щодо його вдосконалення, виявлено їх переваги й недоліки, а також запропоновано внесення змін до деяких законодавчих актів, що регулюють космічну діяльність, задля підсилення її кібербезпеки.

Ключові слова: кібербезпека, інцидент, кіберризик, кіберзагроза, критична інфраструктура, космічна діяльність.

Резюме

Малишева Н.Г., Гурова А.Н. Правовые основы кибербезопасности космической деятельности в США: опыт для Украины.

В статье исследуется развитие правового регулирования и институциональной структуры, составляющие основу кибербезопасности США. Особое внимание уделяется принципам и руководящим нормам, создающим условия для кибербезопасности в сфере космической деятельности, которые не только применяются субъектами хозяйствования США, но и формируют лучшую практику нормотворчества в этой сфере для других космических держав, включая Украину. Проанализировано действующее законодательство Украины в сфере кибербезопасности и перспективные проекты в этой сфере, выявлены их пре-

имущества и недостатки, а также предложено внесение изменений в некоторые законодательные акты, регулирующие космическую деятельность, для усиления ее кибербезопасности.

Ключевые слова: кибербезопасность, инцидент, киберриск, киберугрозы, критическая инфраструктура, космическая деятельность.

Summary

Nataliia Malysheva, Anna Hurova. Legal Framework of the Space Activity Cybersecurity in the USA: Experience for Ukraine.

The article depicts the timeline of the development of the cybersecurity legislation in the USA, which divided into two stages. The first one rises as a response to the large-scale terroristic threats in 2001 and lasted until 2014. The second one starts with the massive and multisectoral cyber incidents and cyber-attacks the US faced in the last five years. In addition, it was analyzed the changes in institutional structure aimed to support the cybersecurity in the US and their branched connections with public and private actors. The main attention was paid to the content of the Memorandum on Space Policy Directive-5 "Cybersecurity Principles for Space Systems", which could be the example of the best law-making practice not only for space actors within the US, but also for law-making actors of all space-faring nations.

The chronology of the elaboration of cybersecurity legislation and the institutional structure of their support in Ukraine analyzed in the second part of this article. On this ground, we observed some weak aspects of national cyber legislation. First is duplication and inconsistency of the basic terms, like "cyberattack", "critical infrastructure". The second one is the absence of an approved list of critical infrastructure facilities and clear requirements for conducting an independent information security audit. The third one is by-laws are aimed primarily at protecting public information resources and do not take into account the requirements for cooperation between the public and private sectors in the protection of critical infrastructure, regardless of its affiliation to any form of ownership.

Analysis of the draft law concerned critical infrastructure permits to make a conclusion about coming to the second stage in the development of cyber legislation in Ukraine, which will enhance the development of particular legislation within to each sector of critical infrastructure. In this regard, it is necessary to elaborate legal background for cybersecurity of space activity. For this aim, we suppose as necessary to designate the State Space Agency of Ukraine as a responsible entity in the field of space activities for the specified sector of critical infrastructure. Furthermore, the article suggested prescribing plans to protect against cyber threats (cyber attacks or cyber incidents) as one of the necessary documents for obtaining a permit to conduct certain types of space activities.

Key words: cybersecurity, incident, cyber risk, cyber threat, critical infrastructure, space activities.

DOI: 10.36695/2219-5521.3.2020.60

УДК 341.22:349.6

М.О. МЕДВЕДЄВА

*Марина Олександрівна Медведєва, доктор юридичних наук, професор, професор Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка**

ORCID: 0000-0003-4010-4659

ЮРИСДИКЦІЙНІ ПИТАННЯ У СПРАВІ OGONI

Постановка проблеми. Наслідки видобутку корисних копалин у нігерійському регіоні *Ogoni*, що здійснювався транснаціональною компанією Шелл (*Royal Dutch Shell*) починаючи з 50-х рр. XX ст., спровокували низку судових проваджень на національному і міжнародному рівнях, а також підживили експертну й наукову дискусію щодо корпоративної соціальної відповідальності, захисту прав корінних народів та етнічних меншин, відповідальності держави за діяльність приватних осіб, зокрема корпорацій, у випадку спричинення екологічної шкоди чи порушень прав людини. Справа *Ogoni*, яка поєднує в собі декілька гучних справ, що розглядались у судах Нігерії, США, Нідерландів, Великої Британії, Африканській комісії з прав людини, Суді Економічного співтовариства держав західної Африки, важлива ще й тим, що завдяки їй у науці активно обговорюються складні питання, зв'язані з юрисдикцією держав, як-от: екстериторіальна юрисдикція, універсальна юрисдикція в цивільних справах, «підняття корпоративної завіси», «пошук зручного суду», доктрини *forum non conveniens*, *forum necessitatis*, тощо. Аналіз зазначеної справи дає можливість прослідкувати, яким чином всі ці питання вирішуються в практичній площині.

Аналіз останніх досліджень і публікацій. Дослідженням юрисдикційних питань справи *Ogoni* займались переважно зарубіжні вчені, такі як B. Konne, B. Manby, E. Willis, E. Weswasi, C. Ryngaert, O. De Schutter, C. Van Dam, Ch. Mandap, G. Van Calster, F. Coomans. Однак цим дослідженням певним чином бракує комплексності.

Формулювання мети статті. Метою нашої статті є аналіз теоретичних та практичних юрисдикційних питань, зв'язаних зі справою *Ogoni*, на прикладі конкретних судових проваджень. Рішення по суті будуть розглядатися лише опосередковано.

© М.О. Медведєва, 2020

* *Maryna Medvedieva, Dr. hab. in Law, Professor, Professor of the Institute of International Relations of Taras Shevchenko National University of Kyiv*