Центр безпекових досліджень

Center for Security Studies

Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки

АНАЛІТИЧНА ДОПОВІДЬ

Київ 2020

Електронну версію видання розміщено на: https://niss.gov.ua .

Автори:

Кондратов С. І. — старший науковий співробітник відділу критичної інфраструктури, енергетичної та екологічної безпеки центру безпекових досліджень НІСД

Суходоля О. М. — завідувач відділу критичної інфраструктури, енергетичної та екологічної безпеки центру безпекових досліджень НІСД

Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О. М. Суходолі. Київ : НІСД, 2020. 28 с.

В аналітичній доповіді розглянуто організаційно-правові питання забезпечення захисту (безпеки) та стійкості критичної інфраструктури з точки зору управлінських підходів. На основі результатів огляду зарубіжного досвіду продемонстровано зв'язок питань захисту (безпеки) критичної інфраструктури та національної безпеки, а також зроблено висновок про вплив фактору зрілості механізмів державного управління сектором безпеки і оборони на вибір тієї чи іншої моделі забезпечення захисту важливих для життєдіяльності інфраструктурних систем і об'єктів. У цьому контексті проаналізовано стан запровадження концепції захисту критичної інфраструктури в Україні та можливі варіанти розвитку державної політики у цій сфері, запропоновано рекомендації щодо її вдосконалення.

Розраховано на представників державних органів, науковців, незалежних експертів, представників громадських організацій та окремих громадян, усіх, хто цікавиться проблемами забезпечення національної безпеки України.

ЗМІСТ

Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки

В аналітичній доповіді досліджено організаційно-правові питання забезпечення захисту (безпеки) та стійкості критичної інфраструктури з точки зору управлінських підходів. На основі результатів огляду національного досвіду ряду країн продемонстровано безпосередній зв'язок питань захисту (безпеки) критичної інфраструктури та національної безпеки, а також зроблено висновок про вплив, який спричиняє фактор зрілості національних механізмів державного управління сектором безпеки і оборони, на вибір організаційно-правових підходів до забезпечення захисту важливих для життєдіяльності інфраструктурних систем і об'єктів. З цієї точки зору проаналізовано стан запровадження концепції захисту критичної інфраструктури в Україні. Проаналізовано можливі варіанти розвитку державної політики у сфері забезпечення захисту (безпеки) та стійкості критичної інфраструктури. Зроблено висновки і запропоновано ряд рекомендацій щодо можливих подальших кроків у цій сфері.

Розраховано на представників державних органів, науковців, незалежних експертів, представників громадських організацій та окремих громадян, усіх, хто цікавиться проблемами забезпечення національної безпеки України.

Вступ

Піонером у розробці та запровадженні концепції критичної інфраструктури (КІ) та її захисту (безпеки) є Сполучені Штати Америки. Саме у цій країні вперше, у 1996 р., було надано визначення терміну "*критична інфраструктура*", яке у подальшому зазнавало змін, набувши свого остаточного вигляду невдовзі після терористичних атак 11 вересня 2001 р., а саме — 23 жовтня 2001 р., коли був прийнятий закон, відомий як *USA PATRIOT Act*[1]. Відповідно до цього закону визначення терміну *"критична інфраструктура"* однозначно вказує на безпосередній зв'язок між станом КІ та національною внутрішньою безпекою[2] (стислий розгляд випадку США див. нижче).

Заявлений у законі зв'язок між внутрішньою безпекою та станом захисту (безпеки) КІ було оформлено і реалізовано через прийняття ряду пов'язаних з цією проблематикою нормативно-правових актів, а також шляхом запровадження відповідних змін у структурі державних органів, розподілі відповідальності, повноважень і функцій між ними та їх партнерами (у т.ч. у приватному секторі) тощо.

Сполучені Штати продовжують зберігати свої лідерські позиції у цій сфері, у т.ч. завдяки застосуванню апробованих на інших напрямах сучасних управлінських

[1] The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.[2] [Електронний ресурс]. – Режим доступу: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

[2] У визначенні терміну вжито термін *homeland security,* який у спеціальній літературі найчастіше перекладають як "*внутрішня безпека".*

підходів, удосконаленню інформаційно-аналітичної підтримки процесу прийняття рішень, використанню новітніх технологій та активному поширенню різноманітних форм і форматів підготовки кадрів і населення задля забезпечення захисту та *стійкості* КІ тощо.

Більш того, США усвідомили необхідність не тільки забезпечення безпеки та стійкості КІ, але й ланцюжків постачання критичних матеріалів, ресурсів, технологій та послуг, поширюючи опрацьований підхід і на інші складові забезпечення національної безпеки і стійкості[3].

Інші розвинені країни світу широко використовують напрацьовані у США підходи, звичайно, враховуючи при цьому власну національну специфіку. Деякі приклади взаємозв'язку національної (державної) безпеки та захисту (безпеки), а також стійкості КІ для кількох розвинених країн розглянуто нижче.

На міжнародному рівні проблематика захисту (безпеки) КІ включена до порядку денного ряду структур і організацій, серед яких для цілей даного дослідження найбільший інтерес представляють підходи НАТО і ЄС, членства в яких Україна прагне набути, а також Організації економічного співробітництва та розвитку (ОЕСР), яка наразі об'єднує 35 розвинених країн світу, що поділяють ідеї ринкової економіки та представницької демократії.

Останніми роками у розвинених країнах світу посилюється тенденція щодо розширення контексту заходів, пов'язаних із забезпеченням функціонування КІ: ***питання захисту (безпеки)*** КІ розглядаються разом із питаннями її ***стійкості***. При цьому, питанням забезпечення *стійкості* приділяється дедалі більше уваги у порівнянні з питаннями *захисту*.

Таке зміщення акценту проблематики обумовлене тим, що сучасне безпекове середовище характеризується появою нових загроз та небезпек на тлі швидких процесів еволюції та трансформації існуючих загроз. Також слід ураховувати можливість випадків їх різноманітних комбінацій.

За таких умов, жодна створена система захисту (безпеки) не може у повній мірі забезпечити захист від усіх загроз і небезпек. Адже поки триває розбудова системи захисту, розрахованої на певні загрози, у світі з'являються нові загрози і небезпеки.

Тому дедалі більше уваги приділяється ***стійкості КІ*** – її здатності «*бути готовою та адаптуватися до умов, що змінюються, а також протистояти змінам і швидко відновлюватися після порушень функціонування*»[4].

[3] Див., наприклад, Executive Order on Delegating Authority Under the DPA with Respect to Food Supply Chain Resources During the National Emergency Caused by the Outbreak of COVID-19. [Електронний ресурс]. – Режим доступу: https://www.whitehouse.gov/presidential-actions/executive-order-delegating-authority-dpa-respect-food-supply-chain-resources-national-emergency-caused-outbreak-covid-19/

[4] Переклад з англійської визначення терміну в законодавстві США.

Стійкість включає здатність протистояти та відновлюватися після навмисних атак, техногенних аварій або реалізації загроз, які мають природне походження, та інших інцидентів.

Доповідь має на меті уточнення потенційних ролі та місця державної системи захисту (безпеки) та стійкості КІ у забезпеченні національної безпеки України на основі урахування зарубіжного досвіду. При цьому автори не ставили перед собою завдання всебічного висвітлення усіх багатоаспектних та багаторівневих зв'язків між згаданою системою та національною безпекою, натомість зосередившись саме на важливості для України усвідомлення такого зв'язку задля узгодженого і послідовного реформування сфери національної безпеки.

У розділі 1 доповіді зроблено огляд форм зв'язку питань національної (державної) безпеки та безпеки (захисту) КІ на прикладах трьох розвинених країн.

Розділ 2 присвячено короткому огляду того, яким чином питання захисту (безпеки) об'єктів і систем, які прийнято відносити до КІ, вирішуються в державах-членах ГУАМ, що знаходяться у перехідних станах.

У розділі 3 представлено обговорення запровадження концепції КІ та її захисту з точки зору зрілості державного управління сектором безпеки і оборони.

Розділ 4 включає аналіз ситуації із запровадженням концепції КІ та її захисту в Україні.

У заключному, п'ятому, розділі аналітичної доповіді представлено ряд висновків та рекомендацій.

1. Огляд регуляторно-правових та організаційно-управлінських форм реалізації зв'язку між захистом критичної інфраструктури та національною безпекою у США, ФРН, Польщі

Щоб проілюструвати основні підходи до запровадження концепції захисту КІ, не переобтяжуючи при цьому текст доповіді, стисло розглянемо національний досвід трьох країн з категорії розвинених, а саме США, ФРН та Польщі.

Зв'язок між станом захисту (безпеки) КІ та національною (державною, внутрішньою) безпекою для цих країн покажемо через визначення ключових термінів, а також через деякі положення правових і нормативних документів та структурні зв'язки у секторах національної безпеки[5].

