УДК 614.8.084:323.28 **DOI: 10.33042/2522-1809-2024-1-182-202-209**

О.В. Азаренко[1], Ю.Ю. Гончаренко[2], М.М. Дівізінюк[3], А.О. Хмирова[4], Р.І. Шевченко[4], О.С. Шевченко[4]

[1]*Науково-дослідний лабораторно-експериментальний центр «БРАНД ТРЕЙД», Харків, Україна*
[2]*Європейський університет, Київ, Україна*
[3]*Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики НАН України, Київ, Україна*
[4]*Національний університет цивільного захисту України, Харків, Україна*

ХАРАКТЕРИСТИКА МЕТОДІВ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ ВІД ТЕРОРИСТИЧНОГО ВПЛИВУ

У роботі наведена характеристика методів захисту критичної інфраструктури держави. Розглянуто відмінність та взаємозв'язок понять критичної інфраструктури та інформаційної критичної інфраструктури. Дана характеристика загальних властивостей різних термінів захисту від терористичного впливу. Проаналізовано визначення форм та методів захисту критичної інфраструктури. Запропоновано узагальнену структуру інформаційно-технічних методів захисту критичної інфраструктури.

Ключові слова: *критична інформаційна інфраструктура, захист, терор, безпека, надзвичайна ситуація терористичного характеру.*

Постановка проблеми

Україна, як воююча держава, вирішує безліч завдань, одним із яких є захист критичної інфраструктури держави від терористичного впливу. Її ефективне вирішення забезпечує як життя мирних громадян, так і відстоювання територіальної цілісності держави [1]. Загалом дослідження шляхів вирішення цього завдання актуальне і у воєнний період, і в умовах мирного часу. Проблема полягає у визначенні форм і методів захисту критичної інфраструктури держави, співвідношенні їх з іншими поняттями, як-от фізичний захист, безпека, захист інформаційної критичної інфраструктури та іншими, що на практиці дозволяє ефективно протидіяти різноманітним засобам терористичного впливу.

Аналіз останніх досліджень і публікацій

Так, низка авторів виділяють у структурі критичної інфраструктури держави окрему складову – критичну інформаційну інфраструктуру [2–12]. Враховуючи її специфіку, необхідно визначити співвідношення термінів: забезпечення безпеки, фізичний захист, захист об'єктів критичної інфраструктури, захист інформаційної критичної інфраструктури, попередження надзвичайних ситуацій терористичного характеру на об'єктах критичної інфраструктури [13–24] – та визначення форм та методів захисту критичної інфраструктури. Надалі це дозволяє узагальнити структуру інформаційно-технічних методів захисту критичної інфраструктури за аналогією підходів.

Мета та завдання статті

Виходячи з вищевикладеного, метою цієї статті є визначення співвідношення методів захисту критичної інфраструктури держави від терористичного впливу, а саме: забезпечення безпеки, фізичний захист, захист об'єктів критичної інфраструктури, захист інформаційної критичної інфраструктури, попередження надзвичайних ситуацій терористичного характеру на об'єктах критичної інфраструктури.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– розглянути відмінність та взаємозв'язок понять критичної інфраструктури та інформаційної критичної інфраструктури;

– дати характеристику загальних властивостей різних термінів, зокрема: забезпечення безпеки, фізичного захисту, захисту об'єктів критичної інфраструктури, захисту інформаційної критичної інфраструктури, попередження надзвичайних ситуацій терористичного характеру на об'єктах критичної інфраструктури;

– проаналізувати з наукових позицій класичні визначення форм та методів захисту критичної інфраструктури;

– запропонувати узагальнену структуру інформаційно-технічних методів захисту критичної інфраструктури;

– визначити можливість застосування інформаційно-технічних методів у різних галузях знань

для захисту критичної інфраструктури держави від терористичного впливу.

Виклад основного матеріалу

Відмінність та взаємозв'язок понять критичної інфраструктури та інформаційної критичної інфраструктури. Під національною або державною інфраструктурою зазвичай розуміють сукупність усіх промислових і сільськогосподарських секторів, будівель, установ, транспортних і комунікаційних мереж, які гарантують життєдіяльність організацій або галузі в країні [2]. Прикладами є залізниці та автомагістралі, трубопроводи та лінії електропередач, мости, аеродроми та порти, житлові та промислові об'єкти, електростанції та сховища різного призначення, телефон та телеграф, радіо та телебачення, Інтернет та інші засоби масової інформації.

В інфраструктурі суверенних держав особливо виділяються мережі, системи і сектори (сукупності різних інфраструктурних елементів), від безпечного функціонування яких залежить стан навколишнього середовища, здоров'я і життєдіяльність громадян та виживання суспільства загалом. Цей комплекс секторів, систем і мереж називають критичною інфраструктурою, оскільки її відмова або порушення функціонування може призвести до криз на національному, регіональному або місцевому рівнях [3].

Наприкінці XX століття зростання терористичної загрози ініціювало в розвинених країнах дискусію про вразливість національних інфраструктур [4]. Увага експертів звернулася не лише до інформаційної (кібернетичної) інфраструктури, а й до всіх інших сфер життєдіяльності суспільства. В Україні поняття критичної інфраструктури було запроваджено на законодавчому рівні у 2017 році [5] та остаточно формалізовано у 2022 році [6]. Це законодавство в Україні містить базове визначення відповідно до європейських стандартів.

