УДК 342.9

Ю. П. ЛІСОВСЬКА

АДМІНІСТРАТИВНО-ПРАВОВИЙ ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В СУЧАСНОМУ КІБЕРПРОСТОРІ

Розглядаються нормативні аспекти підстав й умов застосування сили щодо захисту критичної інфраструктури від будь-яких загроз. Проаналізовано сучасні технології, що впливають на технічні засоби критичної інфраструктури. Зазначається, що інформаційна зброя може бути використана для ініціювання потужних техногенних катастроф, оскільки вона певною мірою може порівнюватися зі зброєю масового ураження, що дасть змогу здійснювати соціогенний вплив як на життя суспільства в цілому, так і на соціально-психологічний та моральний стан кожної особи цього суспільства.

Ключові слова: *глобалізація, спецслужби, ентропія, кібербезпека, інформаційна зброя, квантова комп'ютеризація.*

Lisovska Yuliia. **Administrative and legal protection of critical information infrastructure in cyberspace modern**

The modern technologies that influence the technical means of critical infrastructure are analyzed. It is noted that information weapons can be used to initiate powerful man-made disasters, because it can be compared to weapons of mass destruction to a certain extent, which will enable sociogenic influence on society as a whole and on the socio-psychological and moral condition of each person. of society.

Key words: *globalization, special services, entropy, cyber security, information weapon, quantum computerization.*

В умовах сучасних євроінтеграційних та глобалізаційних перетворень, які відбуваються в Україні, перед спецслужбами держав світу постає низка важливих завдань. Серед них актуального значення набувають забезпечення реалізації людиною та громадянином своїх невід'ємних прав і свобод. За цих обставин дедалі ширше використовується генеративно-цілісний

© *ЛІСОВСЬКА Юлія Петрівна* — кандидат юридичних наук, доцент кафедри адміністративного, фінансового та банківського права Міжрегіональної Академії управління персоналом

підхід щодо забезпечення безпеки систем, об'єктів і ресурсів. Саме вони є критично необхідними для життєдіяльності тієї чи іншої держави або об'єднання держав від злочинних посягань та будь-яких загроз. Хоча термін «критична інфраструктура» ще не отримав свого законодавчого визначення в лексико-семантичному навантаженні правового поля. Проте де-факто вже використовується в таких основоположних документах, як Закон України «Про національну безпеку України»[1]. Адже у законодавстві ЄС та США цим поняттям позначають «системи та ресурси, фізичні чи віртуальні, настільки життєво важливі, що недієздатність або знищення таких систем або ресурсів підриває національну безпеку, національну економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого»[2].

Нині залишається не визначеним на загальнодержавному рівні питання про те, який орган буде здійснюватиме формування державної політики захисту об'єктів критичної інфраструктури, а також відповідний орган (діяльність, формування), на який буде покладена реалізація завдань захисту об'єктів критичної інфраструктури від різного роду загроз.

Означена проблематика є малодосліджуваною, оскільки ще не отримала свого повного визначення на загальнодержавному рівні. Цієї теми торкаються такі сучасні вітчизняні вчені, як В.І. Литвиненко, М.Н. Курко, П.М. Лісовський, О.Г. Комісаров, А.М. Подоляка, С.В. Бємай та ін.

Згідно з чинною редакцією Законів України «Про національну безпеку України», «Про боротьбу з тероризмом» здійснюється захист об'єктів критичної інфраструктури від таких видів посягань, як терористичні акти, диверсії, інші злочини.

При цьому реалізація переважної більшості завдань захисту об'єктів критичної інфраструктури скеровується завданнями щодо боротьби з тероризмом та відбувається на рівнях: 1) Міжвідомчої координаційної комісії Антитерористичного центру при СБУ; 2) надання суб'єктом боротьби з тероризмом, який не входить до структури СБУ, Антитерористичному центру при СБУ необхідних сил і засобів. Починаючи з 2016 року

в Україні функціонує Єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, яка складається з ефективно діючих констант у територіальній та функціональній підсистемах.