1.1. Приклад США

Відповідно до законодавства США (*USA PATRIOT Act)* під *критичною інфраструктурою* розуміються

[5] Поширеними синонімами цього терміну слід вважати такі терміни: «національна критична інфраструктура», «національна інфраструктура».

системи та засоби, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що у випадку їх недієздатності або знищення це може призвести до негативного впливу на національну безпеку, національну економіку, здоров'я або безпеку населення, або може мати своїм результатом будь-яку комбінацію з переліченого.

Представлене визначення терміну однозначно вказує на зв'язок стану КІ з національною безпекою, а також з національною економікою та забезпеченням життєдіяльності населення. Тобто, безпека КІ є одним із компонентів національної безпеки.

У першій *Стратегії внутрішньої безпеки*[6] (2002 р.), прийнятій з метою мобілізації та організації нації задля убезпечення території США від терористичних атак, захист КІ було включено до шести основних напрямів відповідної діяльності, а саме: розвідка та попередження, безпека кордонів і транспорту, контртерористичні заходи на території країни, захист КІ, захист від катастрофічного тероризму, готовність до надзвичайних ситуацій та реагування.

Стратегія внутрішньої безпеки в аспекті захисту КІ в США реалізується через виконання *планів захисту національної інфраструктури (National Infrastructure Protection Plans, NIPPs).*

Безпосередній взаємозв'язок національної (внутрішньої) безпеки та безпеки КІ має чітке відображення й у структурі відповідних державних органів США. Особливо наочно це можна простежити на початкових етапах розбудови національної системи захисту КІ в США, що може представляти значний інтерес для України.

[6] [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf

Рис. 1. Схема (фрагмент) розподілу відповідальності за захист КІ згідно з директивою Президента США PDD-63 (1998)[7].

У наведеній вище організаційній структурі, вибудованій на виконання директиви Президента США від 22 травня 1998 р., взаємозв'язок захисту КІ (включаючи координацію діяльності на федеральному рівні) з національною безпекою ***чітко простежується у віднесенні питань, пов'язаних з безпекою критичної інфраструктури, до компетенції помічника Президента з питань національної безпеки***.

У подальшому, після терактів 11 вересня 2001 р. і створення Міністерства внутрішньої безпеки (*Department of Homeland Security, DHS*), цей зв'язок було урізноманітнено і він набув комплексного характеру, у т.ч. через введений до законодавства термін "*внутрішня безпека*" (*homeland security)*.

З огляду на актуальні тенденції у безпековій сфері важливо відзначити, що у 2018 році у системі Міністерства внутрішньої безпеки було створене окреме Агентство з питань кібербезпеки та безпеки інфраструктури (*Cybersecurity and Infrastructure Security Agency, CISA*[8]), що функціонує як *оперативна складова, яка*

[7] Presidential Decision Directive (PDD NSC-63) May 22, 1998, [Електронний ресурс]. – Режим доступу: https://fas.org/irp/offdocs/pdd/pdd-63.htm .

[8] Створено після підписання Президентом Д. Трампом 16 листопада 2018 р. Закону про Агентство з кібербезпеки та безпеки інфраструктури (Cybersecurity and Infrastructure Security Agency Act of 2018), яке було уповноважене відігравати головну роль у Міністерстві внутрішньої безпеки США (U.S. Department of Homeland Security) у захисті фізичної та кібернетичної критичної інфраструктури та ключових ресурсів від

на національному рівні керує зусиллями, спрямованими на усвідомлення та управління ризиками, сформованими кібер- та фізичними загрозами критичній інфраструктурі країни.

1.2. Приклад ФРН

У Федеративній Республіці Німеччина визначення терміну надається у *Національній стратегії захисту критичної інфраструктури*[9]:

> ***критична інфраструктура (КІ) – це організаційні та фізичні структури та об'єкти настільки життєво важливі для суспільного та економічного існування нації, що їх вихід з ладу або погіршення*** *[функціональності - авт.]* ***могли б призвести до стійких недопоставок*** *[послуг - авт.]****, до утворення значних прогалин у системах державної безпеки, або до інших драматичних наслідків.***

Наведене вище визначення в основному збігається з визначенням цього терміну в американському законодавстві, можливо, за єдиним виключенням, — у німецькому варіанті зроблено спеціальний акцент на важливості забезпечення стійких поставок (послуг, товарів тощо)[10]. Натомість, у ньому також відображено вплив стану КІ на *публічну безпеку* (*public security*) , елементи якої, зазвичай, безпосередньо пов'язані з *державною безпекою.*

Відповідно до Національної стратегії захисту критичної інфраструктури забезпечення захисту інфраструктури є ключовим завданням для заходів, спрямованих на досягнення безпекової готовності, яких вживають промисловість і урядові органи, та є ***центральною проблемою, на розв'язання якої націлена безпекова політика країни.***

Що стосується організаційно-управлінського аспекту взаємозв'язку захисту (безпеки) КІ та національної (державної) безпеки у ФРН, координатором діяльності із забезпечення захисту КІ на національному рівні є *Федеральне міністерство внутрішніх справ (The Federal Ministry of Interior)*, до компетенції якого віднесена *публічна безпека,* яка включає захист громадян від насильства, злочинності, тероризму та екстремізму, контршпіонаж та захист конституційного ладу.

До складу міністерства входять ряд спеціалізованих центрів (центри з протидії тероризму та екстремізму), а також агентств – *Федеральна поліція, Офіс федеральної кримінальної поліції, Федеральний офіс захисту конституції,* які відіграють ключову роль у забезпеченні безпекової політики ФРН. Що стосується

терористичних атак, природних лих та інших катастрофічних подій.

[9] National Strategy for Critical Infrastructure Protection (CIP Strategy) (17.06.2009) [Електронний ресурс]. – Режим доступу: https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf

[10] На наш погляд, такий підхід може мати на меті сприяння аналізу критичності інфраструктурних об'єктів та удосконаленню процедур їх віднесення до національної КІ.

КІ, координаційну роль у цій сфері відіграють *Федеральний офіс з цивільного захисту та допомоги при стихійних лихах (Federal Office for Civil Protection and Disaster Assistance)* та *Федеральний офіс інформаційної безпеки* (*Federal Office for Information Security),* підпорядковані міністерству.

1.3. Приклад Польщі

У польському законі «Про кризове управління» (від *26 квітня 2007 р.)*[11] під критичною інфраструктурою розуміються

> ***системи та взаємозалежні функціональні об'єкти цих систем, включаючи будівлі, установки, обладнання, а також ключові для безпеки держави та її громадян послуги, які надаються для забезпечення ефективного функціонування органів державної влади, а також інших установ та підприємств.***

Слід зазначити, що сучасна Польща є державою, політичне керівництво якої достатньо швидко реагує на зміни у безпековому середовищі як у глобальному, так і у регіональному вимірах. Завдяки цьому в останні роки польське законодавство щодо КІ перебуває у процесі динамічного розвитку, у ході якого здійснюється перехід від концепції забезпечення захисту (безпеки) КІ до забезпечення її стійкості у рамках досягнення національної стійкості. При подальшому обговоренні слід мати на увазі дуже тісний зв'язок між цима напрямами діяльності.

Нижче стисло проілюстровано, як зв'язок між захистом КІ та національною безпекою відображався у нормативно-правових та стратегічних документах РП в останні роки.

Після основоположного закону РП у цій сфері, а саме закону «Про кризове управління», у даному контексті слід виділити регуляторний акт Уряду РП «*Про національну програму захисту критичної інфраструктури*»[12], який було прийнято на виконання згаданого закону.

Зокрема, вже у §1 документа визначено, що цей регуляторний акт встановлює «спосіб виконання обов'язків та співпраці у рамках Національної програми захисту критичної інфраструктури ***між державними органами та службами, відповідальними за національну безпеку та власниками і операторами будівель, обладнання, установок та служб надання послуг***, поіменованих надалі «*операторами критичної інфраструктури*».

[11] ACT of 26 April 2007 on Crisis Management (consolidated text). Journal of Laws] of 2013, item 1166 and of 2015, of 2013, item 1166 and of 2015, item 1485 – hereinafter referred to as: "the Act on Crisis Management". [Електронний ресурс]. – Режим доступу:http://rcb.gov.pl/wp-content/uploads/WERYF_-ACT_Crisis_Management_English-1.pdf .

[12] 541 Regulation of the Council of Ministers of 30 April 2010 on National Critical Infrastructure Protection Programme [Електронний ресурс]. – Режим доступу: https://rcb.gov.pl/wp-content/uploads/REGULATION-on-NATIONAL-CRITICAL-INFRASTRUCTURE-PROTECTION-PROGRAMME-AB.pdf

У контексті теми дослідження показовим є також §3 документу, яким на ***Директора Урядового центру з безпеки***[13] задля підготовки *Національної програми захисту критичної інфраструктури* покладається ***відповідальність за розробку критеріїв віднесення об'єктів та систем до КІ***.

