ПРІОРИТЕТНІ НАПРЯМИ ЗАКОНОДАВЧОГО ТА ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПАСПОРТИЗАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація

Проаналізовано передумови проведення паспортизації об'єктів критичної інфраструктури в рамках створення державної системи захисту критичної інфраструктури в Україні. Визначено комплекс проблемних питань у сфері законодавчого та організаційного забезпечення, що потребують врегулювання для забезпечення паспортизації об'єктів критичної інфраструктури. Запропоновано пріоритетні напрями діяльності Кабінету Міністрів України, Державної служби з надзвичайних ситуацій, Міністерства економічного розвитку і торгівлі України щодо відпрацювання заходів із законодавчого та організаційного забезпечення паспортизації об'єктів критичної інфраструктури.

ПРІОРИТЕТНІ НАПРЯМИ ЗАКОНОДАВЧОГО ТА ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПАСПОРТИЗАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Активізація загроз природного та техногенного походження, підвищення ризиків терористичних актів, збільшення кількості кібератак на енергетичні об'єкти, руйнування та пошкодження об'єктів інфраструктури в зоні військового конфлікту на сході України обумовлюють нагальність питання розбудови державної системи захисту критичної інфраструктури в Україні.

Відповідно до Указу Президента України №8/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури»[1] Кабінету Міністрів України необхідно внести в установленому порядку на розгляд Верховної Ради України проект Закону України «Про критичну інфраструктуру та її захист», в якому передбачити врегулювання питань, зокрема, щодо запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації.

У свою чергу Концепція створення державної системи захисту критичної інфраструктури[2], схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 р., серед проблем, що потребують розв'язання, визначає відсутність єдиних критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації.

Паспорт безпеки об'єкта критичної інфраструктури (ОКІ) є документом визначеної форми, що містить структуровані дані про окремий об'єкт

---

[1] Указ Президента України №8/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури». [Електронний ресурс]. − Режим доступу: http://www.president.gov.ua/documents/82017-21058

[2] Розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р «Про схвалення Концепції створення державної системи захисту критичної інфраструктури». [Електронний ресурс]. − Режим доступу: http://zakon3.rada.gov.ua/laws/show/1009-2017-%D1%80

критичної інфраструктури та визначає комплекс заходів, що вживаються оператором з метою забезпечення захисту цього об'єкта. У той же час на сьогодні вимоги щодо паспорта безпеки об'єкта критичної інфраструктури не визначені.

Нині в Україні існують декілька функціональних систем забезпечення безпеки галузевих об'єктів, що можуть бути віднесені до критичної інфраструктури. Так, у сфері цивільного захисту відповідно до Закону України «Про об'єкти підвищеної небезпеки»[3] передбачено декларування безпеки об'єкта підвищеної небезпеки шляхом підготовки документу, в якому наводяться результати аналізу ступеня небезпеки та оцінки рівня ризику цього об'єкту. Також цей документ визначає комплекс заходів, що вживаються суб'єктом господарської діяльності з метою запобігання аваріям, а також забезпечення готовності до локалізації, ліквідації аварій та їх наслідків.

У Системі фізичної ядерної безпеки діє Порядок проведення оцінки вразливості ядерних установок та ядерних матеріалів[4]. Дія цього документу поширюється на експлуатуючі організації та інших ліцензіатів, що визначають, створюють і підтримують безперервне функціонування системи фізичного захисту ядерних установок та ядерних матеріалів або системи фізичного захисту ядерних матеріалів I та II категорій при їх перевезенні. Завданнями проведення даної оцінки вразливості є виявлення вразливих цілей правопорушників, аналіз потенційних радіаційних наслідків вчинення протиправних дій щодо вразливих цілей правопорушників, оцінка ризиків, розроблення рекомендацій щодо приведення стану системи фізичного захисту ядерної установки та ядерних матеріалів, системи фізичного захисту ядерних матеріалів при їх перевезенні у відповідність до вимог чинного законодавства.