У мирний час контрдиверсійна діяльність є окремим видом державної діяльності щодо захисту об'єктів критичної інфраструктури. У свою чергу, окремі повноваження в системі контрдиверсійної діяльності не покладено на жоден правоохоронний орган чи військове формування. Це випливає із текстів законів України «Про національну безпеку України», «Про Національну гвардію України», «Про національну поліцію», «Про Збройні сили України», «Про Службу безпеки України», «Про розвідувальні органи України», а також із Положення про Єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків. Проте терміни «диверсія», «контрдиверсійна діяльність» та похідні від них не використовуються.

Термін «диверсія» широко застосовується у Законі України «Про використання ядерної енергії та радіаційну безпеку» щодо регулювання фізичного захисту. В Законі України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» — для досягнення цілей фізичного захисту від будь-якого неправомірного вилучення радіоактивних матеріалів.

Саме з цією метою до суб'єктів Державної системи фізичного захисту з 2014 року належить Національна гвардія України, яка, як і сили допомоги ззовні, згідно із законодавством мають здійснювати лише оборону від нападу ззовні та звільнення таких об'єктів від нападників.

Комп'ютерні кібератаки в інформаційному капіталі. З початком кібервійни в першу чергу будуть здійснені кібератаки на комп'ютерні системи і сервери державного управління, установ, фінансових і ділових центрів. Ці атаки будуть підкріплені активацією комп'ютерних вірусів, закладених у математично обчислювальних програмах ще у мирний час. Також «передбачається використовувати спеціальні пристрої, які при вибухові

створюють потужний електромагнітний імпульс, або біологічні засоби, здатні знищувати електронні схеми й ізолюючі матеріали в комп'ютерах»[3].

Адже інформаційна зброя може бути використана, зокрема, для ініціювання потужних техногенних катастроф внаслідок порушення штатного керування об'єктами із значною кількістю небезпечних психотропних речовин, що володіють високими концентраціями енергії. Оскільки інформаційна (зокрема психотронна, психотропна тощо) зброя певною мірою може порівнюватися зі зброєю масового ураження. Водночас інформація, що передається каналами масової комунікації, може здійснювати соціогенний вплив як на життя суспільства в цілому, так і на соціально-психологічний та моральний стан кожної особи цього суспільства.

Квантова комп'ютеризація як сучасний засіб програмно-математичного впливу. У цьому сенсі до сучасних технологій, що впливають на технічні засоби критичної інфраструктури, варто віднести наступні:

– комп'ютерні віруси, що вирізняються імовірною здатністю проникнення в різнобічні канали програмного забезпечення. Це призводить до закріплення (зрощення), розмноження та виведення з їх ладу;

– логічно обумовлена локація в соціально активних точках, що заздалегідь впроваджена в стратегічні центри критичної інфраструктури, а саме: цивільні та військові;

– нейробіолінгвістичні засоби, створені на основі генонанотехнологій, що виводять з ладу оперативну пам'ять відповідного технічного забезпечення.

Впровадження таких засобів здійснюється під час поставок на експорт відповідних комп'ютерних систем, в яких маскують під звичайні пристрої мікроелектроніки спеціальні апаратні закладки. Ці апаратні закладки застосовують для збору, обробки та передачі конфіденційної інформації. «Основні результати застосування такої інформаційної зброї: дезорганізація функціонування автоматизованих систем і зниження доступності інформації, пошук «слабких» місць у

системі захисту інформації автоматизованих систем різного призначення»[4].

До засобів несанкціонованого доступу відносять комп'ютерні програми з потенційно небезпечними наслідками, що виконують функції руйнування коду програм у базовій феноменальній пам'яті. Тому, одним із важливих методів та прийомів проведення інформаційного протиборства від загрозливого впливу є радіоелектронна боротьба. Це синергетично комплексна дія, що ентропійно обумовлена засобами радіоелектронного придушення та функціонального ураження технічних складових систем розвідки та каналів передачі інформації супротивника.

Правові системи провідних країн світу щодо захисту критичної інфраструктури. На сучасному етапі розвитку міжнародних безпекових організацій саме нормативні акти встановлюють підстави й умови застосування сили щодо захисту критичної інфраструктури від будь-яких загроз. При цьому застосуванню підлягають норми та принципи відповідних галузей права. До тематичної інкорпорації застосованих галузей права (зокрема антикорупційного права) призводить необхідність дотримання екологічних норм, одночасне ведення операцій в повітрі, на морі й суходолі, ведення об'єднаних операцій, укладення господарських договорів з іноземними підрядниками.

