

DOI: 10.6084/m9.figshare.11969007

УДК 502.55

Хрутьба Вікторія Олександрівна

Доктор технічних наук, доцент, завідувач кафедри екології та безпеки життєдіяльності, orcid.org/0000-0002-8121-2042

Національний транспортний університет, Київ

Зюсюн Вадим Ігорович

Кандидат технічних наук, доцент кафедри екології та безпеки життєдіяльності, orcid.org/0000-0001-6566-8798

Національний транспортний університет, Київ

Нєведров Дмитро Сергійович

Аспірант кафедри екології та безпеки життєдіяльності, orcid.org/0000-0001-7213-6159

Національний транспортний університет, Київ

Лисак Роксолана Станіславівна

Аспірант кафедри екології та безпеки життєдіяльності, orcid.org/0000-0002-2776-5623

Національний транспортний університет, Київ

ФОРМУВАННЯ МЕТОДІВ УПРАВЛІННЯ ПРОЄКТАМИ ТА ПРОГРАМАМИ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

***Анотація.** Критична інфраструктура включає об'єкти різних секторів економіки. Ці об'єкти є стратегічними для держави, і як наслідок, вразливими, тому потребують особливого захисту. Запропоновано критерії ідентифікації об'єктів критичної інфраструктури та їх деталізацію. Розглянуто деталізований метод ідентифікації об'єктів критичної інфраструктури. Розроблено метод до формування регіональних програм безпеки об'єктів критичної інфраструктури та здійснено деталізацію процесів управління таким типом програм, на основі формування стратегічних завдань та їх декомпозиції в питанні управління ризиками та загрозами для об'єктів критичної інфраструктури. Такі програми будуть спрямовані на попередження ризикових ситуацій та загроз, які можуть супроводжувати весь життєвий цикл функціонування об'єктів критичної інфраструктури, адже найкращий захист – це попередження виникнення небезпечних ситуацій для об'єктів критичної інфраструктури, як природного так і техногенного характеру.*

***Ключові слова:** транспорт; безпека; об'єкт; критична інфраструктура; програма; програмне середовище; проєкт; захист*

Вступ

Питанню захисту критичної інфраструктури приділяється значна увага в країнах ЄС та світу [1]. У 2004 р. Європейська Рада висунула вимогу щодо підготовки загальної стратегії охорони та захисту критичної інфраструктури (КІ). У відповідь на це Комісія ухвалила Повідомлення про охорону та захист КІ в рамках боротьби проти тероризму, в якому було викладено пропозиції щодо можливих заходів ЄС щодо попередження, підготованості та реагування на терористичні акти, пов'язані з КІ.

На початку 2005 р. Комісія ухвалила Зелену книгу з питань європейської програми охорони та захисту КІ, що визначала кілька варіантів політики щодо створення такої програми та Інформаційної мережі попередження щодо загроз критичній інфраструктурі. В отриманих відгуках на Зелену книгу наголошувались додаткові переваги рамок ЄС щодо охорони та захисту КІ. Визнана необхідність

покращення охорони та захисту КІ в Європі та зниження рівня вразливості об'єктів критичної інфраструктури.

В грудні 2005 р. Рада юстиції та внутрішніх справ звернулася до Комісії з проханням внести пропозицію щодо Європейської програми охорони та захисту критичної інфраструктури (програма ЕРСІР) та вирішила, що вона повинна враховувати всі небезпеки і що її пріоритетом має бути протидія терористичним загрозам. Згідно з цим підходом у процесі охорони та/або захисту КІ необхідно враховувати техногенні, технологічні загрози і стихійні лиха, проте пріоритет надається загрози тероризму.

У квітні 2007 р. Рада схвалила висновки щодо програми ЕРСІР, нагадуючи, що держави-члени несуть цілковиту відповідальність за управління механізмами охорони та захисту КІ в межах національних кордонів, вітаючи зусилля Комісії з розроблення європейської процедури ідентифікації

та визначення європейських об'єктів критичної інфраструктури (ЄКІ), а також оцінювання необхідності покращення їх охорони та захисту [3].

