4. Римський статут Міжнародного кримінального суду. URL: https// zakon.rada.gov.ua

УДК 351.86:338.49.

Собакарь А. О.
д.ю.н., професор, завідувач кафедри
адміністративного права,
процесу та адміністративної діяльності,
Дніпропетровський державний університет
внутрішніх справ

ЗАГРОЗИ КРИТИЧНІЙ ІНФРАСТРУКТУРІ ТА ЇХ ВПЛИВ НА СТАН НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Наявність у будь-якій країні об’єктів критичної інфраструктури ставить на порядок денний актуальне питання їх захисту, підвищення безпеки та стійкості такої системи до всього спектру загроз і ризиків, оскільки саме критична інфраструктура забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та добробут, а також належний рівень національної безпеки [1] особливо в нинішніх умовах, коли спостерігається загальносвітова тенденція до різкого посилення екстремізму та тероризму, небувале зростання організованої злочинності тощо.

Однією з головних проблем стійкості критичної інфраструктури є високий рівень зношеності основних фондів промислових підприємств, що в середньому становить 60,3%. Значний ризик техногенних аварій пов’язаний із наявністю на території України численних об’єктів підвищеної небезпеки, що використовують в діяльності значні обсяги небезпечних речовин. При цьому аварії на більшості з них можуть призвести до виникнення надзвичайних ситуацій державного або регіонального рівня.

В житлово-комунальному комплексі протяжності ветхих та аварійних водопровідних мереж в середньому по Україні становить понад 34%, а теплових і парових мереж – понад 18% від загальної протяжності таких мереж, що впливає на втрати води та теплової енергії при їх доставці споживачам, підвищення тарифів, і як наслідок провокує соціальну нестабільність.

До типових прикладів порушення умов безпечного функціонування об’єктів критичної інфраструктури, їх безперервності та стійкості, що створює реальні чи потенційні загрози національній безпеці, вчені відносять:

по-перше, фізичне захоплення об’єктів при збереженні їх функціональності (наприклад, захоплення енергетичних активів Криму);

по-друге, припинення функціонування об’єктів, у тому числі внаслідок фізичного захоплення, для завдання збитків попередньому власнику чи обміну на «потенційні» переваги в інших сферах (задоволення політичних чи економічних вимог, як-от умови постачання вугілля до України, викуп активів, вплив на ринкову вартість компаній та сировини тощо);

по-третє, розукомплектування окремих елементів інфраструктури з метою отримання кримінального доходу (масові факти різання критичної інфраструктури на окупованих територіях Донбасу для продажу у вигляді металобрухту);

по-четверте, фізичне знищення об’єкта для завдання критичної шкоди, збільшення витрат на подолання стану порушення функціонування інфраструктури (наприклад, неможливість доставити ресурси);

по-п’яте, перешкоджання діяльності з відновлення функціональності енергетичної інфраструктури та формування суспільно-політичного невдоволення;

по-шосте, використання транспортної інфраструктури (зокрема повітряного простору України) для провокацій (як у випадку із трагедією авіарейсу МН178), блокування відновлення критичної інфраструктури в зоні бойових дій, блокування транзиту товарів через російський кордон [2];

по-сьоме, несанкціоновані втручання в роботу не лише енергетичної, але й інформаційно-комунікаційної, комунальної інфраструктури тощо.

В групі загроз природні лиха та небезпечні природні явища слід виділити: метеорологічні або надзвичайні погодні умови (снігопади, ожеледь, хуртовини, зливи, градобій, заморозки, посухи, спека, урагани, шквали, смерчі), гідрологічні (повені, селі, паводки, підтоплення, цунамі), геологічні (небезпечні екзогенні геологічні процеси – зсуви, просідання та карст), епідемії та пандемії. Поміж зазначених видів загроз варто виділити метеорологічні, частота яких в Україні значно збільшилася останніми десятиліттями, зокрема таких як обледеніння, підтоплення, посухи тощо. Найнебезпечнішими гідрологічними загрозами за наслідками для критичної інфраструктури є паводки [3].

Іншими словами постає необхідність виявлення небезпек, оцінювання ризиків та прогнозування надзвичайних ситуацій, що можуть завдати непоправної шкоди охоронюваним суспільним інтересам шляхом створення відповідних загроз національній безпеці країни в цілому. З цього приводу слушно каже О.С. Бодрук, що загроза розуміється як практично реальна, але не

фатальна «можливість заподіяння шкоди, майнових, фізичних або моральних (духовних) збитків особистості, суспільству чи державі» [4, с. 8].