Отже, під критичною інфраструктурою слід розуміти сукупність підприємств, мереж та систем на національному, регіональному, місцевому та об'єктовому рівнях, відмова або порушення роботи яких може призвести до втрати контролю або спричинити значну шкоду. Атомні та гідроелектростанції, хімічні та нафтохімічні заводи, металургійні компанії та багато інших державних підприємств і приватних установ, що мають стратегічне значення, зазвичай називають об'єктами критичної інфраструктури (ОКІ).

Акцентуємо увагу на наступному [7].

По-перше, державна критична інформаційна інфраструктура (КІІ) є складовою національної (державної) критичної інфраструктури (КІ).

По-друге, під критичною інформаційною інфраструктурою зазвичай розуміють сукупність підприємств, мереж і систем, вихід з ладу або порушення роботи яких може призвести до втрати контролю і значної шкоди на національному, регіональному, місцевому та об'єктовому рівнях.

По-третє, національна (державна) КІІ призначена для забезпечення процесу управління життєдіяльністю держави. Тому до її складу входять автоматизовані системи керування залізничним та автотранспортом, авіаційними та водними транспортними засобами, лініями електропередач, трубопроводами та іншими інфраструктурами, сукупність автоматизованих систем керування виробничими та технологічними процесами об'єктів підвищеної небезпеки (ОПН) [8] та критично важливих об'єктів (КВО) [9]. Сюди також входять телефон і телеграф, радіо та телебачення, Інтернет та інші засоби масової інформації.

По-четверте, на об'єктовому рівні КІІ розглядається як складова частина критичної інфраструктури, яка не увійшли до провідної групи.

Під КІІ мається на увазі сукупність автоматизованих систем управління виробничими та технологічними процесами (АСУ ВП та АСУ ТП) потенційно-небезпечних, критично важливих та інших ОКІ, що забезпечують їхню взаємодію з іншими інформаційно-телекомунікаційними системами та мережами зв'язку зазвичай більш високого рівня.

Головна ознака приналежності цих систем, мереж та пристроїв до КІІ – це вирішення хоча б одного з трьох наступних завдань [10]:

1) здійснення управління виробничим або технологічним процесом на об'єкті, що розглядається;

2) здійснення інформаційного забезпечення управління виробничим або технологічним процесом на об'єкті, що розглядається;

3) здійснення інформування громадян про надзвичайні ситуації, що виникають на об'єкті, що розглядається.

Щоб впливати на КІІ об'єкта, до неї необхідно отримати фізичний доступ. Цей доступ може бути легальним чи санкціонованим та несанкціонованим.

Отже, під критичною інформаційною інфраструктурою розуміють сукупність автоматизованих систем управління виробничими та технологічними процесами об'єктів критичної інфраструктури та забезпечення взаємодії інформаційно-комунікаційних систем та мереж зв'язку. Вона є невід'ємною складовою кожного об'єкта критичної інфраструктури і всієї критичної інфраструктури кожного регіону і держави загалом.

Характеристика загальних властивостей деяких термінів. Послідовно дамо характеристику наступних чотирьох термінів: забезпечення безпеки, фізичний захист, захист об'єктів критичної інфраструктури, захист інформаційної критичної інфраструктури, попередження надзвичайних ситуацій терористичного характеру на об'єктах критичної інфраструктури.

Забезпечення безпеки. Безпека – це умови, у

яких перебуває складна система, коли дія зовнішніх і внутрішніх чинників не призводить до явищ, які вважаються небезпечними. Інакше безпека – це стан відсутності явної загрози, стан захищеності від шкоди або іншої можливої небезпеки [11]. Під забезпеченням безпеки розуміють планомірну систематичну роботу з усього спектра напрямів: організаційного, інформаційного, агітаційного, навчального та ін. Безпека об'єкта – стан захищеності об'єкта від різних загроз, у якому створено умови щодо його нормального функціонування та суворого дотримання в ньому встановлених режимів [12]. Використовуються чотири ключові напрями безпеки. Це управління ризиками, підвищення стійкості до деструктивних впливів, створення систем та засобів захисту від загроз, знищення (ізоляція) джерел загроз.

Іншими словами, забезпечення безпеки ОКІ – це планомірна систематична робота щодо захисту об'єкта від різних загроз та створення умов для його нормального функціонування та дотримання на ньому встановлених режимів.

Фізичний захист. Спочатку цей термін використовувався виключно в ядерній галузі. Фізичний захист – це діяльність у сфері використання ядерної енергії, спрямована на забезпечення безпеки ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання та зміцнення режиму нерозповсюдження ядерної зброї. Системи фізичного захисту ядерних установок, ядерного матеріалу, радіоактивних відходів, інших джерел іонізуючого випромінювання – це комплекс організаційних, правових та інженерно-технічних заходів, що здійснюються з метою створення умов, спрямованих на мінімізацію можливості диверсії, крадіжки або іншого незаконного вилучення радіоактивного матеріалу та зміцнення режиму ядерного нерозповсюдження [13]. Сьогодні цей термін трактується більш широко. Іншими словами, фізичний захист – це комплекс організаційних заходів, інженерно-технічних заходів та дій підрозділів охорони, спрямованих на запобігання диверсії чи крадіжці [13] або на запобігання протиправним діям щодо об'єктів, які підлягають охороні. Основними його етапами є запобігання несанкціонованому доступу, своєчасне виявлення несанкціонованих дій, затримка (уповільнення) вторгнення правопорушників, припинення несанкціонованих дій та стримування осіб, причетних до підготовки або здійснення диверсії чи крадіжки.

Інакше кажучи, фізичний захист ОКІ – це сукупність організаційних заходів, інженерно-технічних засобів та дій підрозділів охорони з метою запобігання протиправним діянням щодо об'єкта, що охороняється.

