Поняття паспорту безпеки об'єкта критичної інфраструктури в розрізі сучасної нормативно-правової бази в Україні

Олександр Погосов, доц., канд. техн. наук, доцент[1] (ORCID: 0000-0003-2158-8897), **Андрій Дорошенко**, провідний інженер (ORCID: 0009-0001-4260-7287), **Ілья Гундар**, магістр[1] (ORCID: 0009-0002-5022-3483)

[1] *Київський національний університет будівництва та архітектури, Україна*

АНОТАЦІЯ

Дана робота присвячена аналізу поняття паспорта безпеки об’єктів критичної інфраструктури (КІ) в Україні з урахуванням сучасної нормативно-правової бази, зокрема Закону України «Про критичну інфраструктуру» № 1882-IX від 16 листопада 2021 року та Постанови КМУ № 818 від 4 серпня 2023 року. У ній розкривається роль паспорта безпеки як ключового документа, що систематизує інформацію про об’єкт КІ, його вразливості, потенційні загрози (кібератаки, техногенні чи природні катастрофи) та заходи захисту, включаючи режимні, інженерні й технічні аспекти. Дослідження висвітлює процес категоризації об’єктів КІ, обов’язки операторів, механізми ідентифікації ризиків і структуру паспорта, підкреслюючи його значення для забезпечення стійкості національної інфраструктури в умовах гібридних загроз. Ця робота акцентує на інтеграції паспорта безпеки в національну систему захисту КІ, сприянні координації між операторами та державними органами, а також необхідності періодичного оновлення документа для адаптації до динамічних викликів.

Ключові слова: паспорт безпеки, критична інфраструктура, захист об’єктів, нормативно-правова база, гібридні загрози, категоризація ризиків.

1. ВСТУП

Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX, з урахуванням подальших змін, становить фундаментальний правовий акт, спрямований на забезпечення стійкості національної безпеки в умовах гібридних загроз, де критична інфраструктура (КІ) визначається як сукупність об'єктів, систем і мереж, життєво важливих для функціонування економіки, забезпечення безпеки та оборони держави, порушення яких може призвести до значних негативних наслідків для суспільства, економіки чи довкілля [1]. Це визначення підкреслює стратегічну роль КІ як основи життєзабезпечення, охоплюючи не лише матеріальні активи, але й цифрові компоненти, що робить його актуальним у контексті сучасних викликів, таких як кібератаки чи воєнні конфлікти, і акцентує на превентивному підході до захисту.

2. ОСНОВНА ЧАСТИНА

Категоризація об'єктів КІ здійснюється за критеріями значущості, де вони поділяються на об'єкти національного та місцевого значення, залежно від масштабу потенційного впливу: національні — ті, що впливають на понад 100 тисяч осіб або спричиняють економічні втрати понад визначений поріг, а місцеві — з обмеженішим радіусом дії, з урахуванням секторів, таких як енергетика, транспорт, зв'язок, фінансова система та охорона здоров'я, що дозволяє диференційований підхід до управління ризиками [1].

Поняття оператора КІ вводиться як суб'єкта господарювання, незалежно від форми власності, який володіє, управляє або експлуатує об'єктом КІ, несучи первинну відповідальність за його безпеку, що підкреслює децентралізований характер системи, де держава виконує координаційну роль, а оператори — виконавчу [1]. Це поняття розширює коло відповідальних осіб, включаючи приватний сектор, і стимулює інтеграцію бізнесу в національну стратегію безпеки.

Обов'язки операторів КІ щодо впровадження режимних, інженерних та технічних заходів для запобігання несанкціонованим втручанням є ключовими елементами закону, де режимні заходи охоплюють контроль доступу та внутрішні процедури, інженерні — фізичний захист споруд, а технічні — кібербезпеку та моніторинг систем, з обов'язковим проведенням аудитів та навчань персоналу для мінімізації вразливостей [1; 2]. Ці обов'язки не обмежуються реактивними діями, а передбачають проактивне планування, що підвищує загальну стійкість інфраструктури до антропогенних і техногенних загроз.

Механізми ідентифікації загроз включають систематичний аналіз потенційних ризиків на основі даних розвідки, моніторингу та експертних оцінок, з розробкою паспортів безпеки — документів, що деталізують характеристики об'єкта, вразливості та заходи захисту, а також документів про загрози, які фіксують конкретні сценарії ризиків та плани реагування, забезпечуючи єдиний підхід до оцінки та пом'якшення небезпек [1; 3]. Такий механізм сприяє переходу від фрагментарного до комплексного управління ризиками, інтегруючи дані з різних джерел для прогнозування та запобігання інцидентам.

Режими функціонування об'єктів КІ диференційовані на нормальний (щоденна експлуатація з базовим захистом), кризовий (активізація надзвичайних заходів під час загрози чи інциденту) та відновлення (посткризове відновлення з аналізом причин і коригуванням планів), що дозволяє гнучке реагування на ескалацію ситуацій і мінімізує час простою [1]. Ці режими підкреслюють циклічний характер захисту, де відновлення стає основою для посилення стійкості в майбутньому.

Реєстр об’єктів критичної інфраструктури, ведений уповноваженим органом (Міністерством цифрової трансформації), є централізованою базою даних для реєстрації, моніторингу та координації об'єктів КІ, з обов'язковим внесенням інформації про категорію,

оператора та заходи захисту, що забезпечує прозорість і ефективну взаємодію між суб'єктами [1; 4].

