Олег ЗУБАНЬ,
здобувач освіти факультету літакобудування
Національного аерокосмічного університету
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: o.k.zuban@student.khai.edu

Катерина МАЙОРОВА,
кандидат технічних наук, доцент
кафедри технології виробництва літальних апаратів,
Національного аерокосмічного університету
«Харківський авіаційний інститут»,
м. Харків, Україна
ORCID: https://orcid.org/0000-0003-3949-0791
e-mail: k.majorova@khai.edu

DOI: https://doi.org/10.32620/pls.2025.8.54

МЕХАНІЗМИ ДЕРЖАВНОГО КОНТРОЛЮ ЗА КІБЕРЗАХИСТОМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: *Розглянуто сучасну нормативно-правову базу України в частині забезпечення кіберзахисту об'єктів критичної інфраструктури. Зосереджено увагу на механізмах державного контролю за виконанням вимог кібербезпеки. Проаналізовано основні функції уповноважених органів, а також вивчено виклики та пропозиції щодо посилення контролю в умовах воєнного стану. Досліджено постанову Постанова КМУ № 518 -2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», закон Закон України № 4336 -IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», а також указ Указ Президента України № 447/2021 «Про рішення Ради національної безпеки і оборони України щодо кібербезпеки.*

Ключові слова: *кіберзахист, критична інфраструктура, державний контроль, нормативно-правове регулювання, об'єкти критичної інформаційної інфраструктури, аудит інформаційної безпеки, взаємодія держави і бізнесу.*

У сучасному цифровому суспільстві питання кіберзахисту критичної інфраструктури набуває виняткового значення, оскільки від стабільності та безпеки інформаційних систем залежить функціонування практично всіх сфер життєдіяльності держави. Життєво важливі функції та/або послуги критичної інфраструктури наступні:

1) урядування та надання найважливіших публічних (адміністративних) послуг;

2) енергозабезпечення (у тому числі постачання теплової енергії);

3) водопостачання та водовідведення;

4) продовольче забезпечення;

5) охорона здоров'я;

6) фармацевтична промисловість;

7) виготовлення вакцин, стале функціонування біолабораторій;

8) інформаційні послуги;

9) електронні комунікації;

10) фінансові послуги;

11) транспортне забезпечення;

12) оборона, державна безпека;

13) правопорядок, здійснення правосуддя, тримання під вартою;

14) цивільний захист населення та територій, служби порятунку;

15) космічна діяльність, космічні технології та послуги;

16) хімічна промисловість;

17) дослідницька діяльність.

Критичну інфраструктиру розподіляють на 24 сектори, а саме: паливно-енергетичний; сектор; цифрові технології; захист інформації; харчова промисловість та агропромисловий комплекс; державний матеріальний резерв; охорона здоров'я; ринки капіталу та організовані товарні ринки; фінансовий сектор; транспорт і пошта; системи життєзабезпечення; промисловість; сектор громадської безпеки; цивільний захист населення і територій; охорона навколишнього природного середовища; сектор оборони; правосуддя; виконання кримінальних покарань, тримання під вартою та утримання військовополонених;

державна реєстрація; наукові дослідження та розробки; фінансовий сектор; вибори та референдуми; соціальний захист; інформаційний сектор і державна влада.

Отже енергетичні системи, транспортні мережі, телекомунікації, фінансові установи, банківський сектор, об'єкти оборонного призначення та державного управління – усі вони пов'язані спільною інформаційною екосистемою, уразливість якої може призвести до катастрофічних наслідків. Збої в роботі таких систем здатні паралізувати цілі галузі, поставити під загрозу життєзабезпечення населення, а у воєнний час – навіть вплинути на обороноздатність країни. Саме тому кіберзахист сьогодні розглядається не лише як технічне питання, а як складова національної безпеки, що потребує цілеспрямованої державної політики, постійного моніторингу та міжвідомчої координації.