Захист об'єктів критичної інфраструктури. Захист у найширшому сенсі – це гарантія безпеки від будь-чого комусь чи низка дій і заходів щодо здійснення цієї гарантії [14]. Захист критичної інфраструктури – це всі види діяльності, спрямовані на своєчасне виявлення, запобігання та нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації [15]. До того ж кожен ОКІ та вся інфраструктура загалом має бути безпечною, здатною протистояти загрозам та оперативно відновлюватись після реалізованих загроз. Для цього має вестись систематична робота, спрямована на зменшення факторів уразливості, виявлення та усунення загроз, мінімізацію наслідків, а також прискорення заходів реагування та відновлення об'єктів критичної інфраструктури [16].

Тобто захист об'єктів критичної інфраструктури – це цілеспрямована діяльність на своєчасне виявлення, запобігання та нейтралізацію загроз, мінімізацію та ліквідацію наслідків у разі їх реалізації, прискорення заходів реагування та відновлення пошкоджених об'єктів.

Захист інформаційної критичної інфраструктури. Фактично це складова частина діяльності із захисту ОКІ. Як заходи захисту інформації та кібер-захисту об'єктів критичної інформаційної інфраструктури вони об'єднуються в систему інформаційної безпеки. Це сукупність організаційних та технічних заходів, а також засобів та методів захисту інформації, що впроваджуються на об'єкті критичної інформаційної інфраструктури (ОКІ). Їх мета – запобігання кіберінцидентам, виявлення та захист від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються або зберігаються) на об'єкті критичної інформаційної інфраструктури [17]. Як зазначалося раніше, негативний вплив на КІІ об'єкта здійснюється за допомогою несанкціонованого фізичного доступу до системи. Здебільшого цей доступ реалізується трьома шляхами: впливом на апаратну частину системи, впливом на провідні лінії комунікацій та впливом на бездротові лінії зв'язку. Виключення впливів на КІІ з приміщень, розташованих усередині периметра, що охороняється, дозволяє вважати її головними вразливими місцями провідні і бездротові лінії зв'язку та інші пристрої, що розташовуються за межами периметра ОКІ, що охороняється [7].

Іншими словами, захист інформаційної критичної інфраструктури – це сукупність організаційних та технічних заходів, засобів та методів захисту інформації, спрямованих на запобігання кіберінцидентам, збереження інформаційних ресурсів на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Запобігання надзвичайним ситуаціям терористичного характеру на об'єктах критичної інфраструктури. Надзвичайна ситуація (НС) – це обстановка на

певній території або об'єкті, що складається внаслідок загрози катастрофічної події (аварії, небезпечного природного явища, поширення захворювання, стихійного лиха та ін.), яка може спричинити людські жертви, шкоду здоров'ю людей або навколишньому середовищу, значні матеріальні втрати чи порушення умов життєдіяльності людей [2, 7]. Відповідно, причина виникнення надзвичайних ситуацій терористичного характеру (НС ТХ) – це терористичні акти та загрози будь-якого терористичного впливу, наприклад, ударного терористичного впливу [18]. Будь-які надзвичайні ситуації у своєму розвитку проходять п'ять етапів. Це накопичення повсякденних факторів, екстремальний розвиток негативного фактора, катастрофічна подія, мінімізація та ліквідація наслідків цієї події, віддалені наслідки катастрофічної події [2]. Попередження надзвичайних ситуацій – це комплекс заходів, що проводяться завчасно і спрямовані на максимально можливе зменшення ризику виникнення надзвичайних ситуацій, а також на збереження здоров'я людей, зниження розмірів шкоди природному середовищу та матеріальних втрат у разі їх виникнення.

Тобто попередження надзвичайних ситуацій терористичного характеру на об'єктах критичної інфраструктури – це комплекс заходів, що проводяться заздалегідь і спрямовані на максимально можливе зменшення ризику виникнення терористичного впливу проти ОКІ, а також збереження життя та здоров'я людей, зниження розмірів збитків та матеріальних втрат у разі їх виникнення.

Отже, з позиції захисту критичної інфраструктури держави від терористичного впливу терміни забезпечення безпеки, фізичного захисту, захисту об'єктів критичної інфраструктури, захисту інформаційної критичної інфраструктури, попередження надзвичайних ситуацій терористичного характеру на об'єктах критичної інфраструктури є тотожними.

Форми та методи захисту критичної інфраструктури. Терміни «форма» та «методи» походять від загальнонаукового поняття «методологія». Методологія, як трактує переклад із давньогрецької [19], – це вчення про методи, способи та стратегії дослідження предмета. Її прийнято розглядати у двох аспектах. Перший – це теоретична методологія, яка формується розділом філософського знання, що розглядає процеси пізнання (епістемологію та гносеологію). Другий – це практична методологія, яка орієнтована на практичне вирішення проблем щодо цілеспрямованого перетворення світу. Якщо перша (теоретична методологія) прагне моделі ідеального знання, то друга (практична методологія) є програма чи алгоритм, сукупність форм (прийомів) і методів того, як досягти бажаної практичної мети.

Метод (у перекладі з давньогрецької) – це усвідомлення форми внутрішнього саморуху змісту предмета, що вивчається [20]. Він може бути у певній галузі знань чи досліджень. Зазвичай методи є авторськими, тобто створюються конкретною особистістю чи групою людей, науковою чи практичною школою. З огляду на свою обмеженість рамками дії та результату, методи мають тенденцію старіти, перетворюючись на інші методи, розвиваючись відповідно до часу, досягнення технічної та наукової думки, потреб суспільства. Якість (успішність, ефективність) методу перевіряється практикою, вирішенням науково-практичних завдань, тобто пошуком принципів досягнення мети, що реалізуються в комплексі реальних справ та обставин. Розвиток методів є наслідком розвитку наукової думки.

