

УДК 351.863 +338.246.87

ПАСПОРТ БЕЗПЕКИ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ОBOB'ЯЗКОВИЙ ЕЛЕМЕНТ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Олександр ЄРМЕНЧУК,
кандидат юридичних наук,
доцент кафедри оперативно-розшукової діяльності
Дніпропетровського державного університету внутрішніх справ
Міністерства внутрішніх справ України

АНОТАЦІЯ

Проведений аналіз світового досвіду, наукових праць вітчизняних та зарубіжних дослідників і чинної нормативно-правової бази дає підстави стверджувати про доцільність розроблення та впровадження в Україні паспорту безпеки об'єкта критичної інфраструктури як важливого елемента в побудові державної системи захисту критичної інфраструктури. В українському законодавстві паспорт безпеки не є абсолютно новою категорією. Результати дослідження свідчать, що його різні аналоги зустрічаються в державних системах реагування та захисту, зокрема: системі фізичного захисту, цивільного захисту та протидії тероризму. Автор вважає, що метою складання паспортів безпеки об'єктів критичної інфраструктури є попередження та швидке припинення загроз, мінімізація ризиків та визначення сил і засобів, необхідних для забезпечення стійкості об'єктів. Пропонується авторське визначення понять: «паспорт безпеки об'єкта критичної інфраструктури», «паспортизація», «Державний реєстр об'єктів критичної інфраструктури».

Ключові слова: критична інфраструктура, захист критичної інфраструктури, національна безпека, паспорт безпеки об'єкта критичної інфраструктури, паспортизація об'єкта.

SAFETY PASSPORT OF CRITICAL INFRASTRUCTURE OBJECT AS A REQUIRED ELEMENT OF CRITICAL INFRASTRUCTURE PROTECTION SYSTEM

Oleksandr YERMENCHUK,

Candidate of Law Sciences, Associate Professor of the Department of Operational and Investigative Activity of Dnipropetrovsk State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine

SUMMARY

The analysis of world experience, scientific works of domestic and foreign researchers, the current legal and regulatory framework provides grounds for approving the expediency of designing and implementing in Ukraine a security passport of a critical infrastructure object as an important element in the construction of a state system for protecting objects of critical infrastructure. In Ukrainian legislation, the passport of safety is not an entirely new category. Its various counterparts are found in state response and protection systems, including: the system of physical protection, civil protection and counter-terrorism. The author believes that the purpose of drawing up security passports of critical infrastructure objects is to prevent and quickly terminate threats, risks and determine the forces and means necessary for their localization and ensure the stability of objects. The author's definition of concepts is offered: "Passport of the object of critical infrastructure", "certification of the object", "State register of objects of critical infrastructure".

Key words: critical infrastructure, critical infrastructure protection, national security, passport of the object of critical infrastructure, certification of the object.

Постановка проблеми. У Концепції створення державної системи захисту критичної інфраструктури під системою захисту критичної інфраструктури розуміється сукупність об'єктів, які є стратегічно важливими для економіки і безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України [1].

Із метою недопущення порушення функціонування таких об'єктів перед державою постала задача стосовно організації належного їх захисту.

Захист від різного роду загроз починається з вивчення реального стану будь-якого з визначених об'єктів та, відповідно до наявних ризиків та уразливості таких об'єктів, вимагає документального закріплення заходів із підвищення захищеності та визначення ролі і місця залучених учасників із державного та приватного сектору [2]. Такі категорії є складовими частинами паспорта безпеки об'єкта

критичної інфраструктури. Саме тому можна припустити, що невід'ємною складовою частиною побудови системи захисту критичної інфраструктури в Україні та одним із найважливіших етапів у цьому процесі є розроблення та впровадження паспорта безпеки об'єкта критичної інфраструктури.

Водночас наразі робота над розробленням паспорта безпеки об'єкта критичної інфраструктури на науковому та законодавчому рівні триває. Невизначеними залишаються його структура та зміст, підстави для початку його формування стосовно кожного з об'єктів та зон відповідальності залучених учасників.