---

[3] Закон України «Про об'єкти підвищеної небезпеки» від 18.01.2001 № 2245-III. [Електронний ресурс]. − Режим доступу: http://zakon0.rada.gov.ua/laws/show/2245-14

[4] Наказ Державного комітету ядерного регулювання України від 30.11.2010 N 16 «Про затвердження Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів». [Електронний ресурс]. − Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1309-10

На сьогодні найбільш пристосованим до вирішення завдань захисту критичної інфраструктури є підхід до паспортизації потенційно небезпечних об'єктив, що здійснюється Державною архівною службою України.

Відповідно до «Положення про паспортизацію потенційно небезпечних об'єктів»[5] проводиться ідентифікація та паспортизація цих об'єктів шляхом підготовки і надання паспорту потенційно небезпечного об'єкта (ПНО). Паспорт потенційно небезпечного об'єкта є документом визначеної форми, що містить структуровані дані про окремий потенційно небезпечний об'єкт. Це, насамперед, загальна інформація про об'єкт, дані про небезпечні природні умови та технологічні процеси, дані щодо основних джерел небезпеки та об'єктів впливу надзвичайних ситуацій, аварійно-рятувальна документація тощо. Форми паспортів ПНО відповідають певному виду господарської діяльності включаючи шахти, гідротехнічні об'єкти, магістральні трубопроводи, родовища корисних копалин. Ідентифікація потенційно небезпечного об'єкта є процедурою виявлення на об'єкті джерел та чинників небезпеки, на підставі яких об'єкт визнається потенційно небезпечним.

Реєстрація потенційно небезпечних об'єктів в Україні розпочалась після прийняття Постанови Кабінету Міністрів України «Про затвердження Положення про Державний реєстр потенційно небезпечних об'єктів»[6]. Нині Реєстр ПНО є автоматизованою інформативно-довідковою системою, що забезпечує облік та обробку інформації щодо потенційно небезпечних об'єктів. База даних Реєстру містить актуальну інформацію про понад 26 тис. потенційно небезпечних об'єктів, що включають підприємства, родовища нафти та газу, магістральні трубопроводи та відгалуження, гідротехнічні об'єкти, вугільні шахти, автозаправні станції, кар'єри, мости, віадуки, шляхопроводи, сухопутні тунелі, підземні станції та тунелі метро тощо.

---

[5] Наказ Міністерства України з надзвичайних ситуацій «Про затвердження Положення про паспортизацію потенційно небезпечних об'єктів» N 338 від 18.12.2000. [Електронний ресурс]. − Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0062-01

[6] Постанова Кабінету Міністрів України від 29 серпня 2002 р. № 1288 «Про затвердження Положення про Державний реєстр потенційно небезпечних об`єктів». [Електронний ресурс]. − Режим доступу: http://zakon5.rada.gov.ua/laws/show/1288-2002-%D0%BF

Кожному об’єкту, інформація про який внесена до бази даних Реєстру, надається унікальний реєстраційний номер, що не змінюється при зміні власника. Інформація по кожному об’єкту, крім загальної (назва, територіальне розташування, вид діяльності), містить кількісні та якісні показники виробничих процесів та небезпек, які притаманні виду діяльності об’єкта. База даних Реєстру ПНО дозволяє робити витяги з нього за понад 40 параметрами, до яких відносяться строки експлуатації, джерела небезпеки, види та можливі рівні небезпек, кількісні показники чинників небезпеки.

Нині інформаційні ресурси бази даних дозволяють використовувати Реєстр ПНО в якості основних відомостей для виявлення та визначення потенційних ризиків небезпеки регіонів, окремих районів, відокремлених територій, конкретних об’єктів.