Сукупність однорідних методів прийнято називати підходом, який, зі свого боку, визначається галузями науки, де вирішується певне практичне завдання (проблема) чи коло завдань (проблем). Області науки – це основні сфери наукового знання, що склалися внаслідок поділу праці в науці, суттєво різняться між собою з предметної основи та методологічного інструментарію.

Проблему захисту критичної інфраструктури держави та захисту критичної інформаційної інфраструктури від терористичного впливу покликані вирішувати технічні, юридичні, військові, психологічні, медичні, хімічні, біологічні та інші науки. Кожному виду наук, для вирішення практичних завдань запобігання надзвичайним ситуаціям терористичного характеру на об'єктах критичної інфраструктури (НС ТХ ОКІ) будуть відповідати свої методи. Для технічних наук це будуть технічні методи, для юридичних – правові методи, для військових – військові методи та ін.

У галузі технічних наук для вирішення практичних завдань запобігання НС ТХ ОКІ можуть використовуватися інформаційні технології, спеціально розроблені апаратно-програмні засоби та програмні продукти. Відповідно, авторські методи, що реалізують їх, матимуть назву інформаційно-технічних методів запобігання НС ТХ ОКІ. Якщо завдання запобігання НС ТХ на об'єкті, що охороняється, буде вирішуватися із застосуванням нових інженерних засобів, як-от системи обмеження доступу або бар'єри в системах фізичного захисту, нові засоби виявлення або контролю периметра, то авторські методи, що їх реалізують, будуть називатися інженерно-технічними методами запобігання НС ТХ ОКІ.

Запобігання НС ТХ може здійснюватися шляхом оперативно-розшукової роботи (наприклад, за допомогою прихованого знімання мовної інформації, потайного відеоспостереження та ін.) або реформуванням штатних структур, розробкою та впровадженням нових організаційно-технічних заходів. Авторські методи, що реалізують ці наукові розробки, носитимуть назви, відповідно, оперативно-технічних та організаційно-технічних методів запобігання НС ТХ ОКІ.

У разі, якщо для запобігання НС ТХ застосовуються біотехнічні системи, наприклад, з використанням морських тварин (дельфінів) для пошуку та нейтралізації підводних плавців при охороні гребель, шлюзів та інших гідротехнічних споруд, то авторські методи будуть називатися біотехнічними методами запобігання НС ТХ ОКІ.

У сфері юридичних наук авторські методи призначаються на вирішення практичних завдань запобігання НС ТХ ОКІ. Вони можуть мати назви інформаційно-правових методів запобігання НС ТХ ОКІ, коли вирішуються завдання правового використання та доступу до баз даних; інженерно-правових, коли необхідне правове забезпечення встановлення фізичних бар'єрів; оперативно-правових, коли необхідно приховане документування злочинної діяльності, та інші.

За аналогією назви методів, призначених для запобігання НС ТХ ОКІ, можуть формуватись і в інших видах наук.

Отже, проблему захисту критичної інфраструктури держави та захисту критичної інформаційної інфраструктури від терористичного впливу мають вирішувати технічні, юридичні, військові, психологічні, медичні, хімічні, біологічні та інші науки. Кожному виду наук для вирішення практичних завдань запобігання надзвичайним ситуаціям терористичного характеру на об'єктах критичної інфраструктури будуть відповідати свої методи. Для технічних наук це будуть інформаційно-технічні, інженерно-технічні, оперативно-технічні, організаційно-технічні, біотехнічні та інші методи запобігання надзвичайним ситуаціям терористичного характеру.

Узагальнена структура інформаційно-технічних методів захисту критичної інфраструктури. На сьогодні у трьох монографіях [21–23], виданих за результатами виконаних досліджень, описано шість інформаційно-технічних методів. Їхня структура складається з трьох складових частин, а саме: математичної моделі, що описує процес; керуючого алгоритму, що реалізує математичну модель; процедур, що визначають порядок дій щодо застосування методу.

У загальному випадку математична модель – це математичне уявлення реальності [24], яка призначена для прогнозування поведінки реального об'єкта, чи певної міри його ідеалізації. Керуючий алгоритм – це послідовність команд з управління об'єктом, що призводить до заздалегідь поставленої мети. Ключовим моментом у розробці цього алгоритму є число логічних змінних, кількість і послідовність операцій, що виконуються з ними, а також порядок їх прямих та зворотних зв'язків. Структурно-логічна схема керуючого алгоритму є основою для програмної реалізації математичної моделі. Перелік процедур (або протоколів) визначають послідовність дій щодо застосування методу.