Стан наукового дослідження. Окремі питання, пов'язані із захистом критичної інфраструктури, були порушені в наукових працях таких українських вчених, як: Бірюкова Д.С., Брежнева Є.В., Бобро Д.Г., Величка О.Ф., Дубова Д.В., Горбуліна В.П., Іванюти С.П., Зубарева В.В. Колах В.К.,

Кондратова С.І., Мірошника М.В., Насвіт О.І., Ожевана М.А., Панченко В.М., Петрова В.В., Рижова І.М., Скурського П.П., Суходолі О.М., Щербини В.М., Юрченка О.М., однак сучасний стан нормативно-правової бази у сфері захисту об'єктів критичної інфраструктури та розроблення паспорта безпеки як обов'язкового елемента в побудові системи захисту таких об'єктів потребує комплексного наукового дослідження.

Зазначені обставини зумовлюють актуальність теми дослідження та стали основою для наукових пошуків автора та підготовки цих матеріалів.

Мета і задачі статті. Захист критичної інфраструктури (далі – КІ) визначено одним із пріоритетних напрямів державної політики національної безпеки України. У цьому процесі основу складають: комплексне вдосконалення правової основи захисту КІ, створення системи державного управління її безпекою, посилення охорони об'єктів КІ. Комплексні заходи із захисту об'єктів вимагають системних та послідовних дій. Наразі існує реальна необхідність в аналізі міжнародного досвіду та вітчизняного законодавства з метою встановлення доцільності створення паспорта безпеки об'єктів КІ, визначення суті та змісту документу й основних учасників процесу, алгоритму їх дій.

Виклад основного матеріалу. Забезпечення безпеки об'єктів критичної інфраструктури належить до ключових напрямів державної політики національної безпеки України.

Необхідність організації захисту об'єктів КІ в Україні передбачено Основним Законом держави. У ст. 3 Конституції України закріплено, що безпека людини визнається найвищою соціальною цінністю. Водночас відповідно до ст. ст. 16, 17 захист суверенітету держави, забезпечення її економічної, інформаційної та екологічної безпеки належать до найважливіших функцій держави та є справою всього Українського народу.

Серед найбільш пріоритетних загроз національній безпеці Стратегія національної безпеки України визначає уразливість об'єктів критичної інфраструктури та недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій, неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення [3].

Водночас в інших концептуальних актах розвитку безпеки і оборони з метою попередження і припинення дії загроз передбачено проведення перевірок захищеності та необхідності створення умов для стійкого функціонування в разі надзвичайних ситуацій і в особливий період об'єктів критичної інфраструктури, а також посилення їх охорони і захисту [4; 5].

З метою вирішення поставлених керівництвом держави задач доцільно розглянути можливість розроблення та запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації [6; 7].

Слід констатувати, що досвід паспортизації об'єктів національної інфраструктури в українському законодавстві вже має певну історію та є частково апробованою складовою частиною механізму захисту національної безпеки від деяких видів загроз.

Зокрема, в єдиній державній системі цивільного захисту паспортизація потенційно небезпечних об'єктів здійснюється ще з 2000 р.

«Паспортом потенційно небезпечного об'єкта» є документ визначеної форми, який містить структуровані дані про окремий потенційно небезпечний об'єкт.

Зазначене поняття, а також регулювання суспільних відносини, пов'язаних із паспортизацією та сферою функціонування потенційно-небезпечних об'єктів (далі – ПНО) і забезпечення техногенної безпеки, передбачає Наказ

«Про затвердження Положення про паспортизацію потенційно небезпечних об'єктів» [8].

Для використання як емпіричної основи дослідження у процесі вивчення та побудови системи захисту критичної інфраструктури важливою для розгляду є процедура ідентифікації та паспортизації об'єктів.

Так, паспортизація здійснюється відповідно до переліків потенційно небезпечних об'єктів, затверджених комісіями, які складаються на підставі результатів ідентифікації потенційно небезпечного об'єкта. Метою її проведення є життєво важливих упереджувальних заходів із захисту ПНО [9].

За наявності хоча б одного джерела небезпеки, що може спричинити надзвичайну ситуацію об'єктового, місцевого, регіонального або державного рівнів, об'єкт ідентифікується як потенційно небезпечний. За результатами ідентифікації ПНО складається повідомлення про результати ідентифікації щодо визначення потенційної небезпеки, яке узгоджується з відповідним місцевим органом державного нагляду у сфері цивільного захисту.