Якщо говорити про Україну, то на сьогодні її законодавчо-нормативна документація не забезпечує необхідного рівня захисту об'єктів критичної інфраструктури, адже Закон України «Про критичну інфраструктуру та її захист» перебуває на стадії розгляду, а більшість вчених у своїх дослідженнях посилаються на міжнародний досвід у питанні захисту критичної інфраструктури.

19 квітня 2019 року відбулось засідання Міжвідомчої експертної групи з питань захисту критичної інфраструктури під головуванням Міністра економічного розвитку і торгівлі України С. Кубіва [4]. Було зазначено, що наразі в Україні єдина державна система захисту критичної інфраструктури сформована неповністю, а забезпечення захисту стратегічно важливих державних об'єктів здійснюється несистемно. Тому разом слід докорінно змінити підходи до захисту об'єктів та ресурсів, які становлять критично важливі елементи системи і є важливими для функціонування держави. Робота експертної групи повинна напрацювати дієві інструменти для вирішення проблемних питань у цій сфері до прийняття Верховною Радою відповідного законопроекту. Слід створити дієві механізми запобігання загрозам на стратегічно важливих інфраструктурних об'єктах. Для цього потрібна низка важливих рішень у різних сферах, якісна координація та взаємодія між цілою низкою державних органів, установ та організацій.

Кубів С. зазначив про важливість забезпечення якісного моніторингу та оцінки стану безпеки і захисту об'єктів критичної інфраструктури, визначення дієвого режиму функціонування державної системи захисту критичної інфраструктури, а також необхідність розроблення та внесення змін до чинного законодавства України, включаючи цілком нові нормативні документи.

Вищезазначені фактори ще раз підтверджують важливість і необхідність дослідження питань, пов'язаних з критичною інфраструктурою.

Тому для загальної безпеки держави необхідно розробити і мати у повсякденному використанні процедури ідентифікації об'єктів критичної інфраструктури, а також сприяти активному формуванню та реалізації регіональних програм безпеки об'єктів критичної інфраструктури (РПБОКІ). Крім того, важливою задачею є вироблення єдиного підходу для оцінювання необхідності покращення охорони та захисту об'єктів критичної інфраструктури з метою сприяння захисту населення та формування стабільного економічного становища держави.

Аналіз останніх досліджень і публікацій

За останні роки питання функціонування об'єктів критичної інфраструктури та її захисту розглядалося у низці робіт, зокрема, Д.С. Бірюкова [5], С.О. Гнатюка [6], О.М. Суходолі, Ю.І. Бабича, Ю.П. Рака, О.Б. Зачка [6; 11], В.М. Лядовської [7], В.О. Євсєєва [8],

В.Г. Ковальова, Н.М. Цабенко, М.А. Потеєвої [9]. Питання програмного та проектного управління представлені в роботах С.Д. Бушуєва [10], Н.С. Бушуєвої, В.А. Рача, Ф.А. Ярошенка [10], Х. Танаки [10].

Мета статті

Метою роботи є розроблення процедури ідентифікації об'єктів критичної інфраструктури та формування регіональних програм безпеки об'єктів критичної інфраструктури, а також вироблення єдиного підходу для оцінювання необхідності покращення охорони та захисту таких інфраструктур з метою сприяння захисту населення та формування стабільного економічного становища держави.

Виклад основного матеріалу

Всі визначені об'єкти КІ повинні мати ухвалені інструменти безпеки (ІБ), або аналогічні інструменти ідентифікації важливих об'єктів, оцінювання ризиків й ідентифікації, відбору та встановлення пріоритетності запобіжних заходів і процедур в рамках РПБОКІ.

Інструменти, принципи, настанови, в тому числі інструменти ЄС і двосторонні та/або багатосторонні схеми співпраці, що передбачають наявність плану, аналогічних або рівноцінних ІБ, або координатора з питань безпеки, чи іншої аналогічної відповідальної особи, повинні вважатися такими, що задовольняють вимоги підходу, що розробляється з питань безпеки.

Координатори з питань безпеки мають бути ідентифіковані для всіх визначених об'єктів критичної інфраструктури (ОКІ) з метою сприяння співпраці та комунікаціям з відповідними державними органами охорони та захисту критичної інфраструктури.

