УДК 614.841.3
DOI: https://doi.org/10.31731/2524-2636.2021.5.1.-5-14

Олена Азаренко*[1]*, д-р ф.-м. наук, професор (ORCID: 0000-0003-2927-5545),
Юлія Гончаренко*[2]*, д-р техн. наук, професор (ORCID: 0000-0003-2045-0263),
Михайло Дівізінюк*[3]*, д-р техн. наук, професор (ORCID: 0000-0002-5657-2302),
Олександр Тищенко*[4]*, канд. техн. наук, професор (ORCID: 0000-0001-7303-6360),
Олег Мирошник*[4]*, д-р техн. наук, доцент (ORCID: 0000-0001-8951-9498),
Олег Землянський*[4]*, канд. техн. наук, доцент, (ORCID: 0000-0002-2728-6972),
Дмитро Лесечко*[4]*, (ORCID: 0000-0002-4792-5284),
[1]Національний авіаційний університет,
[2]Європейський університет,
[3]Інститут геохімії навколишнього середовища НАН України,
[4]Черкаський інститут пожежної безпеки імені Героїв Чорнобиля
Національного університету цивільного захисту України

ПРОТИРІЧЧЯ ПРОЦЕСУ УПРАВЛІННЯ БЕЗПЕКОЮ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Робота присвячена обґрунтуванню об'єктивних протиріч в процесі управління безпекою об'єкта критичної інфраструктури. Показано, що головна мета управління безпекою об'єкта критичної інфраструктури (або управління надзвичайною ситуацією природного, техногенного або терористичного характеру на цьому об'єкті) – це недопущення катастрофічної події, навколо якої розвивається надзвичайна ситуація, а в разі її (катастрофічної події) настання – мінімізація збитків та можливих наслідків.

Для дослідження цієї мети були вирішені такі наукові завдання. По-перше, дано визначення терміна процес управління безпекою об'єкта критичної інфраструктури. Під терміном процес управління безпекою об'єкта критичної інфраструктури розуміється діяльність керівництва підприємства і системи його безпеки на ліквідацію зовнішніх і внутрішніх загроз його існування і функціонування, обумовлених потенційними (прогнозованими) катастрофічними подіями природного, техногенного та терористичного характеру. По-друге, сформульовані основні принципи управління процесами безпеки функціонування підприємства і їх математичної формалізації. Показано, що управління безпекою об'єкта критичної інфраструктури зводиться в кінцевому підсумку до розробки математичних моделей виникнення конкретної катастрофічної події на цьому об'єкті і їх (математичних моделей) подальшого використання для розробки превентивних заходів, що перешкоджають настанню цієї катастрофічної події, а в разі її настання – мінімізації можливих наслідків. По-третє, визначені деякі системні суперечності в процесі управління безпекою об'єкта критичної інфраструктури. У використовуваних двох підходах управління безпекою об'єктів критичної інфраструктури існують об'єктивні протиріччя. У першому випадку, коли час настання катастрофічної події є необмеженою випадковою величиною, теоретична аварія настає через мільйони років, що робить моделі управління безпекою об'єктів некоректними. У другому випадку, коли час настання катастрофічної події є обмеженою випадковою величиною, теоретична аварія стовідсотково настає за час експлуатації об'єкта, що так само суперечить здоровому глузду і робить некоректними оцінки ймовірності ризику настання катастрофічної події.

Ключові слова: *безпека, управління безпекою, об'єкт критичної інфраструктури, ймовірність, ризик, випадкова величина.*

Постановка проблеми. Під критичною інфраструктурою прийнято розуміти сукупність підприємств, мереж, систем, вихід з ладу або порушення функціонування яких може викликати втрату управління або завдати шкоди на загальнодержавному, регіональному місцевому або об'єктовому рівні [1]. Присутні в її складі атомні і гідроелектростанції, хімічні і нафтохімічні комбінати, металургійні заводи, безліч інших державних підприємств і приватних установ стратегічного призначення прийнято називати об'єктами критичної інфраструктури [2]. Забезпечення безпеки цих об'єктів є актуальною науковою проблемою, яку необхідно вирішувати як в рамках окремого підприємства, так і в масштабах всієї держави Україна [3].