Важливим етапом розвитку підходів до забезпечення захисту КІ у РП стало включення до *Стратегії національної безпеки Республіки Польща 2014*[14] низки положень щодо захисту КІ. Загалом цей документ визначив такі стратегічні напрями діяльності у сфері (національної) безпеки: оборонна діяльність, захисна діяльність та діяльність у сфері соціально-економічної безпеки. З точки зору ілюстрації зв'язку між захистом КІ та національною безпекою виділимо, зокрема, пункти 80 та 86 розділу 3.2. *Захисна діяльність*.

Згідно з п. 80, "*сутністю захисної діяльності є забезпечення умов, які дозволяють підтримувати* ***конституційний лад, загальну стабільність держави, забезпечувати публічну безпеку та суспільний порядок,*** *надавати доступ як до загальних, так і до індивідуальних фізичних або віртуальних ресурсів, а також* ***забезпечувати функціонування критичної інфраструктури".*** Тобто, як ми бачимо, ***захисні дії щодо КІ поставлені в один ряд із забезпеченням стабільності держави, публічної безпеки і суспільного порядку***.

Натомість у п. 86 Стратегії стверджується, що "*вкрай важливо забезпечити умови для захисту критичної інфраструктури. Інфраструктура охоплює ключові системи та елементи, що* ***гарантують безпеку держави та її громадян, а також ефективне функціонування органів державного управління,*** *[суспільних – авт.]* ***інститутів та бізнесу***.

В організаційно-управлінській площині включення проблематики КІ до сфери національної безпеки Польщі можна простежити у ряді положень *Національної програми захисту критичної інфраструктури, НПЗКІ, (2015)*[15].

Так у розділі документа *2.1. Сфера застосування* сказано, що програма НПЗКІ *"...є доповненням до* ***Стратегії розвитку системи національної безпеки*** *РП 2022*[16] *та до* ***Стратегії національної безпеки Республіки Польща*** [2014 – авт.].

Під впливом останніх подій, включаючи пандемію COVID-19, у травні 2020 року було прийнято нову *Стратегію національної безпеки Республіки Польща 2020*[17], що характеризує безпекове середовище, в якому зараз перебуває країна, як «*невизначене та непередбачуване*», що створює перешкоди для захисту національних інтересів РП та досягнення поставлених нею стратегічних цілей.

---

[13] Government Centre for Security

[14] National Security Strategy of The Republic of Poland Of Poland (2014) [Електронний ресурс]. – Режим доступу: https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf

[15] The National Critical Infrastructure Protection Programme 2015 [Електронний ресурс]. – Режим доступу: https://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf .

[16] Strategy of development of the national security system of the RP 2022

[17] National_Security_Strategy_of_the_Republic_of_Poland_2020. [Електронний ресурс]. – Режим доступу: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf .

Загалом, зміст документа засвідчує серйозні зміни у підходах до забезпечення національної безпеки у РП, які потребують спеціального поглибленого дослідження. У контексті обговорення слід виділити той факт, що документ зосереджено на цілях забезпечення готовності РП ***реагувати на нові загрози та небезпеки через підвищення національної стійкості, зокрема через удосконалення управління сферою національної безпеки***, а також через ***приділення значно більшої уваги до проблем кібербезпеки***.

Дійсно, у новій стратегії нацбезпеки РП підкреслено роль *комунікаційних систем*, які визначені як «***ключовий компонент в системі національної безпеки і в заходах з підготовки до управління у кризових ситуаціях, що, таким чином, робить їх*** [комунікаційні системи – авт.] ***важливим елементом національної критичної інфраструктури»***.

Очевидно, що у зв'язку із недавнім прийняттям Стратегії національної безпеки Республіки Польща 2020, у подальшому слід очікувати і певних змін у підходах до забезпечення захисту КІ в країні, але на данний момент усі цитовані вище нормативно-правові акти, що є основоположними для цієї сфери у РП, залишаються чинними.

Більш детальні огляди національних підходів показують, що типовою є ситуація, коли взаємозв'язок між питаннями захисту (безпеки) КІ та національної (внутрішньої, державної) безпеки встановлюється у національних законодавствах вже при визначенні терміну «критична інфраструктура». І навіть, коли цей взаємозв'язок не сформульований у дефініції терміну в явному вигляді, його легко можна виявити через розгляд тих функцій, які виконує КІ, і тих послуг, які вона забезпечує для підтримання повсякденного життя населення, сталого існування суспільних і державних інститутів.

2. Огляд організаційно-правових форм реалізації зв'язку між захистом (безпекою) критичної інфраструктури та національною (державною, внутрішньою) безпекою у трьох державах-членах ГУАМ[18]

Для розгляду цієї категорії національних практик у дослідженні були обрані кілька держав — колишніх республік у складі СРСР, а саме: Грузія, Молдова та Азербайджан. Стосовно цих держав, які разом з Україною входять до міжнародного об'єднання ГУАМ, можна відзначити значні збіги у їх пострадянській історії, включаючи періоди збройних конфліктів на їх теренах. Усі ці держави, щонайменше у певні періоди своєї новітньої незалежності, намагалися здійснювати активні кроки у напрямі європейської та євроатлантичної інтеграції, але й досі

[18] У країнах-партнерах України по організації ГУАМ реалізовані підходи, які, для цілей даної доповіді, отримали назву ***фрагментарних.*** До особливих випадків таких підходів, на погляд авторів, можна також віднести національні практики таких розвинених країн, як Німеччина та Австрія, в яких заходи із забезпечення захисту (безпеки) та стійкості КІ в організаційно-правовому плані скоріше оформлені у важливі напрями вжиття заходів з кібербезпеки, ніж у цілісні національні системи захисту КІ.

перебувають у перехідних станах[19], спільним чинником яких є *наявність серйозних безпекових проблем*.

4.1. Приклад Грузії

Пошук у відкритих джерелах використання термінів «*критична інфраструктура*» або його синоніму — «*національна інфраструктура*» грузинською, англійською та російською мовами (у т.ч. у базах даних з національного законодавства)[20] дав нульовий результат. Також відсутні повідомлення з міжнародних форумів про створення і функціонування в країні національної системи захисту КІ. Все це дозволяє стверджувати, що в країні концепцію захисту КІ не запроваджено.

Натомість Грузія увійшла до числа колишніх радянських республік, які досить успішно запроваджують сучасні підходи у сфері кібербезпеки. Зокрема, згідно з Глобальним індексом кібербезпеки (*Global Cybersecurity Index, GCI*) Міжнародного союзу електрозв'язку (*International Telecommunication Union, ITU*)[21], Грузія посідає дуже високі місця у європейському регіоні та у світі (відповідно, 9-е та 18-е) з точки зору кібербезпеки. При цьому, на відміну від національного законодавства, саме у відомчих документах стосовно кібербезпеки можна зустріти термін «*критична інфраструктура»*[22].

Однією з головних причин такої посиленої уваги Грузії до питань кібербезпеки, включаючи захист життєво-важливих для існування держави об'єктів, систем і послуг, стали уроки, винесені з аналізу подій під час російсько-грузинського збройного конфлікту 2008 р. Як відзначають Б. С. Бакленд, Ф. Шрайєр та Т. Х. Вінклер[23], унікальність цього конфлікту полягає у тому, що *«саме тоді вперше в історії військові дії однієї зі сторін супроводжувалися масованими хакерськими атаками на сервери державних та фінансових установ на території супротивника...».*

І хоча експерти женевського центру зауважили, що у підсумку ці атаки не завдали суттєвої шкоди, оскільки більша частина економіки та об'єктів КІ Грузії знаходилися поза межами інтернет-простору, але внаслідок цих атак *«у самі*

---

[19] Така наша оцінка може не повністю збігатися з точкою зору самих країн. Зокрема, у проекті документу, розміщеного на сайті Президента Азербайджану Development Concept «Azerbaijan - 2020: Outlook for the Future», стверджується, що «перехідний період вже завершився».

[20] Саме на цих трьох мовах представлені нормативно-правові акти Грузії.

[21] Внаслідок затримки у публікації Глобального індексу кібербезпеки (GCI) за 2019 рік, зумовленої пандемією COVID-19, тут і далі по тексту посилання стосуються GCI 2018 [Електронний ресурс]. – Режим доступу: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[22] Див. наприклад, документ RFC 2350 CSIRT Description for CERT-GOV-GE. [Електронний ресурс]. – Режим доступу: https://dea.gov.ge/uploads/Articles/CERT-GOV-GE%20RFC2350.pdf .

