УДК 004.056

АНАЛІЗ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Богдан Кобільник
Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Вікторія Сидоренко, к.т.н., доц.

Ключові слова: критична інформаційна інфраструктура; нормативно-правове забезпечення; SWOT-аналіз; інформаційна безпека.

Цифровізація та гібридна агресія створюють нові загрози для інформаційної безпеки, що особливо актуально для проектування захищеної критичної інформаційної інфраструктури (КІІ) держави. Сьогодні, зростання кількості загроз, пов'язаних із розвитком інформаційних технологій, підвищує необхідність впровадження нових нормативно-правових рішень, які будуть актуальними в умовах сучасних викликів та ведення війни.

Нормативно-правова база України включає Закон «Про критичну інфраструктуру» (2021) та інші документи, що регулюють кібербезпеку, зокрема Стратегію кібербезпеки України (2021–2025), яка окреслює основні напрямки захисту критичних інформаційних систем. Крім того, прийнято численні підзаконні акти, що встановлюють стандарти захисту, категоризацію об’єктів, моніторинг безпеки, аудит, обмін інформацією про кіберінциденти та ведення державного реєстру КІІ [1].

Дослідження спрямоване на аналіз нормативно-правового забезпечення у сфері проектування захищеної критичної інформаційної інфраструктури держави з визначенням сильних і слабких сторін, можливостей і загроз за допомогою проведення SWOT-аналізу.

SWOT-аналіз нормативно-правового забезпечення у сфері проектування захищеної критичної інформаційної інфраструктури держави

Серед сильних сторін **(Strengths)** слід відзначити наявність спеціалізованого законодавства, яке вперше визначає поняття критичної інфраструктури та обов’язки суб’єктів, а також розвинену підзаконну базу з затвердженими вимогами і процедурами кіберзахисту. Додатково, створено ефективні координаційні механізми із залученням кращих міжнародних практик, що сприяє стабільному функціонуванню системи захисту та створенню основи для подальшого розвитку нормативно-правової бази.

Серед слабких сторін **(Weaknesses)** спостерігається неповна імплементація нормативної бази – практичні механізми, такі як реєстр об’єктів та аудит, перебувають у стадії впровадження. Виявлено також законодавчі прогалини щодо довгострокового розвитку та фінансування КІІ, нечіткий розподіл повноважень між суб’єктами, обмежені матеріальні та

кадрові ресурси, а також недостатньо розвинені механізми відповідальності за невиконання вимог. Ці недоліки створюють ризики для неефективного застосування нормативних положень та можуть перешкоджати оперативному реагуванню на сучасні загрози.

Щодо можливостей **(Opportunities)**, адаптація міжнародного досвіду, впровадження норм ЄС і НАТО у сфері захисту КІІ, а також підтримка союзників сприяють модернізації нормативної бази. Післявоєнне відновлення та розвиток державно-приватного партнерства, поряд із зростанням обізнаності суспільства про важливість кібербезпеки, відкривають нові перспективи для вдосконалення законодавства. Використання цих можливостей дозволить не лише модернізувати нормативно-правову базу, а й підвищити рівень національної кібербезпеки.

Зовнішні загрози **(Threats)** включають триваючу агресію та спрямовані кібератаки, що створюють високий рівень ризику для критичної інфраструктури. Крім того, стрімка еволюція кіберзагроз може випереджати оновлення законодавства, а економічні й політичні обмеження, людський фактор та залежність від імпортних технологій залишаються важливими викликами. Ці фактори потребують негайного реагування та стратегічного планування для мінімізації потенційних наслідків для системи захисту [2-4].

Висновок. Результати проведеного аналізу нормативно-правового забезпечення у сфері проектування захищеної критичної інформаційної інфраструктури держави свідчать про існування базових механізмів для забезпечення певного рівня кібербезпеки, але також показують суттєві недоліки, що потребують оперативного удосконалення. Крім того, продовженням дослідження стане використання визначених у дослідженні можливостей, а саме адаптації міжнародного досвіду, впровадження норм ЄС для підвищення рівня національної кібербезпеки КІІ держави.

Список використаних джерел:

1. Melnyk, D. (2022). Захист національної критичної інфраструктури: актуальні проблеми та шляхи їх вирішення. *Адміністративне право і процес, 3*(38), 5–16.

2. Kudryashov, V. (2021). Державне регулювання критичної інфраструктури. *Фінанси України, 7*, 72–92.

3. Petrunenko, I. (2022). Regulation of cybersecurity of Ukraine's critical infrastructure: Legal aspects and standards of sustainable protection. *Law, Business and Sustainability Herald, 2*(3), 42–57.

4. Sokiran, M. (2021). Basic principles of public administration of critical information infrastructure: The example of Ukraine. *Advanced Space Law, 7*, 63–72.