Ефективна ідентифікація ризиків, загроз і вразливостей конкретних секторів економіки держави вимагає комунікації як між координаторами на ОКІ, так і між державними установами, які займаються питаннями розроблення та впровадження РПБОКІ. Кожний координатор ОКІ повинен збирати інформацію про ОКІ, розміщену на її території. Державні контролюючі органи мають отримувати загальну інформацію від координаторів конкретних ОКІ про ризики, загрози та вразливості

для ОКІ, в тому числі у відповідних випадках, інформацію про можливі покращення рівня безпеки ОКІ та загального розвитку об'єкта в цілому.

Задля сприяння покращенню охорони та захисту ОКІ слід розробити та мати загальні методи ідентифікації та класифікації ризиків, загроз та вразливостей об'єктів інфраструктури.

Координаторам з питань безпеки на ОКІ необхідно надавати доступ до кращих практик та методик стосовно охорони та захисту критичних інфраструктур переважно через відповідні державні органи забезпечення.

Передусім при формуванні методів управління проектами та програми безпеки об'єктів критичної інфраструктури необхідно визначитися із формулюванням основних термінів, а саме:

1) критична інфраструктура – це об'єкти, порушення функціонування або руйнування яких призведе до найсерйозніших наслідків для соціальної та економічної сфери держави, негативно вплине на рівень її обороноздатності та національної безпеки, а також підтримання життєво важливих функцій в суспільстві [12];

2) аналіз ризиків та загроз означає розгляд відповідних сценаріїв загроз з метою оцінки вразливості і потенційного впливу порушення функціонування або знищення ОКІ;

3) інформація групи «S», яка стосується захисту критичних інфраструктур – це факти про критичну інфраструктуру, які, в разі їх розголошення, можуть бути використані для планування та здійснення дій з наміром порушити функціонування або знищити устаткування ОКІ;

4) захист – об'єднує всі види діяльності, спрямовані на забезпечення функціональності, безперервності і цілісності критичних інфраструктур з метою недопущення, зменшення наслідків і нейтралізації загрози, ризику або вразливості;

5) регіон визначення об'єктів критичної інфраструктури – певна адміністративна одиниця (район, область, економічний регіон), в географічних межах якої може здійснюватися ідентифікація об'єктів критичної інфраструктури, а також для якого може бути розроблена регіональна програма безпеки об'єктів критичної інфраструктури.

Процедура ідентифікації об'єктів критичної інфраструктури може здійснюватися на основі критеріїв визначення ОКІ (рис. 1) та згідно алгоритму ідентифікації ОКІ (рис. 2).

Координатори в регіонах, для яких має бути розроблена РПБОКІ, повинні підтримувати постійний процес ідентифікації потенційних ОКІ, внесення їх до відповідного реєстру регіональних ОКІ. На основі цього реєстру і буде розроблятися РПБОКІ.

Інформація про потенційний ОКІ, що пройшов наведену на рис. 2 процедуру, може повідомлятися лише координаторам тих регіонів, що можуть зазнати істотного впливу цього потенційного ОКІ. Потенційні ОКІ, що не відповідають вимогам одного або кількох наведених вище критеріїв, будемо вважати такими, що «не є ОКІ» і виключаються із процедури.