[23] Демократическое управление и вызовы кибербезопасности. Женевский центр демократического контроля над вооруженными силами (DCAF), DCAF Horizon 2015 Working paper No.1.Ru, Женева 2013 [Електронний ресурс]. – Режим доступу: https://www.dcaf.ch/sites/default/files/publications/documents/Horizon_1_Good_Governance_CyberSecurity_RUS.pdf.

критичні дні боїв російські ЗМІ могли представляти своє бачення війни, у той час як грузини фактично опинилися в умовах кіберблокади».

Безпосередній зв'язок між безпекою тих систем і об'єктів, які у більшості розвинених країн світу відносять до КІ, та питаннями національної безпеки Грузії встановлено, зокрема, у Законі Грузії «*Про інформаційну безпеку*» визначенням терміну «*критична інформаційна система»,* під якою розуміється *«інформаційна система, безперевне функціонування якої має важливе значення для оборони або (та) економічної безпеки країни, нормального функціонування органів державної влади або (та) суспільства»*[24].

4.2. Приклад Молдови

Наявна у відкритих джерелах інформація стосовно захисту КІ у Республіці Молдова (РМ) показує картину, аналогічну ситуації в Грузії, а саме – в країні докладають достатньо серйозних зусиль щодо кіберзахисту, і це відбувається значною мірою під впливом і за допомоги держав-членів НАТО та ЄС. Відповідно до останньої публікації Глобального індексу кібербезпеки Міжнародного союзу електрозв'язку, РМ посідає в європейському регіоні та у світі 31-е та 53-є місця відповідно.

При цьому у певний період часу ситуація навколо захисту КІ в РМ розвивалася шляхом, подібним до грузинського, а саме: у *Національній стратегії розвитку інформаційного суспільства* «*Цифрова Молдова* 2020», ухваленій урядовою постановою у жовтні 2013 року[25], у розділі 4.3. *Захищене та безпечне цифрове середовище* було сформульоване, серед іншого, специфічне завдання - *1) підвищення рівня кібербезпеки критичних національних інфраструктур (державних органів / установ, мереж електронних комунікацій, водопроводів, енергетичних систем, транспортних мереж)*. Цим пунктом було передбачено зокрема *визначення національних критичних інфраструктур, які мають бути захищені від кібератак.*

Щоправда, вивчення відкритих джерел інформації показує, що на даний момент це завдання, скоріш за все, було за якихось причин знято з порядку денного, адже ні національне законодавство, ні чинні плани уряду РМ[26] згадок про захист або безпеку КІ вже не містять[27].

---

[24] Закон Грузії «Про інформаційну безпеку». [Електронний ресурс]. – Режим доступу: https://matsne.gov.ge/en/document/download/1679424/3/ru/pdf.

[25] [Електронний ресурс]. – Режим доступу: http://old.mtic.gov.md/ru/postanovlenie-o-nacionalnoy-strategii-razvitiya-informacionnogo-obshchestva-cifrovaya-moldova-2020 .

[26] Див., наприклад, План дій Уряду на 2020 – 2023 роки, затверджений урядовою постановою в грудні 2019 року [Електронний ресурс]. – Режим доступу: https://gov.md/sites/default/files/document/attachments/pag_2020-2030-ru.pdf .

[27] Певним натяком на те, що ситуація може змінитися є інформація про заплановану участь представників Молдови у міжнародному форумі в Румунії (жовтень 2020), який присвячений захисту КІ.

Натомість, до специфічної риси державного планування у РМ можна віднести ***дуже широке використання поняття «інфраструктура» стосовно усіх сфер життєдіяльності країни,*** починаючи від воєнної інфраструктури та ІТ-інфраструктури, і закінчуючи спортивною і культурною інфраструктурами, а також інфраструктурою переробки сільгосппродукції[28].

Таким чином, у випадку Молдови у контексті теми, що розглядається, можна говорити лише про ***взаємозв'язок між кібербезпекою та національною безпекою***, який на урядовому рівні чітко усвідомлюється, про що свідчить План дій Уряду на 2020 – 2023 роки, в якому пункти плану щодо кібербезпеки віднесені до *Розділу XI. Безпека і оборона*.

4.3. Приклад Азербайджану

В Азербайджані ***основна увага приділяється безпеці інфраструктури, пов'язаної з виробництвом і транспортуванням енергоресурсів*** у плані зменшення її вразливості до стихійних лих, надзвичайних ситуацій та диверсій. Зокрема, про це йдеться у профільному для національної безпеки законі, датованому 2004 роком[29].

Вивчення відкритих джерел інформації щодо національного законодавства показує відсутність у ньому більш загальних термінів, а саме: «*критична інфраструктура*» або «*національна інфраструктура*». І лише у документах, що стосуються співробітництва Азербайджану з НАТО, можна зустріти термін «*критична інфраструктура*», але, знову ж таки, у контексті обговорення співробітництва з Альянсом щодо забезпечення безпеки фрагменту КІ, а саме — *критичної енергетичної інфраструктури*.

За інформацією Інституту інформаційних технологій Національної академії наук Азербайджану, станом на 2 березня 2020 року в країні тривала робота над проектом «*Національної стратегії Азербайджанської Республіки з інформаційної безпеки та кібербезпеки на 2020 – 2025 роки»,* яка підтримується європейськими та євроатлантичними структурами.

Національне законодавство Азербайджану та офіційні документи, що стосуються співробітництва країни з ЄС та НАТО, свідчать про чітке усвідомлення політичним керівництвом країни ***взаємозв'язку між безпекою критичної енергетичної інфраструктури та національною безпекою***.

3. Запровадження концепції критичної інфраструктури та її захисту з точки зору зрілості механізмів управління сектором безпеки і оборони

Попередні розділи доповіді показують, що у сучасному світі далеко не

[28] Загалом, у Плані дій Уряду на 2020 – 2023 роки згадується 17 інфраструктур.
[29] The Law of the Republic of Azerbaijan No. 712-IIQ «On National Security» of 29 June 2004 [Електронний ресурс]. – Режим доступу: https://www.legislationline.org/download/id/5410/file/CODEXTER%20Profile%202014%20Azerbaijan.pdf /

завжди очевидна для кожної держави необхідність забезпечення захисту (безпеки) та стійкості життєво-важливих систем і об'єктів з точки зору безпеки населення, а також суспільних і державних інститутів призводить до створення національних (державних) систем захисту КІ.

При цьому, навіть ***усвідомлення рівня загроз та ризиків для національної КІ, як неприйнятного, може виявитися недостатнім для створення державної системи захисту КІ***.

Дійсно, на прийняття та реалізацію необхідних рішень можуть також впливати фактори, спричинені перехідним станом економіки; несприятливі безпекові умови, наприклад, у вигляді наслідків збройних конфліктів на території країни, а також фактор *зрілості управлінських механізмів у сфері безпеки* тієї чи іншої країни.

Аналіз запровадження концепції КІ і питання необхідності створення державної системи захисту КІ як управлінської проблеми дозволяє висвітлити деякі специфічні особливості цього процесу та, за певних обставин, оцінити пов'язані з ним завдання з точки зору їх вчасності та пріоритетності.

У процесі подальшого обговорення будемо спиратися на ряд доволі очевидних припущень і фактів, а саме:

1. Розвинені країни світу, які функціонують на принципах демократії та ринкової економіки, мають достатньо зрілі механізми державного управління.

2. Механізми управління сектором безпеки і оборони є специфічною, але, при цьому, невід'ємною частиною загального процесу державного управління.

3. Створення цілісних державних (національних) систем захисту КІ (застосування *цілісних підходів*[30]*)* притаманне, як правило, розвиненим країнам світу.

4. Досягнення стану зрілості механізмів державного управління, у т.ч. сектором безпеки і оборони, є певним, протяжним у часі, процесом зі своїми етапами та послідовностю їх виконання.

5. У менш розвинених країнах, у т.ч. тих, економіка яких знаходиться у перехідних станах, та/або які перебувають у складних безпекових умовах, застосовуються, здебільшого, *фрагментарні підходи*[31] до захисту важливих інфраструктур, які, за певних умов, можна вважати початковими етапами застосування *цілісних підходів.*

---

[30] Для цілей цієї доповіді під ***цілісним підходом*** розуміється підхід до забезпечення захисту (безпеки) та стійкості КІ, яким передбачено створення єдиної державної системи забезпечення захисту та стійкості КІ проти усіх видів фізичних загроз та кіберзагроз. Цей підхід реалізується у більшості розвинених країн світу (у т.ч. країн-членів НАТО та ЄС).

[31] Для цілей цієї доповіді під ***фрагментарним підходом*** розуміється підхід до забезпечення безпеки та стійкості важливих інфраструктурних об'єктів і систем, коли відповідні безпекові заходи щодо інфраструктурних об'єктів і систем здійснюються за окремими безпековими напрямами (кібербезпеки, енергетичної безпеки тощо).

