КОНСТИТУЦІЙНИЙ ЛАД ТА ПРАВА ЛЮДИНИ. ПИТАННЯ АДМІНІСТРАТИВНОГО ПРАВА.

Єрменчук О.П.

ПОБУДОВА СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ З ВИКОРИСТАННЯМ ДОСВІДУ СЕКТОРУ БЕЗПЕКИ ІНОЗЕМНИХ ДЕРЖАВ

Нормативно-правовими актами нашої держави визначено необхідність побудови системи захисту критичної інфраструктури (КІ) України та розробки відповідного законодавства.

Створення системи захисту КІ України безумовно передбачає участь у цьому складному багатовекторному та багатоелементному механізмі Служби безпеки України, як органу, який відповідає за забезпечення державної безпеки.

Так, у відповідності до Указу Президента України від 26.01.2017 №8/2017 про введення в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» передбачено розробити основоположні нормативно-правові акти для захисту критичної інфраструктури України, а СБ України вжити заходів щодо удосконалення контррозвідувального забезпечення та захисту критичної інфраструктури.

Зазначене питання є безумовно актуальним, що пов'язано з тим, що сьогодні держава протистоїть найсерйознішому за роки своєї незалежності виклику у сфері забезпечення державної безпеки. Військовий конфлікт на сході України, торгівельні війни, економічна експансія, різке посилення тероризму, небувалий ріст злочинності, руйнування та пошкодження численних підприємств, у тому числі стратегічно важливих, інфраструктурних об'єктів, втрата новітніх технологій все це та інші ризики вимагають від держави нових підходів до виявлення загроз та їх по-

передження і припинення. Проведений аналіз вказаних та інших масштабних комплексних викликів регіональній і глобальній системам безпеки, висуває на порядок денний завдання із захисту критично важливих для існування держави сукупності частин (секторів) галузей національної економіки, суб'єктів права різних організаційно-правових форм, матеріальних чи нематеріальних ресурсів, природних ресурсів, що забезпечують життєдіяльність людини і громадянина, суспільства і держави, її суверенітет і територіальну цілісність.

Саме тому в Україні на загальнодержавному рівні розпочато створення системи захисту критичної інфраструктури. Для цього ведеться розробка над визначенням стратегічних цілей державної політики в сфері захисту критичної інфраструктури, принципів побудови системи захисту критичної інфраструктури та завдання такої системи. Проте, на даний час ще відсутній системний підхід до управління захистом та безпекою усього комплексу, об'єктів та ресурсів, з урахуванням взаємопов'язаності об'єктів, які прийнято відносити до критичної інфраструктури. Крім того, досі відсутній механізм попередження можливих ризиків та загроз, що виникають в процесі функціонуванням критичної інфраструктури.

Захист критичної інфраструктури має посісти належне місце в діяльності органів СБ України та стати об'єктом забезпечення в міжвідомчій безпековій системі координат. Безумовно важливу роль у цьому процесі має відігравати СБ України, як орган на який покладено задачу із забезпечення державної безпеки. Важливим напрямом діяльності СБ України має стати попередження ризиків та загроз критичній інфраструктурі держави.

Відповідно, в Службі безпеки України назріла доцільність визначення на нормативно-правовому та організаційному рівнях напрямів захисту критичної інфраструктури та удосконалення діючих форм та методів роботи.

Аналіз підходів до організації захисту критичної інфраструктури свідчить про те, що в США, Канаді та Європі уже функціонують відповідні системи.

Їх детальний розгляд дозволяє стверджувати, що підходи до захисту КІ та ролі і місця спецслужб у цьому процесі можна поділити на дві основні групи (моделі функціонування): «американську», де значні повноваження надані органам державної безпеки та розвідувальним органам, при них організовані та діють органи із захисту КІ, функціонують досить потужні аналітичні центри, державним органам доводиться актуальна аналітична інформація для прийняття управлінського рішення, вживаються заходи із виявлення та локалізації загроз. Іншою групою є так звана «урядова». При Уряді створюються спеціально уповноважені органи для захисту КІ, однак дещо вужчі повноваження спецслужб, які в основному залучаються до відпрацювання окремих завдань органів із захисту КІ, участі у визначенні критично-важливих об'єктів, припинення загроз у сфері тероризму тощо.

