Теленик Сергій Сергійович,
здобувач Національної академії внутрішніх справ, кандидат юридичних наук

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У ФРН

Становлення інституту захисту критичної інфраструктури в Україні відбувається в умовах певного, вже сформованого національного нормативного та практичного досвіду, що ґрунтується на застосуванні законодавства та роботі органів публічної адміністрації у різних сферах діяльності відповідного сектору. Як відомо, запроваджуваний інститут покликаний об'єднати усі найважливіші його складові.

У більшості європейських країн та США згаданий інститут діє протягом тривалого часу, а отже, напрацьовано значний та різнобічний досвід. До таких напрацювань потрібно звертатись не тільки з метою оцінки можливих позитивних запозичень, а й задля прогнозування та запобігання недоліків та помилок у національній законотворчій та правозастосовній практиці.

У цій статті проаналізовано досвід адміністративно-правового регулювання інституту захисту критичної інфраструктури у ФРН; зосереджено увагу на визначенні поняття критичної інфраструктури, зазначено суб'єктів, які здійснюють захист критичної інфраструктури та нормативні акти, що регулюють відповідні правовідносини.

Отже, критична інфраструктура у ФРН визначається як організації і установи, що мають найважливіше значення для держави і суспільства, відмова або порушення роботи яких призведуть до перебоїв у постачанні, значним порушенням суспільної безпеки або іншим драматичним подіям. Зважаючи на особливе значення, поширену сферу впливу та розгалужені зв'язки, окремо визначають поняття інформаційної критичної інфраструктури. Критична інформаційна інфраструктура – сектор інформаційних технологій і телекомунікацій, а також основані на інформаційній критичній інфраструктурі, інфраструктури інших секторів [1].

Основними суб'єктами, які займаються питаннями захисту критичної інфраструктури є: Федеральне міністерство внутрішніх справ, Федеральне управління цивільного захисту і допомоги у випадку стихійних лих, Федеральне відомство з інформаційної безпеки, оператори критичної інфраструктури (переважно, приватний сектор), федеральні землі (несуть відповідальність за цивільний захист

у своїх межах, забезпечують зв'язок між локальними критичними інфраструктурами), муніципалітети (беруть участь у цивільному захисті шляхом розроблення планових рішень і планів дій у надзвичайних ситуаціях: пожежні і рятувальні служби).

Нормативну основу складають документи у відповідній сфері, серед яких:

Стратегія державно-приватного партнерства щодо захисту критичних інфраструктур у якій встановлено умови взаємодії між державними органами та операторами критичної інфраструктури, права та обов’язки цих суб’єктів;

Стратегія кібербезпеки для Німеччини, у якій визначено засади політики у сфері кібербезпеки, сформовано міжвідомчі стратегічні напрями для діяльності федерального уряду щодо кібербезпеки;

Національна стратегія захисту критичних інфраструктур узагальнює цілі, політичний та стратегічний підхід федерального уряду із захисту критичної інфраструктури, регулює питання співпраці між різними партнерами та зацікавленими сторонами, визначає механізми і інструменти для досягнення цілей захисту.

У сфері захисту фізичних об’єктів критичної інфраструктури Федеральне міністерство внутрішніх справ, Федеральне управління цивільного захисту та допомоги у випадку стихійних лих та Федеральне управління кримінальної поліції розробили базову концепцію захисту критичної інфраструктури, метою якої є зниження уразливості критичних інфраструктур від впливу природних явищ та аварій, а також терористичних актів, злочинних дій. Концепцією визначено та передбачено:

– небезпечні та уразливі зони (небезпеки, пов’язані з природними явищами, людським чинником, технічними проблемами, терористичними загрозами, злочинною діяльністю);

– аналіз потреб у захисті (порядок аналізу потреб у захисті, урахування залежностей та взаємодії на об’єктовому та суб’єктному рівнях, визначення цілей захисту, заходи задля досягнення мети захисту, внутрішній і зовнішній захист, персонал, організація і управління;

– управління ризиками (аварійне планування, ризик і кризова комунікація, планування простою та управління безперервністю бізнесу, управління якістю захисних заходів, документування захисних заходів).

Аналіз і планування включають виявлення ризиків, наступний огляд та адаптацію захисних заходів. Ця діяльність структурована наступним чином:

1. Формування категорій небезпеки: райони стихійних лих, нещасні випадки, тероризм і злочинність.