Проілюструємо це на прикладі. Інформаційно-технічний метод запобігання надзвичайним ситуаціям терористичного характеру з використанням активних імпульсних радіолокаційних засобів на об'єктах критичної інфраструктури в умовах, наближених до ідеальних [21]. Він заснований на математичній моделі радіолокаційного виявлення та ідентифікації людей та інших небезпечних цілей на підходах до об'єктів критичної інфраструктури, що охороняються. Вона є сукупністю чотирьох функціональних залежностей. Перша з них визначає можливість радіолокаційного виявлення небезпечної мети залежно від ширини або радіуса контрольованої зони навколо об'єкта, очікуваної дальності виявлення небезпечної мети, часу її перебування в контрольованій зоні та робочого часу пошукової системи. Друга дозволяє отримати очікувану дальність виявлення небезпечної мети за п'ятьма основними технічними параметрами станції радіолокації (коефіцієнта розпізнавання, чутливості приймача, коефіцієнта посилення антени, імпульсної потужності, частоти), двома параметрами мети (відображувальної здатності та висоти польоту) і коефіцієнта аномалії. Третя описує робочий час пошукової системи залежно від значень швидкості огляду простору та коефіцієнтів розпізнавання станцій радіолокації. Четверта визначає функції поглинання електромагнітного випромінювання тканинами біооб'єкта за певною кількістю лінійних інтегралів, що залежать від розмірів об'єкта і довжини хвиль випромінювання, і дозволяє розрахувати мінімальні значення коефіцієнтів розпізнавання радіолокаційних станцій, необхідних для виявлення та ідентифікації людей та інших небезпечних цілей на підходах.

Керуючий алгоритм, що реалізує модель, складається з десяти структурних блоків, розташованих на шести ієрархічних рівнях, пов'язаних з логічними зв'язками. Спочатку він забезпечує систематизацію даних про ймовірних зловмисників, їх екіпірування та озброєння, технічні параметри радіолокаційних станцій, що забезпечують спостереження в контрольованих зонах, даних геоінформаційної системи про особливості рельєфу місцевості, рослинності та забудови, а також оперативну інформацію від начальника служби фізичного захисту охорони. Потім він забезпечує розрахунок ймовірностей виявлення небезпечних цілей на підходах до об'єкта, що охороняється, критичної інфраструктури за раніше визначеними параметрами: шириною контрольованої зони, дальністю виявлення небезпечної мети, часом перебування мети в зоні виявлення РЛС і робочого часу пошукової системи.

Сам метод призначений для визначення ймовірності радіолокаційного виявлення небезпечних цілей на підходах до об'єкта, що охороняється, за уточненими даними радіолокаційних характеристик небезпечних та інших цілей, робочим часом пошу-

кової системи, очікуваними дальностями радіолокаційного виявлення цих цілей та оперативною інформацією, що визначає тривалість перебування зловмисників у контрольованій зоні. Його застосування передбачає послідовне виконання п'яти процедур, а саме: визначення вихідних даних; введення вихідних даних; розрахунок проміжних параметрів та основного параметра; подання розрахункових даних; передача розрахункових даних споживачам.

Отже, узагальнена структура інформаційно-технічних методів захисту критичної інфраструктури складається із трьох складових частин: математичної моделі, що описує процес, що відбувається на об'єкті критичної інфраструктури; керуючого алгоритму, що реалізує математичну модель; процедур, що визначають порядок дій щодо застосування методу.

Висновки

Можемо зробити висновок, що узагальнена структура інформаційно-технічних методів захисту критичної інфраструктури складається із трьох складових частин. Серед них: математична модель, що описує процес, що відбувається на об'єкті критичної інфраструктури; керуючий алгоритм, що реалізує математичну модель; процедури, що визначають порядок дій щодо застосування методу.

Проблему захисту критичної інфраструктури від терористичного впливу мають вирішувати технічні, юридичні, військові, психологічні, медичні, хімічні, біологічні та інші науки. Кожному виду наук для вирішення практичних завдань запобігання надзвичайним ситуаціям терористичного характеру на об'єктах критичної інфраструктури відповідатимуть свої методи. Для технічних наук це будуть інформаційно-технічні, інженерно-технічні, оперативно-технічні, організаційно-технічні, біотехнічні та інші методи запобігання надзвичайним ситуаціям терористичного характеру, які потрібно розробляти в найближчому майбутньому.