Рисунок 1 – Критерії ідентифікації об'єктів критичної інфраструктури

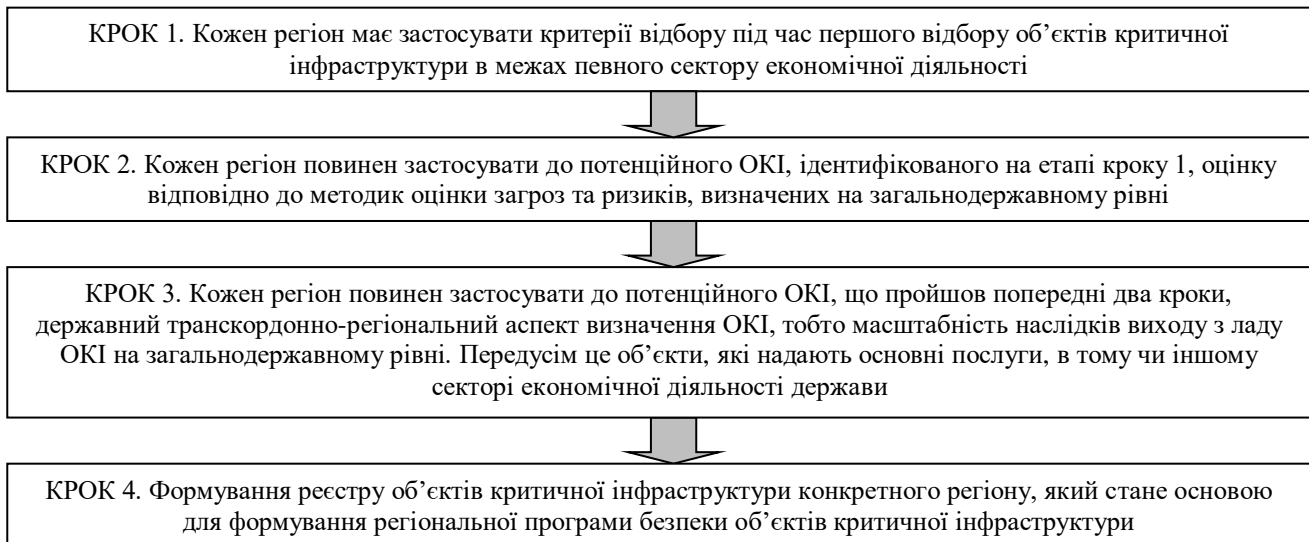


Рисунок 2 – Алгоритм ідентифікації об'єктів критичної інфраструктури

Для допомоги в процесі ідентифікації може бути створена комісія, наприклад Державна комісія з питань критичної інфраструктури (Держкомісія), яка за запитом від регіону, зможе надати допомогу їй в питаннях ідентифікації потенційних ОКІ.

Держкомісія може звернути увагу відповідного регіону на існування потенційних критичних інфраструктур, які можна вважати відповідними критеріям, необхідним для визначення як ОКІ.

На державному рівні разом з регіонами має бути розроблено настанови щодо застосування наскрізних і секторальних критеріїв, а також розраховано граничні значення, що використовуватимуться для ідентифікації ОКІ.

Граничні значення критеріїв мають визначатися з урахуванням серйозності наслідків, спричинених пошкодженням або знищенням конкретної інфраструктури. Точні граничні значення критеріїв мають визначатися для конкретних об'єктів кожного із секторів економічної діяльності держави. Кожен регіон повинен щорічно звітувати про кількість інфраструктур в кожному секторі, щодо яких проводилися обговорення про граничні значення критеріїв.

Ще одним важливим фактором є інформація групи «S», пов'язана із захистом об'єктів критичної інфраструктури. Будь-яка особа, яка має справу з секретною інформацією від імені регіону або на керівному державному рівні, повинна пройти перевірку благонадійності відповідного рівня.

Координатори в регіонах і відповідні наглядові органи повинні гарантувати, що інформація групи «S», пов'язана із захистом ОКІ, надана регіонами, не використовується для жодних інших цілей, крім охорони та захисту об'єктів критичних інфраструктур.

Наступним етапом у питанні захисту критичної інфраструктури є розроблення регіональних програм безпеки об'єктів критичної інфраструктури.

Розробляючи РПБОКІ, необхідно ідентифікувати об'єкти критичної інфраструктури та сформулювати рішення із забезпечення безпеки, що вже існують або ще впроваджуються для їх охорони та захисту. Мінімальний зміст процедури розробки РПБОКІ наведено нижче.

РПБОКІ міститиме в собі дані про ідентифіковані об'єкти критичної інфраструктури та рішення для забезпечення безпеки, що вже існують або впроваджуються для їх охорони та захисту. Процедура розроблення РПБ для ОКІ охопить щонайменше:

- опрацювання реєстру ідентифікованих об'єктів критичної інфраструктури;
- проведення аналізу ризиків та загроз на основі сценаріїв головних загроз, ступеня вразливості кожного об'єкта;
- ідентифікацію, відбір та встановлення пріоритетності запобіжних заходів і процедур, що поділяються на: 1) постійні заходи забезпечення безпеки, що ідентифікують необхідні рівні фінансування та механізми захисту, що повинні застосовуватися на всіх етапах. Цей підпункт включатиме інформацію про загальні заходи, такі як технічні заходи (у т. ч. встановлення засобів виявлення, контролю доступу, захисту, попередження); організаційні заходи (у т. ч. процедури попередження про небезпеку, управління кризами); заходи контролю і верифікації; комунікації; підвищення рівня обізнаності й підготовки; безпеку інформаційних систем; 2) поетапні заходи забезпечення безпеки, що активуються залежно від рівнів ризику і загроз.