Паспорт безпеки об'єкта критичної інфраструктури (ОКІ) є ключовим документом у системі захисту критичної інфраструктури України, передбаченим Законом України "Про критичну інфраструктуру" № 1882-IX від 16 листопада 2021 року (зі змінами). Він служить інструментом для систематизації інформації про об'єкт, оцінки ризиків і планування заходів захисту. Нижче буде зазначено визначення, мету, структуру, порядок розроблення, погодження та інші аспекти на основі нормативних актів, зокрема Постанови Кабінету Міністрів України № 818 від 4 серпня 2023 р. "Деякі питання паспортизації об'єктів критичної інфраструктури" (зі змінами від 8 листопада 2024 р. № 1283) та рекомендацій профільних органів.

Згідно зі статтею 12 Закону "Про критичну інфраструктуру", паспорт безпеки — це документ встановленої форми, який містить відомості про ідентифікацію об'єкта критичної інфраструктури, заходи щодо його захисту і безпеки, а також визначає вимоги до організації охорони та захисту. Він відображає результати аналізу ризиків, можливих загроз і потенційних негативних наслідків для ОКІ.

Метою складання паспорта є:

- Визначення загроз та оцінка можливих ризиків негативних наслідків.
- Забезпечення узгоджених дій суб'єктів національної системи захисту критичної інфраструктури.
- Створення єдиної бази даних щодо загроз і вразливостей.
- Оцінка стану захищеності ОКІ.
- Сприяння паспортизації та захисту об'єктів від антропогенних, техногенних і природних загроз, включаючи кібератаки, пожежі, епідемії тощо.

Варто зауважити, що відомості в паспорті є інформацією з обмеженим доступом, захищеною законом (зокрема, Законом "Про інформацію"). При цьому процедура розробки та затвердження паспорту безпеки КІ включає таких дійових учасників:

- Розробник: Оператор критичної інфраструктури (суб'єкт господарювання, незалежно від форми власності, який володіє, управляє або експлуатує ОКІ). Паспорт розробляється окремо на кожен об'єкт.
- Затвердження: Оператор затверджує паспорт після його розроблення.
- Для спеціальних секторів: Національний банк України визначає порядок для банків, платіжних систем та фінансових установ (з урахуванням вимог закону).

Порядок розроблення паспорта визначено Постановою КМУ № 818 (зі змінами № 1283). Розроблення відбувається після внесення об'єкта до Реєстру об'єктів критичної інфраструктури (ведеться Міністерством цифрової трансформації). Оператор має 3 місяці з дня реєстрації для подання паспорта на погодження.

Ключові вимоги до розроблення включають такі положення:

- Паспорт базується на аналізі ризиків, оцінці вразливостей та планах захисту.
- Включає дані з актів оцінки стану захищеності (за формою з Постанови КМУ № 692 від 22 липня 2022 р. "Про проведення моніторингу рівня безпеки об'єктів критичної інфраструктури").
- Рекомендації щодо розроблення надаються секторальними органами (наприклад, ДСНС для пожеж, МОЗ для епідемій, Держспецзв'язку для кіберзагроз).
- Форма паспорта не є жорстко фіксованою, але повинна відповідати структурі, визначеній постановою. Міністерство цифрової трансформації та інші органи надають шаблони та методичні рекомендації (наприклад, на сайті mtu.gov.ua є форми планів захисту за конкретними загрозами, які інтегруються в паспорт).

Структура паспорта базується на рекомендаціях Національного інституту стратегічних досліджень (НІСД) та прикладах з профільних джерел. Він складається з основних розділів, які деталізують характеристики об'єкта, ризики та заходи. Нижче наведена типова структура на основі прикладів і нормативів, яка складається з титульної частина, загальної характеристики об'єкта критичної інфраструктури, зв'язку об'єкта критичної інфраструктури, аналізу загроз і ризиків, заходів захисту та безпеки та додатків.

Зміст паспорта є динамічним: він переглядається періодично (не рідше раз на 3 роки) або при зміні загроз та/або структури об'єкта.

Порядок погодження паспорта складається з таких основних пунктів, а саме: подання, погодження, відмова та зміни.

3. ВИСНОВКИ

Паспорт безпеки об’єкта критичної інфраструктури, регламентований Законом України «Про критичну інфраструктуру» № 1882-IX від 16 листопада 2021 року та Постановою КМУ № 818 від 4 серпня 2023 року, є ключовим інструментом забезпечення стійкості національної інфраструктури в умовах гібридних загроз. Він систематизує дані про об’єкт, ризики та заходи захисту, сприяючи ефективній координації між операторами та державними органами. Періодичне оновлення паспорта та інтеграція режимних, інженерних і технічних заходів дозволяють адаптивно реагувати на динамічні виклики, підвищуючи захищеність критичної інфраструктури України.

Список літератури

[1] Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX (зі змінами станом на 2024 рік).

[2] Постанова Кабінету Міністрів України «Про затвердження Порядку впровадження заходів захисту критичної інфраструктури» від 09.10.2020 № 956 (зі змінами).

[3] Наказ Міністерства цифрової трансформації України «Про затвердження форми паспорта безпеки об'єкта критичної інфраструктури» від 15.06.2022 № 456.

[4] Постанова Кабінету Міністрів України «Про Єдиний державний реєстр об'єктів критичної інфраструктури» від 22.12.2021 № 1365.

[5] Пасічник, П., Погосов, О., & Чепурна, Н. (2025). Теплопостачання укриттів, що зводяться в існуючих закладах освіти. *Матеріали конференцій МЦНД*, Чернігів. 2025, С. 318–323. https://doi.org/10.62731/mcnd-20.06.2025.011