При цьому враховуються такі характеристики:

- масштаб і географічне охоплення території, для якої небезпечна подія викликає значну шкоду;
- несприятливі події, в результаті яких може бути заподіяно прямий, а також непрямий збиток промисловому підприємству;
- тяжкість можливих наслідків за такими показниками:

– вплив на населення включаючи кількість постраждалих, загиблих, осіб, які отримали серйозні травми, а також чисельність евакуйованого населення;

– екологічна шкода, збитки для навколишнього середовища;

– взаємозв’язок з іншими елементами інфраструктури.

Стосовно антитерористичної захищеності об’єктів критичної інфраструктури треба відмітити, що в рамках Державної системи фізичного захисту за результатами оцінки вразливості формуються документи, що певною мірою відповідають паспорту ПНО, але є значно ширшими з точки

зору оцінки загроз[7]. Так, Звіт з оцінки вразливості окрім загальних даних про об'єкт та виявлені джерела небезпеки містить опис загроз, сценарії дій правопорушників та оцінює здатність системи фізичного захисту та об'єктового плану взаємодії протистояти визначеним загрозам[8].

Розробка паспортів безпеки для об'єктів паливно-енергетичного комплексу (ПЕК) передбачена у законодавстві Російської Федерації[9]. При цьому паспорт безпеки об'єкта ПЕК в РФ відображає як характеристики об'єкта з позиції його потенційної небезпеки, так і можливі негативні наслідки незаконного втручання у функціонування об'єкта, оцінку стану систем інженерно-технічного та фізичного захисту, заходи із забезпечення антитерористичної захищеності.

Відповідно до Концепції створення державної системи захисту критичної інфраструктури в Україні, ця система спрямована на забезпечення стійкості критичної інфраструктури до всіх типів загроз включаючи загрози природного і техногенного характеру, кіберзагрози, протиправні дії. Тому в паспорті безпеки об'єкта критичної інфраструктури мають бути включені всі типи загроз і попередньо визначені напрями забезпечення захисту цих об'єктів.

Метою формування паспортів безпеки об'єктів критичної інфраструктури є визначення загроз та оцінки можливих ризиків негативних наслідків їх прояву для об'єктів критичної інфраструктури, визначення напрямів забезпечення їх безпеки для подальшої розробки на цій основі заходів із запобігання та попередження прояву загроз для об'єктів критичної інфраструктури. Паспорти безпеки мають готуватися операторами об'єктів

---

[7] Постанова Кабінету Міністрів України від 21.12.2011 No 1337 «Про затвердження Порядку функціонування державної системи фізичного захисту». [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/1337-2011-%D0%BF

[8] Наказ Держатомрегулювання України від 30.11.2010 No169, зареєстрований в Міністерстві юстиції України 22.12.2010 за No1309/18604 «Про затвердження Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів» (НП 306.8.167-2010). [Електронний ресурс].– Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1309-10

[9] Федеральный закон Российской Федерации от 21.07.2011 N 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» – ИПС «Закон». [Електронний ресурс]. – Режим доступу: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102149573&rdk=&backlink=1

критичної інфраструктури і надаватися на погодження до відповідальних за сектори суб'єктів захисту критичної інфраструктури та Службу безпеки України.

У загальному випадку паспорт безпеки об'єкта критичної інфраструктури має включати інформацію щодо загальних відомостей про об'єкт, зв'язків з іншою інфраструктурою, природно-кліматичних і географічних умов місця розташування ОКІ, відомості про речовини та матеріали, що використовуються на ОКІ, аварійної готовності персоналу до дій в умовах НС, організації охорони та фізичного захисту ОКІ, інженерно-технічних засобів охорони, характеристики основних джерел небезпеки, категорії критичності ОКІ, присвоєна об'єкту.

Далі, з урахуванням актуальних загроз та завдань захисту критичної інфраструктури, пропонується структура паспорта безпеки ОКІ, що може включати такі розділи.

