**УДК 351.81**

# ЩОДО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

**Онищенко Юрій Миколайович,**
кандидат наук з державного управління, доцент,
заступник декана з навчально-методичної роботи факультету № 4
**Чукалов Кирило Едуардович,**
**Синжерян Андрій Андрійович**
курсанти факультету № 4
Харківський національний університет внутрішніх справ,
м. Харків, Україна

**Анотація:** розглянуто й проаналізовано аспекти адміністративно-управлінського та законодавчого регулювання питань забезпечення захисту об'єктів критичної інфраструктури, сформульовано основні кроки у побудові та реалізації системи захисту об'єктів критичної інфраструктури України в найближчій перспективі.

**Ключові слова:** об'єкти критичної інфраструктури, державна політика, захист, ризик, кібербезпека.

У світлі сучасних викликів і загроз, які можуть походити як від природних катастроф, так і від кібератак, терористичних загроз або геополітичних конфліктів, захист об'єктів критичної інфраструктури стає важливою завданням для забезпечення національної безпеки країни.

Закони та нормативні документи у сфері забезпечення безпеки об'єктів критичної інфраструктури визначають стандарти безпеки, обов'язки власників та операторів об'єктів, а також механізми реагування на можливі загрози. Отже, даний матеріал охопить аналіз важливих аспектів законодавчого регулювання цієї сфери в Україні.

15 грудня 2021 року набрав чинності вкрай важливий закон «Про критичну інфраструктуру». Закон визначає правові та організаційні засади

створення та функціонування критичної інфраструктури і є складовою законодавства України у сфері національної безпеки. Він дає основні визначення та, поряд з вже прийнятими Постановами Кабінету Міністрів України, дає підґрунтя для комплексного забезпечення захисту критичної інфраструктури [1].

Особливості захисту об’єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду регулюються законами України "Про правовий режим воєнного стану", "Про правовий режим надзвичайного стану", "Про функціонування єдиної транспортної системи України в особливий період" та "Про оборону України". Окремим законом регулюються відносини щодо забезпечення кіберзахисту та кібербезпеки об’єктів критичної інфраструктури.

Розділ ІІ Закону регламентує основні засади державної політики у сфері контролю безпеки об’єктів критичної інфраструктури України. Державна політика у сфері захисту критичної інфраструктури регламентується статтею 4 Закону, ґрунтується на засадах:

1) визнання необхідності забезпечення безпеки та стійкості критичної інфраструктури;

2) визначення законодавчих вимог до принципів, пріоритетів, стратегічних завдань, підходів щодо захисту критичної інфраструктури;

3) визначення суб’єктів національної системи захисту критичної інфраструктури, їх повноважень та засад відповідальності, порядку взаємодії;

4) створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, на зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів;

5) створення системи раннього виявлення загроз критичній інфраструктурі;

6) запровадження державно-приватного партнерства, взаємодії суб’єктів господарювання та населення з питань забезпечення захисту та стійкості

критичної інфраструктури;

7) забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури;

8) створення умов швидкого відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування критичної інфраструктури [2].

Світові тенденції до посилення загроз природного та техногенного характеру, підвищення рівня терористичних загроз, збільшення кількості та підвищення складності кібератак, а також пошкодження інфраструктурних об'єктів у східних та південних регіонах України внаслідок збройної агресії Російської Федерації зумовили актуалізацію питання захисту систем, об'єктів і ресурсів, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки [3].

Отже, метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури.

До завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури належать:

1) запобігання проявам несанкціонованого втручання в її функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури;

2) попередження кризових ситуацій, що порушують безпеку критичної інфраструктури;

3) створення, впровадження, розвиток та забезпечення функціонування національної системи захисту критичної інфраструктури, у тому числі шляхом визначення уповноваженого органу у сфері захисту критичної інфраструктури України, а також визначення повноважень у сфері захисту критичної

інфраструктури інших суб’єктів національної системи захисту критичної інфраструктури;

4) розроблення нормативно-правової та нормативно-технічної бази з питань забезпечення безпеки об’єктів критичної інфраструктури;

