ТЕОРЕТИКО-ПРАВОВІ ПРОБЛЕМИ АНАЛІЗУ ТА ОЦІНКИ ЗАГРОЗИ БЕЗПЕЦІ ОБ'ЄКТАМ АЕРОКОСМІЧНОГО КОМПЛЕКСУ УКРАЇНИ

Олег Ігорович ШИНКАРЕНКО,

здобувач вищої освіти ступеня доктора філософії (PhD), Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут»
http://orcid.org/0000-0002-6913-4667

Ігор Ростиславович ШИНКАРЕНКО,

PhD (канд. юрид. наук), професор, Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут", м. Харків, Україна
https://orcid.org/0000-0001-5524-2259
sir2009@ukr.net

Ірина Ігорівна ШИНКАРЕНКО,

PhD (канд. юрид. наук),доцент, доцент кафедри оперативно-розшукової діяльності та розкриття злочинів Харківського національного університету внутрішніх справ факультету № 2
http://orcid.org/0000-0001-7136-3333
i_shinkarenko@ukr.net

In the work, it is determined that the threats to the objects of the aviation and space sector of critical infrastructure in the conditions of martial law are not only the Russian troops, but also the activities of joint criminal, radical-terrorist groups of various directions;

It was determined that despite the cyber attacks on the space and aviation infrastructure of Ukraine and other countries, after the start of full-scale aggression on February 24, 2022, its impact on the economy and defense capability of Ukraine increased. This requires the formation of an organizational and legal model of the security of the aerospace industry of Ukraine, as a component of critical infrastructure.

It has been proven that the importance of the aerospace industry lies in its resilience against internal and external threats. It was determined that one of the factors of threats to the aviation and space infrastructure is the unauthorized leakage of information about the production facilities, technology, and logistics of enterprises that develop promising types and manufacture various components of aviation and rocket and space technology, repair civil, dual-use and military aircraft, and aeronautical devices , the location of objects of control and information support, the system of physical protection and various types of security of the specified objects, which was carried out by persons who were accomplices of the occupiers. This affects the sustainability of the entire aerospace industry and its individual facilities. It was determined that the model of stability of any critical infrastructure object consists of: regulatory support system; the system of bodies - security subjects; risk assessment systems and identification of threats to various types of object security; systems of action algorithms in regular and emergency situations.

It was determined that the directions for improving the legal and organizational-tactical provision of information security in order to increase its stability are the formation of a modern system

of organizational-legal provision of the stability of the aerospace complex based on the provision of scientific, methodical and technological support for the activities of subjects of protection against threats to the objects of the aerospace complex of Ukraine and risk assessment by determining: 1) threats to a specific object, as well as means and methods of a possible attack; 2) probabilities of threat occurrence; 3) consequences of the attack; 4) vulnerabilities; 5) residual risk.

Keywords: *object of space activity, information security, risk, security threats, risk assessment, sustainability.*

24 лютого 2022 року Російські війська почали вторгнення на територію України та ракетні обстріли всіх основних аеродромів України, намагаючись позбавити її можливості забезпечувати протиповітряну оборону. Як наслідок, з 35 аеродромів було пошкоджено:

- 11 військових аеродромів - на суму 0,4 млрд дол. США та літак АН-225 “Мрія” - на суму 0,3 млрд дол. США;
- 12 цивільних аеропортів;
- 7 подвійного призначення.

Загальні прямі та непрямі збитки за у цій сфері за війну досягли понад 12 млрд дол. США. [1,с. 19-20].

В той же час авіаційний сектор аерокосмічної галузі України не обмежується вказаними об’єктами. До його складу відноситься:

- науково-конструкторська та дослідницька-випробувальна інфраструктура:
- промислова інфраструктура, що виготовляє окремі авіаційні об’єкти (повітряні судна та БПЛА), а також комплектуючи;
- експлуатаційна інфраструктура, що забезпечує повсякденну експлуатацію повітряних суден, об’єктів аеронавігації, систем життєдіяльності об’єктів авіаційної інфраструктури;
- ремонтні установи, що здійснюють регламентні ремонти повітряних суден цивільного, подвійного та військового призначення, засоби ППО, БПЛА та склади їх зберігання [2, с. 229-233.].