Аналіз останніх досліджень і публікацій.

Головна мета управління безпекою об'єкта критичної інфраструктури (або управління надзвичайною ситуацією природного, техногенного або терористичного характеру на цьому об'єкті) – це недопущення катастрофічної події, навколо якої розвивається надзвичайна ситуація, а в разі її (катастрофічної події) настання – мінімізація збитків і можливих наслідків [4].

Реалізація безперервного процесу управління безпекою підприємства, як і будь-якого іншого управлінського процесу, здійснюється з використанням контуру управління [5] або структурно-логічної схеми управління [6]. Безумовно, найбільш загальні закономірності структурно-логічних схем управління, передбачають особливості, характерні для кожної галузі, наприклад, водних транспортних засобів [7], систем моніторингу надзвичайних ситуацій [8], безпеки критично важливого об'єкта [9], підприємства України, що охороняється [10] або екологічно небезпечних об'єктів (підприємств ядерного паливного циклу) [11]. Управління безпекою об'єкта критичної інфраструктури відбувається на підставі суб'єктивних оцінок (експертних, інформаційних, математичних та інших) об'єктивно відбувається функціонування підприємства (в ряді випадків прихованих від технічних систем контролю і органів сприйняття операторів) [12, 13], для опису яких традиційно використовуються методи теорії ймовірностей і математичної статистики [14-16]. Вони так само дозволяють визначити деякі протиріччя в процесі управління безпекою функціонування підприємства.

Формулювання цілей статті. Мета даної роботи – визначити деякі системні суперечності в процесі управління безпекою об'єкта критичної інфраструктури. Для досягнення поставленої мети необхідно вирішити наступні наукові завдання. По-перше, дати визначення терміна процес управління безпекою об'єкта критичної інфраструктури. По-друге, сформулювати основні принципи управління процесами безпеки функціонування підприємства і їх математичної формалізації. По-третє, визначити деякі системні суперечності в процесі управління безпекою об'єкта критичної інфраструктури.

Виклад основного матеріалу дослідження.

Визначення терміна «процес управління безпекою об'єкта критичної інфраструктури».

У найширшому сенсі під безпекою слід розуміти стан захищеності життєво важливих інтересів особистості, суспільства, держави від внутрішніх і зовнішніх загроз, або здатність предмета, явища або процесу зберігатися при руйнівних впливах [13]. Її прийнято розділяти на особисту (захищеність людини від психологічного, фізичного або іншого насильницького посягання) і громадську безпеку (здатність соціальних інститутів суспільства забезпечити стійкий, вільний і самостійний розвиток цього суспільства і його відносин). На уявну безпеку (існуючу лише в уяві людей) і державну безпеку (систему суспільних і державних гарантій, що захищають основні джерела життєдіяльності, цивільні права та свободи людини, суверенітет і територіальну цілісність держави).

Залежно від національних правових основ в державах визначають такі види безпеки як: авіаційну, автодорожню, залізничну, безпеку систем управління та інформаційну безпеку, пожежну, екологічну, радіаційну, ядерну та інші.

На сьогодні з'явився новий міждисциплінарний напрямок фундаментальної науки – теорія безпеки, яка вивчає стан захищеності життєвоважливих інтересів людини, суспільства

і держави від надзвичайних ситуацій різного (природного, техногенного, терористичного) характеру. Тут безпека використовується як одна з характеристик функціонування і розвитку соціальних, економічних, технічних, екологічних і біологічних і інших систем. Тому в теорії безпеки – безпека трактується як відсутність небезпеки, збереження системи і надійність її функціонування. Воно (поняття безпеки) тісно пов'язане з такими поняттями як загроза, небезпека, шкода, збиток, ризик та інші. Ці терміни, відповідно до теорії управління, поділяються на зовнішні і внутрішні загрози. Іншими словами, поняття безпеки має дві сторони: зовнішню і внутрішню безпеку.