Зокрема, яскравим прикладом «урядової» моделі залучення спецслужб у процес захисту критичної інфраструктури є діючі системи у Польщі та Литві.

У Польщі захист критичної інфраструктури покладений на Урядовий центр безпеки (Government Centre for Security), який підпорядкований безпосередньо Прем'єр-міністру. Цим центром, із залученням міністрів і керівників центральних органів влади, розробляється Національний план управління кризовими ситуаціями та провінційні, окружні і муніципальні плани кризового управління та Національна програма захисту критичної інфраструктури.

Національний план антикризового управління містить Звіт про загрози національній безпеці, який готують міністри, керівники центральних органів державної влади та воєводи під координацією Урядового центру безпеки, а в частині, що стосується терористичних загроз, які можуть призвести до виникнення кризової ситуації, - Голови Агентства внутрішньої безпеки. Звіт затверджує Уряд (Рада Міністрів).

Основними елементами плану є: a) характеристики небезпек і оцінка ризику їх виникнення, в тому числі пов'язаних з критичною інфраструктурою, а також карти ризику і карти загроз, b) завдання і обов'язки учасників антикризового управління у фор-

мі сітки безпеки, c) склад сил і засобів, які планується використовувати в надзвичайних ситуаціях, d) завдання, визначені короткостроковими планами дій [1].

У Литві, урядом створена комісія з оцінки відповідності потенційних учасників до інтересів національної безпеки (далі - Комісія). Уряд призначає до Комісії своїх представників та представників компетентних органів в сфері національної безпеки та визначає основні засади організації захисту підприємств та об'єктів, які є стратегічно важливими для національної безпеки, та інших підприємств, які є важливими для національної безпеки. Органи державної безпеки (Департамент державної безпеки) спільно з іншими визначеними відомствами, такими, як Міністерство закордонних справ Республіки Литва, Міністерство внутрішніх справ, органами досудового розслідування, генеральною прокуратурою та іншими, здійснюють оцінку відповідності потенційних учасників до інтересів національної безпеки та передають свої висновки до Комісії. Вказана перевірка здійснюється за ініціативи потенційних учасників [2].

Значно ширші повноваження спецслужб у сфері захисту критичної інфраструктури в Німеччині, Великобританії, Канаді та США, так звана «американська модель».

Так, у Німеччині за захист критичної інфраструктури на національному рівні відповідає Федеральне міністерство внутрішніх справ (Federal Ministry of the Interior), яке забезпечує захист конституційного ладу, протидію тероризму, виконує окремі контрозвідувальні задачі. Згідно з Національною стратегією захисту критичної інфраструктури, підвищення захисту критичної інфраструктури є спільною відповідальністю Федерального уряду та урядів земель [3]. Федеральне міністерство внутрішніх справ із залученням організацій та установ здійснює оцінку загроз критичній інфраструктурі, аналізує поточні ризики і загрози та розробляє концепції та плани захисту критичної інфраструктури.

У Великій Британії, Центр захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI), що знаходиться при Уряді, підпорядкований Генеральному директору Служби безпеки (MI5), надає консультативні послуги

приватним компаніям та організаціям щодо фізичної безпеки національної інфраструктури. Уряд затверджує План розвитку національної інфраструктури, в якому йдеться про необхідність забезпечення стійкості та безпеки об'єктів, визначається перелік об'єктів критичної інфраструктури, що підлягають захисту [4]. Основна відповідальність за стійкість критичної інфраструктури покладається на власників та операторів. Водночас захист критичної інфраструктури урядом та контролюючими органами має на меті не лише забезпечення безпеки, а і сприяння інвестиціям та стабільності економіки [5].

Першими діяльність із захисту критичної інфраструктури започаткували США. Хоча робота у зазначеному напрямку велась продовж останніх десятиліть, як реакція на терористичні акти 2001 та для попередження і припинення стихійних лих і для значного підвищення рівня взаємодії різних державних органів та суб'єктів господарювання стало створення у 2002 році Міністерства внутрішньої безпеки США, яке сьогодні налічує понад 240 тис. співробітників та включає понад 15 різних спецслужб.