Література

1. *Ключове завдання нашої держави та наших партнерів – посилювати у Росії відчуття, що їй не вдасться нічого добитися в Україні – звернення Президента Володимира Зеленського [Електрон. ресурс] / Президент України. Офіційне інтернет-представництво : сайт. – Київ, 2024. – Оновлюється постійно. – Режим доступу: https://www.president.gov.ua/news/klyuchove-zavdannya-nashoyi-derzhavi-ta-nashih-partneriv-pos-80501, вільний (дата звернення: 10.03.2024).*
2. *Теоретичні засади парадигми «Цивільний захист» : монографія / М. М. Дівізінюк, С. А. Єременко, О. А. Лєвтєров, А. В. Пруський, В. В. Стрілець, В. М. Стрілець, Р. І. Шевченко. – Київ : ТОВ "АЗИМУТ-ПРІНТ", 2022. – 335 с.*
3. *Hofreiter L. Critical infrastructure – content, structure and problems of its protection / L. Hofreiter // Securitologia. – 2014. – No. 1 (19). – P. 141–152. – Regime of access: https://civitas.edu.pl/wp-content/uploads/2015/03/Securitologia1_19_2014_141-152.pdf, free (date of the application: 10.03.2024).*
4. *Ochrana objektov kritickej dopravnej infraštruktúry / L. Hofreiter, K. Boc, Š. Jangl, T. Loveček, V. Mach, M. Seidl, P. Selinger, A. Veľas ; Žilinská univerzita v Žiline. – 1 ed. – Žilina (Slovakia) : EDIS, 2013. – 238 p.*
5. *Про 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 січ. 2017 р. № 8/2017 [Електрон. ресурс] / Президент України. Офіційне інтернет-представництво : сайт. – Київ, 2024. – Оновлюється постійно. – Режим доступу: https://www.president.gov.ua/documents/82017-21058, вільний (дата звернення: 10.03.2024).*
6. *Про критичну інфраструктуру : Закон України від 16 листоп. 2021 р. № 1882-IX : в редакції від 01 січ. 2024 р. [Електрон. ресурс] / Верховна Рада України : сайт. – Київ, 1994–2024. – Оновлюється постійно. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text, вільний (дата звернення: 10.03.2024).*
7. *Захист критичної інфраструктури держави від терористичного впливу / О. В. Азаренко, Ю. Ю. Гончаренко, М. М. Дівізінюк, М. І. Ожиганова. – Київ : ДУ "ІГНС НАН України", 2018. – 82 с.*
8. *Про об'єкти підвищеної небезпеки : Закон України від 18 січ. 2001 р. № 2245-III : в редакції від 01 січ. 2024 р. [Електрон. ресурс] / Верховна Рада України : сайт. – Київ, 1994–2024. – Оновлюється постійно. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2245-14#Text, вільний (дата звернення: 10.03.2024).*
9. *Об'єкти критичної інфраструктури [Електрон. ресурс] / Вікіпедія : сайт. – Сан-Франциско, Каліфорнія (США), 2001–2024. – Оновлюється постійно. – Режим доступу: https://uk.wikipedia.org/w/index.php?title=Об'єкти_критичної_інфраструктури&oldid=38146098, вільний (дата звернення: 10.03.2024).*
10. *Леоненко Г. П. Проблеми забезпечення інформаційної безпеки систем критично важливої інформаційної інфраструктури України / Г. П. Леоненко, О. Ю. Юдін // Collection "Information Technology and Security". – 2013. – № 2 (1). – С. 44–48. – DOI: 10.20535/2411-1031.2013.2.1.58384.*
11. *Безпека [Електрон. ресурс] / Вікіпедія : сайт. – Сан-Франциско, Каліфорнія (США), 2001–2024. – Оновлюється постійно. – Режим доступу: https://uk.wikipedia.org/w/index.php?title=Безпека&oldid=41465005, вільний (дата звернення: 10.03.2024).*
12. *Франчук В. І. Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи / В. І. Франчук, П. Я. Пригунов, С. І. Мельник // Соціально-правові студії. – 2021. – Вип. 3 (13). – С. 142–148. – DOI: 10.32518/2617-4162-2021-3-142-148.*
13. *Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання : Закон України від 19 жовт. 2000 р. № 2064-III : в редакції від 16 жовт. 2022 р. [Електрон. ресурс] / Верховна Рада України : сайт. – Київ, 1994–2024. – Оновлюється постійно. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2064-14#Text, вільний (дата звернення: 10.03.2024).*
14. *Захист [Електрон. ресурс] / Вікіпедія : сайт. – Сан-Франциско, Каліфорнія (США), 2001–2024. – Оновлюється постійно. – Режим доступу: https://uk.wikipedia.org/w/index.php?title=Захист&oldid=41085300, вільний (дата звернення: 10.03.2024).*
15. *Про критичну інфраструктуру та її захист : Проект Закону України від 27 трав. 2019 р. № 10328 [Електрон. ресурс] / Верховна Рада України : сайт. – Київ, 1994–2024. – Оновлюється постійно. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996, вільний (дата звернення: 10.03.2024).*
16. *Захист критичної інфраструктури: досвід США*

[Електрон. ресурс] / ІГС Україна : сайт. – Київ, 2019–2024. – Оновлюється постійно. – Режим доступу: https://ig-security.tech/zahist-kritichnoi-infrastrukturi-dosvid-ssha.html, вільний (дата звернення: 10.03.2024).

17. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19 черв. 2019 р. № 518 : в редакції від 07 верес. 2022 р. [Електрон. ресурс] / Верховна Рада України : сайт. – Київ, 1994–2024. – Оновлюється постійно. – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text, вільний (дата звернення: 10.03.2024).

18. Fire Induced Damage in Structures and Infrastructure: Analysis, Testing and Modeling / A. Ibrahimbegovic, A. Boulkertous, L. Davenne, M. Muhasilovic, J. Duhovnik, A. Pokrklic // Damage Assessment and Reconstruction after War or Natural Disaster / ed. by A. Ibrahimbegovic, M. Zlatar. – Dordrecht (Netherlands) : Springer Science + Business Media B. V., 2009. – P. 309–329. – (NATO Science for Peace and Security Series C: Environmental Security). – DOI: 10.1007/978-90-481-2386-5_12.

19. Методологія [Електрон. ресурс] / Вікіпедія : сайт. – Сан-Франциско, Каліфорнія (США), 2001–2024. – Оновлюється постійно. – Режим доступу: https://uk.wikipedia.org/w/index.php?title=Методологія&oldid=40569721, вільний (дата звернення: 10.03.2024).

20. Метод [Електрон. ресурс] / Вікіпедія : сайт. – Сан-Франциско, Каліфорнія (США), 2001–2024. – Оновлюється постійно. – Режим доступу: https://uk.wikipedia.org/w/index.php?title=Метод&oldid=41315693, вільний (дата звернення: 10.03.2024).

21. Papalou A. Assessing Structural Damage after a Severe Wildfire: A Case Study / A. Papalou, D. K. Baros // Buildings. – 2019. – Vol. 9, Issue 7. – Article 171. – DOI: 10.3390/buildings9070171.

22. Operational Analysis of Fire Alarm Systems with a Focused, Dispersed and Mixed Structure in Critical Infrastructure Buildings / K. Jakubowski, J. Paś, S. Duer, J. Bugaj // Energies. – 2021. – Vol. 14, Issue 23. – Article 7893. – DOI: 10.3390/en14237893.