Результатом цього є поява у правових системах країн світу феномена операційного права (або права операцій, *Operational Law*) — сукупності правових норм, що регулюють здійснення всього спектру операцій. Саме операційне право є сукупною матрицею міжнародного права із захисту прав людини, права міжнародної безпеки, морського, повітряного, інформаційного, господарського / договірного, трудового, екологічного, міжнародного приватного права тощо. Адже «успішність такої систематизації підтверджується виданням у Збройних Силах США Довідника з операційного права, який щорічно з 2001 року публікується відділом міжнародного та операційного права Центру (Школи) вивчення права Воєнно-юридичної служби Збройних Сил (Шарлотсвілль, штат Вірджинія)[5].

Таким чином, правове забезпечення у системі превентивних заходів щодо захисту стратегічно обумовленої критичної інфраструктури є дотриманням норм і принципів реагування силових структур як міжвідомчого характеру, так і громадськості. Саме такий злагоджений міжвідомчий процес з одночасним застосуванням різних галузей права дозволяє превентивну можливість оперативно реагувати на будь-які загрози як в національному, так і світовому безпековому процесі.

Шляхи розвитку оборонно-промислового комплексу України. Оскільки сьогодні Україна перебуває у стані гібридної війни, то на державному рівні вдалося синхронізувати заходи з розвитку озброєння і військової техніки, із заходами реформування та розвитку оборонно-промислового комплексу. Ці заходи спрямовані на: реструктуризацію, реорганізацію і корпоратизацію підприємств оборонно-промислового комплексу та удосконалення системи управління таким комплексом; впровадження механізму стратегічного менеджменту ОПК; забезпечення фінансового контролю підприємств; інтеграція науки та виробництва; вдосконалення системи стандартизації, уніфікації та управління якістю.

Отже, вперше за останні роки на базовій основі єдиного комплексного підходу було сформовано програму розвитку української оборонної промисловості. Саме така програма поєднала у собі як інституційні та законодавчі перетворення, так і заходи з модернізації виробничих можливостей підприємств оборонної промисловості. Проте, варто озвучити ризики, пов'язані з недосконалістю нормативно-правової бази функціонування приватних компаній оборонної промисловості; корупційні ризики у сфері виконання оборонної промисловості тощо. Тому, на наш погляд, необхідно завершити роботу над Законом України: «Про режим інвестування в оборонно-промислову сферу України». Крім того, необхідно внести зміни до законів України «Про інноваційну діяльність» та до законодавства про інтелектуальну власність щодо врахування специфіки оборонної продукції.

Перспективи розвитку квантової безпеки у системі цифрових комунікацій сучасного кіберпростору. У сучасних умовах інтер-

полярного світу, який стрімко змінюється, актуального значення набуває така молода міжгалузева наука, як квантологія, складовою якої є квантова безпека. Ця фундаментальна наука про випромінювання як енергетичний посил містить у собі сучасні досягнення та розробки в сфері не лише нанотехнологій, а й ментально-ціннісних настанов щодо особи, держави та суспільства.

З огляду на це здійснення фундаментальних і прикладних досліджень, зокрема у сфері квантових наукових розробок, має відповідати критеріям, визначеним у ст. 1 Закону України «Про наукову і науково-технічну діяльність»[6]. Адже відповідно до Закону саме інтелектуальна творча діяльність цілеспрямована на одержання інноваційних знань у сучасну квантову епоху як докорінних перетворень у науково-технологічному прогресі.

При цьому ентропія як фізична величина, що характерна температурним режимом, часом та простором, відіграє важливу роль у квантовій безпеці. Адже ентропія визначає якісно новий семантичний стан особи, держави та суспільства в процесі їх самоздійснення. Це може бути кризовий стан, воєнний стан, надзвичайний стан тощо в процесі правової відповідальності людини та громадянина.