Оскільки процес управління – це діяльність, спрямована на досягнення певної мети шляхом реалізації обраних методів управління, то під безпекою об'єкта критичної інфраструктури слід розуміти реакцію керівництва цього підприємства або організації на зовнішні і внутрішні загрози. Процес управління безпекою, як і будь-який інший управлінський процес, реалізується через контур управління або систему безпеки об'єкта критичної інфраструктури [5]. Її (систему безпеки об'єкта критичної інфраструктури) поділяють на дві складові частини: пасивну та активну. Перша (пасивна) орієнтована головним чином на захист об'єкта. Друга (активна) передбачає виконання функцій прогнозування, визначення цілей і завдань забезпечення безпеки, спрямованих на запобігання та ліквідацію виникаючих внутрішніх і зовнішніх загроз, планування і реалізацію заходів щодо забезпечення безпеки, контроль їх виконання, аналіз отриманих результатів та інших.

Відомий також термін – управління безпекою адміністративної території [3, 4]. Він має на увазі комплексну цілеспрямовану діяльність органів управління відповідних рівнів влади щодо забезпечення безпеки населення, об'єктів економіки і навколишнього середовища від впливу катастрофічних подій, навколо яких розвиваються надзвичайні ситуації природного, техногенного та терористичного характеру. Ця діяльність вимагає реалізації політичних, адміністративно-правових, економічних, санітарно-гігієнічних, культурологічних, психологічних та інших управлінських заходів.

Таким чином, під терміном процес управління безпекою об'єкта критичної інфраструктури, будемо розуміти діяльність керівництва підприємства і системи його безпеки, спрямовану на ліквідацію зовнішніх і внутрішніх загроз його існування і функціонування, обумовлених потенційними (прогнозованими) катастрофічними подіями природного, техногенного та терористичного характеру.

Основні принципи управління процесами безпеки функціонування підприємства і їх математичної формалізації

Системна теорія управління процесами безпеки функціонування підприємства ґрунтується на певних детерміністичних і стохастичних законах. Конкретний зміст кожного з цих законів сформульовано у відповідних теоріях. Вони вивчають зовнішні та внутрішні загрози для безпеки функціонування підприємства, оцінюють необхідну кількість сил і засобів, час на реалізацію превентивних заходів, досліджують ризики експлуатації об'єкта при прогнозованих загрозах, визначають критерії прийняття управлінських рішень, забезпечують конфіденційність, цілісність і доступність інформації. З їх допомогою алгоритмізують збір і обробку інформації про загрози для безпеки, оптимізують зниження травматизму і аварійності, покращують умови праці на основі систем управління якістю тощо.

Ці закони визначають наступні сім принципів управління процесами безпеки функціонування підприємства [5,8,11,13].

Перший – принцип об'єктивної суб'єктивності локального підходу. Кожна локальна теорія неминуче має непереборні методологічні обмеження і методичну похибку, які неможливо визначити в рамках аксіоматики даної локальної теорії. Внаслідок цього об'єктивно неминучі деякі суб'єктивні висновки з комплексної проблеми безпеки, коли вони ґрунтуються тільки на цій аксіоматиці. Тому цей принцип вимагає з'ясування зазначених обмежень та оцінку методичної похибки локальних методів.

Другий – принцип акумулюючої здатності навколишнього середовища. Акумулююча здатність навколишнього середовища відображає її властивості по накопиченню і нейтралізації негативних впливів шкідливих речовин, згідно спостерігається в природі круговороту речовин. Він виконується за умови, що значення параметрів потоків негативного впливу не перевищує допустимих норм.

Третій – принцип адаптації об'єкта (його безпеки). Мінімальна похибка управління об'єктом з метою забезпечення стану його безпеки для унікальних (статистично нестійких) умов виникнення катастрофічних подій досягається на основі принципу адаптації. Він полягає в пристосуванні (регулюванні) локальних властивостей об'єкта в реальному масштабі часу до вимог, що визначаються необхідним рівнем безпеки з урахуванням конкретних умов настання катастрофічної події і поточних характеристик експлуатації.