Різні міністерства тісно співпрацюють з Міністерством внутрішньої безпеки (Department of Homeland Security– DHS), зокрема його управлінням розвідки та аналізу, яке здобуває та аналізує інформацію про загрози галузям промисловості з різних джерел. Частину даних щодо поточного стану інфраструктури та фактори відхилення його від нормальної діяльності надає профільне міністерство. Міністерства спільно з DHS проводить також аналіз інформації від Берегової охорони США (U.S. Coast Guard– USCG), Управління по безпеці на транспорті (Transportation Security Administration– TSA), Служби імміграційного та митного контролю, митного та прикордонного контролю і інших структур розвід спільноти.

Оцінка загроз здійснюється у взаємодії з управлінням директора національної розвідки (Office of the Director of National Intelligence - ODNI), яке забезпечує організацію взаємодії спецслужб різних відомств. Для відповідного реагування на наявні загрози відбувається координація дій та обмін інформацією з центрами спостереження DHS, а саме Національним центром

управління, Національним центром по координації інфраструктури, Національним центром зв'язку, а також Групою з забезпечення комп'ютерної безпеки США. Крім того, з метою реалізації заходів національної безпеки профільні міністерства співпрацюють з іншими постійними та спеціальними спостережними центрами ФБР, Міністерства юстиції та Секретною службою Мінфіну.

Узагальнення інформації про загрози діяльності КІ здійснює Центр аналізу загроз та ризиків для національної інфраструктури США (Homeland Infrastructure Threat and Risk Analysis Center–HITRAC) при DHS. Він також забезпечує інформування галузей інфраструктури про можливі ризики для них та наслідки від них, а також розробляє довгострокову стратегічну оцінку ризиків для галузей промисловості [6].

Схожий з американським підхід використовується у Канаді, де аналогічні функції, за виключенням питань безпеки на морі, виконує Міністерство суспільної безпеки та готовності до надзвичайних ситуацій Канади (Ministry of Public Safety and Emergency Preparedness of Canada) [7].

Вибір для України тієї чи іншої організаційної моделі захисту критичної інфраструктури свідчить про доцільність ретельного вивчення наявного зарубіжного досвіду та врахування особливостей національної організації функціонування державного механізму, а також необхідності захисту економічного потенціалу держави в умовах гідбридної війни.

Стосовно питання загальної координації діяльності у цій сфері, доцільно розглянути можливість створення Національного центру з захисту критичної інфраструктури чи Центру захисту національної інфраструктури. Центр може бути утворений як окремий орган, або як структурна частина в межах діючого органу влади, який буде визначений як відповідальний за координацію діяльності із захисту критичної інфраструктури. Це може бути, як орган підпорядкований Прем'єр-міністру чи РНБО так і орган у складі СБ України (на базі підрозділів контррозвідувального захисту інтересів держави у сфері економічної безпеки, тощо). До складу зазначеного центру мають на правах членів входити представники задіяних міністерств та відомств.

Не менш важливим є питання організаційних механізмів функціонування вказаної системи.

Досить ефективним засобом організації захисту КІ є розробка та виконання відповідних планів (програм) захисту.

Для прикладу, в США, для захисту різних секторів КІ передбачений тісний взаємозв'язок між Президентом, Урядом, Міністерством внутрішньої безпеки, спецслужбами та приватним сектором економіки. Так, у відповідності до Директиви Президента США про Національну безпеку, розроблений «План захисту критичної інфраструктури США», у відповідності до нього спецслужби разом з міжвідомчими партнерами та представниками приватного сектору промисловості здійснюють його спільну розробку та реалізацію [6].

Враховуючи зазначене, вважається за доцільне запровадити відповідну практику в Україні, розробки Програми захисту КІ та Програми захисту секторів економіки України. Програми повинні бути зв'язані з механізмами державної підтримки та стимулювання розвитку економіки, а тому розроблятися у рамках відповідних державних цільових програм. Це сприятиме їх фінансовому забезпеченню.

