DOI 10.36074/logos-13.12.2024.055

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ВІД КІБЕРЗАГРОЗ

Скибицький Вадим Олександрович[1]

1. Студент групи БСДМ-51
Державний університет інформаційно-комунікаційних технологій, м. Київ, УКРАЇНА

Критична інфраструктура (КІ) являє собою комплекс систем, що забезпечують життєдіяльність держави та суспільства. Вона складається з ключових елементів, таких як енергетичні мережі, транспортні системи, водопостачання, фінансові установи та телекомунікаційні мережі, які забезпечують основні потреби людей і функціонування державних інститутів. Однак з розвитком цифрових технологій ці системи стали вразливими до кібернападів, що можуть призвести до серйозних наслідків для національної безпеки, економіки та благополуччя громадян. Втрата або порушення роботи цих об'єктів через кібернапади може призвести до серйозних економічних, соціальних і навіть політичних наслідків.

Кіберзагрози для критичної інфраструктури постійно змінюються та стають все більш складними. Якщо раніше зловмисники зосереджувалися на банальних атаках за допомогою вірусів або троянських програм, то зараз вони використовують більш складні методи, зокрема, цілеспрямовані атаки на уразливості систем SCADA (системи контролю та збору даних, які широко використовуються на підприємствах і в енергетичній сфері). Така атака вимагає глибоких знань у галузі інфраструктурних технологій і здатна спричинити масові збитки.

Однією з найвідоміших кібератак, що вплинули на критичну інфраструктуру, стала атака на енергетичні мережі України в 2015 році. Внаслідок цього інциденту 230 000 людей залишилися без електрики на кілька годин. Атака була здійснена за допомогою спеціально розробленого шкідливого програмного забезпечення, яке мало на меті порушити роботу системи управління енергетичними мережами. Цей випадок показав, наскільки уразливими є енергетичні об'єкти до кіберзагроз і як великі

наслідки можуть мати навіть тимчасові збої у роботі цієї критичної інфраструктури.

Виходячи з наведеної вище інформації, захист критичної інфраструктури України є важливою складовою національної безпеки, що має регулюватись низкою законів, постанов та нормативних актів. Основні потреби в цій сфері полягають у чіткому визначенні та категоризації об'єктів критичної інфраструктури (ОКІ), створенні їх реєстру та проведенні паспортизації. Це дає змогу ідентифікувати ключові об'єкти, оцінити рівень їхньої важливості для держави, а також врахувати потенційні ризики, пов'язані з їхньою діяльністю.

Ідентифікація ключових об'єктів критичної інфраструктури, оцінка їхньої важливості та врахування потенційних ризиків здійснюється шляхом визначення критеріїв критичності, таких як вплив на національну безпеку, економічну стабільність та життєзабезпечення суспільства. Цей процес включає категоризацію об'єктів, аналіз їхньої діяльності, оцінку можливих загроз і вразливостей, а також розроблення паспортів об'єктів із зазначенням їхніх характеристик, ризиків і заходів реагування [1]. Для забезпечення належного захисту проводиться моніторинг стану безпеки, незалежний аудит, розробляються плани захисту з урахуванням потенційних загроз та сценаріїв реагування. Важливою складовою є організація взаємодії між усіма суб'єктами національної системи захисту для обміну інформацією та координації дій, що сприяє ефективному реагуванню на інциденти і забезпеченню стабільної роботи об'єктів.

Інформаційні системи ОКІ повинні відповідати комплексним вимогам щодо захисту, які охоплюють як технічні, так і організаційні заходи для забезпечення стійкості до загроз [2]. Основні вимоги включають забезпечення конфіденційності, цілісності, доступності інформації, захисту від несанкціонованого доступу та мінімізації впливу кіберінцидентів [3]. Організаційно-технічні моделі кіберзахисту можуть включати системи багаторівневого захисту, централізоване управління безпекою, системи виявлення вторгнень, резервне копіювання даних, шифрування, а також регулярне оновлення програмного забезпечення та засобів захисту [3]. Перевірки ефективності захисту проводяться шляхом проведення незалежного аудиту інформаційної безпеки, який оцінює відповідність встановленим стандартам та рівень захищеності об'єкта. Моніторинг рівня безпеки здійснюється через регулярний аналіз стану кіберзахисту, виявлення уразливостей, оцінку нових загроз та контроль за виконанням рекомендацій з підвищення захищеності [4]. Результати перевірок та моніторинг сприяють адаптації системи кіберзахисту до нових ризиків та забезпеченню безперебійної роботи ОКІ навіть за умов зростаючого рівня кіберзагроз.

