ОСОБЛИВОСТІ РОЗВИТКУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У ЗАРУБІЖНИХ КРАЇНАХ

А.О. Ващишин*, аспірант*
Національній університет водного господарства
та природокористування, м. Рівне

Поняття критичної інфраструктури досить нове. У будь-якому суспільстві є можливість виділити мережі, сектори, системи, які є життєво необхідні для суспільства, функціонування яких є обов'язковим, виведення яких із строю може привести до безповоротно негативного становища суспільства, або до припинення існування цілих соціальних груп. Це може відбуватися на місцевому, державному, міжнародному рівнях в залежності від виду системи. Комплекс цих складових називають критичною інфраструктурою.

Спочатку саме поняття критичної інфраструктури з'явилось в європейських та американських ділових та наукових колах. Цю проблематику почали розвивати з 1998 року у зв'язку зі зростанням випадків терористичних атак в розвинених країнах світу. Причому терористи не обмежувались кібернетичною інфраструктурою. Атаки такою ж мірою були направлені на інші життєво важливі економічні галузі і суспільно важливі сектори країн.

Згідно з PresedentialDecisionDirective критичну інфраструктуру визначили таким чином: «Це основні системи, які можуть мати матеріальну або кібернетичну платформу і мають дію на функціональність економіки держави». Ці системи включають енергосистеми, системи телекомунікації, транспортну систему, банківський та фінансовий сектори і служби, постачання води та рятувальні служби [1].

Роздивимось підтримку критичної інфраструктури у США. Національні критичні системи інфраструктури цієї країни, її об'єкти, активи та мережі надають основні послуги, які служать основою американської національної економіки, безпеки та здоров'я і можуть бути атаковані тими, хто прагне заподіяти шкоду Сполученим Штатам та їх інтересам. Збереження надійної, функціональної і стійкої критичної інфраструктури вимагає активних та скоординованих зусиль. Ці заходи засновані на загальній відповідальності федеральних, державних, місцевих та територіальних одиниць, а також державних та приватних власників та операторів критичної інфраструктури. Головний аспект збереження безпечної критичної інфраструктури − контроль доступу, обмеження доступу до фізичних засобів та активів тільки тими, хто має законну потребу і був перевірений. Це забезпечить відсутність певного ризику. Хоча Федеральний уряд володіє малою частиною критичної інфраструктури.

Департамент національної безпеки (DHS) є провідним федеральним агентством, відповідальним за внутрішній захист критичної інфраструктури, але інші федеральні відомства несуть відповідальність за контроль різних секторів критичної інфраструктури, таких, як оборонно- промисловий сектор та енергетичний сектор. План захисту національної інфраструктури визначає функції та обов'язки Департаменту національної безпеки та агентств специфічних галузей − федеральних відомств та відомств по захисту критичної інфраструктури у шістнадцяти її секторах. У 2006 році у відповідь на Президентську Директиву національної безпеки Департамент національної безпеки створив Скринінговий координаційний офіс, розташований в політичному офісі DHS. Скринінговий координаційний офіс несе відповідальність за нагляд Департаменту національної безпеки та контроль акредитаційних заходів, в тому числі тих, що орієнтовані на доступ до критичної інфраструктури. Акредитація в цьому контексті відноситься до процесу визначення права особи на певну ліцензію, привілеї чи статус від заявки на доступ до використання інформації і до визначення терміну закінчення дії, або потенційного відкликання видання облікового запису [2].

Департамент національної безпеки та інші федеральні відомства допомагають контролювати доступ через найрізноманітніші фізичні засоби та активи секторів інфраструктури, за які вони несуть відповідальність. Ці федеральні адміністратори допомагають операторам захищати важливі інфраструктурні об'єкти від атак, диверсій, крадіжки або неправильного використання під час відкриття законного доступу, що допомагає забезпечити потік бізнесових операцій. При обслуговування потреб оператора адміністратори також повинні забезпечити відповідність федеральним законам та нормам. Федеральні агентства грають різноманітні ролі, які допомагають досягти цього балансу, включаючи, але не обмежуючись:

– володінням та експлуатацією певних видів інфраструктури;

– оптовою торгівлею, експлуатацією та управлінням програмами акредитації для конкретних видів інфраструктури;

– частковою роботою та управлінням активами програм;

– наданням інструкцій для допомоги власникам, що реалізують ефективний контроль доступу.