У цьому сенсі освіта, наука та виховання як кодифіковано-пізнавальний алгоритм системи знань у квантовій безпеці є тим ментально-ціннісним продуктом, що відповідально передається від покоління до покоління. В свою чергу, квантова свідомість людини саме сьогодні потребує негайних перетворень як постійний вихід за межі себе у пошуках реалізації своєї екзистенції. Це насамперед мають бути багатовимірні координати Часу, Простору та Розвитку в гіпотетичній картині «множинності світів». Тому форми страху людини, що відтворюють певний час та простір, як категорії свободи в онтології духовного капіталу, дихотомічно поступаються одна одній з позасвідомо-невизначеної сфери трансцендентного в предметній формі. І, навпаки, такі форми страху спонукають людину до креаційної творчості на атомно-молекулярному рівні, що властиво для квантової безпеки.

Адже покоління як майбутнє соціуму, в якому людина постає в усій повноті правового існування, має здійснювати саме фундаментальні розробки, що відбуваються:

– за широкої участі наукового колективу;

– шляхом складання, затвердження, виконання планів науково-дослідних робіт;

– в результаті аналізу та узагальнення досягнень світової науки за світовим профілем;

– реалізацією міжнародних програм;

– прогнозуванням нових напрямків науки і техніки;

– проведенням конкурсів щодо наукових робіт;

– шляхом підготовки наукових кадрів через аспірантуру та докторантуру.

Для підтримки та розвитку фундаментальних досліджень на світовому рівні, нових перспективних міждисциплінарних напрямів наукових досліджень і науково-технічних розробок, координації спільної діяльності та ефективного використання фінансових, матеріально-технічних та кадрових ресурсів за визначеним науковим напрямом, наукова група відповідної навчально-наукової інституції може входити до державної ключової лабораторії, як об'єднання наукових груп наукових установ та вищих навчальних закладів на основі договору про спільну наукову діяльність, у порядку, визначеному Законом України[7].

Таким чином, згідно із законодавством України, нормативно-правовими актами, навчально-науковій установі надано право в межах наявних коштів самостійно розробляти і затверджувати її структуру і штатний розпис; вирішувати питання використання колективних договорів і конкретних форм оплати праці та елементів внутрішнього інститутського господарського розрахунку, а також преміювати працівників відповідно до положення про преміювання; здійснювати інші види стимулювання праці співробітників. Відповідно до Кодексу Законів про працю України, Законів України «Про колективні договори і угоди»[8], «Про оплату праці»[9] та інших нормативно-правових актів трудового законодавства дирекція навчаль-

но-наукової установи з її профспілковою організацією укладає колективний договір, що має регламентувати взаємовідносини між трудовим колективом і роботодавцем. Тому сучасні наукові дослідження міжвідомчого / міждисциплінарного характеру мають бути системними в єдиному сумарному транскордонному полі правового забезпечення.

Отже, сучасні виклики і загрози кіберобумовленій критичній інфраструктурі як стратегічному об'єкту держави демонструють нагальну потребу гарантування та ефективно діючого удосконалення як законодавчих, так й інституційних та інших інструментів реалізації державної інформаційної політики. При цьому критична інфраструктура України в своїй фундаментальній основі має сектор безпеки і оборони, що складається з чотирьох взаємообумовлених складових: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання. Для цього має бути підкреслено, що в інституційному механізмі забезпечення критичної інформаційної інфраструктури України особливі завдання покладені на Службу безпеки України. Це, насамперед стосується контрозвідувального захисту державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу. Крім того, на належному рівні має бути налагоджена національна система конфіденційного зв'язку, формування та реалізація державної політики у сферах кіберзахисту, а саме: криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку тощо.

1. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19. **2.** Власова О.І., Литвиненко К.О. Наслідки діяльності сепаратистських рухів для гуманітарної безпеки України. *Стан та перспективи реформування сектору безпеки і оборони України:* матеріали ІІ Міжнародної науково-практичної конференції (30 листопада 2018 року). Київ: ФОП Кандиба Т.П. 2018. С. 281. **3.** Смолян Г., Цыгичко В., Черешкин Д. Оружие, которое может быть опаснее ядерного: Реалии