Четвертий – принцип управління безпекою об'єкта (основний). Локальний об'єкт може бути перетворений в безпечну систему при виконанні двох умов. По-перше, в початковий момент перетворення об'єкт знаходився в безпечному стані. По-друге, в процесі його експлуатації, технічного обслуговування і ремонту, стан безпеки об'єкта забезпечується за допомогою контуру зворотного зв'язку. Це досягається як шляхом превентивного усунення причин виникнення катастрофічної події, так і регулювання властивостей локального об'єкта відповідно до принципу адаптації об'єкта.

П'ятий – принцип єдності детерміністичного і стохастичного підходів. Теорія управління безпекою містить апріорне і апостеріорне управління. Апріорне управління базується на теорії ймовірностей, стохастичних закономірностей всієї сукупності несумісних станів безпеки об'єкта в умовах статистичної стійкості. Апостеріорне управління ґрунтується на індивідуальних (детерміністичних) закономірностіях об'єкта без вимог їх статистичної стійкості. Воно служить для забезпечення безпеки в реальних поточних умовах регулювання одного з можливих несумісних станів безпеки об'єкта з метою недопущення катастрофічної події.

Шостий – принцип інтервалу абсолютної індивідуальної надійності. Критерії надійності (безвідмовності роботи) визначають, що кількісні зміни властивостей елемента в силу інерції відбуваються на кінцевому обмеженому інтервалі часу. Цей інтервал інерції називають інтервалом абсолютної індивідуальної надійності елемента. Він залежить від властивостей конкретного елемента, умов експлуатації, виробництва, зберігання і інше. Згідно поняття інтервалу абсолютної індивідуальної надійності випливає важливий практичний висновок. Якщо час роботи до відмови елемента можна трактувати як обмежену безперервну випадкову величину, то число його відмов і напрацювання на відмову представляються обмеженими дискретними випадковими величинами.

Сьомий – принцип повної групи видів потенційно можливих катастрофічних подій. Повна група включає три види потенційно можливих катастрофічних подій. Перша – практично неминучі катастрофічні події, що підкоряються детерміністичним закономірностям. Друга – практично неминучі катастрофічні події, що підкоряються стохастичним закономірностям. Третя – віртуальні катастрофічні події, для яких відсутні детерміністичні або стохастичні закономірності.

На підставі цих семи принципів розроблені і використовуються два основних методологічних підходи в управлінні безпекою локального об'єкта. Це інженерно-технологічний і логіко-математичний підходи, які дозволяють формалізувати (описати за допомогою математичних символів і формул) управління процесами безпеки функціонування підприємства.

В основу інженерно-технологічного підходу покладені уявлення про закономірності зв'язку елементів технічних підсистем управління, що спостерігаються на практиці, і фізичні, технологічні, енергетичні, інформаційні та інші процеси, що відбуваються в них. Їх специфіка визначається практичною необхідністю конкретних однозначних рішень, прийнятих окремо згідно з відповідними локальними теоріями, такими як теорія автоматичного управління, теорія систем, теорія інформації, теорія енергетичних систем та інші. Ці рішення об'єднуються в теорію управління безпекою на основі якісних (інформаційно-логічних) уявлень.

Логіко-математичний підхід націлений на побудову моделі аналізу безпеки на основі алгебри логіки, теорії ймовірностей і математичної статистики. Використовуються математичні поняття, такі як ймовірність, граничний перехід і інші, які виключають практичну наочність і однозначність. У той же час цей підхід є основоположним в сучасній теорії безпеки та ілюструється деревом подій, яке реалізує розроблену математичну модель.

Іншими словами, застосування сучасної теорії безпеки (використовується інженерно-технічний або логіко-математичний методологічний підхід в управлінні безпекою локального об'єкта) зводиться до двох етапів. На першому здійснюється розробка математичних моделей виникнення конкретної катастрофічної події на локальному об'єкті, в певних (заданих) умовах. На другому – розробка превентивних заходів, що перешкоджають настанню цієї катастрофічної події, а в разі її настання – мінімізації можливих наслідків.

Таким чином, управління безпекою об'єкта критичної інфраструктури зводиться в кінцевому підсумку до розробки математичних моделей виникнення конкретної катастрофічної події на цьому об'єкті і її (математичної моделі) подальшого використання для розробки превентивних заходів, що перешкоджають настанню цієї катастрофічної події, а в разі її настання – мінімізації можливих наслідків.