23. Aliş B. Investigation of Fire Effects on Reinforced Concrete Members via Finite Element Analysis / B. Aliş, C. Yazici, F. M. Özkal // ACS Omega. – 2022. – Vol. 7, Issue 30. – P. 26881–26893. – DOI: 10.1021/acsomega.2c03414.

24. Математична модель [Електрон. ресурс] / Вікіпедія : сайт. – Сан-Франциско, Каліфорнія (США), 2001–2024. – Оновлюється постійно. – Режим доступу: https://uk.wikipedia.org/w/index.php?title=Математична_модель&oldid=42270203, вільний (дата звернення: 10.04.2024).

References

1. Zelenskyi, V. (2023, January 19). *The key task of our state and our partners is to intensify Russia's feeling that it will not achieve anything in Ukraine – address by President Volodymyr Zelenskyy*. President of Ukraine. Official website. https://www.president.gov.ua/en/news/klyuchove-zavdannya-nashoyi-derzhavi-ta-nashih-partneriv-pos-80501

2. Diviziniuk, M. M., Yeremenko, S. A., Lievtierov, O. A., Pruskyi, A. V., Strilets, V. V., Strilets, V. M., & Shevchenko, R. I. (2022). *Theoretical Foundations of the "Civil Defence" Paradigm: monograph*. TOV "AZYMUT-PRINT" [in Ukrainian]

3. Hofreiter, L. (2014). Critical infrastructure – content, structure and problems of its protection. *Securitologia*, (1(19), 141–152. https://civitas.edu.pl/wp-content/uploads/2015/03/Securitologia1_19_2014_141-152.pdf

4. Hofreiter, L., Boc, K., Jangl, Š., Loveček, T., Mach, V., Seidl, M., Selinger, P., & Veľas, A. (2013). *Protection of critical transport infrastructure objects*. EDIS [in Slovak]

5. Poroshenko, P. (2017, January 16). *On the Decision of the National Security and Defence Council of Ukraine of 29 December 2016 "On Improving Measures to Ensure the Protection of Critical Infrastructure Objects": Decree of the President of Ukraine of 16 January 2017 No. 8/2017*. President of Ukraine. Official website. https://www.president.gov.ua/documents/82017-21058 [in Ukrainian]

6. Verkhovna Rada of Ukraine. (2024, January 1). *On Critical Infrastructure: Law of Ukraine of 16 November 2021 No. 1882-IX*. https://zakon.rada.gov.ua/laws/show/1882-20#Text [in Ukrainian]

7. Azarenko, O. V., Honcharenko, Yu. Yu., Diviziniuk, M. M., & Ozhyhanova, M. I. (2018). *Protecting the state's critical infrastructure from terrorist influence*. SI "IEG NAS of Ukraine".

8. Verkhovna Rada of Ukraine. (2024, January 1). *On Extremely Dangerous Objects: Law of Ukraine of 18 January 2001 No. 2245-III*. https://zakon.rada.gov.ua/laws/show/2245-14#Text [in Ukrainian]

9. Critical Infrastructure Objects. (2023, January 26). In *Wikipedia*. https://uk.wikipedia.org/w/index.php?title=Об'єкти_критичної_інфраструктури&oldid=38146098 [in Ukrainian]

10. Leonenko, H., & Yudin, O. (2013). Problems of ensuring information security of Ukraine critical information infrastructure systems. *Collection "Information Technology and Security"*, *2*(1), 44–48. https://doi.org/10.20535/2411-1031.2013.2.1.58384

11. Safety. (2024, January 19). In *Wikipedia*. https://uk.wikipedia.org/w/index.php?title=Безпека&oldid=41465005 [in Ukrainian]

12. Franchuk, V. I., Pryhunov, V. Ya., & Melnyk, S. I. (2021). Safety of Critical Infrastructure Facilities in Ukraine: Organizational and Regulatory Problems and Approaches. *Social and Legal Studios*, *3*(13), 142–148. https://doi.org/10.32518/2617-4162-2021-3-142-148 [in Ukrainian]

13. Verkhovna Rada of Ukraine. (2022, October 16). *On the Physical Protection of Nuclear Facilities, Nuclear Materials, Radioactive Waste, and Other Sources of Ionising Radiation: Law of Ukraine of 19 October 2000 No. 2064-III*. https://zakon.rada.gov.ua/laws/show/2064-14#Text [in Ukrainian]

14. Protection. (2023, December 6). In *Wikipedia*. https://uk.wikipedia.org/w/index.php?title=Захист&oldid=41085300 [in Ukrainian]

15. Cabinet of Ministers of Ukraine. (2019, May 27). *On Critical Infrastructure and its Protection: Draft Law of Ukraine of 27 May 2019 No. 10328*. Verkhovna Rada of Ukraine. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996 [in Ukrainian]

16. Bonk, A. (2019, November 10). *Protecting critical infrastructure: the US experience*. IGS Ukraine. https://ig-security.tech/zahist-kritichnoi-infrastrukturi-dosvid-ssha.html [in Ukrainian]

17. Cabinet of Ministers of Ukraine. (2022, September 7). *On Approval of the General Requirements for Cyber Defence of Critical Infrastructure Objects: Resolution of the Cabinet of Ministers of Ukraine of 19 June 2019 No. 518*. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text [in Ukrainian]

18. Ibrahimbegovic, A., Boulkertous, A., Davenne, L., Muhasilovic, M., Duhovnik, J., & Pokrklic, A. (2009). Fire Induced Damage in Structures and Infrastructure: Analysis, Testing and Modeling. In A. Ibrahimbegovic, & M. Zlatar (Eds.), *Damage Assessment and Reconstruction after War or Natural Disaster* (pp. 309–329). Springer Science + Business Media B. V. http://doi.org/10.1007/978-90-481-2386-5_12