Водночас, запровадження вищевказаних перетворень неможливе без системного удосконалення діючої нормативно-правової бази та вимагає внесення змін до Законів України про «Основи національної безпеки», «Про Службу безпеки України», «Про контррозвідувальну діяльність», «Про основи державно-приватного партнерства», «Про засади внутрішньої і зовнішньої політики», «Про критичну інфраструктуру та її захист», в яких доцільно передбачити: створення державної системи захисту критичної інфраструктури; визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури, економічного та науково-технічного потенціалу; функцій, повноважень та відповідальності центральних органів виконавчої влади та інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури; запровадженняєдиноїметодологіїпроведенняоцінкизагрозкритичнійінфраструктурі та реа-

гування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій; запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації; засад державно-приватного партнерства та ресурсного забезпечення у сфері захисту критичної інфраструктури; міжнародного співробітництва у сфері захисту критичної інфраструктури.

Забезпечення стійкості національної критичної інфраструктури та ефективність діяльності спецслужб значною мірою залежить від стану приватно-публічного партнерства. Світова практика засвідчує те, що значна частина об'єктів критичної інфраструктури знаходиться в приватній власності. У цьому разі від процесу налагодження обміну інформацією залежить кінцевий результат - рівень захищеності об'єктів. Важливо згадати, що зазначений процес у більшості розвинутих країн побудований таким чином, що відповідальність за безпеку об'єктів критичної інфраструктури покладається на їх власників (операторів). Саме до їх обов'язків входить забезпечення стабільного функціонування об'єкту, його живучість та стійкість, при цьому роль держави полягає у забезпеченні належного інформування власників об'єктів, розробка нормативно-правової бази та створення умов для залучення інвестицій.

Прикладом організації взаємодії та спільних заходів із захисту КІ може слугувати німецька «Концепція основних заходів по захисту КІ, рекомендація для підприємств». У вказаному акті зазначається, що високий рівень безпеки елементів інфраструктури відповідає кровним інтересам підприємств та громадян держави [8].

Вищевказане засвідчує необхідність створення нормативно правової-бази щодо врегулювання питань взаємних зобов'язань безпекового сектору держави та суб'єктів недержавної форми власності у діяльності із захисту критичної інфраструктури. Сьогодення вимагає запровадження практики аналізу ризиків та загроз, готовності до реагування на них, переходу на новий рівень з питань взаємодії та обміну інформацією між суб'єктами госпо-

дарювання різних форм власності з відповідними державними органами.

Висновки. Побудова системи захисту КІ в Україні значно залежить від наступних факторів.

1. Нормативного закріплення термінів «інфраструктура держави», «критична інфраструктура держави», «об'єкти критичної інфраструктури», «захист критичної інфраструктури». При цьому, якість процесу захисту КІ та злагодженість діяльності суб'єктів захисту, вірний вибір об'єктів забезпечення безперечно залежить від повноти та чіткості вищезазначених термінів у законодавстві.

2. Спільна розробка та виконання відповідних планів (програм) захисту КІ може значно посилити взаємодію між учасниками процесу та чітко визначить повноваження кожного із них.

3. Організація захисту КІ можлива лише завдяки комплексному підходу до протидії зовнішнім та внутрішнім загрозам, створення відповідної нормативно-правової бази. В першу чергу доцільно вжити заходи з удосконалення Законів України про «Основи національної безпеки», «Про Службу безпеки України», «Про контррозвідувальну діяльність», «Про основи державно-приватного партнерства», «Про засади внутрішньої і зовнішньої потіики» та розробити Закон України «Про критичну інфраструктуру та її захист», де мають бути закладені норми, які передбачать стабільність функціонування і недопущення небезпечних наслідків для національної безпеки, підвищать інвестиційну привабливість економіки та закладуть основи організації захисту КІ. Підзаконні нормативно-правові акти мають забезпечити відсутність пробілів у функціонуванні вказаної сфери та якісний різновекторний зв'язок (за принципом отримання інформації щодо загрози - її локалізація) між суб'єктами та об'єктами захисту у цій сфері.

4. Якісна та результативна взаємодія і кінцевий результат можливі лише завдяки удосконаленню механізму приватно-публічного партнерства та переходом на новий рівень з питань взаємодії та обміну інформацією між суб'єктами господарювання різних форм власності з відповідними державними органами.