Спираючись на наведені вище припущення, можна стверджувати, що перехід на якісно новий рівень управління, якого потребує ***запровадження концепції КІ та створення державної системи захисту КІ, має здійснюватися більш-менш синхронізовано з процесами реформування механізмів державного управління у цілому***. Було б помилково сподіватися, що можливо забезпечити належні процедури координації дій, взаємодії та обміну інформацією (КДВОІ) лише за окремим безпековим напрямом, не реформуючи інші напрями і сектори у сфері національної безпеки.

Разом з тим, це не означає, що усі заінтересовані сторони (у даному випадку, у запровадженні концепції КІ[32]) мають обов'язково чекати на якісь спеціальні сигнали про початок реформ. Адже прогрес, досягнутий за окремим напрямом, може стати драйвером реформування усього сектору безпеки і оборони держави.

Для планування його реформування, таким чином, є важливим визначення пріоритетних напрямів цього процесу, вчасності висунення до категорії пріоритетних тих чи інших програм або завдань.

З цієї точки зору одним із показників, які слід ураховувати в процесі пріоритетизації завдань з реформування сектору безпеки і оборони, має стати ***оцінка зрілості існуючих систем управління за окремими безпековими напрямами***, що, зокрема, передбачає усвідомлення необхідності та розуміння кінцевих цілей реформування, а також наявність необхідних умов для започаткування процесу. Останнє, серед іншого, включає розуміння того, що при реформуванні існуючих та розбудові нових систем управління безпекою слід дотримуватися певної послідовності виконання етапів процесу (на рис. 2 зображені типові етапи розбудови безпекової системи).

[32] Кабінет Міністрів України. Розпорядження від 6 грудня 2017 р. № 1009-р «Про схвалення Концепції створення державної системи захисту критичної інфраструктури». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text .

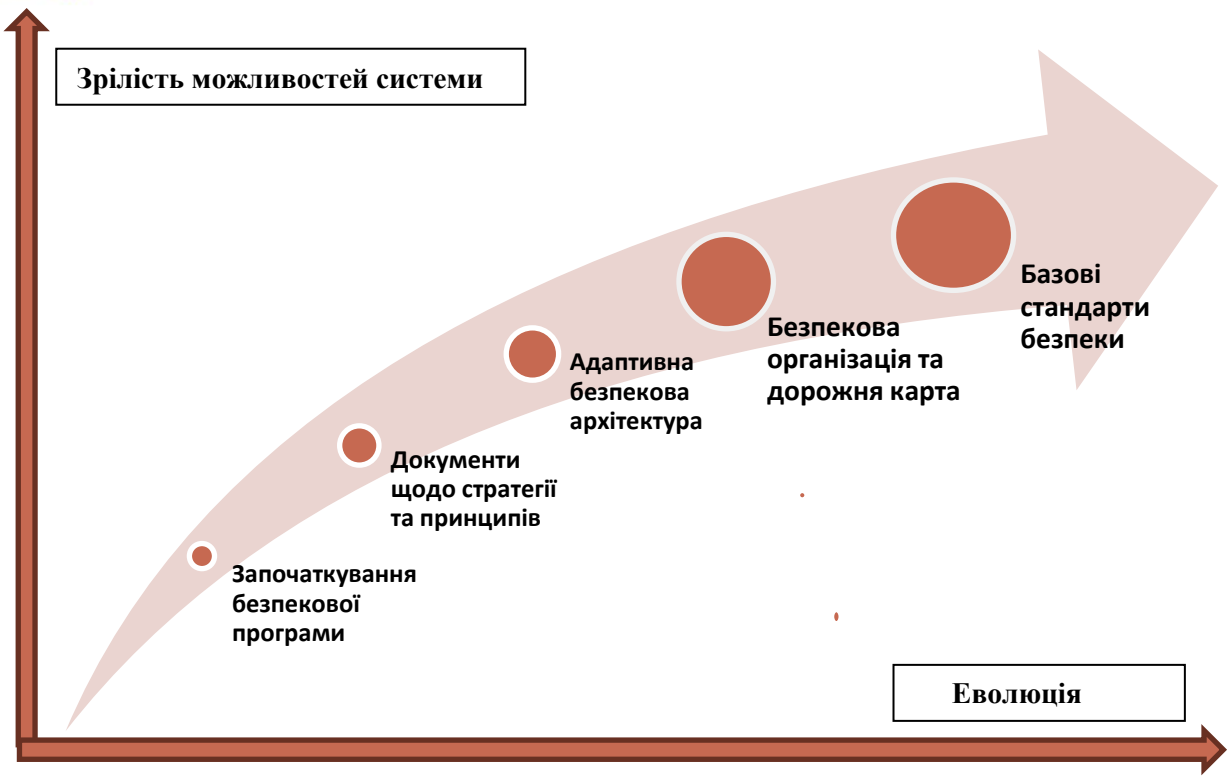

Рис. 2. Приклад підходу до визначення послідовності етапів створення системи управління у сфері безпеки[33].

Беручи до уваги наведені вище приклади національних практик з точки зору взаємозв'язку питань національної безпеки, а також захисту (безпеки) КІ та кібербезпеки, можна зробити такі висновки:

1. У більшості розвинених країн світу[34] реалізовано концепцію захисту КІ; міжнародні організації у своїх документах відображають пріоритетну роль питань захисту (безпеки) КІ, безпосередньо пов'язаних з питаннями національної безпеки.
2. У референтній групі країн, до якої ми включили колишні радянські республіки – члени ГУАМ (Грузію, Молдову та Азербайджан) за ознаками перехідних станів їх національних економік, наявності на їхніх територіях зон збройних конфліктів при високому рівні відносин з європейськими та євроатлантичними структурами, спостерігається реалізація *фрагментарних підходів до безпеки інфраструктурних об'єктів, важливих для забезпечення життєдіяльності країн,* які варіюються в залежності від специфічності безпекових та економічних умов, в яких знаходиться кожна

[33] Guidelince «Resilience of Critical Infrastructure Protection», p.23, Project Recipe 2015 Report,EC Humanitarian Aid and Civil Protection Directorate. [Електронний ресурс]. – Режим доступу: https://ec.europa.eu/echo/sites/echo-site/files/recipe_guidelines.pdf .

[34] Йдеться, насамперед, про держави-члени НАТО, ЄС та ОЕСР. Певними виключеннями серед цих держав можна вважати такі європейські держави, як ФРН та Австрія, у національних законодавствах яких термін «критична інфраструктура» визначений, існують переліки об'єктів КІ, але відповідна діяльність будується, головним чином, навколо забезпечення кібербезпеки об'єктів КІ.

з країн. Зокрема, питанням захисту інфраструктурних об'єктів і систем приділяється увага у рамках забезпечення їхньої інформаційної безпеки та кібербезпеки[35] або безпеки критичної енергетичної інфраструктури, а відповідні напрями діяльності віднесені до сфери національної безпеки.

3. Така ситуація із впровадженням концепції КІ, а також питаннями забезпечення її захисту (безпеки) та стійкості у різних країнах світу дозволяє зробити припущення, що повномасштабна реалізація згаданої концепції більш характерна для розвинених країн, що мають зрілі механізми державного управління, у т.ч. управління секторами національної безпеки, а також більші фінансові можливості.

Таким чином, з точки зору вирішення питань необхідності реформування безпекових систем (у даному випадку – пов'язаних із захистом і стійкістю КІ), а також вибору можливих моделей, строків та етапів відповідних процесів великої ваги можуть набувати результати ***оцінки зрілості відповідних систем (механізмів) державного управління.***

Вивчення літературних джерел з цієї проблематики не дає інформації стосовно використання таких підходів щодо КІ в цілому, але певні напрацювання можна знайти у сфері кібербезпеки. Ознайомлення з ними показує, що ***методологія оцінки зрілості державних систем кібербезпеки може бути розповсюджена, практично без виключень, на сферу безпеки КІ***.

Як і для сфери кібербезпеки, при оцінюванні зрілості системи забезпечення захисту (безпеки) та стійкості КІ ключовими є відповіді про наявність:

a. ***офіційно прийнятої стратегії або політики забезпечення захисту та стійкості КІ*** (засади державної політики можуть також бути закріплені у профільному законодавстві);

b. ***державного органу, на який покладено відповідальність за забезпечення захисту та стійкості КІ***;

c. ***державної структури, відповідальної за інформування та обробку інформації*** про інциденти (кризи), пов'язані з КІ (у випадку КІ це може включати мережу ситуаційних та інформаційно-аналітичних центрів);

d. ***державної програми міжвідомчого співробітництва*** у сфері захисту та стійкості КІ;

e. ***офіційно прийнятої програми співробітництва державного і приватного секторів*** у сфері забезпечення захисту та стійкості КІ.