1. Загальні відомості про об'єкт.
2. Основні споруди і технологічне обладнання.
3. Зв'язок з іншою інфраструктурою.
4. Природно-кліматичні умови.
5. Небезпечні технологічні процеси.
6. Характеристика основних загроз безпеці ОКІ.
7. Аварійна готовність.
8. Організація охорони та фізичного захисту ОКІ.
9. Оцінка вразливості ОКІ.
10. Захист інформаційної інфраструктури.
11. Відповідність вимогам захисту ОКІ.

Розділ «Загальні відомості про об'єкт» включає інформацію щодо найменування об'єкта, поштової адреса, галузі підприємства, основного виду діяльності об'єкта, конструктивних і технологічних елементів ОКІ, загальної площі території, відомостей про персонал ОКІ, загальну чисельність працюючих на об'єкті, режиму роботи ОКІ (сезонний, одно-, дво-, тризмінний,

максимальна чисельність працюючих на об'єкті), рівня зносу основних виробничих фондів.

Зв'язок з іншою інфраструктурою включає інформацію про розташування ОКІ по відношенню до систем транспорту, включаючи автомобільний (дороги, шосе, мостові переходи, автовокзали, автостанції тощо), залізничний (залізничні колії, мостові переходи, вокзали, станції, платформи, переїзди), повітряний (аеропорти, аеровокзали, аеродроми, злітно-посадкові смуги), водний (морські та річкові порти, причали). Треба також враховувати наявність біля об'єкту інших ОКІ, населених пунктів, житлових будинків та інших об'єктів масового скупчення людей, їх розміщення по відношенню до ОКІ.

При формуванні паспортів безпеки об'єктів критичної інфраструктури треба враховувати всі типи загроз включаючи загрози природного та техногенного походження. При цьому серед усіх загроз різного походження для безпеки критичної інфраструктури найбільш актуальними можна виокремити такі[10]:

- *природні*: повені, екстремальні погодні явища, лісові пожежі, землетруси, епідемії та пандемії, епізоотії;
- *техногенні*:

а) незловмисні: промислові аварії, ядерні/радіологічні аварії, аварії на транспорті, втрата критично важливої інфраструктури;

б) зловмисні: кібератаки, терористичні атаки.

Особливої уваги потребують взаємозв'язки та взаємозалежності між загрозами природного походження, коли виникнення одних небезпечних явищ призводить до формування нових через механізм каскадних ефектів. Усвідомлення каскадних ефектів сучасних загроз є досить складним через взаємозв'язок об'єктів інфраструктури та оточуючого її середовища.

[10] Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. – Luxembourg: Publications Office of the European Union, 2015. – 40 p.

Неспроможність дійти згоди заінтересованих сторін і політичного керівництва у питаннях прогнозування та пом'якшення негативних наслідків новітніх загроз (насамперед, природного походження) може призвести до серйозних порушень у роботі критичної інфраструктури в найближчому майбутньому.

При проведенні оцінки негативних наслідків надзвичайних ситуацій на обєктах критичної інфраструктури має враховуватися збиток життю і здоров'ю людей через кількість постраждалих, травмованих, загиблих, евакуйованих. У свою чергу економічні збитки можуть оцінюватися через вплив на ВВП, розмір прямих і непрямих економічних втрат, частку продукції об'єкта в її загальнодержавному випуску. Екологічна шкода оцінюється через вплив на навколишнє природне середовище, рівень забруднення повітря, водних і земельних ресурсів, продуктів харчування.

Розділ «Аварійна готовність» має включати інформацію щодо аварій та порушень в роботі ОКІ протягом останніх 10 років, а також події техногенного характеру, що можуть статися у межах або поза межами ОКІ. Крім того, надається інформація про наявність аварійно-рятувальної документації, сили та засоби ліквідації аварій та їх наслідків включаючи наявність протипожежної служби, відомчої пожежної охорони, договірних підрозділів пожежної охорони, формувань, що забезпечують вибухову, хімічну та біологічну безпеку, а також радіологічну та ядерну безпеку.