Координатори кожного визначеного регіону повинні перевірити наявність ІБ або аналогічних інструментів, спрямованих на вирішення питань, пов'язаних із захистом ОКІ.

Якщо координатори регіону встановили, що ІБ або аналогічні інструменти не були розроблені, вона повинна будь-якими методами, на їх думку доцільними, забезпечити підготовку РПБОКІ в терміновому порядку.

Для забезпечення ефективного захисту ОКІ бажано відразу з моменту визначення критичної інфраструктури як ОКІ розпочати розроблення механізмів захисту, а саме: розробки РПБОКІ, а також впевнитися в їх регулярному її перегляді та доповненні.

Висновки

В роботі запропоновано критерії ідентифікації об'єктів критичної інфраструктури та розглянуто деталізований метод ідентифікації об'єктів критичної інфраструктури. Розроблено метод до формування регіональних програм безпеки об'єктів критичної інфраструктури та здійснено деталізацію процесів управління даним типом програм, на основі формування стратегічних завдань та їх декомпозиції в питанні управління ризиками та загрозами для об'єктів критичної інфраструктури. Такі програми будуть спрямовані на попередження ризикових ситуацій та загроз, які можуть супроводжувати весь життєвий цикл функціонування об'єктів критичної інфраструктури на регіональному рівні, як природного так і техногенного характеру.

Список літератури

1. Хрутьба В.О. *Огляд науково-теоретичних аспектів безпеки об'єктів критичної інфраструктури транспорту* / В.О. Хрутьба, В.І. Зюзюн, Д.С. Неведров // *Вісник Національного технічного університету «ХПИ»*. Серія : *Стратегічне управління, управління портфелями, програмами та проектами* . – 2019. – № 2. – С. 60 – 65.
2. *Зелена книга з питань захисту критичної інфраструктури в Україні* : збірник матеріалів міжнародної експертної наради / Упоряд. Д.С. Бірюков, С.І. Кондратов ; за заг. ред. О.М. Суходолі. – К. : НІСД, 2016. – 176 с.
3. *Директива Ради Європи № 2008/114/ЄС. Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту*. – 2008.
4. *Міжвідомча робоча група почала роботу над створенням єдиної державної системи захисту критичної інфраструктури*. Урядовий портал. Міністерство економічного розвитку і торгівлі України: веб-сайт. URL: <https://www.kmi.gov.ua> (дата звернення: 26.04.2019).
5. Бірюков Д.С. *Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики* / Д.С. Бірюков // *Науково-інформаційний вісник Академії національної безпеки*. – 2015. – № 3-4. – С. 155 – 170.
6. Зачко О.Б. *Моделі управління безпекою інфраструктурних проектів на стадії планування* / О.Б. Зачко, Д.С. Кобилкін, Р.Р. Головатий // *Вісник Національного технічного університету «ХПИ»*. Серія : *Стратегічне управління, управління портфелями, програмами та проектами* . – 2019. – № 2. – С. 43 – 49.
7. *Лядовська В.М. Визначення критичної інформаційної інфраструктури та її захист: аналіз підходів* / В.М. Лядовська, М.О. Рябий, С.О. Гнатюк // *Зв'язок*. – 2014. – №4. – С. 3 – 7.
8. *Євсєєв В.О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду* / В.О. Євсєєв // *Збірник наукових праць Харківського національного університету Повітряних Сил*. – 2016. – № 4(49). – С. 168 – 172.
9. *Потєєва М.А. Удосконалення механізму державного регулювання транспортної інфраструктури України* / М.А. Потєєва // *Продуктивні сили і регіональна економіка*. – 2008. – Ч. 2. – С. 127 – 133.
10. *Ярошенко Ф.А. Управление инновационными проектами и программами на основе системы знаний Р2М: монография* / Ярошенко Ф.А., Бушуев С.Д., Танака Х. – К.: «Саммит-Книга», 2012. – 272 с.
11. *Зачко, О.Б. Теоретические подходы к управлению безопасностью в проектах развития сложных систем* / О.Б. Зачко // *Управління розвитком складних систем*. – 2015. – № 22 (1), – С. 48 – 53.
12. *Khurutba V. Formation of mechanisms of management of regional programs for safety of objects of critical infrastructure of transportation* / V. Khurutba, V. Ziuziun, D. Nevedrov // *Scientific letters of Academic society of Michal Baludansky*. – 2019. – № 7. – P. 69 – 74.