Органи виконавчої влади та місцевого самоврядування сприяють відповідальним особам в організації і проведенні ідентифікації та контролюють додержання установлених вимог стосовно ідентифікації.

Місцеві органи державного нагляду у сфері цивільного захисту щороку уточнюють переліки таких об'єктів та подають їх до відповідного територіального органу державного нагляду у сфері цивільного захисту. У подальшому переліки потенційно небезпечних об'єктів затверджуються комісією з питань ТЕБ та НС і направляються до Державної архівної служби та Державної служби з питань надзвичайних ситуацій (далі – ДСНС). Державний департамент страхового фонду документації України (далі – СФД) здійснює державний облік потенційно небезпечних об'єктів, готує розпорядчий документ щодо проведення паспортизації. Він відповідає за ведення Державного реєстру техногенно та екологічно небезпечних об'єктів, а також за видачу юридичним та фізичним особам – власникам цих об'єктів свідоцтва про їх реєстрацію [10].

Територіальний орган державного нагляду у сфері ЦЗ щорічно до 1 січня надає на машинному та паперовому носіях затверджений регіональний перелік потенційно небезпечних об'єктів до Державного департаменту СФД для здійснення державного обліку ПНО, готує розпорядчий документ щодо проведення паспортизації ПНО, а також організовує контроль за станом паспортизації ПНО.

На оформлення паспорта відповідальним особам на об'єктах, що ідентифіковані як ПНО, надається тридцятиденний термін після отримання акта (розпорядчого документа) територіального органу державного нагляду у сфері захисту. Копія паспорта залучається до наглядової справи ПНО.

Існують різні форми паспортів у залежності від виду діяльності суб'єкта господарської діяльності. Наприклад: ІНС – підприємство, 2НС – вугільна шахта, 3НС – гідротехнічний об'єкт і т.д. Ці форми розміщуються на офіційному сайті МНС України. Форми паспортів потенційно небезпечних об'єктів та зміни до них затверджуються наказами ДСНС України.

Заповнення паспорта окремо на кожен об'єкт здійснюється державною мовою з обов'язковою вказівкою повної офіційної і скороченої назв об'єкта, з додержанням вимог щодо чіткості заповнення та однозначного тлумачення наведеної інформації та завіряється підписом керівника та печаткою.

Персональну відповідальність за несвоєчасне подання паспорта ПНО, змін до нього, неповний обсяг інформації та подання недостовірної інформації несуть його керівники.

Паспорти підлягають обов'язковому переоформленню кожні п'ять років. Повідомлення про зміни в паспорті потенційно небезпечного об'єкта надсилаються в десятиденний термін.

Правом здійснювати контроль щодо обсягу, достовірності та своєчасності наданої в паспорті ПНО інформації також наділені територіальні та місцеві органи державного нагляду у сфері ЦЗ. Вони також організують збирання та шоквартальне надсилання отриманих паспортів потенційно небезпечних об'єктів на адресу НДІ мікрографії для подальшого їх оброблення та внесення інформаційних даних до Державного реєстру ПНО [8].

Моніторинг ПНО здійснюється з метою отримання даних про їх поточний стан та актуалізації інформації, що міститься в базі даних Державного реєстру потенційно небезпечних об'єктів для запобігання надзвичайним ситуаціям та мінімізації їх наслідків [9].

Паспорт безпеки, ознак продукції існує також у хімічній промисловості. Зокрема, він затверджений ДСТУ 30333:2009: Паспорт безпечності хімічної продукції. Тут паспорт безпеки визначається обов'язковою складовою частиною технічної документації на хімічну продукцію (речовина, суміш, матеріал, відходи промислового виробництва) і призначений для забезпечення споживача достовірною інформацією з безпеки промислового застосування, зберігання, транспортування та утилізації хімічної продукції, а також її використання в побутових цілях [11].

Аналогом паспорту безпеки в Державній системі фізичного захисту, яка функціонує для захисту ядерних матеріалів, ядерних установок, радіоактивних відходів, інших джерел іонізуючого випромінювання, є декларація безпеки об'єктів підвищеної небезпеки (далі – ОПН). Під нею розуміють документ, який визначає комплекс заходів, що вживаються суб'єктом господарської діяльності з метою запобігання аваріям, а також забезпечення готовності до локалізації, ліквідації аварій та їх наслідків [12].