5) розроблення та реалізація державних цільових програм із захисту критичної інфраструктури;

6) розроблення комплексу заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об’єктах критичної інфраструктури;

7) встановлення обов’язкових вимог із забезпечення безпеки об’єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації;

8) аналіз викликів та загроз, що впливають на стійкість критичної інфраструктури, оцінка стану її захищеності;

9) розроблення методології аналізу результативності державної політики у сфері захисту критичної інфраструктури;

10) підготовка, перепідготовка, підвищення кваліфікації, тренування працівників національної системи захисту критичної інфраструктури;

11) забезпечення взаємодії національної системи захисту критичної інфраструктури з відповідними міжнародними системами, насамперед європейськими та євроатлантичними.

Для коригування захисту були розроблені певні рівні національного захисту, які набули чинності на загальнодержавному рівні, управління на якому здійснюється Кабінетом Міністрів України, уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень згідно з Законом України «Про критичну інфраструктуру», іншими центральними органами виконавчої влади та державними органами, Національним банком України. Усі рівні були поділені на певні сектори, починаючи від регіонального рівня до рівня контролю глобальних об’єктів.

Регіональний та галузевий рівні, управління на яких здійснюється центральними та місцевими органами виконавчої влади, визначеними в установленому законом порядку відповідальними за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури та відповідальними за функціонування окремих державних систем захисту та реагування.

Місцевий рівень, управління на якому здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі створення), органами місцевого самоврядування в межах покладених на них повноважень.

Об'єктовий рівень, управління на якому здійснюється оператором критичної інфраструктури на підставі нормативно-правових та регуляторних актів у сфері захисту критичної інфраструктури. Розподіл на рівні контролю було затверджено статтею 7 Закону України «Про критичну інфраструктуру», де визначились функції кожного з рівнів національної програми захисту ОКІ.

Віднесення об'єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму. До таких критеріїв належать:

1) виконання функцій із забезпечення життєво важливих національних інтересів;

2) існування викликів і загроз, що можуть виникати щодо об'єктів критичної інфраструктури;

3) ймовірність завдання значної шкоди нормальним умовам життєдіяльності населення.

Категоризація об'єктів критичної інфраструктури регламентується

статтею 10 Закону України «Про критичну інфраструктуру», яка визначає вимоги щодо забезпечення захисту об’єктів критичної інфраструктури відповідно до рівня їх важливості для забезпечення окремих життєво важливих функцій у межах секторів критичної інфраструктури. Категоризація об’єктів критичної інфраструктури здійснюється секторальними органами у сфері захисту критичної інфраструктури відповідно до секторальної специфіки, вимог секторального законодавства та чотирьох визначених категорій критичності та важливості об’єктів.

В Україні захист об’єктів, які згідно зі світовою практикою належать до категорії «критична інфраструктура», регламентується численними нормативно-правовими актами переважно внутрішньовідомчого характеру. Така ситуація склалася природним чином: кожне окреме відомство виділяло певний спектр загроз для підпорядкованих об’єктів та володіло певним набором інструментів і ресурсів для забезпечення їх безпеки. У результаті в чинному законодавстві України визначено низку категорій об’єктів, для яких регламентуються особливі умови забезпечення захисту, зокрема підприємства, що мають стратегічне значення для економіки та безпеки держави; особливо важливі об’єкти електроенергетики й нафтогазової галузі; потенційно небезпечні об’єкти, об’єкти підвищеної небезпеки; об’єкти, що підлягають обов’язковій охороні підрозділами Державної служби охорони, та об’єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій та в особливий період; інші об’єкти й системи, такі як системи зв’язку, платіжні системи тощо [4].

Наслідком широкого переліку документів, що врегульовують окремі питання кібербезпеки є розшарованість, неоднорідність, колізійність, а подекуди, й відсутність вимог до кібербезпеки окремих секторів критичної інфраструктури, що, в свою чергу, зумовлено низкою обставин, зокрема, широким переліком сфер/секторів критичної інфраструктури, відсутністю протягом тривалого періоду часу спеціалізованого законодавства та вимог щодо заходів кіберзахисту критичної інфраструктури, а також чіткого переліку

уповноважених суб’єктів, переліку їх компетенцій та завдань у сфері захисту критичної інфраструктури, неналагодженістю взаємодії та координації державних органів, низьким рівнем реалізації державно-приватної взаємодії тощо.