Дослідження ризиків та загроз об’єктам цивільної авіації в умовах воєнного стану свідчить, що загрозами об’єктів авіації є не тільки війська РФ але й:

- злочинна спільнота;
- радикально-терористичні угрупування різного спрямування;
- витоки інформації пов’язані з не виконанням правил розповсюдження інформації обмеженого користування суб’єктами інформаційної діяльності;
- діяльність російських ДРГ.

Проведені у дослідженнях попередників наукові розвідки щодо безпеки та стійкості критичної інфраструктури особливо до військової агресії Росії свідчить, що в останній час здійснюється виокремлення космічної інфраструктури та формування окремих напрямів державної інфраструктурної політики у сфері авіаційно-космічної діяльності та вдосконалення законодавства України, що регулює відносини у сфері інфраструктури [3, С. 144 - 148].

На сьогодні аерокосмічна галузь стла одним з важелей нашої перемого. Так у своєму виступі Ж. Борель вказує, що «збройна агресія Росії проти України підкреслила значення існуючих космічних технологій для безпеки й оборони

Європи, виявила певні вразливості у цій сфері та підштовхнула ЄС до розробки оновленої стратегії із розвитку власних космічних спроможностей та підвищення стійкості критичної інфраструктури [4]».

Незважаючи на кібератаки по космічній та авіаційній інфраструктурі України та інших країн після початку повномасштабної агресії 24 лютого 2022 року, лише у 2022 році світовий космічний бюджет зріс на 9% до абсолютного показника у 103 мільярди євро. Серед цих витрат фінансування «військового» космосу збільшилося на 16% та склало 48 мільярдів євро, така пропорція у показниках зростання є свідченням того, які пріоритети зараз людство надає у розвитку космічних технологій. Наразі навколо Землі обертаються близько 5500 супутників, і майже 10% (близько 500 одиниць) належать або керуються військовими організаціями.

Значний вплив аерокосмічного комплексу на національну безпеку стає підґрунтям того, що виникають виклики щодо формування організаційно-правової моделі безпеки авіакосмічної галузі України, як складової критичної інфраструктури.

Формуючі таку модель слід враховувати окрім авіаційної складової ще й космічну . До складу космічного комплексу України входять: — ракети-носії; — космічні апарати; — наземні комплекси [5].

Важливе значення аерокосмічної галузі постає у її стійкості від внутрішніх та зовнішніх загроз. Особливе це торкається щодо забезпечення стійкості наземних комплексів космічної складової визначається їх багатоаспектністю у сфері інформаційного забезпечення космічної діяльності.

Окрім того суб'єктам господарювання у космічному секторі аерокосмічної галузі дозволено здійснювати:

- наукові космічні дослідження;
- використання космічного простору;
- розроблення об'єктів космічної діяльності (в тому числі їх агрегатів та складових частин);
- виробництво об'єктів космічної діяльності (в тому числі їх агрегатів та складових частин);
- ремонт та технічне обслуговування об'єктів космічної діяльності (в тому числі їх агрегатів та складових частин);
- експлуатація об'єктів космічної діяльності (в тому числі їх агрегатів та складових частин);
- забезпечення запуску апаратів, їх складових частин.

Враховуючи думки фундаторів ЄС можливо визначити, що космічні технології сприяють:

- розвитку космічної картографії;
- космічного зв'язку;
- розвитку ключових секторів критичної інфраструктури , включаючи транспорт, ІТ, телекомунікації;
- забезпечують розвиток сектора безпеки й оборони перспективним озброєнням , послугами зв'язку та поточною інформацією.

Як вбачається? основною складовою ефективності та стійкості цих комплексів в умовах мінливої обстановки воєнного періоду є рівень

інформаційної безпеки кожного об'єкта та суб'єкта господарювання, а також стійкість до різних терористичних загроз [6, с. 93-110].