информационной войны. URL: http: http://evartist.narod.ru/text4/58.htm. **4.** Караяни А.Г. Информационно-психологическое протибоство в современной войне. Москва: ВУ, 1997. 275 с. **5.** Operational Law Handbooks. URL: www.loc.gov/rr/frd/ Military- Law /operational — law — havdbooks. html. **6.** Про наукову і науково-технічну діяльність: Закон України від 26.11.2015 № 848-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/848-19. **7.** Про колективні договори і угоди: Закон України від 01.07.1993 № 3356-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3356-12. **8.** Про оплату праці: Закон України від 24.03. 1995 № 108/95-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/108/95-%D0%B2%D1%80. **9.** Лісовська Ю.П. Інформаційна безпека України: навч. посіб. Київ: Кондор-Видавництво, 2017. 199 с. **10.** Литвиненко В.І., Лісовська Ю.П., Лісовський П.М. Антикорупційне право: навчн посіб. Видавничий дім «КОНДОР», 2018. 240 с. **11.** Литвиненко В.І., Лісовська Ю.П., Шашкова-Журавель І.О. Міжнародне право: кіберінфраструктура та охорона здоров'я: навч. посіб. Київ: Видавничий дім «Кондор», 2019. 236 с.

***Lisovska Yuliia*. Administrative and legal protection of critical information infrastructure in cyberspace modern**

The purpose of the article is the administrative and legal provision of critical infrastructure as a strategic object of the state in the sphere of security and defense of Ukraine. The author uses methods and techniques of logic, including analysis, generalization and defining. Due to the use of the analysis method, the author can deploy his own opinion on the issues raised and draw conclusions. A formal legal method is used to assess and interpret the provisions of legal acts. The results of the study envisage the implementation of institutional and functional reforms of the public administration system in the field of defense-industrial complex.

The article is devoted to the security problems of systems, objects and resources necessary for the life of a state, or the unification of states from criminal encroachments and all kinds of threats.

The modern technologies that influence the technical means of critical infrastructure are analyzed. It is concluded that at the state level the body, which will implement the state policy of protecting objects of critical infrastructure, as well as the relevant body (activity, formation), which will be assigned the task of protecting objects of critical infrastructure from various types of threats.

According to the results of the study, it was established that the legal support in the system of preventive measures to protect strategically determined critical infrastructure is the observance of the norms and principles of the response of the security forces, both interagency and the public. The author

considers it expedient to carry out modern scientific researches of interdisciplinary character systematically and in a single comprehensive cross-border field of legal support.

Key words: globalization, special services, entropy, cyber security, information weapon, quantum computerization.

УДК 342.9.07

П. О. БАРБУЛ

ФУНКЦІЇ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ

Розглядаються види функцій Міністерства оборони України. Автор зупиняється на поділі функцій на загальні (основні); спеціальні (спеціалізовані), які відображають специфіку конкретного суб'єкта управління або керованого об'єкта; допоміжні (обслуговуючі) функції, які обслуговують виконання загальних і спеціальних функцій. Основною і ключовою функцією Міноборони названо забезпечення формування та реалізації державної політики у визначеній сфері управління. До основних функцій Міноборони також віднесено координацію діяльності державних органів та органів місцевого самоврядування з підготовки держави до оборони. Спеціальною функцією визначено здійснення військово-політичного та адміністративного керівництва ЗСУ. Як допоміжні функції розглядаються організація і проведення воєнно-наукових досліджень, розвиток військової освіти та міжнародне співробітництво.

Ключові слова: *загальні (основні) функції, спеціальні (спеціалізовані) функції, допоміжні (обслуговуючі) функції, формування державної політики.*

***Barbul Pavlo*. Functions of the Ministry of defence of Ukraine**

The article deals with the types of functions of the Ministry of Defence of Ukraine. The author dwells on the division of functions into general (basic); special (specialized), that reflect the specifics of a particular management entity or managed entity; auxiliary (servicing) functions that serve the implementation of general and special functions. The provision of public policy making and implementation in a certain management sphere is named the main and key function of the Ministry of Defence. The main functions of the Ministry of Defence also include the coordination of activities of public and local self-governing bodies

---

© *БАРБУЛ Павло Олексійович* — аспірант відділу проблем державного управління та адміністративного права Інституту держави і права імені В. М. Корецького НАН України