Ідентифікація об'єктів підвищеної небезпеки здійснюється суб'єктами господарської діяльності, що ними володіють. Під нею слід розуміти порядок визначення об'єктів підвищеної небезпеки серед потенційно небезпечних об'єктів.

Після ідентифікації суб'єкт господарської діяльності готує і подає до місцевих органів виконавчої влади декларацію безпеки ОПН.

Декларація безпеки складається на основі дослідження суб'єктом господарювання ступеня небезпеки та оцінки рівня ризику виникнення аварій (далі – рівня ризику), що пов'язані з експлуатацією ОПН.

Декларація включає: результати всебічного дослідження ступеня небезпеки та оцінки рівня ризику; оцінку готовності до експлуатації об'єкта підвищеної небезпеки відповідно до вимог безпеки промислових об'єктів; перелік прийнятих із метою зниження рівня ризику рішень і здійснених із метою запобігання аваріям заходів; відомості про заходи щодо локалізації і ліквідації можливих наслідків аварій.

За своїм змістом до неї входять такі складові частини:
– установчі дані. Зокрема: реєстраційний номер (код) декларації безпеки в Державному реєстрі об'єктів підвищеної небезпеки, найменування об'єкта (об'єктів) підвищеної небезпеки, код об'єкта (об'єктів) підвищеної небезпеки в Державному реєстрі об'єктів підвищеної небезпеки, повна та скорочена назва суб'єкта господарювання, форма власності, ідентифікаційний код суб'єкта господарювання, орган, до сфери управління якого належить суб'єкт господарювання, юридична адреса суб'єкта господарювання, місцезнаходження об'єкта (об'єктів) підвищеної небезпеки;

– загальні відомості про об'єкт (об'єкти) підвищеної небезпеки.

– заходи щодо забезпечення безпеки об'єкта (об'єктів) підвищеної небезпеки та локалізації і ліквідації наслідків аварій;

– результати аналізу ступеня небезпеки та оцінки рівня ризику.

– дані про розробника декларації безпеки (в разі розроблення іншим суб'єктом господарювання);

– розрахунково-пояснювальна частина.

– висновок (узагальнена оцінка ступеня небезпеки та рівня ризику виникнення аварій на об'єкті (об'єктах) підвищеної небезпеки).

Декларація безпеки, разом із позитивним висновком експертизи повноти дослідження ступеня небезпеки та оцінки рівня ризику, а також обґрунтованості та достатності прийнятих рішень щодо зменшення рівня ризику, готовності до дій із локалізації і ліквідації наслідків аварій, подається відповідним територіальним органам Держпраці, ДСНС, Держекоінспекції, державної санітарно-епідеміологічної служби, Держархбудінспекції, а також відповідній місцевій держадміністрації або виконавчому органу місцевої ради.

Місцеві держадміністрації або виконавчі органи місцевих рад протягом 30 днів після отримання декларації безпеки оприлюднюють у друкованих засобах масової інформації регіональної сфери розповсюдження відомості про об'єкт підвищеної небезпеки.

Декларація безпеки переглядається суб'єктом господарювання один раз на п'ять років.

Оригінал декларації безпеки та висновку експертизи зберігаються в суб'єкта господарювання, у власності або користуванні якого є ОПН.

Включення декларації безпеки до Державного реєстру об'єктів підвищеної небезпеки здійснюється протягом 30 робочих днів після її подання суб'єктом господарювання до територіального органу Держпраці. Територіальний орган Держпраці проводить реєстрацію декларацій безпеки з присвоєнням кожній реєстраційного номера (коду), що зазначається на її титульному аркуші.

За повноту та достовірність відомостей, поданих у декларації безпеки, суб'єкти господарювання несуть відповідальність згідно із законодавством. Подання декларації безпеки або іншої звітної документації не звільняє суб'єктів господарської діяльності від державного нагляду і контролю за їх діяльністю [13].

Контроль за наявністю на об'єктах підвищеної небезпеки декларацій безпеки та результатів ідентифікації таких об'єктів, а також за наявністю на потенційно небезпечних об'єктах результатів їх ідентифікації та паспортів потенційно небезпечних об'єктів здійснює ДСНС України [14].