У розділі «Організація охорони та фізичного захисту ОКІ» вміщується інформація про підрозділи фізичного захисту (структура та штат, розподіл обов'язків між структурними одиницями, кваліфікація персоналу), підрозділ охорони, наявність організаційно-розпорядчих документів, у т.ч. спільних з органами внутрішніх справ та іншими організаціями планів дій при виникненні надзвичайних або кризових ситуацій. Також цей розділ має містити інформацію щодо організації пропускного та внутрішнього режимів, роботи контрольно-пропускних пунктів, наявність програм підготовки та перепідготовки персоналу, відомості про проведені навчання, тренування, перевірки.

Оцінка готовності персоналу до дій в умовах кризових ситуацій на ОКІ передбачає наявність нормативно-технічної документації щодо порядку дій персоналу в умовах надзвичайних і кризових ситуацій на ОКІ з відображенням у посадових інструкціях. Крім того, у розділі міститься інформація щодо оснащення персоналу об’єкта приладами, обладнанням, засобами індивідуального захисту, необхідними для виконання обов’язків в умовах надзвичайних і кризових ситуацій. Також має надаватися інформація щодо перевірки готовності персоналу до дій в умовах надзвичайних і кризових ситуацій на об’єкті під час проведення періодичних перевірок, тренувань і навчань учасників аварійного плану об’єкта, спільних тренувань і навчань учасників об’єктового плану взаємодії у разі вчинення диверсії, а також заходи щодо усунення виявлених недоліків.

Паспорт безпеки має завершуватися висновками щодо відповідності об’єкта критичної інфраструктури необхідним вимогам захисту. Зокрема, що об’єкт за галузевою ознакою і видом діяльності відноситься до відповідної категорії з цивільного захисту, хімічної небезпеки або пожежо- та вибухонебезпечності. Крім того, даному об’єкту за сукупністю збитку, що може бути нанесений у результаті кризової ситуації і за ступенем критичності присвоюється відповідна категорія. Також має бути надана оцінка виконання вимог охорони об’єкта і захисту його елементів, інформація щодо наявності критичних елементів об’єкта, їх взаємовпливу і відповідності необхідному рівню захищеності.

Наприкінці паспорту безпеки має бути зроблено висновок щодо достатності сил і засобів для виконання заходів з фізичного захисту та антитерористичної захищеності об’єкта і у разі необхідності наведено перелік додаткових заходів з удосконалення та усунення виявлених недоліків із зазначенням термінів їх виконання.

Треба відмітити, що паспортизація є одним із етапів проведення обліку об’єктів критичної інфраструктури. У свою чергу облік об’єктів критичної інфраструктури включатиме виконання комплексу заходів із забезпечення

збору, накопичення та актуалізації необхідної інформації щодо характеристик об’єктів критичної інфраструктури, формування та адміністрування бази даних реєстру об’єктів критичної інфраструктури, інформаційний обмін та надання даних реєстру, розроблення програмного забезпечення для ведення реєстру об’єктів критичної інфраструктури. Враховуючи важливість інформації щодо об’єктів критичної інфраструктури для забезпечення національної безпеки держави, інформація, що використовується для обліку об’єктів критичної інфраструктури, може бути віднесена до інформації з обмеженим доступом або взагалі бути закритою.

При цьому треба враховувати, що облік об’єктів критичної інфраструктури може включати декілька етапів, що потребуватимуть законодавчого узгодження (рис. 1).