Деякі системні суперечності в процесі управління безпекою об'єкта критичної інфраструктури

Як було показано вище, принциповим положенням теорії управління безпеки є розробка (вибір) математичної моделі, яка описує конкретну катастрофічну подію (або час її настання, або інший її параметр). У логіко-математичному підході, що реалізується в методі дерева подій, використовується уявлення про необмежену випадкову безперервну величину часу настання катастрофічної події n, щільність ймовірності якої $\psi(y)$. Значення випадкової величини n належать напівнескінченному інтервалу

$$y \in [0;\infty],$$

тоді справедливо

$$P\{n \in [0;\infty]\} = \int_0^\infty \psi(y)dy = 1 . \qquad (1)$$

Імовірність катастрофічної події на тимчасовому інтервалі $[0;\tau]$ терміну експлуатації об'єкта дорівнюватиме

$$P\{n \in [0;\tau]\} = \int_0^\tau \psi(y)dy = 1 - \int_\tau^\infty \psi(y)dy . \qquad (2)$$

Конкретизуємо приклад. Нехай об'єкт критичної інфраструктури це АЕС, а катастрофічна подія – це важка аварія, викликана руйнуванням активної зони реактора (як на Чорнобильській АЕС). Нормоване допустиме значення подібної катастрофічної події дорівнює 10^{-7} реактор/рік. При терміні служби (експлуатації) реактора рівному 30 років (τ = 30 років), ймовірність подібної аварії за період експлуатації складе

$$P\{n \in [0;\tau]\} = \int_0^\tau \psi(y)dy = 3 * 10^{-6} \text{ (реактор/термін експлуатації)} . \qquad (3)$$

Така ймовірність катастрофічної події дуже мала, що на думку фахівців-нормувальників, робить важку аварію, подібну Чорнобильській, практично неможливою.

Необхідно відзначити, що тут виникає принципове протиріччя в процесі управління безпекою об'єкта критичної інфраструктури. Тут не враховується похибка апроксимації обмеженого терміну експлуатації об'єкта необмеженою випадковою величиною. Це призводить до наступної некоректності математичної моделі.

Для необмеженої випадкової величини n часу аварії, подібної до Чорнобильської, значення ймовірності катастрофічної події на інтервалі $[\tau;\infty]$ після зняття АЕС з експлуатації складе

$$P\{n \in [\tau;\infty]\} = \int_{\tau}^{\infty} \psi(y)dy = 0{,}999\,997\,. \qquad (4)$$

Отримуємо, що найбільша (майже стовідсоткова) ймовірність аварії, подібної до Чорнобильської, настане після зняття АЕС з експлуатації. Подібне суперечить здоровому глузду, тому що після зняття реактора з експлуатації з нього витягують все ядерне паливо, розбирають системи забезпечують роботу реактора і виконуються інші демонтажні заходи. Очевидно, що після зняття з експлуатації ядерного реактора, аварія подібна до Чорнобильської, статися не може.

Іншими словами, моделі, в яких час настання катастрофічної події є необмеженою випадковою величиною не можуть бути прийняті для коректної оцінки ймовірності ризику її (катастрофічної події) настання.

Нехай в нашому арсеналі є моделі, де час настання катастрофічної події μ з щільністю ймовірності $\varphi(x)$, є обмеженою випадковою величиною (обмеженою терміном експлуатації об'єкта). Тоді все значення випадкової величини x кінцевому інтервалу μ, який визначається терміном служби (або експлуатації) об'єкта, тобто $x \in \mu \in [0;\tau]$.

Тоді ймовірність катастрофічної події – аварії, подібної до Чорнобильської, буде визначатися як

$$P\{\mu \in [0;\tau]\} = \int_{0}^{\tau} \varphi(x)dx = 1. \qquad (5)$$

Тобто, згідно з моделями, в яких час настання катастрофічної події обмежено часом експлуатації об'єкта, ймовірність її настання стовідсоткова. Тому, незалежно від прийнятих заходів щодо забезпечення безпеки об'єкта критичної інфраструктури, найважча аварія, подібна до Чорнобильської, все одно відбудеться за час експлуатації АЕС. Безумовно, це суперечить здоровому глузду.