Заслуговує на увагу також досвід оцінки вразливості ядерних установок та ядерних матеріалів, що проводиться групою фахівців, які входять до складу комісії з перевірки готовності системи фізичного захисту до введення в дію. Оцінка проводиться в ході функціонування системи фізичного захисту ядерної установки та ядерних матеріалів на етапах будівництва, введення в експлуатацію, експлуатації та зняття з експлуатації ядерної установки, в подальшому не рідше одного разу на 5 років та в разі зміни проектної загрози.

Інформація про проведення оцінки вразливості та корегувальні заходи, вжиті за її результатами, відображаються у плані забезпечення фізичного захисту ядерної установки та ядерних матеріалів.

За результатами проведення оцінки вразливості готується Звіт з оцінки вразливості ядерних установок та ядерних матеріалів. До його структури входять такі основні

елементи: 1. Вступ (розкриває підстави для проведення оцінки вразливості, сили та засоби проведення). 2. Опис ядерної установки (місцезнаходження та характеристики установки, цілі правопорушників). 3. Загрози ядерній установці (об'єктова проектна загроза, криміногенна ситуація). 4. Організація фізичного захисту ядерної установки (план забезпечення фізичного захисту, характеристики системи фізичного захисту, об'єктовий план взаємодії). 5. Сценарій дій правопорушників (зовнішніх та внутрішніх правопорушників). 6. Здатність системи фізичного захисту та об'єктового плану взаємодії протистояти (включає ризики під час здійснення конкретного сценарію дій правопорушників, вразливі цілі правопорушників, виявлені під час проведення оцінки вразливості). 7. Ефективність системи фізичного захисту за результатами оцінки вразливості. 8. Рекомендації з удосконалення системи фізичного захисту [15].

Персонально відповідальним за проведення оцінки вразливості є керівник експлуатуючої організації чи ліцензіата.

Підняття на якісно новий рівень боротьби з тероризмом в Україні вимагає вдосконалення механізму функціонування загальнодержавної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків. З метою запобігання терористичній діяльності існує необхідність у підвищенні ефективності систем і режимів охорони найбільш уразливих об'єктів можливих терористичних посягань, у тому числі шляхом розроблення та впровадження уніфікованих стандартів, правил, технічних умов і вимог, обов'язкового оформлення паспортів антитерористичної захищеності таких об'єктів.

Тому зовсім нещодавно (березень 2019 р.) на рівні підзаконних актів Президента України запроваджено розроблення «паспорту антитерористичної захищеності найбільш уразливого об'єкта можливих терористичних посягань». Під ним законодавець розуміє документ із відомостями про призначення такого об'єкта, особливості його розташування, основні технічні характеристики та систему захисту тощо. Він є обов'язковим для врахування під час побудови системи антитерористичного забезпечення [16].

У світі також існує практика здійснення подібних заходів для гарантування безпеки об'єктів критичної інфраструктури.

Так, в Іспанії передбачено розроблення Національного каталогу критичної інфраструктури [17]. Каталог має гриф обмеження доступу «таємно», оскільки містить інформацію про всі найважливіші об'єкти на території країни (понад 3500), їх місцезнаходження, право власності, їх послуги, необхідний для них рівень забезпечення безпеки.

Для підвищення безпеки та антитерористичної захищеності основних об'єктів іспанської економіки, відповідно до назрілих проблем у сфері державної безпеки та зважаючи на директиву Європейської комісії від 20 жовтня 2004 р., був створений Національний центр захисту критичної інфраструктури (ісп., Centro Nacional de Protección de Infraestructuras Críticas, CNPIC) [18]. CNPIC забезпечує цілодобовий моніторинг об'єктів КІ, таких як дороги, електроенергія або водопостачання та продовольство, що входять до каталогу критичної інфраструктури. Фахівці займаються спостереженням за фізичною і ІТ-безпекою, сприяють підвищенню стійкості і надійності мереж електронного зв'язку. CNPIC забезпечує керівництво, координацію дій залучених учасників та контроль за захистом національної критичної інфраструктури.