Отже, необхідність розроблення поняття «загроза» визначається: 1) пануванням диверсифікаційного підходу щодо дослідження категорій націобезпекознавства; 2) недостатньою розробленістю поняття «загроза» і питань його відмежування від інших споріднених понять, таких, як «небезпека», «виклик», «ризик», «фактор»; 3) наявністю невирішеної проблеми формування категорійно-понятійного апарату націобезпекознавства, де пропонований нами категорійний ряд «моніторинг - загроза - небезпека - управління - система національної безпеки - національна безпека» посідає чільне місце; 4) можливістю на підставі теоретичних розробок даного категорійного ряду формувати адекватну систему моніторингу і управління загрозами та небезпеками [5, с. 266].

Серед усіх загроз різного походження для безпеки критичної інфраструктури найбільш типовими є: а) природні (незловмисні): повені, екстремальні погодні явища, лісові пожежі, землетруси, епідемії та пандемії, епізоотії; б) техногенні (незловмисні): промислові аварії, ядерні/радіологічні аварії, аварії на транспорті; б) зловмисні дії: кібератаки, терористичні атаки, втрата елементів критично важливої інфраструктури.

Отже, об’єкти критичні інфраструктури відіграють значну роль в економіці багатьох країн. В останні два десятиліття найважливішими критичними інфраструктурними галузями в світі були електроенергетичні системи, транспорт, водопостачання та харчування, сільське господарство та життєво важливі промислові підприємства. У сучасному світі інформація та телекомунікаційні технології, засоби масової інформації, банківська справа та фінанси, а також навколишнє середовище віднесені до критичної інфраструктури.

Кожна держава визначає власні критерії віднесення тих чи інших об’єктів до системи критичної інфраструктури відповідно з вимогами своєї національної політики. Попри те, що ЄС має певні критерії такого розподілу, кожна держава вільна самостійно оцінювати власні критично важливі для країни інфраструктурні об’єкти. Результати практики засвідчують у тому, що найбільш важливими інфраструктурними об’єктами є електроенергетичні системи, енергопостачання, виробництво, транспортування та зберігання небезпечних речовин, транспортна, інформаційна та телекомунікаційна інфраструктури тощо.

Залежно від типу інфраструктури, загрози її безпечному та сталому функціонуванню прийнято класифікувати на дві групи: фізичні загрози та кібератаки. Зрозуміло, що трубопроводи, підстанції, склади, комунікаційна інфраструктура та промислові заводи в основному піддаються фізичним

загрозам. На противагу ним, кіберзагрози піддають небезпеці системи моніторингу та контролю, бази даних, функціональні системи, програмне забезпечення, автоматизовані виробничі засоби тощо.

Для кожної групи критично інфраструктурних об'єктів характерним є свої критерії вразливості. Так, наприклад, генератори, мережі розподілу та інформації та телекомунікаційні мережі – це вразливість енергетичних систем. У джерелах енергії та розподільних мережах – це газ і нафтопроводи, виробництво та склади. У виробництві та поводженні з небезпечними речовинами вразливими групами є транспортування та зберігання речовин. У транспорті та перевезеннях найбільш уразливими є такі споруди як аеропорти, мости та тунелі.

На сьогодні можна сказати, що загрозами критичної інфраструктури є:

- недостатній розвиток організаційно-технічного забезпечення захисту об'єктів критичної інфраструктури і державних електронних інформаційних ресурсів;
- брак спроможностей суб'єктів сектору безпеки і оборони для забезпечення захисту об'єктів критичної інфраструктури та боротьби з кіберзагрозами, кібершпигунством, кібертероризмом та кіберзлочинністю, які негативно впливають на їх стале функціонування;
- запізнення та неефективність дій органів державної влади та силових структур з реагування на загрозу пошкодження критичної інфраструктури та забезпечення її відновлення тощо.

ЛІТЕРАТУРА:

1. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / Упоряд. Д.С. Бірюков, С.І Кондратов ; за заг. ред. О.М.Суходолі. К. : НІСД, 2016. 176 с.

2. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети*. 2016. № 3 (40). С. 62-76.

3. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки) (аналітична записка) URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/zagrozi-kritichniy-infrastrukturi-ta-ikh-vpliv-na-stan-nacionalnoi

4. Мунтіян В.І. Економічна безпека України / В.І. Мунтіян. К.: КИИЦ, 1999. 463 с.

5. Канцір В.С. Терористична діяльність і національна безпека. *Часопис Київського університету права*. 2011. № 1. С. 265-269.