Стаття надійшла до редколегії 03.10.2019

Хрутьба Виктория Александровна

Доктор технических наук, доцент, заведующая кафедрой экологии и безопасности жизнедеятельности, orcid.org/0000-0002-8121-2042

Национальный транспортный университет, Киев

Зюзюн Вадим Игоревич

Кандидат технических наук, доцент кафедры экологии и безопасности жизнедеятельности, orcid.org/0000-0001-6566-8798

Национальный транспортный университет, Киев

Неведров Дмитрий Сергеевич

Аспирант кафедры экологии и безопасности жизнедеятельности, orcid.org/0000-0001-7213-6159

Национальный транспортный университет, Киев

Лысак Роксолана Станиславовна

Аспирант кафедры экологии и безопасности жизнедеятельности, orcid.org/0000-0002-2776-5623

Национальный транспортный университет, Киев

**ФОРМИРОВАНИЕ МЕТОДОВ УПРАВЛЕНИЯ ПРОЕКТАМИ И ПРОГРАММАМИ БЕЗОПАСНОСТИ
ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ**

Аннотация. Критическая инфраструктура включает объекты различных секторов экономики. Данные объекты являются стратегическими для государства, и как следствие, уязвимыми, поэтому нуждаются в особой защите. Предложены критерии идентификации объектов критической инфраструктуры и их детализация. Рассмотрен детализированный метод идентификации объектов критической инфраструктуры. Разработан метод формирования региональных программ безопасности объектов критической инфраструктуры и осуществлена детализация процессов управления данным типом программ на основе формирования стратегических задач и их декомпозиции в области управления рисками и угрозами для объектов критической инфраструктуры. Данные программы будут направлены на предупреждение рискованных ситуаций и угроз, которые могут сопровождать весь жизненный цикл функционирования объектов критической инфраструктуры, поскольку лучшая защита – это предупреждение возникновения опасных ситуаций для объектов критической инфраструктуры, как природного так и техногенного характера.

Ключевые слова: транспорт; безопасность; объект; критическая инфраструктура; программа; программная среда; проект; защита

Khrutba Viktoriia

DSc (Eng.), Associate Professor, Head of Ecology and Safety of Vital Function, orcid.org/0000-0002-8121-2042

National Transport University, Kyiv

Ziuziun Vadym

PhD (Eng.) Associate Professor, Department of Ecology and Safety of Vital Function, [rcid.org/0000-0001-6566-8798](https://orcid.org/0000-0001-6566-8798)

National Transport University, Kyiv

Nevedrov Dmytro

Postgraduate student, Department of Ecology and Safety of Vital Function, orcid.org/0000-0001-7213-6159

National Transport University, Kyiv

Lysak Roksolana

Postgraduate student, Department of Ecology and Safety of Vital Function, orcid.org/0000-0002-2776-5623

National Transport University, Kyiv

**FORMATION OF METHODS OF PROJECT MANAGEMENT
AND CRITICAL INFRASTRUCTURE OBJECTS SECURITY PROGRAM**

Abstract. The critical infrastructure includes objects in different sectors of the economy. These objects are strategic for the state, and as a consequence, vulnerable, therefore, need special protection. In the article criteria of identification of objects of critical infrastructure and their detailing are offered. The article deals with the detailed method of identifying objects of critical infrastructure. A method has been developed for the formation of regional security programs for critical infrastructure objects and a detailed description of the management processes of this type of program, based on the formation of strategic tasks and their decomposition in the area of risk management and threats for critical infrastructure objects. These programs will be aimed at preventing risk situations and threats that may accompany the entire lifecycle of critical infrastructure objects, since the best protection is the prevention of emergencies for critical infrastructure objects, both natural and man-made.