Наприклад, Адміністрація транспортної безпеки (TSA) керує процесом Акредитації кваліфікації транспортних працівників за ідентифікацією процесів, включаючи реєстрацію, фонові перевірки та підтримку облікових даних. Однак, для області безпечної ідентифікації значка дисплея, який полегшує доступ в аеропортах і частково керований TSA, оператори аеропорту використовують інформацію перевірки TSA та в кінцевому підсумку приймають остаточні рішення щодо доступу до аеропорту та видачі значків. Аналогічно Атомна регуляторна комісія видає нормативні акти, що стосуються вимог щодо контролю доступу, які повинні бути реалізовані комерційними атомними станціями, та членами Комітету по захисту, також американськими військовими об'єктами та об'єктами з використання Спільної карти доступу як одного із способів полегшення доступу до напівзакритої зони в межах установок.

Розглянемо досвід європейських країн, які недавно стали членам Євросоюзу. Великобританія є другою державою ЄС, яка почала визначати і захищати свою критичну інфраструктуру. У 1999 р. у Великобританії був створений Координаційний центр з безпеки національної інфраструктури, який входив до складу Міністерства внутрішніх справ, пізніше була створена Рада національного центру з безпеки. Ці організації з 2007 р. замінює Центр по захисту національної критичної інфраструктури [3]. У Великобританії національна критична інфраструктура визначається на підставі постійного забезпечення основних послуг.

У Словаччині у 2007 році було ухвалено «Концепцію критичної інфраструктури Словацької Республіки, її захисту та оборони». В ній визначені стратегії щодо захисту життєво важливих об'єктів. Залишилось окреслити детальний план дій у кризових ситуаціях. Він був прийнятий у 2011 році в Законі про критичну інфраструктуру Словацької Республіки. В ньому також було чітко визначено об'єкти критичної інфраструктури, органи дебржавної влади, які відповідають за захист цих об'єктів.

У Чехії до 2002 року до критичної інфраструктури відносили, в першу чергу, комп'ютерні мережі. В нормативно-правових документах цієї країни у якості критичної інфраструктури виступають системи, руйнування або зменшення функціональності яких мали би серйозний вплив на суспільну і економічну стабільність, безпеку і функціонування держави, її обороноздатність.

У Польщі уряд схвалив Закон про управління кризовими ситуаціями. В рамках цього закону подано розуміння параметрів та об'єктів критичної інфраструктури, її захисту [4].

В Угорщині в 2012 році було прийнято закон про захист критичної інфраструктури, який є одним з найбільш комплексних документів у цій сфері. Цей закон пояснив принципи та порядок віднесення об'єктів до системи критичної інфраструктури, умови проведення інспекцій, забезпечення їхньої безпеки, а також порядок взаємодії між державними інститутами в критичних ситуаціях.

Таким чином, прийнявши до уваги викладене вище, можна сформулювати таке визначення критичної інфраструктури – це ключові сфери діяльності суспільства країни, органів державного сектора, приватних підприємств, в результаті надання шкоди яким зростає ризик руйнування всієї економіки, сфери життєдіяльності людини в цій країні, її обороноздатності.

Перелік посилань:

1. Presedential Decision Directive/NSC-63 [Electronic resource] Presedential Decision Directives – Mode of access: https://fas.org/irp/offdocs/pdd/pdd-63.htm

2. Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts Вибір федерально керованої критичної інфраструктури та опис дій щодо контролю доступу у США [Electronic resource] Critical Infrastructure Protection – Mode of access: https://www.gao.gov/assets/690/682547.pdf

3. Сметана М. Подходы государств Европейского Союза к определению элементов критической инфраструктуры / М. Сметана // Защита критической инфраструктуры – 2014. – С. 60

4. Ustawa npo bezprieczenstwie obywatelskim z dn. 21.08.2003 [Electronic resource] – Mode of access: http://www.eduskrypt.pl/art-59-bezpieczenstwo_czy_pokoj.html