Таким чином суб'єкти господарювання різних форм власності охоплюють весь технологічних цикл науково-конструкторського, промислового та експлуатаційного забезпечення виготовлення, випробування та експлуатації космічних та наземних об'єктів у сфері космічної діяльності. Станом 24 лютого 2022 року до сфери управління ДКА України входило 23 суб'єкти господарювання (таблиця 5.11) – 15 державних підприємств (ДП), 3 публічні акціонерні товариства (ПАТ), 5 бюджетних установ [5; 7, с.421-422;]. Розвиток означених суб'єктів та формування їх стійкості здійснювалося у межах шості космічних програм, двох стратегій кібербетичної безпеки України, Стратегії інформаційної безпеки, [8].

Попередні наші наукові розвідки свідчать, що одним з чинників загроз авіаційно-космічної інфраструктури є несанкціонований виток інформації про виробничі потужності, технологію, логістику підприємств на яких розробляють перспективні види та виготовляють різни комплектуючі авіаційної та ракетно-космічної техніки, ремонтують літаки цивільного, подвійного та військового призначення, аеронавігаційні прилади, розташування об'єктів Укравероруху, систему фізичної охорони та різних видів убезпечення означених об'єктів, що здійснений особами – пособниками окупантів [9, С.37-43].

На тлі означеного змінився і рівень суспільної небезпеки деяких загально кримінальних злочинів та формування сучасної методики протидії новітнім та традиційним інформаційним кримінальним правопорушенням у період військової агресії. Означене визначило низку викликів щодо правоохоронних органів та Влади України взагалі та забезпечення інформаційної безпеки об'єктів космічної діяльності.

Слід відзначити, що інформаційна безпека пройшла низку етапів у своєму розвитку. В умовах сьогодення відносно аерокосмічного комплексу України, реалізується етап, що почався зі створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних інформаційно-комунікаційних систем. Означене визначає необхідність створення макросистеми інформаційної безпеки людства під егідою ведучих міжнародних форумів. [10].

Не зважаючі на складність військового періоду необхідно будувати систему стійкості аерокосмічної галузі України особливо у сфері інформаційної безпеки.

У цьому сенсі слід враховувати, що сучасна наукова спільнота визначає стійкість, як здатність функціонувати і розвиватись в умовах мінливого внутрішнього і зовнішнього середовища [11].

Враховуючі думки науковців з НІСД та представників української наукової школи безпекознавства, можливо виокремити ознаки стійності на рівні конкретних об'єктів, галузей та держави в цілому:

- спроможність надійно функціонувати у штатному режимі;
- адаптуватися до умов, що постійно змінюються**;**
- протистояти та швидко відновлюватися після реалізації загроз будь-якого виду: природного і техногенного характеру, загроз, що спричинені протиправними діями, та інших загроз [12, с. 17-18];

- рівноважне співвідношення зовнішніх та внутрішніх загроз, що й обумовлює її динамічний розвиток [13, с. 141].

Враховуючі думки інших представників української наукової спільноти, можемо констатувати, що формування стійкості системи – об'єкта залежить від спроможності суб'єктів убезпечення сформувати систему моніторингу ризиків та загроз безпеки, побудови організаційно-тактичної моделі запобігання, стримування, нейтралізації або пом'якшення наслідків терористичних дій спрямованих на знищення, виведення з ладу або зловмисне використання критичної інфраструктури в цілому та об'єктів аерокосмічного комплексу України, взагалі.

Як наслідок підгрунтям модель стійкості будь якого об'єкта критичної інфраструктури складається з: системи нормативного забезпечення; системи органів – суб'єктів убезпечення; системи оцінки ризиків та визначення загроз різним видам безпеки об'єктів; системи алгоритмів дій у штатних та надзвичайних обставинах.

Важливе значення щодо формування системи оцінки ризиків та визначення загроз різним видам безпеки об'єктів аерокосмічного комплексу України має система стандартів та нормативного регулювання оцінки ризиків та загроз використанням конкретних технологій особливо у інформаційній сфері.