В умовах триваючої війни проти України кіберпростір став ще одним фронтом, де ведеться боротьба за інформаційну перевагу та контроль над критично важливими ресурсами. Кібератаки на енергетичні компанії, банки, урядові портали та телекомунікаційні мережі набули системного характеру, часто супроводжуючись інформаційно-психологічними операціями. За даними Державної служби спеціального зв'язку та захисту інформації України, лише у 2024 році кількість зафіксованих кіберінцидентів зросла у кілька разів порівняно з довоєнним періодом. Це свідчить про зростання технологічних ризиків і про необхідність вдосконалення механізмів контролю за станом кіберзахисту. У таких умовах держава повинна діяти на випередження, забезпечуючи не лише реагування на атаки, а й системне запобігання їм через розвиток інфраструктури, кадрового потенціалу та нормативно-правової бази.

Ефективний державний контроль у сфері кібербезпеки стає одним із ключових пріоритетів національної безпеки України. Його мета полягає у створенні комплексної системи моніторингу, аудиту та координації дій усіх суб'єктів, відповідальних за захист критичної інформаційної інфраструктури. Такий контроль охоплює як перевірку технічної готовності об'єктів, так і оцінку організаційних заходів, кадрового забезпечення та інформаційної культури.

Перші кроки щодо формування системи державного управління кіберзахистом були зроблені після ухвалення Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, який визначив основні принципи, суб'єктів та напрями реалізації державної політики у сфері кібербезпеки. Одним з ключових положень цього закону є встановлення вимог до кіберзахисту об'єктів критичної інфраструктури, що мають особливе значення для економічної та національної безпеки держави [1].

Відповідно до постанови Кабінету Міністрів України № 518 від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», державний контроль здійснюється через уповноважені органи, насамперед Державну службу спеціального зв'язку та захисту інформації України (ДССЗЗІ). Цей орган уповноважений проводити аудити, перевірки, моніторинг стану кіберзахисту, а також координувати діяльність інших державних структур у сфері інформаційної безпеки [2].

До основних механізмів державного контролю належать: проведення державного аудиту інформаційної безпеки; категоризація об'єктів критичної інфраструктури за рівнями важливості; перевірка виконання суб'єктами господарювання вимог із кіберзахисту; моніторинг інцидентів у кіберпросторі та реагування на них; обов'язкове звітування операторів критичної інфраструктури перед ДССЗЗІ та Радою національної безпеки і оборони України.

Згідно з Указом Президента України № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про вдосконалення системи забезпечення кібербезпеки України"», держава впроваджує політику системного контролю за кіберзахистом через створення єдиної національної системи кібербезпеки. Основна увага приділяється моніторингу ризиків, координації дій державних і приватних структур, створенню механізмів обміну інформацією між суб'єктами безпеки [3].

Попри наявність правового поля, реалізація державного контролю у цій сфері стикається з низкою труднощів. По-перше, відсутня достатня кількість фахівців, здатних проводити якісні аудити та оцінку відповідності вимогам кіберзахисту. По-друге, законодавство потребує подальшої гармонізації із європейськими стандартами, зокрема Директивою (ЄС) 2022/2555 (NIS2), яка визначає підхід до управління ризиками у критичній інфраструктурі. По-третє, необхідно посилити відповідальність суб'єктів за порушення правил безпеки інформаційних систем.

Державний контроль у сфері кіберзахисту має спиратися на принципи системності, превентивності та взаємодії [4]. Це означає, що перевірки повинні бути не лише формальними, а й спрямованими на попередження загроз, а сам контроль – поєднувати інструменти оцінювання, навчання та підтримки операторів критичних об'єктів. Ефективна система державного контролю повинна забезпечувати постійний зворотний зв'язок між контролюючими органами та суб'єктами критичної інфраструктури, стимулювати не лише дотримання мінімальних стандартів безпеки, а й розвиток внутрішніх механізмів самоконтролю та внутрішнього аудиту інформаційної безпеки. Зокрема, доцільним є запровадження регулярних тренувань із реагування на кібератаки, симуляцій кризових

ситуацій та обов'язкових звітів про усунення виявлених недоліків.

Важливим напрямом є впровадження системи постійного моніторингу кіберінцидентів із використанням технологій штучного інтелекту, машинного навчання та аналітики великих даних, що дозволить оперативно виявляти потенційні загрози, прогнозувати можливі ризики та підвищувати рівень проактивного захисту державних і приватних об'єктів критичної інфраструктури.