19. Methodology. (2023, October 5). In *Wikipedia*. https://uk.wikipedia.org/w/index.php?title=Методологія&oldid=40569721 [in Ukrainian]

20. Method. (2023, December 29). In *Wikipedia*. https://uk.wikipedia.org/w/index.php?title=Метод&oldid=41315693 [in Ukrainian]

21. Papalou, A., & Baros, D. K. (2019). Assessing Structural Damage after a Severe Wildfire: A Case Study. *Buildings*, *9*(7), 171. http://doi.org/10.3390/buildings9070171

22. Jakubowski, K., Paś, J., Duer, S., & Bugaj, J. (2021). Operational Analysis of Fire Alarm Systems with a Focused, Dispersed and Mixed Structure in Critical Infrastructure Buildings. *Energies*, *14*(23), 7893. http://doi.org/10.3390/en14237893
23. Aliş, B., Yazici, C., & Özkal, F. M. (2022). Investigation of Fire Effects on Reinforced Concrete Members via Finite Element Analysis. *ACS Omega*, *7*(30), 26881–26893. http://doi.org/10.1021/acsomega.2c03414
24. Mathematical model. (2024, April 6). In *Wikipedia*. https://uk.wikipedia.org/w/index.php?title=Математична_модель&oldid=42270203 [in Ukrainian]

Рецензент: д-р техн. наук, проф., заступник начальника з навчальної та наукової роботи О.М. Мирошник, Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України, Україна.

Автор: АЗАРЕНКО Олена Василівна
доктор фізико-математичних наук, професор, заступник керівника
Науково-дослідний лабораторно-експериментальний центр «БРАНД ТРЕЙД»
E-mail – azarenko_ev@ukr.net
ID ORCID: http://orcid.org/0000-0003-2927-5545

Автор: ГОНЧАРЕНКО Юлія Юріївна
доктор технічних наук, доцент, професор кафедри кібербезпеки та захисту інформації
Європейський університет
E-mail – vup@e-u.in.ua
ID ORCID: http://orcid.org/0000-0003-2045-0263

Автор: ДІВІЗІНЮК Михайло Михайлович
доктор фізико-математичних наук, професор, головний науковий співробітник
Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики НАН України
E-mail – divizinyuk@ukr.net
ID ORCID: http://orcid.org/0000-0002-5657-2302

Автор: ХМИРОВА Анастасія Олегівна
кандидат наук з державного управління, викладач-методист факультету оперативно-рятувальних сил
Національний університет цивільного захисту України
E-mail – khmyrova.anast@gmail.com
ID ORCID: https://orcid.org/0000-0002-0680-7505

Автор: ШЕВЧЕНКО Роман Іванович
доктор технічних наук, професор, начальник кафедри автоматичних систем безпеки та інформаційних технологій
Національний університет цивільного захисту України
E-mail – shevchenko605@i.ua
ID ORCID: http://orcid.org/0000-0001-9634-6943

Автор: ШЕВЧЕНКО Ольга Станіславівна
кандидат технічних наук, провідний фахівець
Національний університет цивільного захисту України
E-mail – shevchenkoolga2008@gmail.com
ID ORCID: http://orcid.org/0000-0003-2106-5009

CHARACTERISATION OF METHODS OF PROTECTING THE STATE'S CRITICAL INFRASTRUCTURE FROM TERRORIST ACTIVITIES

O. Azarenko[1], Yu. Honcharenko[2], M. Diviziniuk[3], A. Khmyrova[4], R. Shevchenko[4], O. Shevchenko[4]
[1]Scientific Research Laboratory and Experimental Center "BRAND TRADE", Kharkiv, Ukraine
[2]European University, Kyiv, Ukraine
[3]Center for Information-Analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
[4]National University of Civil Defence of Ukraine, Kharkiv, Ukraine

The study describes methods for protecting the critical infrastructure of a state. The article aims to determine the combination of protecting methods of the state's critical infrastructure from terrorist activities, namely security, physical protection, protection of critical infrastructure, protection of critical information infrastructure, and prevention of emergencies of a terrorist nature at objects of critical infrastructure.

It is necessary to fulfil the following objectives to achieve the aim: to consider the difference and interrelation of the concepts of critical infrastructure and information critical infrastructure; to characterise the general properties of various terms, in particular: security, physical protection, protection of critical infrastructure, protection of information critical infrastructure, prevention of terrorist emergencies at objects of critical infrastructure; to analyse from the scientific point of view the classical definitions of forms and methods of critical infrastructure protection; to propose a generalised structure of information and technical methods of critical infrastructure protection; to determine the possibility of using information and technical methods in various fields of knowledge to protect the state's critical infrastructure from terrorist influence.

In summary, the structure of information and technical methods for critical infrastructure protection consists of three components: a mathematical model that describes the process occurring at critical infrastructure, a control algorithm that implements the mathematical model, and procedures that indicate the order of actions for applying the method.

The problem of protecting critical infrastructure from terrorist activities requires technical, legal, military, psychological, medical, chemical, biological, and other sciences to address it. Each type of science will use its specific methods to solve practical problems of preventing terrorist emergencies at critical infrastructure. For technical sciences, there will be information-technical, engineering-technical, operational-technical, organisational-technical, biotechnical, and other methods to prevent emergencies of a terroristic nature that need development shortly.

Keywords: *critical information infrastructure, protection, terror, security, terrorist emergency.*