Найвідоміші стандарти, які використовуються на території України: ISO 27001, ISO 27005, ISO 17799 оцінки ризиків та визначення загроз різним видам безпеки об'єктів, є:

1. Міжнародний стандарт ISO/IEC 27001:

- визначає процеси контролю і підтримки ефективної системи інформаційної безпеки на грунті: вимог до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої системи управління інформаційною безпекою відповідно існуючих ризиків;
- реалізуються в рамках документованих процесів управління інформаційноою безпекою, за моделлю PDCA (Plan-Do-Check-Act);
- дозволяє здійснювати оцінку ризиків, проектування і реалізацію системи інформаційної безпеки, управління і переоцінку нею.

2. Міжнародний стандарт ISO/IEC 27005:

- призначений для визначення в організації підходу до управління ризиками в залежності, області застосування управління ризиків;
- забезпечує рекомендації для управління ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації;
- підтримує загальні концепції, визначені в ISO/IEC 27001, і призначений для сприяння адекватного забезпечення інформаційної безпеки на основі підходу, пов'язаного з управлінням ризику;
- застосовується для організацій усіх типів (наприклад, комерційних підприємств, державних установ, некомерційних організацій), які планують здійснювати управління ризиків інформаційної безпеки об'єкта господарювання.

3. Міжнародний стандарт ISO/IEC 17799**:**

- вимагає при створенні ефективної системи безпеки увагу слід приділити комплексному підходу до управління інформаційною безпекою;
- елементи управління розглядаються не тільки технічні, але й організаційно- адміністративні заходи, спрямовані на забезпечення наступних вимог до інформації: 1) конфіденційність; 2) цілісність; 3) достовірність; 4) доступність. [14]

В той же час проведений аналіз нормативної та організаційної складової стійкості аерокосмічного комплексу України свідчить про низку недоліків:

1. Недоліки законодавства:
- відсутність нормативно закріплених критеріїв визначення оцінки негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему критичної інфраструктури;
- відсутність у чинному законодавстві з регулювання поняття термін «стійкість» об'єкта та його нормативновизначених складових.

2. Недоліки організації ризик аналізу відносно об'єктів космічної діяльності у інформаційній сфері: відсутність *мап процесу оцінки ризику*, яка включає виявлення характерних проблем, оцінку залишкового ризику та підготовку рекомендацій

Висновки. Напрями вдосконалення правового та організаційно-тактичного забезпечення інформаційної безпеки з метою підвищення стійкості, формування ефективної системи аналізу та оцінки загрози безпеці об'єктам аерокосмічного комплексу України:

1. На рівні законодавчих актів у сфері регулювання діяльності об'єктів критичної інфраструктури, транспорту, космічної діяльності та інших, сформувати нормативні вимоги щодо механізмів та інструментів діяльності суб'єктів кбезпечення інформаційної стійкості об'єктів аерокосмічного комплексу України.

2. Визначити на нормативному рівні критерії оцінки конкретних ступеня ризиків та загроз інформаційній безпеці у наслідок кібератак на інформаційно-телекомунікаційні системи у сфері космічної діяльності, шляхом:
- формування сигнальної систему моніторингу ризиків та загроз інформаційній безпеці аерокосмічного комплексу України;
- визначення алгоритму діагностування та оцінки зовнішніх і внутрішніх загроз інформаційній безпеці конкретних об'єктів, їх нейтралізації на всіх рівнях управління аерокосмічним комплексом України;
- розробки та впровадження загальнодержавної системи визначення та моніторингу порогових значень показників (індикаторів), що характеризують рівень інформаційної захищеності об'єктів аерокосмічного комплексу та ризики реальних загроз національній безпеці України;

3. Закріпити у законодавстві принципи та на нормативному рівні організаційно-тактичні рекомендації захисту інформаційної безпеки об'єктів аерокосмічного комплексу України на ґрунті:
- формування типових моделей та алгоритмів проведення заходів щодо нейтралізації інформаційних атак на об'єкти аерокосмічного комплексу України;

- формування на стратегічному, оперативному та тактичному рівні превентивних заходів спрямованих на нейтралізацію загроз інформаційній безпеці об'єктів аерокосмічного комплексу України;
- побудови ефективної системи координації діяльності суб'єктів убезпечення об'єктів космічної діяльності у інформаційній сфері ;
- розробки комплексної організаційно-тактичної моделі захисту інформаційної складової безпеки космічної діяльності;
- вдосконалення технічних засобів захисту інформаційних ресурсів об'єктів аерокосмічного комплексу України;
- забезпечення науково - методичної й технологічної підтримки діяльності суб'єктів захисту від загроз об'єктів аерокосмічного комплексу України та оцінки ризиків шляхом визначення: 1) загрози для конкретного об'єкта, а також засобів та методів можливого нападу; 2) ймовірності виникнення загрози; 3) наслідків нападу; 4) вразливостей; 5) залишкового ризику.

