УДК 504.37(043.2) https://doi.org/10.18372/2786-8168.20.21218
І. О. Демченко, студент
Національний університет Київський авіаційний інститут,Київ

ОЦІНКА ТА АНАЛІЗ РИЗИКІВ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ КІБЕРЗАГРОЗ

Анотація. *У роботі розглянуто взаємозв'язок між кіберстійкістю об'єктів енергетики та транспорту та рівнем екологічної безпеки. Проаналізовано ризики виникнення техногенних аварій внаслідок кібератак на автоматизовані системи керування.*
Ключові слова: Критична інфраструктура, кіберстійкість, техногенно-екологічні ризики, АСУ ТП, енергетична безпека.

Вступ. Сучасна критична інфраструктура (КІ) України, зокрема енергетичний та транспортний сектори, перебуває у стані цифрової трансформації. Впровадження систем складного моніторингу та АСУ ТП (SCADA) підвищує ефективність управління, але водночас створює нові вектори вразливості. В умовах гібридної агресії кіберзагрози перестали бути лише проблемою IT-сектору, перетворившись на реальний фактор екологічної небезпеки.

Постановка проблеми. Специфіка об'єктів енергетики та транспорту полягає у їхній високій потенційній небезпеці для довкілля. Кібератака, спрямована на зміну алгоритмів роботи систем охолодження на АЕС, тиску в нафтогазопроводах або систем диспетчеризації небезпечних вантажів на залізниці, може спровокувати викиди токсичних речовин, пожежі або розливи палива. Таким чином, аналіз кіберризиків є невід'ємною частиною оцінки екологічної стійкості держави.

Аналіз останніх подій та загроз. Досвід атак на енергосистему України (наприклад, BlackEnergy) продемонстрував можливість дистанційного відключення підстанцій. Проте найбільш критичними з точки зору екології є атаки типу *Stuxnet* або *Triton*, що втручаються в роботу систем протиаварійного захисту (SIS). У транспортній галузі вразливість систем керування рухом суден чи потягів із хімічними речовинами створює ризики масштабного забруднення акваторій та ґрунтів.

Методологія оцінки ризиків. Для аналізу стійкості КІ пропонується комплексний підхід, що базується на моделі **NIST Cybersecurity Framework** з інтеграцією параметрів екологічної шкоди:

1. **Ідентифікація активів:** Визначення критичних вузлів, вихід з ладу яких спричинить екологічне лихо.
2. **Моделювання загроз:** Аналіз ймовірності злому через вразливості нульового дня (0-day) або соціальну інженерію.
3. **Оцінка наслідків:** Розрахунок потенційного обсягу викидів шкідливих речовин та вартості рекультивації територій у разі успішної кібератаки.

Результати дослідження. Аналіз показує, що стійкість КІ залежить не лише від наявності фаєрволів, а й від здатності системи підтримувати безпечний стан (fail-safe) навіть при втраті цифрового управління. Ключовим ризиком визнано каскадний ефект: кібератака на електромережу призводить до зупинки очисних

споруд або систем вентиляції на хімічних підприємствах, що спричиняє вторинну екологічну шкоду.

Висновки. Кібербезпека об’єктів енергетики та транспорту має розглядатись як базовий елемент екологічної безпеки країни. . Необхідно впроваджувати концепцію «Security by Design», де екологічні ризики враховуються ще на етапі проектування цифрових систем управління. Стійкість критичної інфраструктури в умовах кіберзагроз вимагає створення ізольованих резервних контурів управління та регулярного стрес-тестування персоналу на випадок техногенних інцидентів, спричинених втручанням у мережу.