Іншими словами, моделі, в яких час настання катастрофічної події є обмеженою випадковою величиною, наприклад, часом експлуатації об'єкта або часом експлуатації ядерного реактора, не можуть бути прийняті для коректної оцінки ймовірності ризику її (катастрофічної події) настання.

Таким чином, в двох підходах управління безпекою об'єктів критичної інфраструктури, що використовуються, існують об'єктивні протиріччя. У першому випадку, коли час настання катастрофічної події є необмеженою випадковою величиною, теоретична аварія настає через мільйони років, що робить моделі управління безпекою об'єктів некоректними. У другому випадку, коли час настання катастрофічної події є обмеженою випадковою величиною, теоретична аварія стовідсотково настає за час експлуатації об'єкта, що так само суперечить здоровому глузду і робить некоректними оцінки ймовірності ризику настання катастрофічної події.

Висновки

1. Під терміном процес управління безпекою об'єкта критичної інфраструктури, будемо розуміти діяльність керівництва підприємства і системи його безпеки на ліквідацію зовнішніх і внутрішніх загроз його існування і функціонування, обумовлених потенційними (прогнозованими) катастрофічними подіями природного, техногенного та терористичного характеру.

2. Управління безпекою об'єкта критичної інфраструктури зводиться в кінцевому підсумку до розробки математичних моделей виникнення конкретної катастрофічної події на цьому об'єкті і її (математичної моделі) подальшого використання для розробки превентивних заходів, що перешкоджають настанню цієї катастрофічної події, а в разі її настання – мінімізації можливих наслідків.

3. У двох підходах управління безпекою об'єктів критичної інфраструктури, що використовуються, існують об'єктивні протиріччя. У першому випадку, коли час настання катастрофічної події є необмеженою випадковою величиною, теоретична аварія настає через мільйони років, що робить моделі управління безпекою об'єктів некоректними. У другому випадку, коли час настання катастрофічної події є обмеженою випадковою величиною, теоретична аварія стовідсотково настає протягом часу експлуатації об'єкта, що так само суперечить здоровому глузду і робить некоректними оцінки ймовірності ризику настання катастрофічної події.

ПЕРЕЛІК ПОСИЛАНЬ

1. Азаренко Е.В. Защита критической инфраструктуры государства от террористического воздействия / Е. В. Азаренко, Ю. Ю. Гончаренко, М. М. Дивизинюк, М. И. Ожиганова - Киев: ГП «ИГОС НАН Украины», 2018. 84 с. ISBN 978-617-7187-25-6

2. Информационно-технические методы предотвращения чрезвычайных ситуаций террористического характера на объектах критической инфраструктуры. Часть 1. С использованием активных импульсных радиолокационных средств / за ред. Дивизинюк М. М. Киев: ГП «ИГОС НАН Украины», 2019. 164 с. ISBN 978-617-7187-33-1.

3. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О. М. Суходолі. Київ : НІСД, 2020. 28 с.

4. Андронов В. А., Науково-конструкторські створення комплексної системи моніторингу надзвичайних ситуацій в Україні: Монографія / В. А. Андронов, М. М. Дівізінюк, В. Д. Калугін, В. В. Тютюник. – Х.: НУЦЗУ, 2016. – 319 с. ISBN 978-617-7474-74-5.

5. Герасимов Б.М. Системы поддержки принятия решений: проектирование, применение, оценка эффективности: монография / Б. М. Герасимов, М. М. Дивизинюк, И. Ю. Субач // Севастополь: СНИЯЭиП, 2004. 318 с.

6. Азаренко Е. В Структурно-логическая модель управления чрезвычайной ситуацией террористического характера и ее особенности, обусловленные скрытым электромагнитным воздействием на оперативный состав охраняемого объекта критической инфраструктуры / Е. В. Азаренко, Ю. Ю. Гончаренко, М. М. Дивизинюк, В. И. Мирненко, Ю. А. Сирица // Social development & Security, Vol. 10, No. 1, – 2020. P. 177 – 187.