Звичайно, детальний аналіз не може бути обмеженим лише відповідями на ці питання, але вони мають ключове значення, оскільки дозволяють визначити відсутність/наявність та стан (у разі наявності) ряду базових елементів безпекової архітектури забезпечення функціонування КІ.

[35] Досвід зазначених країн показує, що важливу роль у висуненні питань безпеки інфраструктур відіграє співробітництво зазначених країн з НАТО та ЄС.

4. Спроба запровадження концепції критичної інфраструктури та її захисту в Україні: пошук моделі інтегрування до сфери національної безпеки

У попередніх розділах доповіді автори, спираючись на зарубіжний досвід, стисло проаналізували роль і місце діяльності із забезпечення захисту (безпеки) і стійкості КІ у сфері національної безпеки.

При цьому були розглянуті не тільки підходи і практики, характерні для розвинених країн, в яких досягнуто високих рівнів зрілості управління секторами безпеки і оборони, але й випадки країн, які знаходяться у перехідних станах та мають безпекові проблеми.

Виходячи з представленої вище інформації, яка свідчить про те, що країни, які знаходяться у різних політичних, безпекових, економічних та інших умовах, можуть застосовувати суттєво відмінні підходи до захисту критично важливих об'єктів і систем, на нашу думку, ***одним із факторів, які впливають на вибір тієї чи іншої архітектури (моделі) захисту, є ступінь зрілості механізмів державного управління*** сектором безпеки і оборони, особливо в частині його спроможності реагувати на кризові ситуації.

З нашої точки зору, пошук відповіді на питання: ***чому запровадження системи захисту КІ в Україні достатньо тривалий час не здійснюється відповідно до визначених термінів,*** є необхідною умовою для подальших усвідомлених кроків у напрямі забезпечення захисту національної КІ, які мають базуватися на результатах виявлення та аналізу чинників, вплив яких завадив реалізації рішення Ради національної безпеки і оборони (РНБО) України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», введеного в дію Указом Президента України від 16 січня 2017 року № 8[36].

4.1. Стислий аналіз процесу виконання рішення РНБО України щодо критичної інфраструктури

Незважаючи на те, що у зазначеному рішенні РНБО України питання захисту КІ були віднесені до числа пріоритетних напрямів державної політики національної безпеки України[37], з низки завдань, визначених цим документом, повністю було виконане лише одне — стосовно розробки і ухвалення Урядом Концепції створення державної системи захисту критичної інфраструктури (далі – Концепція)[38]. При

[36]Указ Президента України від 16 січня 2017 року № 8/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/8/2017.

[37] У контексті теми, що розглядається, слід відзначити, що зазначене рішення РНБО України прямо вказує на безпосередній зв'язок між захистом КІ та національною безпекою.

[38] Витяг з рішення РНБОУ: «2) у двомісячний строк після схвалення концепції створення державної системи захисту критичної інфраструктури розробити за участю Служби безпеки України, Служби зовнішньої розвідки України і Національного банку України та внести в установленому порядку на розгляд Верховної

цьому Концепцію було ухвалено урядовим розпорядженням лише в грудні 2017 р. (запізнення майже у 9 місяців). У свою чергу, процес розробки та внесення в установленому порядку на розгляд ВРУ проекту Закону України «*Про критичну інфраструктуру та її захист*» також відбувався недостатньо швидко. На це вплинула, зокрема, відсутність серед більшості членів створеної при Мінекономрозвитку робочої групи спільного бачення актуальності та цілей закону. Зрештою у травні 2019 р., із серйозним запізненням, законопроект було внесено на розгляд Верховної Ради[39].

Попереднім складом парламенту законопроект розглянуто не було, і у зв'язку із обранням нового складу ВР України та затвердженням нового складу Уряду проект закону було відкликано. При цьому підготовлений згаданою робочою групою текст законопроекту низкою своїх положень і введених термінів суттєво відрізнявся не тільки від загальновизнаних у світі принципів побудови систем захисту КІ, але й від сформульованих у рішенні РНБО завдань.

Участь представників НІСД у цій роботі дозволяє нам стверджувати, що в процесі розробки та погодження законопроекту ***зусилля міністерств і відомств звелися, значною мірою, до просування положень, які відображали поточні, суто відомчі інтереси,*** тоді як реалізація концепції захисту КІ має бути спрямована, головним чином, на формування нових, ефективних надвідомчих і міжвідомчих механізмів управління, забезпечення, щонайменше на початкових етапах, дієвої координації дій, взаємодії та обміну інформацією (КДВОІ) між існуючими в країні системами забезпечення безпеки та кризового реагування.

У ході діяльності робочої групи з розробки законопроекту ряд відомств відстоювали позицію, що усі необхідні питання забезпечення безпеки відповідних об'єктів, включаючи КДВОІ, вже достатньо добре врегульовані у рамках існуючих систем.

З приводу цієї аргументації можна погодитися лише з тим, що життєво важливі об'єкти і системи в Україні, як і в більшості країн світу, ніколи не перебували поза зоною уваги державних органів, інших акторів у цій сфері. Але чи є цей факт достатнім, щоб стверджувати, що у рамках існуючих державних систем заходи з безпеки та стійкості життєво важливих інфраструктурних об'єктів і систем відповідають сучасним викликам та загрозам, на які має реагувати Україна?

У низці досліджень НІСД було вказано, що ***за відсутності державної системи захисту (безпеки) та стійкості КІ відповідні об'єкти***[40] ***не можуть бути ефективно захищені існуючими в Україні системами безпеки та кризового***

Ради України проект Закону України «Про критичну інфраструктуру та її захист» .

[39] ВР України отримала проект Закону 27.05.2019 р. (майже на два роки пізніше терміну, передбаченого рішенням РНБО України). [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996.

[40] Для цілей даного обговорення термін *об'єкти* включає усі об'єкти, системи, мережі і ресруси, які зазвичай відносять до критичної інфраструктури.

реагування, особливо у випадках реалізації масштабних комплексних загроз і небезпек.

Дійсно, системи і об'єкти, які зазвичай відносять до КІ, в нашій країні розподілені по більш ніж десяти категоріях. Лише частина з них:

– *підприємства, які мають стратегічне значення для економіки та безпеки держави;*

– *особливо важливі об'єкти електроенергетики;*

– *особливо важливі об'єкти нафтової галузі;*

– *об'єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період;*

– *об'єкти можливих терористичних посягань;*

– *об'єкти підвищеної небезпеки;*

– *радіаційно небезпечні об'єкти* тощо.

Відповідальність за їх безпеку покладено на різні міністерства і відомства, які забезпечують функціонування відповідних систем. При цьому кожна система має «власні» набори загроз та ризиків, якими вона опікується, «власні» режими функціонування у різних безпекових умовах, «власні» плани і процедури реагування, викладені із застосуванням відомчої системи термінів і понять.

До того ж визначені у положеннях і планах механізми і процедури взаємодії між існуючими національними системами безпеки і кризового реагування здебільшого є недостатньо відпрацьованими та апробованими для випадків масштабних кризових ситуацій, оскільки в країні до цього часу практика міжвідомчих навчань і тренувань на рівнях, вищих ніж об'єктовий, була розвинута слабко. Натомість ***головне призначення систем забезпечення захисту (безпеки) та стійкості КІ полягає у запобіганні саме масштабним комплексним кризам та у реагуванні на них***, якщо вони все ж трапляються.

При цьому слід відзначити, що ситуація навколо запровадження концепції КІ в Україні змінювалася достатньо динамічно, а позиції міністерств і відомств еволюціонували під впливом складних безпекових процесів як ззовні, так і всередині країни. Слід відмітити, що за низкою принципових напрямів ідея створення державної системи захисту КІ упродовж певного періоду часу отримувала підтримку з боку правоохоронних органів і спецслужб, зокрема, таких ключових акторів у цій сфері як МВС, СБУ і Держспецзв'язку.

Зокрема, МВС оперативно створило профільний підрозділ з питань захисту КІ у своєму складі. СБУ значно посилила напрям контррозвідувального захисту критичної інфраструктури. Держспецзв'язку активно співпрацювала з іншими відомствами, вбачаючи можливості для досягнення певної синергії між зусиллями зі створення державної системи захисту КІ та державної системи кібербезпеки.

Тим не менше, процес розробки законопроекту проходив досить суперечливо. Упродовж нього ряд міністерств та відомств так і не змогли повністю вийти за рамки поточних суто відомчих інтересів, і опублікована остаточна редакція документа була піддана доволі серйозній критиці, зокрема з боку представників приватного сектору економіки.

Урахування фактору зрілості управлінських механізмів дає змогу дещо по-іншому розглянути процес запровадження концепції КІ в Україні, а також взаємозв'язок питань безпеки інфраструктурних об'єктів і систем, оцінивши, зокрема, вчасність та пріоритетність завдань, визначених відповідним рішенням РНБО України.