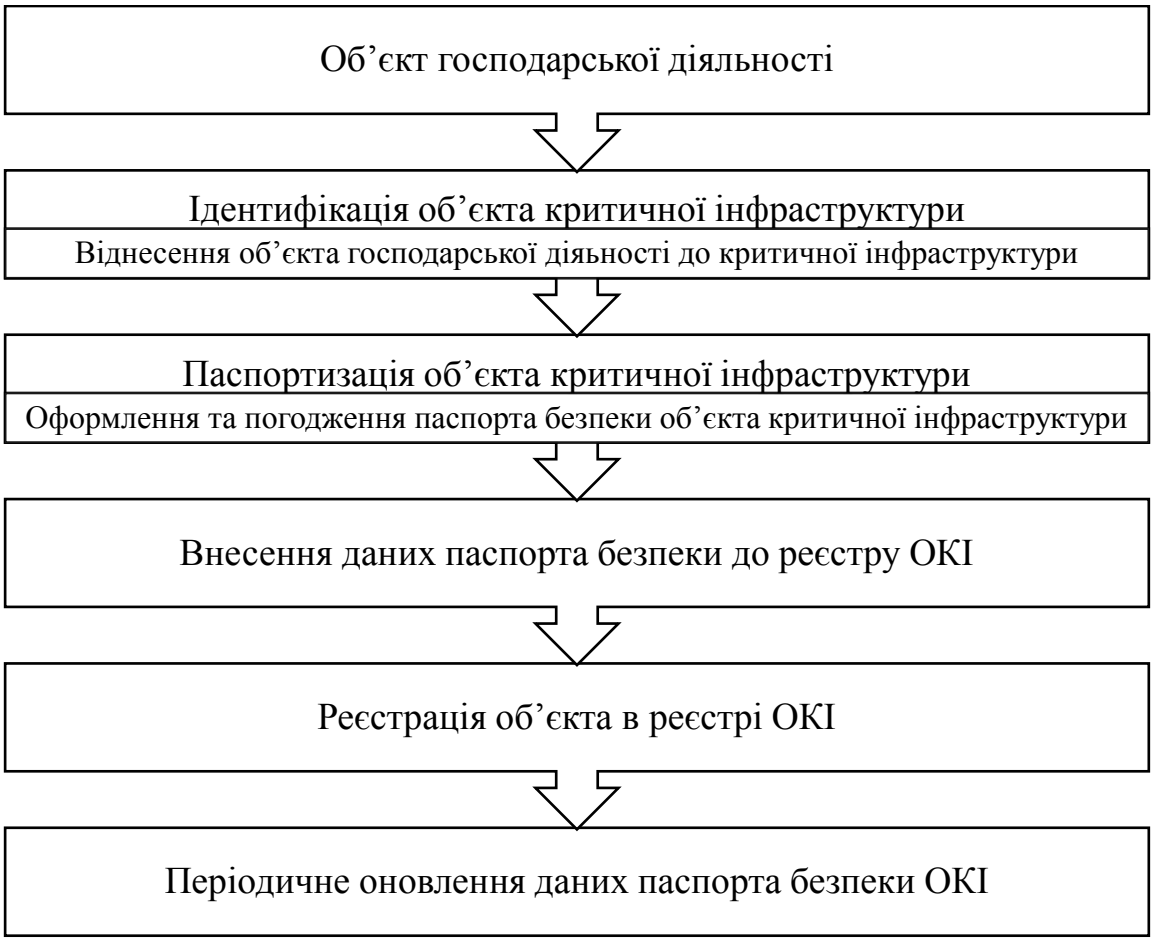

Рис.1. Етапи формування реєстру та обліку об’єктів критичної інфраструктури

Так, ідентифікація об’єкта критичної інфраструктури передбачатиме процедуру виявлення на об’єкті різних джерел і чинників небезпеки, на

підставі яких даний об’єкт буде визначатися як об’єкт критичної інфраструктури. При цьому віднесення об’єктів до критичної інфраструктури може відбуватися за сукупністю критеріїв, що визначають їх важливість для національної безпеки держави, свідчать про наявність ризиків для них, можливість виникнення нештатних та аварійних ситуацій через активізацію загроз різного походження. Ідентифікація об’єктів здійснюється відповідальними органами державної влади за відповідні сектори критичної інфраструктури.