Варто також відзначити вагому роль міжнародного співробітництва у сфері забезпечення кібербезпеки України. У сучасних умовах глобальної цифрової взаємозалежності ефективний захист кіберпростору неможливий без тісної взаємодії між державами, міжнародними організаціями та приватним сектором. Саме тому Україна активно інтегрується у міжнародні ініціативи, спрямовані на посилення кіберзахисту, обмін досвідом і розробку спільних стандартів реагування на кіберзагрози. Співпраця з міжнародними партнерами дає змогу не лише отримувати доступ до сучасних технологічних рішень, але й формувати власну експертизу, здатну забезпечити захист критичної інформаційної інфраструктури навіть у кризових умовах.

Україна вже кілька років бере активну участь у програмах НАТО з кіберзахисту, що дозволяє залучати досвід країн-членів Альянсу у сфері протидії кібератакам, обміну розвідувальними даними про потенційні загрози та проведення спільних навчань. Особливу увагу приділено підвищенню готовності державних структур до реагування на складні багатовекторні кібератаки, зокрема через участь у багатонаціональних тренуваннях Cyber Coalition та Locked Shields, які організовує НАТО Cooperative Cyber Defence Centre of Excellence (CCDCOE) у Таллінні [5]. Такі ініціативи дозволяють українським спеціалістам відпрацьовувати практичні навички захисту систем управління, енергетичних мереж та інформаційних баз, а також налагоджувати ефективну комунікацію між урядовими структурами, приватним сектором і військовими кіберпідрозділами.

Не менш важливою є співпраця України з Європейським агентством з кібербезпеки (ENISA). Ця взаємодія охоплює обмін найкращими практиками з управління ризиками, розробку стандартів кіберстійкості, а також гармонізацію національного законодавства у сфері кіберзахисту з європейськими нормами. Завдяки таким партнерствам Україна посилює інституційний потенціал, розширює можливості навчання та підготовки фахівців, а також інтегрується у спільну європейську кібермережу. Участь у міжнародних програмах сприяє тому, що держава поступово переходить від реактивної до проактивної моделі кіберзахисту, що базується на передбаченні, аналізі та попередженні загроз. Саме міжнародна кооперація створює передумови для побудови стійкої, гнучкої та технологічно розвиненої системи контролю й реагування на кіберінциденти в Україні.

Удосконалення механізмів державного контролю за кіберзахистом критичної інфраструктури потребує комплексного підходу, що включає оновлення законодавчої бази, посилення кадрового потенціалу, інтеграцію сучасних технологій моніторингу та розширення міжнародного партнерства. Реалізація цих заходів сприятиме підвищенню кіберстійкості держави, зменшенню ризиків кібератак і забезпеченню безперервності функціонування ключових секторів національної безпеки.

Бібліографічні посилання

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 24.10.25).

2. Постанова Кабінету Міністрів України № 518 від 19.06.2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF (дата звернення: 24.10.25).

3. Указ Президента України № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про вдосконалення системи забезпечення кібербезпеки України"». URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 24.10.25).

4. Мануілов Я. С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни / Я. С. Мануілов // Інформація і право. 2023. № 1(44). С. 154–167.

5. Цяпа С. М. Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак / С. М. Цяпа // Інформація і право. 2021. № 4(39). С. 121–128.

O. Zuban, K. Majorova

Mechanisms of state control over cyber-protection of critical infrastructure objects.

Abstract. This paper examines the current legal framework in Ukraine concerning the cyber-protection of critical infrastructure objects, focusing on state mechanisms for controlling compliance with cybersecurity requirements. It analyzes the primary functions of authorized state bodies, identifies key challenges and recommends strengthening control mechanisms under martial law conditions. The study covers the Cabinet of Ministers Resolution No. 518-2019 on General Requirements for Cyber-Protection of Critical Infrastructure Objects, Law of Ukraine No. 4336-IX on Amendments to Some Laws regarding Information Protection and Cyber-Protection of State Information Resources and Critical Information

Infrastructure, and Presidential Decree No. 447/2021 on the decisions of the NSDC of Ukraine about cybersecurity.

Keywords: cybersecurity, critical infrastructure, state control, legal regulation, critical information infrastructure objects, information security audit, state-business cooperation.

Зразок для цитування:

Зубань О., Майорова К. Механізми державного контролю за кіберзахистом об'єктів критичної інфраструктури. Пропілеї права та безпеки, 2025. №8. С. 214-217. DOI: https://doi.org/10.32620/pls.2025.8.54.