Keywords: transport; safety; object; critical infrastructure; program; software; project; protection.

References

1. Khrut'ba, V.O., Ziuziun, V.I., Nieviedrov, D.S. (2019). Review of scientific and theoretical aspects of safety of objects of critical infrastructure of transport. Bulletin of National technical university «KHPI». Seria : Strategic management, 2, 60 – 65.
2. Birjukov, D.S., Kondratov, S.I. (2016). Green Book on Critical Infrastructure Protection in Ukraine: a collection of materials for the international expert meeting. Kyiv, NISD, 176.
3. Council Directive 2008/114 / EC. On the identification and definition of European critical infrastructures and the assessment of the need to improve their protection and protection.
4. Mizhvidomcha robocha hrupa pochala robotu nad stvorennjam jedynoji derzhavnoji systemy zakhystu krytychnoyi infrastruktury. Urjadovyy portal. Ministerstvo ekonomichnoho rozvytku i torhivli Ukrainy, URL: <https://www.kmu.gov.ua> (accessed 26.04.2019).

5. Birjukov, D.S. (2015). *Protecting critical infrastructure in Ukraine: from scientific thinking to policy formulation*. *Naukovo-informacijnyj visnyk Akademiji nacional'noji bezpeky*, 3-4, 155 – 170.
 6. Zachko, O.B., Kobylkin, D.S., Holovatyj, R.R. (2019). *Models of safety management of infrastructure projects at the planning stage*. *Bulletin of National technical university «KHPI» Seria : Strategic management*, 2, 43 – 49.
 7. Ljadovs'ka, V.M. (2014). *Definition of critical information infrastructure and its protection: analysis of approaches*. *Zv'jazok*, 4, 3-7.
 8. Jevsjejev, V.O. (2016). *Possible ways to improve the protection of critical infrastructure of Ukraine in the light of world experience*. *Zbirnyk naukovykh prac' Harkivs'kogo nacional'nogo universytetu Povitrjanyh Syl*, 4 (49), 168 – 172.
 9. Potejeva, M.A. (2008). *Improvement of the mechanism of state regulation of transport infrastructure of Ukraine*. *Produktyvni syly i regional'na ekonomika*, 2, 127 – 133.
 10. Jaroshenko, F.A., Bushuev, S.D., Tanaka, H. (2012). *Management of innovative projects and programs based on P2M knowledge system: monograph*. Kyiv, Sammit-Book, 272.
 11. Zachko, Oleg. (2015). *Theoretical Approaches To Safety Management In The Projects Of Development Of Complex Systems*. *Management of Development of Complex Systems*, 22 (1), 48 – 53.
 12. Khrutba, V., Ziuziun, V., Nevedrov, D. (2019). *Formation of mechanisms of management of regional programs for safety of objects of critical infrastructure of transportation*. *Scientific letters of Academic society of Michal Baludansky*, 7, 69 – 74.
-

Посилання на публікацію

- APA Khrutba, Viktoriia, Ziuziun, Vadym, Nevedrov, Dmitro & Lysak, Roksolana. (2019). *Formation of methods of project management and critical infrastructure objects security program*. *Management of Development of Complex Systems*, 40, 69 – 75, [in Ukrainian]; [dx.doi.org\10.6084/m9.figshare.11969007](https://doi.org/10.6084/m9.figshare.11969007).
- ДСТУ Хрутьба В.О. *Формування методів управління проєктами та програми безпеки об'єктів критичної інфраструктури [Текст] / В.О. Хрутьба, В.І. Зюзюн, С.Д. Невєдров, Р.С. Лисак // Управління розвитком складних систем. – 2019. – № 40. – С. 69 – 75; [dx.doi.org\10.6084/m9.figshare.11969007](https://doi.org/10.6084/m9.figshare.11969007).*