Реалізація означених пропозицій повинна здійснюватися на грунті формування системи моніторингу та оцінки ризиків і загроз безпекового характеру об'єктам аерокосмічного комплексу України, що призведе до підвищення його стійкості в умовах надзвичайних подій.

Список використаних джерел:

1. Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії Росії проти України за рік від початку повномасштабного вторгнення. Київ: KSE Institut, 2023 С. 19-20. URL: https://kse.ua/wp-content/uploads/2023/03/UKR_Feb23_ FINAL_ Damages-Report-1.pdf (датазвертання 01.06.23).
2. Шинкаренко І.Р. Актуалізація правових досліджень щодо убезпечення авіаційно-космічної галузі України у період військової агресії Росії. *Міжнародна науково-практична конференція: Український дослідницький простір в умовах війни: адаптація й перезавантаження технічних і юридичних наук. Харків-Рига.* Харків: НАУ, 2022 С. 229-233.
3. Зубко Г.Ю. Безпека космічної інфраструктури як напрям державної інфраструктурної політики України. *Актуальні проблеми вітчизняної юриспруденції.* № 4. 2019. С. 144 – 148.
4. Борель Ж. Війна Рф проти України підкреслила значення космосу у сучасних бойових діях. URL: https://www.ukrinform.ua/rubric-polytics/3659739-borrel-vijna-rf-proti-ukraini-pidkreslila-znacenna-kosmosu-u-sucasnih-bojovih-diah.html (дата звертання 01.06.23).
5. Державне космічне агентство України (2021). URL: https://www.nkau.gov.ua/ (дата звернення: 18.05.2023).
6. Cain, J. R. ed. byCharles S. Cockell (2016). Space Terrorism -A New Environment; New Causes. Dissent, Revolution and Liberty Beyond Earth. Springer. Switzerland. P. 93-110. DOI 10.1007/978-3-319-29349-3 [English].
7. Випорханюк Д. М. , Ковбасюк С. В. Основи космічної ситуаційної обізнаності (Space Situational Awareness, SSA). Іноземний і вітчизняний досвід космічної діяльності у сфері оборони: Монографія. Житомир: Видавець О. О. Євенок, 2018. 532 с. ISBN 978-617-7703-34-0.
8. Стратегія інформаційної безпеки: Указ президента «Про Стратегію інформаційної безпеки» № 685/2021від 28 грудня 2021р. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.
9. Шинкаренко І.Р. Правові та криміналістичні проблеми виявлення осіб, що сприяють військовій агресії Росії проти України. *Науково практична конференція: Організаційно-правові аспекти взаємодії правоохоронних та судових органів під час розслідування кримінальних правопорушень, пов'язаних з військовою агресією РФ проти України*, 30.04 22, м. Дніпро . Дніпро, 2022. С.37-43. ISBN 978-617-616-090-8.
10. Інформаційна безпека і кібербезпека - в чому різниця?. URL: *https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/.*

11. Ткаченко С.М. Сутність економічної стійкості підприємств та її складові. Електронний журнал «Ефективна економіка» №5. 2011. URL: http://www.economy.nayka. com.ua/?op=1&z=1350.

12. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г.,Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. – К. : НІСД, 2019. – 224 с. ISBN 978-966-554-258-2.

13. Соломіна Г.В. Забезпечення фінансово – економічної безпеки підприємництва: навчальний посібник/. - Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. - 234 с. URL: https://er.dduvs.in.ua/bitstream/123456789/1694/1/Posibnik%20ZFEBP.pdf.

14. Даник Ю.Г. та ін. Основи кібербезпеки та кібероборони: підручник. [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. ISBN 978-617-582-069-8 с.295-296