Розроблення паспортів безпеки для об'єктів паливно-енергетичного комплексу передбачено і в законодавстві Російської Федерації. Паспорт безпеки об'єкта паливно-енергетичного комплексу – документ, що містить інформацію про забезпечення антитерористичної захищеності

об'єкта паливно-енергетичного комплексу і план заходів щодо забезпечення антитерористичної захищеності об'єкта [19]. Такий документ складається на підставі результатів категоризації об'єкта в залежності від ступеня його потенційної небезпеки, а також на підставі оцінки достатності інженерно-технічних заходів, заходів із фізичного захисту і охорони об'єкта від терористичних загроз. У паспорті безпеки об'єкта паливно-енергетичного комплексу відображаються характеристика об'єкта, можливі наслідки в результаті здійснення акту незаконного втручання, категорія об'єкта, стан системи інженерно-технічного, фізичної захисту, пожежної безпеки, а також містяться відповідні висновки та рекомендації.

Захист промислових об'єктів і об'єктів інфраструктури від терористичних дій здійснюється спеціально уповноваженими на це органами виконавчої влади та спецслужбами. Планування заходів щодо попередження терористичних акцій і локалізації їх наслідків здійснюється на підставі паспорта безпеки адміністративно-територіальних одиниць, що розробляється відповідним органом виконавчої влади відповідно до вимог законодавства [20].

Планування заходів безпеки об'єктів КІ у Франції здійснює Підрозділ з державного захисту та безпеки (PSE). Французький підхід також базується на управлінні ризиками та попередженні загроз, розробленні планів реагування та обміну інформації між учасниками. Генеральний секретаріат із питань оборони та національної безпеки (SGDSN) аналізує відкриту інформацію та розвідані спецслужб у сфері захисту КІ, слідкує за недопущенням загроз.

У Німеччині акцент у захисті об'єктів КІ зміщений на захист економічної інформації, протидії розвіддільності організованих спецслужбами іноземних держав, протидії кібершпигунству [21].

У США узагальнення інформації, подібної за змістом до тієї, що має систематизуватися в паспортах безпеки об'єктів КІ, здійснюється Управлінням захисту критичної інфраструктури Департаменту внутрішньої безпеки (Office of Infrastructure Protection DHS, IP). Збір даних, необхідних для швидкого реагування на основні загрози та подальшого відновлення функціонування об'єктів КІ у разі їх ураження, здійснює у складі Управління підрозділ збору інфраструктурної інформації (The Infrastructure Information Collection Division, IICD). IICD також є власником своєрідного шлюзу захисту інфраструктури США (Infrastructure Protection Gateway), який є єдиним програмним інтерфейсом, через який усі партнери DHS можуть отримати доступ до цілого ряду інтегрованих програмних інструментів і даних щодо комплексної оцінки уразливості та аналізу ризиків об'єктів КІ [22]. Основною метою такої діяльності IP DHS є забезпечення стійкості КІ США, визначення нових видів загроз, проведення оцінки уразливостей і наслідків ураження об'єктів КІ [23].

Висновки. Таким чином, аналіз світового досвіду, наявних наукових напрацювань, чинної нормативно-правової бази та результати даного дослідження автора дають підстави стверджувати про доцільність розроблення та впровадження в Україні паспорта безпеки об'єкта критичної інфраструктури як важливого елемента в побудові державної системи захисту об'єктів критичної інфраструктури.

В українському законодавстві поняття паспорта безпеки не є новим. Такий термін чи подібні йому за змістом зустрічаються в державних системах реагування та захисту, зокрема: системі фізичного захисту, цивільного захисту та протидії тероризму. Тому під час його створення в державній системі захисту критичної інфраструктури доцільно використовувати напрацювання, що вже існують у згаданих інших сферах.

Метою складання паспортів безпеки об'єктів критичної інфраструктури має стати попередження та швидке припинення загроз, а також оцінка і мінімізація можливих ризиків негативних наслідків від їх прояву для об'єктів критичної інфраструктури, визначення напрямів забезпечення їх безпеки, сил та засобів необхідних для цього.

Практика застосування документу, що містить дані про об'єкт критичної інфраструктури та заходи гарантування їх безпеки, є поширеною у світі. Аналіз досвіду США, Німеччини, Франції, РФ чи Іспанії свідчить, що це можуть бути різні за формою документи, від каталогів критичної інфраструктури та електронних баз даних до безпосередньо паспортів безпеки об'єктів. Водночас основною метою їх створення є визначення загроз та ризиків, оцінка уразливостей і наслідків ураження об'єктів КІ для забезпечення стійкості КІ.