2. Визначення відповідного рівня захисту.

3. Розроблення сценаріїв збитків та загроз.

4. Аналіз уразливостей.

5. Формулювання мети захисту та визначення захисних та контрзаходів.

6. Визначення необхідності дій (координація між державними та приватними заходами та суб'єктами).

7. Реалізація дій.

8. Регулярний огляд аналізу та процесу планування у контексті управління якістю [2].

Повноваження у сфері кібербезпеки, захисту критичної інфраструктури, інтернет-безпеки, криптографії, контрспостереження, сертифікації продуктів для забезпечення безпеки та акредитацію випробувальних лабораторій безпеки здійснює Федеральне агентство (управління) з інформаційної безпеки (нім. Bundesamt für Sicherheit in der Informationstechnik (BSI); англ. Federal Office for Information Security (FOIS). Діяльність BSI регулюється спеціальним Законом про Федеральне відомство з інформаційної безпеки.

У спеціальному законі передбачено низку вимог для різних суб'єктів, які працюють у сфері інформаційних технологій і телекомунікацій, наприклад, для власників інтернет-магазинів висуваються вимоги до технічних і організаційних заходів щодо захисту даних їх клієнтів та IT-систем, які використовуються; телекомунікаційні компанії повинні попереджувати своїх клієнтів у випадку підозри, що з'єднання клієнта може використовуватись для IT-атак; на операторів критичної інфраструктури покладено обов'язок захищати IT-інфраструктуру, необхідну для надання їх основних послуг і здійснювати перевірку стану безпеки раз на два роки, оператори також зобов'язані повідомляти про значні інциденти інформаційної безпеки BSI. Обов'язок сповіщати про значні інциденти у сфері інформаційної безпеки поширюється на операторів атомних електростанцій та телекомунікаційних компаній, води та продовольства, а також фінансовому, страховому, транспортному і медичному секторах. BSI узагальнює цю та іншу інформацію та поширює її серед операторів критичної інфраструктури для того, щоб вони сформували уявлення про небезпеки та здійснили адекватну оцінку своїх IT-систем [1].

Дія закону поширюється на такі сектори: енергетика, вода, продукти харчування, інформаційні технології і телекомунікації,

транспорт, охорона здоров'я, фінанси, страхування (загалом близько 2000 операторів). Підзаконними актами визначено критерії, за якими оператори можуть встановити належність їх об'єктів до критичної інфраструктури.

Отже, модель нормативно-правового регулювання та організації діяльності суб'єктів, які здійснюють захист критичної інфраструктури у ФРН відрізняється від підходу, який запроваджується в Україні (ухвалення окремого спеціального закону, визначення єдиного органу, який буде відповідати за координацію всіх суб'єктів, діяльність яких пов'язана з експлуатацією або іншим використанням об'єктів критичної інфраструктури, визначення переліку таких об'єктів та ін.)

Список використаних джерел

1. Bundesamt für Sicherheit in der Informationstechnik. Офіційний сайт. URL: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/Strategie/KRITIS/kritischeinfrastrukturen_node.html

2. Защита критической инфраструктуры – Концепция основных мер защиты. Рекомендации для предприятий. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritische-infrastrukturen-basisschutzkonzept-rus.pdf?__blob=publicationFile&v=2

Новачук Сергій Андрійович
аспірант докторантури та ад'юнктури Національної академії внутрішніх справ

ОСОБЛИВОСТІ ДОСЛІДЖЕННЯ ПРЕДМЕТА ЗЛОЧИННОГО ПОСЯГАННЯ ПРИ РОЗСЛІДУВАННІ ПОРУШЕННЯ ВИМОГ РЕЖИМУ РАДІАЦІЙНОЇ БЕЗПЕКИ

Предмет злочинного посягання як елемент криміналістичної характеристики злочинів, передбачених ст. 267-1 КК України має важливе значення для розслідування, оскільки детермінує спосіб учинення злочину, пов'язаний з особою злочинця та може впливати на кримінально-правову кваліфікацію.

Заборона переміщення за межі зони відчуження будь-яких об'єктів зумовлена ризиками неконтрольованого обігу радіоактивно забруднених об'єктів, що може створювати небезпеку для життя і здоров'я людей, забруднення навколишнього середовища.

Особливо небезпечним є потрапляння радіоактивно забруднених продуктів харчування у організм людини.