В наслідок російської агресії в умовах дії правового режиму воєнного стану в Україні особливої важливості набуло питання забезпечення належного рівня захисту об’єктів критичної інфраструктури, отже в найближчому майбутньому вирішення чекають проблеми нормативно-правового, адміністративно-управлінського, координаційного та, звісно, фінансового характеру.

Враховуючи досвід провідних країн світу, а також роботи українських фахівців щодо захисту критичної інфраструктури, можна виділити такі напрями подальшої розбудови в Україні державної системи захисту критичної інфраструктури: розробка та регулярний перегляд нормативної бази; деталізація функцій головного державного координаційного органу у цій сфері; удосконалення методологічних підходів, на основі яких формується перелік критичної інфраструктури; підготовка кваліфікованих кадрів у сфері захисту критичної інфраструктури; організація обміну інформацією та кращими практиками у форматі міжнародного та державно-приватного партнерства [5].

**Вбачається доцільним сконцентрувати увагу на наступних кроках у побудові та реалізації системи захисту об’єктів критичної інфраструктури України в найближчій перспективі:**

1. ***Розвиток стратегії та планування:*** Україні потрібно розробити та постійно вдосконалювати комплексну стратегію захисту об'єктів критичної інфраструктури, а також плани дій під час виникнення надзвичайних ситуацій. Це дозволить країні краще готуватися до можливих загроз і ефективно реагувати на них.

2. ***Інвестиції у кібербезпеку:*** підвищення обізнаності персоналу, регулярний аудит систем безпеки, реалізація комплексного підходу до забезпечення кібербезпеки вимагають суттєвих фінансових витрат, але реально

допоможуть запобігти серйозним кібератакам та їх наслідкам.

3. ***Співпраця з міжнародними партнерами:*** активна співпраця з міжнародними партнерами для обміну досвідом та інформацією щодо захисту об'єктів критичної інфраструктури дозволить вчасно виявляти та реагувати на загрози.

4. ***Навчання та підготовка персоналу:*** персонал, який відповідає за безпеку об'єктів критичної інфраструктури, має систематично проходити перепідготовку та підвищення кваліфікації для отримання знань та навичок з виявлення та реагування на ризики та надзвичайні ситуації.

5. ***Державно-приватне партнерство*** **є запорукою** створення якісної системи захисту об'єктів критичної інфраструктури, адже, як свідчить досвід зарубіжних країн, ефективність реагування на кіберінциденти та кібератаки можлива лише за умови об’єднання зусиль зазначених сторін.

Захист об'єктів критичної інфраструктури в Україні є завданням, яке потребує серйозної уваги та ресурсів. Лише завдяки комплексному підходу та співпраці на різних рівнях уряду, бізнесу, громадськості та міжнародних партнерів Україна зможе забезпечити надійний захист своєї критичної інфраструктури та національної безпеки.

## СПИСОК ЛІТЕРАТУРИ:

1. Закон України «Про критичну інфраструктуру»: сподівання та реалії URL: https://uifuture.org/publications/zakon-ukrayiny-pro-krytychnu-infrastrukturu-spodivannya-ta-realiyi/

2. Закон України про критичну інфраструктуру від 16.11.2021 № 1882-IX URL: https://zakon.rada.gov.ua/laws/show/1882-20/ed20221205#Text

3. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: розпорядження Кабінету Міністрів України від 06.12.2017 № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

4. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній

інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4 (37). С. 83–93. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=spe_2015_4_12

5. Бобро Д. Г. Методологія оцінки рівня критичності об’єктів інфраструктури. Стратегічні пріоритети. 2016. № 3 (40). С. 77–86. URL: https://shron1.chtyvo.org.ua/Bobro_Dmytro/Metodolohiia_otsinky_rivnia_krytychnosti_obiektiv_infrastruktury.pdf?PHPSESSID=e42scruak1ifebqfqsm81bcun7