Сьогодні в Україні вимоги до паспорта безпеки об'єкта критичної інфраструктури не визначені.

Нами вважається, що паспортом безпеки об'єкта критичної інфраструктури має стати документ визначеної форми, що містить інформацію про окремих об'єкт критичної інфраструктури, яка є важливою для організації захисту та планування заходів із недопущення чи мінімізації загроз і забезпечення стійкості об'єкта критичної інфраструктури, а також обов'язковий для врахування під час побудови системи захисту об'єктів критичної інфраструктури.

Паспортизація об'єкта критичної інфраструктури – встановлений порядок оформлення і надання паспорта безпеки такому об'єкту. Вона має проводитись відповідно до переліків об'єктів критичної інфраструктури, які складаються на підставі результатів процедури розпізнавання об'єктів критичної інфраструктури. Після проведення паспортизації дані щодо об'єктів критичної інфраструктури мають вноситись до Державного реєстру об'єктів критичної інфраструктури. Державний реєстр об'єктів критичної інфраструктури – автоматизована система обліку та оброблення інформації щодо об'єктів критичної інфраструктури.

Ураховуючи викладене, з метою створення ефективної системи реагування на загрози та захисту об'єктів критичної інфраструктури, доцільно:

– здійснити розроблення та впровадження алгоритму паспортизації та категоризації об'єктів;

– визначитись із доцільністю включення до структурованих даних паспорта безпеки об'єкта критичної інфраструктури вимог щодо врахування всіх видів загроз (природного та техногенного характеру, кіберзагроз та загроз виникнення дій терористичного характеру, а також від зловмисних дій);

– розглянути доцільність створення Єдиної інформаційної системи функціонування об'єктів критичної інфраструктури в Україні з урахуванням досвіду США. Вона може мати програмний інтерфейс для доступу визначених користувачів до цілого ряду інтегрованих програмних інструментів та даних щодо комплексної оцінки уразливості та аналізу ризиків об'єкту КІ. У цьому випадку окремим її фрагментом міг би бути розділ, присвячений створенню паспортів безпеки;

– розробити основні вимоги та завдання для створення Державного реєстру об'єктів критичної інфраструктури як бази даних, що міститиме велику кількість актуальної інформації про об'єкти КІ та буде функціонувати у складі захищеної, відповідно до вимог з технічного захисту інформації, автоматизованої паспортної системи. За зразок під час створення паспортів пропонується розглянути форму і зміст паспортів ПНО Державного реєстру потенційно небезпечних об'єктів (містить актуальну інформацію про понад 26500 ПНО та перевищує дані інших інформаційних

ресурсів, таких як Державний реєстр об'єктів підвищеної небезпеки, Реєстр об'єктів утворення, оброблення та утилізації відходів, реєстри місць видалення відходів та інші);

– передбачити розроблення заходів із паспортизації об'єкта одночасно з визначенням загроз для економіки держави, загроз для певного сектору економіки та безпосередньо об'єкта;

– за визначення наявних та потенційних загроз для об'єктів КІ покласти спільну відповідальність на операторів КІ, органи безпеки та відповідні органи державної влади;

– визначити державний контролюючий орган, відповідальний за створення паспортів безпеки.

Таким чином, паспорт безпеки має стати не лише обов'язковим елементом у побудові системи захисту об'єктів критичної інфраструктури, а й основою у плануванні захисту кожного такого об'єкта та забезпеченні його стійкості.

Список використаної літератури:

1. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 06 грудня 2017 р. № 1009-р. / Кабінет Міністрів України. *Офіційний вісник України*. 23.01.2018. 2018 р. № 7. С. 39. Стаття 271. Код акта 88807/2018.

2. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: ДДУВС, 2018. 180 с.

3. Про затвердження рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015 / Президента України. *Урядовий кур'єр*. 29.05.2015. № 95.