Інформаційна взаємодія між суб'єктами національної системи захисту критичної інфраструктури здійснюється через централізовану систему обміну інформацією, що забезпечує своєчасну передачу даних про інциденти, загрози та вразливості [5]. Учасники зобов'язані надавати інформацію у стандартизованих форматах із використанням безпечних каналів зв'язку для запобігання несанкціонованому доступу. Регламентовано чіткий порядок звітності, передачі даних і координації дій, що включає оперативні механізми реагування у разі надзвичайних ситуацій. Регулярний перегляд протоколів взаємодії та тестування систем забезпечує її готовність до реагування на нові виклики.

Плани захисту, які враховують загрози національного рівня, як-от кібератаки чи фізичні інциденти, включають комплекс заходів із запобігання, реагування та відновлення роботи об'єктів критичної інфраструктури [6]. Вони розробляються на основі оцінки ризиків та аналізу проектних загроз і охоплюють кілька ключових компонентів:

1. Визначення відповідальних осіб та команд для управління інцидентами, створення системи оповіщення, проведення навчань і тренувань персоналу щодо дій у надзвичайних ситуаціях.

2. Впровадження систем моніторингу та виявлення вторгнень, резервне копіювання даних, шифрування інформації, створення захищених каналів зв'язку, систем відновлення після збоїв і сценаріїв резервного функціонування у разі фізичних чи кіберзагроз.

3. Посилення контролю доступу до критичних об'єктів, використання систем відеоспостереження, бар'єрів для захисту від фізичних нападів, а також охорона об'єктів підрозділами безпеки.

4. Оперативний план дій на випадок кіберінциденту чи фізичної атаки, включно з процедурами локалізації, нейтралізації загроз і мінімізації шкоди. Передбачено використання кризових центрів і оперативної комунікації з правоохоронними органами та державними структурами.

5. Порядок відновлення нормального функціонування об'єкта, включаючи перевірку систем після інциденту, оцінку завданої шкоди, актуалізацію заходів захисту для запобігання подібним подіям у майбутньому.

6. Періодична перевірка та актуалізація плану з урахуванням нових загроз, технологій і змін у структурі об'єкта.

Загалом захист критичної інфраструктури потребує комплексного підходу, що включає нормативно-правове регулювання, технічні заходи, моніторинг стану безпеки, підготовку кваліфікованих кадрів та активну інформаційну взаємодію між усіма учасниками процесу. Враховуючи сучасні виклики, такі як кібератаки чи природні катастрофи, пріоритетом має бути

постійна адаптація систем захисту до нових загроз, що забезпечить безперервне функціонування критично важливих об’єктів для держави та суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

[1] Кабінет Міністрів України. (2023). Постанова від 28 квітня 2023 р. №415 «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього». Офіційний вісник України.
[2] Кабінет Міністрів України. (2019). Постанова від 19 червня 2019 р. №518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури». Офіційний вісник України.
[3] Кабінет Міністрів України. (2021). Постанова від 29 грудня 2021 р. №1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту». Офіційний вісник України.
[4] Кабінет Міністрів України. (2022). Постанова від 22 липня 2022 р. №821 «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури». Офіційний вісник України.
[5] Кабінет Міністрів України. (2022). Постанова від 14 жовтня 2022 р. №1174 «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури». Офіційний вісник України.
[6] Адміністрація Державної служби спеціального зв’язку та захисту інформації України. (2023). Наказ від 4 жовтня 2023 р. №877 «Про затвердження форми Плану захисту об’єкта критичної інфраструктури за проєктною загрозою національного рівня “кібератака/кіберінцидент”». Офіційний вісник України.