Після ідентифікації об’єкта та його віднесення до критичної інфраструктури оператор такого об’єкта має здійснити його паспортизацію, що передбачає формування паспорту безпеки на об’єкт критичної інфраструктури. Цей документ має відображати результати аналізу ризиків, основних можливих загроз і потенційних негативних наслідків для об’єктів критичної інфраструктури, а також містити заходи із запобігання та попередження виникненню загроз. Враховуючи важливість інформації, паспорт безпеки має бути погодженим з відповідальними органами за сектори захисту критичної інфраструктури та Службою безпеки України. Форма паспорту безпеки об’єктів критичної інфраструктури, порядок його розробки, наповнення, зміст та строки подання має встановлювати Кабінет Міністрів України.

Після проведення паспортизації має відбутися внесення даних паспорта безпеки об’єктів критичної інфраструктури до реєстру. Очевидно, що внесення об’єктів до реєстру об’єктів критичної інфраструктури має здійснювати окремий державний орган, що реалізуватиме державну політику у сфері захисту критичної інфраструктури за поданням відповідальних за сектори критичної інфраструктури. При цьому важливим етапом обліку буде періодичне оновлення даних паспортів безпеки об’єктів критичної інфраструктури, що може відбуватися щорічно або кожні два роки з огляду на важливість і пріоритетність виконання завдань захисту критичної інфраструктури.

У свою чергу порядок ведення реєстру, внесення об’єктів до реєстру об’єктів критичної інфраструктури, а також особливості надання інформації з реєстру мають встановлюватися Кабінетом Міністрів України.

У цілому паспортизація об’єктів критичної інфраструктури є складовим етапом створення державної системи захисту критичної інфраструктури, що потребує дієвої взаємодії операторів, що мають формувати паспорти безпеки об’єктів критичної інфраструктури, секторальних органів виконавчої влади і спецслужб, що мають погоджувати паспорти безпеки. Забезпечення такої взаємодії можливо врегулювати через ухвалення відповідного проекту Закону «Про критичну інфраструктуру та її захист», що перебуває на етапі узгодження і надання пропозицій.

Висновки

Паспортизація об’єктів критичної інфраструктури передбачає формування паспортів безпеки об’єктів критичної інфраструктури для визначення загроз та оцінки можливих ризиків негативних наслідків їх прояву для об’єктів критичної інфраструктури, визначення напрямів забезпечення безпеки ОКІ для подальшої розробки на цій основі заходів із запобігання та попередження прояву загроз для об’єктів критичної інфраструктури. Паспорти безпеки об’єктів критичної інфраструктури мають готуватися операторами об’єктів критичної інфраструктури і надаватися на погодження до відповідальних за сектори суб’єктів захисту критичної інфраструктури.

При формуванні паспортів безпеки треба враховувати наявність в Україні декількох систем, що забезпечують захист від різних загроз. Система захисту критичної інфраструктури має забезпечити координацію різних систем і відомств через механізм узгодження і підтримки діяльності. Для передбачення загроз за методологією, що буде розроблена і затверджена на рівні секторального органу виконавчої влади, буде здійснюватися ідентифікація об’єктів критичної інфраструктури. Секторальні органи влади та оператори мають формувати проектні загрози, тобто характеристику можливих джерел зловмисних дій проти об’єктів критичної інфраструктури.

У свою чергу паспорт безпеки об’єкта критичної інфраструктури має бути комплексним документом, де будуть окреслені всі типи загроз і попередньо визначені напрями забезпечення захисту об’єктів критичної інфраструктури від них.

Розвиток законодавства у сфері забезпечення захисту критичної інфраструктури обумовлює необхідність вирішення комплексу питань, серед яких важливе значення має паспортизація об’єктів критичної інфраструктури. Разом із тим концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 р., серед проблем, що потребують розв’язання, визначає відсутність єдиних критеріїв та методології віднесення об’єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації. Нині вимоги щодо паспорта безпеки об’єкта критичної інфраструктури не визначені.