4. Про затвердження рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України»: Указ Президента України від 14 березня 2016 року № 92/2016 / Президент України. *Урядовий кур'єр*. 18.03.2016. № 52

5. Про уведення в дію рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України»: Указ Президента України від 24 вересня 2015 року № 555/2015 / Президент України. *Урядовий кур'єр*. 26.09.2015. № 178.

6. Про уведення в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури»: Указ Президента України від 16 січня 2017 р. № 8/2017 / Президент України. *Урядовий кур'єр*. 18.01.2017. № 9.

7. Про уведення в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року № 96/2016 / Президент України. *Урядовий кур'єр*. 18.03.2016. № 52.

8. Про затвердження Положення про паспортизацію потенційно небезпечних об'єктів: Наказ Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків чорнобильської катастрофи від 18.12.2000 № 338 / МНС. *Офіційний вісник України*. 09.02.2001 р. № 4. С. 345, стаття 164, код акта 17659/2001.

9. Про затвердження Положення про моніторинг потенційно небезпечних об'єктів: Наказ Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків чорнобильської катастрофи від 06.11.2003 № 425 / МНС. *Офіційний вісник України*. 09.01.2004 – 2003 р., № 52, том 2, с. 610, стаття 2857, код акта 27319/2003.

10. Про страховий фонд документації України: Закон України від 22 березня 2001 р. № 2332-III. *Голос України*. 27.04.2001. № 76.

11. ДСТУ ГОСТ 30333: 2009. Паспорт безпечності хімічної продукції. Загальні вимоги (ГОСТ 30333-2007, IDT). Затверджений Наказом Технічного комітету зі стандартизації від 15.10.2009. № 376. Про надання чинності в Україні міждержавним стандартам, змінам до міждержавних стандартів та скасування нормативних документів.

12. Про об'єкти підвищеної небезпеки: Закон України від 18.01.2001 р. № 2245-III / Верховна Рада України. *Урядовий кур'єр*. 07.03.2001. № 43.

13. Про ідентифікацію та декларування безпеки об'єктів підвищеної небезпеки: Постанова Кабінету Міністрів України від 11 липня 2002 р. № 956 / Кабінет Міністрів України. *Урядовий кур'єр*. 24.07.2002. № 133.

14. Деякі питання Державної служби України з надзвичайних ситуацій: Указ Президента України від 16 січня 2013 р. № 20/2013 / Президент України. *Урядовий кур'єр*. 22.01.2013. № 13.

15. Про затвердження Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів : Наказ Державного комітету ядерного регулювання України від 30.11.2010 № 169 / Державний комітет ядерного регулювання України. *Офіційний вісник України*. 04.01.2011 - 2010 р. № 100. Стор. 165. Стаття 3582. Код акта 54129/2010.

16. Про концепцію боротьби з тероризмом в Україні : Указ Президента України від 5 березня 2019 р. № 53/2019 / Президент України. *Урядовий кур'єр*. 2019. № 48.

17. Офіційний сайт Національного центру захисту критичної інфраструктури Іспанії. URL : <http://www.cnpic.es>.

18. Офіційний сайт Міністерства Внутрішніх Справ Іспанії. URL : <http://www.interior.gob.es>.

19. О безопасности объектов топливно-энергетического комплекса : Закон РФ. Принят Государственной Думой 6 июля 2011 года.

20. ГОСТ Р 22.2.03-97. Безопасность в чрезвычайных ситуациях / Держстандарт Російської Федерації : Постанова Держстандарту Російської Федерації від 28.01.1997 р. № 21.

21. Офіційний сайт Федерального відомства з охорони Конституції Німеччини. URL : <https://www.verfassungsschutz.de>.

22. Офіційний сайт Міністерства внутрішньої безпеки США. URL : <https://www.dhs.gov/iicd>.

23. Офіційний сайт Міністерства внутрішньої безпеки США. URL : <https://www.dhs.gov/national-protection-and-programs-directorate>.

ІНФОРМАЦІЯ ПРО АВТОРА

Єрменчук Олександр Петрович – кандидат юридичних наук, доцент кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ Міністерства внутрішніх справ України

INFORMATION ABOUT THE AUTHOR

Yermenchuk Oleksandr Petrovych – Candidat of Law Sciences, Associate Professor of the Department of Operational and Investigative Activity of Dnipropetrovsk State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine

eop242012@gmail.com