Необхідно також взяти до уваги той факт, що на формування, м'яко кажучи, «обережного» ставлення до планів створення державної системи захисту КІ з боку ряду державних органів, без сумніву, вплинули численні попередні реформи в системі державного управління України та їх суперечливі результати.

Ураховуючи наведені вище міркування, які базуються на аналізі ситуації із запровадженням концепції КІ в Україні, автори вважають, що неприпустиме для ефективного управління національною безпекою ***затягування процесу розробки проекту профільного закону та створення державної системи захисту КІ не пов'язані з умисним блокуванням виконання завдань,*** сформульованих у відповідних нормативно-правових актах***, а, скоріш за все, є наслідком незрілості механізмів державного управління***, зокрема у сфері національної безпеки.

Слід згадати те, що для розглянутих у Розділі 2 країн, в яких ефективність державного управління ще не досягла рівнів, характерних для більшості розвинених країн світу, невипадковим виглядає запровадження саме *фрагментарних підходів* до захисту важливих для життєдіяльності населення, суспільства і держави об'єктів і систем. Недостатня зрілість державного управління, очевидно, у прямий та непрямий способи пов'язана з тим, що економіки згаданих країн перебувають у перехідних станах (знаходяться під впливом перехідних процесів), а їхні сектори безпеки і оборони зазнають своєрідного деформуючого впливу важких безпекових умов, у яких перебувають ці країни.

4.2. Оцінка зрілості наявних в Україні систем управління безпекою об'єктів, які відносять до критичної інфраструктури

Якщо спробувати дати оцінку зрілості наявних в Україні систем управління безпекою об'єктів, які у розвинених країнах відносять до КІ, ***безпосередньо поширивши на сферу безпеки КІ підхід, який вже використовується для оцінки зрілості національних систем кібербезпеки*** (див. перелік питань *а.* – *е.* у Розділі 3), то результат такої оцінки буде досить очікуваним.

Дійсно, в Україні лише у 2016 - 2017 рр. розпочато розбудову державної системи захисту КІ і на цьому шляху виконане повністю тільки одне з намічених рішенням РНБО України завдань – розробка та прийняття концепції створення

державної системи захисту КІ. Натомість решта відповідей про наявність індикаторів (елементів системи), які свідчать про зрілість механізмів управління в цій сфері, буде негативною.

До такого ж висновку можна дійти, використовуючи підхід, проілюстрований на Рис. 2, вважаючи, що у нашому випадку безпековою системою є державна система захисту КІ. Відповідно до графіку рекомендованої послідовності етапів створення безпекової системи, в Україні у сфері захисту КІ були виконані лише перше та частково друге завдання.

До специфічних умов ситуації в Україні навколо запровадження концепції КІ, особливо на початку процесу, слід також віднести й те, що після років стагнації тривалий час було витрачено на усвідомлення експертним співтовариством, науковцями та фахівцями актуальності питань захисту КІ, створення необхідного рівня фахової підтримки для винесення цієї проблематики на вищий політичний рівень.

Таким чином, резюмуючи наведені вище міркування, можна сказати, що ***причини тривалої затримки у запровадженні концепції КІ в Україні мають не випадковий, а системний характер і, значною мірою, обумовлені недостатньою зрілістю механізмів управління національною безпекою***.

4.3. Можливі варіанти забезпечення захисту (безпеки) та стійкості об'єктів і систем критичної інфраструктури в Україні

З висновку про закономірність серйозної затримки у виконанні завдань, сформульованих у відповідних нормативно-правових актах щодо КІ в Україні, ***випливає необхідність у більш чіткому визначенні подальшої траєкторії руху щодо забезпечення захисту (безпеки) та стійкості КІ в Україні***. Адже на даний момент, після того як у серпні 2019 р. законопроект «Про критичну інфраструктуру та її захист» було відкликано з ВР України, у питаннях забезпечення захисту (безпеки) та стійкості КІ в Україні можна констатувати суттєву невизначеність.

Дійсно, опрацювання розробленого законопроекту новим складом Уряду України та його підготовка до повторного внесення на розгляд Верховної Ради проходить недостатньо енергійно, у т.ч. внаслідок відсутності чіткого усвідомлення актуальності цієї проблематики та її прямого зв'язку з питаннями національної безпеки.

Натомість безпеку та стійкість життєво важливих інфраструктур, як і досі, відносять до числа пріоритетних більшість національних урядів, а винесені з аналізу кризового реагування на глобальну пандемію COVID-19 уроки, очевидно, стануть основою для формування нових завдань щодо розвитку механізмів та інструментів забезпечення функціонування національних КІ у надзвичайних умовах, аналогічних тим, які виникали при введенні та знятті карантинних обмежень.

Слід також зазначити, що у той час як Україна загальмувала у процесі впровадження концепції захисту КІ, у світі під впливом глобальних безпекових процесів швидко відбувається формування нової тенденції – ***посилення уваги до забезпечення стійкості виконання життєво-важливих функцій та надання життєво-важливих послуг задля забезпечення національної стійкості.*** Це означає новий етап розвитку безпекових підходів, на якому ще більше зростає роль діяльності державних органів, приватного сектору, населення та інших суб'єктів процесу, спрямованої на забезпечення захисту та стійкості КІ , як одного з основних елементів системи забезпечення національної стійкості.

4.4. Деякі попередні спостереження щодо уроків, винесених з початкових етапів реагування України на пандемію COVID-19

Досвід реагування на пандемію у різних країнах світу показав, що, навіть там, де існували достатньо ефективні механізми кризового управління і були створені системи забезпечення захисту (безпеки) та стійкості КІ, внаслідок безпрецедентного масштабу кризи національні уряди зіткнулися з серйозними труднощами, зокрема при визначенні тих об'єктів і систем, що повинні продовжувати своє функціонування в умовах карантниу, а також при знятті карантинних обмежень, коли з'явилася необхідність у поступовому і почерговому відновленні функціонування таких об'єктів і систем.

Що стосується України, попередній аналіз показує, що з цієї точки зору ***на початок пандемії за багатьма напрямами Україна не мала ефективних інструментів, технічних та організаційних можливостей, а також достатніх ресурсів для реагування на цю глобальну загрозу*** (детальніше див. публікацію[41]). Відтак, більшість складних рішень (зокрема, про введення карантину) керівництво держави приймало безпосередньо у процесі реагування на кризову ситуацію, що впливало на їх якість і послідовність, потребувало низки додаткових корегуючих заходів тощо.

Попри масштабність і унікальність проблем реагування на пандемію COVID-19, можна стверджувати, що низка завдань, які виникали у ході реагування, могла би вирішуватися швидче й у більш послідовний спосіб, якщо би в Україні були закладені основи захисту КІ, не кажучи вже про наявність діючої державної системи захисту КІ, або суттєвих її фрагментів (див. також публікацію[42]).

Функціонування такої системи включає, серед іншого, ***створення та обслуговування списку (реєстру) об'єктів і систем, віднесених до КІ, встановлює***

[41] Деякі проблеми реагування на поширення COVID-19 у контексті забезпечення безпеки та стійкості критичної інфраструктури. Аналітична записка. [Електронний ресурс]. – Режим доступу: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/deyaki-problemi-reaguvannya-na-poshirennya-covid-19-u-konteksti.

[42] Стійкість критичної енергетичної інфраструктури: світовий досвід функціонування енергетичних компаній в умовах поширення COVID-19. Аналітична записка. [Електронний ресурс]. – Режим доступу: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/stiykist-kritichnoi-energetichnoi-infrastrukturi-svitoviy-dosvid.

режими їх функціонування за різних безпекових умов тощо. Очевидно, що відповідна нормативно-правова база значно полегшила би планування і реалізацію належних заходів (у т.ч. введення та поступове послаблення режиму карантину), слугувала би надійною основою у разі прийняття та введення в дію необхідних актів для вирішення оперативних завдань, що виникали у процесі реагування.

Широко визнається, що реагування на глобальні події, на кшталт пандемії COVID-19, потребує, серед іншого, якісно нового рівня КДВОІ між державними і місцевими органами, бізнесом і населенням, іншими акторами, у т.ч. для мобілізації усіх наявних в країні можливостей, урахування каскадних ефектів та ефектів доміно тощо. Натомість створення національних (державних) систем захисту та стійкості КІ і має одним з головних завдань саме створення й удосконалення механізмів і процедур КДВОІ.

Таким чином, повертаючись до проблеми запровадження концепції КІ в Україні, можна резюмувати:

Якщо наша країна має стратегічні плани увійти до числа розвинутих країн світу з ринковою економікою та державним управлінням, яке грунтується на демократичних засадах, то раціональних альтернатив подальшому просуванню у напрямі забезпечення захисту та стійкості КІ не існує.