1. *Закон Республіки Польща «Про антикризове управління» від 26.04.2007.*
2. *Закон Литовської республіки «Про підприємства та об'єкти, які є стратегічно важливими для національної безпеки, та інші підприємства, які є важливими для національної безпеки» від 10.10.2002.*
3. *Nationale Strategiezum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) [Електронний ресурс]. – BMI, 2009. – Режим доступу: http://www.kritis.bund.de.*
4. *National Infrastructure Plan 2014 [Електронний ресурс]. – HM Treasury, 2014 – Режим доступу: www.gov.uk.*
5. *Keeping the Country Running: Natural Hazards and Infrastructure. – Civil Contingencies Secretariat, Cabinet Office. [Електронний ресурс]. – Режим доступу: https://www.gov.uk.*
6. *Єрменчук О.П. Організація захисту критичної інфраструктури оборонно-промислового комплексу з використанням досвіду США / Єрменчук О.П., Скурський П.П. // Інформаційна безпека. – 2011. – С. 54-63.*
7. *Зелена книга з питань захисту критичної інфраструктури. / Д. Бірюков [та ін.] ; Нац. інс-т. стратегічних досліджень. Експерти. Офіс зв'язку НАТО в Україні. – Київ, 2015. – 35 с.*
8. *Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий. – Bundesministerium des Innern, 2006. – [Електронний ресурс]. – Режим доступу: www.bmi.bund.de.*

Єрменчук О.П. Побудова системи захисту критичної інфраструктури в Україні з використанням досвіду сектору безпеки іноземних держав

В Україні на загальнодержавному рівні розпочато створення системи захисту критичної інфраструктури. Для цього ведеться розробка над визначенням стратегічних цілей державної політики в сфері захисту критичної інфраструктури, принципів побудови системи захисту критичної інфраструктури та завдання такої системи. Проте, на даний час ще відсутній системний підхід до управління захистом та безпекою усього комплексу, об'єктів та ресурсів, з урахуванням взаємопов'язаності об'єктів, які прийнято відносити до критичної інфраструктури. Крім того, досі відсутній механізм попередження можливих ризиків та загроз, що виникають в процесі функціонуванням критичної інфраструктури.

Захист критичної інфраструктури має посісти належне місце в діяльності органів СБ України та стати об'єктом забезпечення в міжвідомчій безпековій системі координат. Безумовно важливу роль у цьому процесі має відігравати СБ України, як орган на який покладено задачу із забезпечення державної безпеки. Важливим напрямом діяльності СБ України має стати попередження ризиків та загроз критичній інфраструктурі держави.

Відповідно, в Службі безпеки України назріла доцільність визначення на нормативно-правовому та організаційному рівнях напрямів захисту критичної інфраструктури та удосконалення діючих форм та методів роботи.

Ключові слова: критична інфраструктура, сектор безпеки, Служба безпеки України

Yermenchuk O.P. Construction of the critical infrastructure protection system in Ukraine using the experience of the foreign security sector

In Ukraine, the creation of a critical infrastructure protection system has been initiated at the national level. For this purpose, the development of defining the strategic objectives of the state policy in the field of critical infrastructure protection, the principles of building a critical infrastructure protection system, and the tasks of such a system is underway. However, at the present time there is no systematic approach to managing the protection and security of the whole complex, objects and resources, taking into account the interconnectedness of objects that are assigned to the critical infrastructure. In addition, there is still no mechanism for preventing possible risks and threats occurring during the operation of a critical infrastructure.

The protection of critical infrastructure should take proper place in the activities of the bodies of the Security Council of Ukraine and be the object of provision in the interdepartmental security coordinate system. Undoubtedly, an important role in this process is to be played by the Security Council of Ukraine, as the body entrusted with the task of ensuring state security. An important activity of the SCU should be the prevention of risks and threats to the critical infrastructure of the state.

Accordingly, the Security Council of Ukraine has expedited the expediency of defining, at the regulatory and legal levels, the critical infrastructure protection and improvement of existing forms and methods of work.

Key words: critical infrastructure, security sector, Security Council of Ukraine