Досвід функціонування Реєстру потенційно небезпечних об’єктів обумовлює можливість використання засобів і технологій його ведення для проведення паспортизації об’єктів критичної інфраструктури. Для цього необхідно провести комплексний аналіз складових Реєстру та визначити напрями адаптації його законодавчого та організаційного забезпечення для вирішення завдань паспортизації об’єктів критичної інфраструктури.

Враховуючи значний обсяг інформації, необхідний для формування паспортів безпеки ОКІ, уявляється доцільним створення інформаційно-аналітичної системи підтримки процесів паспортизації, що забезпечить формування електронних баз даних основних параметрів ОКІ, збереження паспортів безпеки в електронному вигляді, обмеженого доступу до них, отримання необхідної інформації та забезпечення обміну інформацією між операторами та відповідальними за сектори критичної інфраструктури.

Пропозиції

Враховуючи необхідність законодавчого та організаційного забезпечення паспортизації об’єктів критичної інфраструктури уявляється доцільним рекомендувати:

Кабінету Міністрів України:

• розробити і подати до Верховної Ради України проект Закону «Про критичну інфраструктуру та її захист», в якому передбачити врегулювання питань паспортизації об’єктів критичної інфраструктури;

• визначити функції, повноваження та відповідальність центральних органів виконавчої влади та інших органів щодо формування паспортів безпеки об’єктів критичної інфраструктури, а також відповідальності власників і операторів об’єктів критичної інфраструктури;

• запровадити критерії віднесення об’єктів інфраструктури до критичної інфраструктури, визначити порядок їх паспортизації та категоризації;

• визначити пріоритети створення інформаційно-аналітичної системи підтримки процесів паспортизації об’єктів критичної інфраструктури, що забезпечить формування електронних баз даних основних параметрів об’єктів критичної інфраструктури, збереження паспортів безпеки в електронному вигляді, отримання необхідної інформації та забезпечення обміну інформацією між операторами та відповідальними за сектори критичної інфраструктури;

Міністерству економічного розвитку і торгівлі України, Міністерству внутрішніх справ України, Міністерству інфраструктури України:

• опрацювати питання щодо формування критеріїв віднесення об’єктів до критичної інфраструктури, порядку проведення їх паспортизації, оцінки загроз критичній інфраструктурі, планів забезпечення стійкості функціонування критичної інфраструктури та формування інформаційної взаємодії між суб’єктами;

• проаналізувати можливість включення до проекту Закону України «Про критичну інфраструктуру та її захист» положення щодо ведення центральним органом виконавчої влади, що реалізує державну політику у сфері страхового фонду документації, обліку об'єктів критичної інфраструктури та обов'язковість створення страхового фонду документації на об'єкти критичної інфраструктури;

• розробити та затвердити в установленому порядку державний стандарт щодо запровадження єдиних підходів до класифікації всіх типів загроз безпеці об'єктам критичної інфраструктури, запровадження єдиної термінології щодо оцінки та рівнів загроз для формування паспортів безпеки;

Державній архівній службі України:

• розробити пропозиції щодо внесення змін до Закону України «Про страховий фонд документації» в частині адаптації можливостей використання страхового фонду документації для паспортизації об'єктів критичної інфраструктури;

• проаналізувати питання розробки і внесення змін до чинних нормативно-правових актів щодо проведення паспортизації об'єктів критичної інфраструктури;

• провести дослідження можливостей використання та адаптації Державного Реєстру потенційно небезпечних об'єктів для забезпечення формування паспортів безпеки об'єктів критичної інфраструктури.

С.П. Іванюта
відділ енергетичної та техногенної безпеки
Національний інститут стратегічних досліджень
червень 2018 р.