Слід зауважити, що у такому випадку досягти планомірності та послідовності у проведенні необхідних реформ буде неможливо без чіткого ***усвідомлення приналежності питань захисту (безпеки) та стійкості КІ до проблематики національної безпеки***, що має знайти своє відображення у низці взаємоузгоджених концептуальних і стратегічних документів та у національному законодавстві.

Таким чином, найближчим часом на державному рівні необхідно вирішити, якими мають бути наступні організаційно-правові кроки у напрямі розв'язання проблем забезпечення захисту (безпеки) та стійкості КІ[43].

При цьому у пошуках відповіді, на думку авторів, нам ***слід відразу виключити можливість залишити поза увагою керівництва держави сучасні світові тенденції щодо посилення у той чи інший спосіб захисту національних інфраструктур від усіх фізичних та кіберзагроз***, адже бездіяльність у цьому стратегічному напрямі стане свідченням втрати необхідної динаміки (політичної волі) у процесі реформування сектору безпеки і оборони, що, зрештою, може загрожувати самому існуванню України як незалежної держави.

Виходячи з цього***, слід терміново виконати аналіз ситуації навколо створення державної системи захисту КІ***.

[43] Звичайно, відповідь на це питання не може бути відокремленою від більш загальних питань стратегічного планування у сфері національної безпеки.

При проведенні такого аналізу слід більш детально вивчити зарубіжний досвід та національні практики широкого кола країн, включивши до них і країни-члени ГУАМ, які на даний момент реалізують *фрагментарні підходи* до захисту своїх інфраструктур.

З точки зору авторів, на цьому етапі ***найбільш перспективним з багатьох точок зору виглядає висновок щодо необхідності та можливості створення цілісної державної системи забезпечення захисту (безпеки) та стійкості КІ на основі апробованих підходів і практик, застосованих у розвинених країнах світу (насамперед державах-членах НАТО та ЄС).***

У такому разі для організації подальшої роботи у цьому напрямі має бути розроблений чіткий робочий план, в якому передбачені спеціальні управлінські заходи для виключення системних перешкод, що стали на заваді вчасному розробленню та прийняттю профільного закону та переведення процесу розбудови системи захисту КІ у практичну площину, а в даний момент гальмують процес опрацювання законопроекту

При цьому в умовах значної турбулентності глобальних економічних та безпекових процесів, які не можуть не впливати на Україну, не можна повністю виключати і необхідність спрямування зусиль держави на забезпечення захисту (безпеки) та стійкості КІ на основі поетапної імплементації концепції захисту КІ (*фрагментарного підходу)*.

Огляд зарубіжного досвіду у цій сфері показує, що за будь-якого обраного курсу політики щодо захисту (безпеки) та стійкості життєво-важливих об'єктів ***до першочергових кроків слід віднести створення та обслуговування реєстру об'єктів,*** включених до відповідних національних інфраструктур, що, у свою чергу, ***потребує розробки і затвердження методик та процедур віднесення об'єктів до згаданих реєстрів***.

Успішне вирішення згаданих завдань буде неможливим без усвідомлення тієї суттєвої ролі, яку відіграє КІ у сфері безпечного функціонування сучасної держави, і можна сподіватися, що запровадження у тому чи іншому вигляді концепції КІ стане суттєвим внеском у процес реформування усієї системи державного управління, у т.ч. сектором національної безпеки і оборони.

Таким чином, включення питань захисту (безпеки) та стійкості КІ до проблематики національної безпеки потребуватиме подальших кроків задля узгодження у цілому політики в цій сфері, у т.ч. шляхом оновлення і гармонізації низки стратегічних і концептуальних документів.

У зв'язку з наведеними вище міркуваннями останнім часом особливий інтерес викликають зусилля, спрямовані на запровадження в Україні концепції *національної стійкості*, що відповідає сучасним безпековим підходам. У цій доповіді було пояснено співвідношення між *захистом (безпекою)* та *стійкістю* КІ і на основі зарубіжного досвіду показано, що історично запровадження концепції

захисту КІ передувало запровадженню концепції її *стійкості.* Ураховуючи цей факт, перед початком практичної реалізації концепції *національної стійкості,* на наш погляд, було б доцільно провести спеціальне дослідження стосовно можливого впливу фактору зрілості механізмів управління у сфері національної безпеки у цьому випадку.

Висновки та рекомендації

Робота над цією доповіддю виконувалася на тлі бурхливих і неоднозначних процесів і подій, які кардинально змінили та продовжують змінювати безпековий ландшафт у глобальному, регіональному та національному вимірах.

Більшість згаданих процесів у той чи інший спосіб пов'язані з можливостями та здатністю національних урядів, а у деяких випадках і спеціалізованих міжнародних організацій, оцінювати ризики, загрози і небезпеки криз (надзвичайних ситуацій різного походження), реагувати на такі кризи, забезпечуючи при цьому, наскільки це можливо, безпеку населення, стале функціонування державних і суспільних інститутів.

У свою чергу, саме згадані аспекти безпеки значною мірою визначаються наявністю систем захисту національних КІ, їх дієвістю та стійкістю.

Так само, як були переглянуті глобальні та національні безпекові підходи після Чорнобильської катастрофи 1986 р., терористичних актів 2001 р., відповідні уроки будуть винесені, а підходи будуть змінені й після пандемії COVID-19, а також масових заворушень у США та в інших країнах.

За результатами розгляду теми доповіді автори вважають за потрібне зробити такі **висновки**:

1. Для більшості національних урядів забезпечення сталого функціонування критично важливих для повсякденного життя країн об'єктів (***критичної інфраструктури***), завдяки чому населення, суспільні та державні інститути мають можливість доступу до життєво важливих ресурсів та послуг, ***залишається серед пріоритетних завдань у сфері національної безпеки***.

2. Огляд іноземного досвіду показує, що відповідні завдання здебільшого вирішуються шляхом запровадження концепці КІ. При цьому внаслідок різноманітності умов (насамперед безпекових та фінансово-економічних), в яких перебувають різні країни світу, а також у залежності від рівня зрілості механізмів державного управління ці завдання реалізуються з використанням різних підходів, які умовно можна поділити на дві основні категорії:

а. ***цілісні підходи*** (створюються державні системи забезпечення захисту та стійкості КІ проти усіх видів фізичних загроз та кіберзагроз) – більш характерні для розвинених країн світу (у т.ч. держав-членів НАТО та ЄС);

b. ***фрагментарні підходи*** (питання захисту та стійкості важливих інфраструктурних об'єктів і систем вирішуються у рамках створення систем за окремими безпековими напрямами (кібербезпеки, енергетичної безпеки тощо) – більш характерні для країн, які ще не досягли належного рівня зрілості державного управління; при цьому застосування фрагментарного підходу за певних умов можна разглядати як початковий етап реалізації цілісного підходу.

3. Аналіз стану створення державної системи захисту КІ в Україні дозволяє зробити обгрунтоване припущення, що основні причини невиконання рішення РНБО України мають системний характер і обумовлені, значною мірою, недостатньою зрілістю механізмів управління у сфері національної безпеки.

4. Попередній аналіз досвіду реагування на пандемію COVID-19 у світі та в Україні показав високу пріоритетність питання забезпечення функціонування КІ.

5. На даний момент назріла необхідність активізації державної політики щодо забезпечення захисту (безпеки) та стійкості КІ.

На основі проведеного аналізу та зроблених висновків вважаємо за доцільне **рекомендувати*:***

1. Визначити безпеку та стійкість критичної інфраструктури одним із напрямів забезпечення національної безпеки, що потребує внесення відповідних змін до частини четвертої статті 3 Закону України «Про національну безпеку України», а також статті 27 цього Закону щодо проведення огляду стану критичної інфраструктури як складової комплексного огляду сектору безпеки і оборони.

2. Кабінету Міністрів України:

2.1. Внести на розгляд Верховної Ради України законопроект про безпеку та стійкість критичної інфраструктури;

2.2. Розробити і затвердити порядок віднесення об'єктів до критичної інфраструктури;

2.3. Забезпечити створення та обслуговування реєстру об'єктів, віднесених до критичної інфраструктури.

З виконанням цього завдання в подальшому можливо передбачити переформатування наступних завдань і перехід до реалізації першого підходу (див. п. 2а), тобто до створення державної системи захисту КІ.

2.4. Розробити і затвердити Національний план захисту критичної інфраструктури України.

3. Апарату Ради національної безпеки і оборони України:

3.1. Опрацювати питання щодо утворення тимчасової міжвідомчої робочої групи з питань безпеки та стійкості критичної інфраструктури, завданням якої визначити комплексне опрацювання питань розбудови національної системи безпеки та стійкості критичної інфраструктури;

3.2. Розглянути стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об’єктів критичної інфраструктури», введеного в дію Указом Президента України від 16 січня 2017 року № 8, в порядку контролю за виконанням рішень РНБО України.