7. Азаренко О. В. Особливості управління надзвичайною ситуацією на водному транспортному засобі / О. В. Азаренко, М. М. Дівізінюк, Е. В. Иванов, В. І. Мірненко, О. В. Фаррахов // Journal of Scientific Papers "Social development & Security". 2019. № 9 (3). С. 137–152. https://doi.org/10.33445/sds.2019.9.3.11.

8. Андронов В. А. Науково-технічні основи синтезу системи моніторингу надзвичайних ситуацій на території України в рамках державної політики в галузі цивільного захисту / В. А. Андронов, О. В Азаренко, М. М. Дівізінюк, В. Д. Калугін, В. В. Тютюник // Збірник наукових праць Харківського національного університету Повітряних Сил імені Івана Кожедуба. Харків: Харківський Національний університет Повітряних Сил імені Івана Кожедуба, 2016. Вип. 4 (49). С. 150 – 160 http://www.hups.mil.gov.ua /periodic-app/article/17268.

9. Гончаренко Ю. Ю., Структурно-логическая модель управления безопасностью критически важного объекта / Ю. Ю. Гончаренко, Н. В. Касаткина, Г. В. Камышенцев, С. В. Лазаренко // Інформаційна безпека – науковий журнал східноукраїнського національного університету імені Володимира Даля. Северодонецьк: СУНУ ім. В. Даля, №1(25), 2017. С. 63 – 69. http://www.lib.nau.edu.ua/ praci/12008Lazarenko.pdf.

10. Гончаренко Ю. Ю. Структура модели управления чрезвычайной ситуацией по уровням и этапам на охраняемых предприятиях Украины / Ю. Ю. Гончаренко // Збірник наукових праць СНУЯЕтаП. Севастополь: СНУЯЕтаП,2011. Вип. 19. С. 10 – 19.

11. Пампуро В. И. Оптимальное управление безопасностью экологически опасних объектов / В. И. Пампуро // Киев: Наукова думка, 2012, 599с. ISBN 978-9666-00-1155-7.

12. Азаренко Е. В. Процесс развития чрезвычайной ситуации на охраняемом объекте критической инфраструктуры / Е. В. Азаренко, Ю. Ю. Гончаренко, М. М. Дивизинюк, В. И. Мирненко, Ю. А. Сирица, В. Н. Олиферук // Journal of Scientific Papers "Social Development and Security". 2019. 9 (6). 132-146.

13. Безопасность. Доступ: https://ua.wikipedia.org/wiki/%D0%91%D0%

14. Гихман И. И. Теория случайных процессов, т. I / И. И. Гихман, А. В. Скороход // М., «Наука», 1971. 664 с.

15. Гихман И. И. Теория случайных процессов, т. II / И. И. Гихман, А. В. Скороход // М., «Наука», 1975. 630 с.

16. Гихман И. И. Теория вероятностей и математическая статистика / И. И. Гихман, А. В. Скороход, М. И. Ядренко // Киев: Вища школа, 1979. 408 с.

REFERENCES

1. Azarenko E. V. Zashchyta krytycheskoi ynfrastrukturu hosudarstva ot terrorystycheskoho vozdeistvyia / E. V. Azarenko, Yu. Iu. Honcharenko, M. M. Dyvyzyniuk, M. Y. Ozhyhanova - Kyev: HP «YHOS NAN Ukrayny», 2018. 84 s. ISBN 978-617-7187-25-6.

2. Ynformatsyonno-tekhnycheskye metody predotvrashchenyia chrezvuchainukh sytuatsyi terrorystycheskoho kharaktera na obyektakh krytycheskoi ynfrastruktury. Chast 1. S yspolzovanyem aktyvnukh ympulsnukh radyolokatsyonnыkh sredstv / za red. Dyvyzyniuk M. M. Kyev: HP «YHOS NAN Ukrayny», 2019. 164 s. ISBN 978-617-7187-33-1.

3. Derzhavna systema zakhystu krytychnoi infrastruktury v systemi zabezpechennia natsionalnoi bezpeky: analit. dop. / za red. O. M. Sukhodoli. Kyiv : NISD, 2020. 28 s.

4. Andronov V. A., Naukovo-konstruktorski stvorennia kompleksnoi systemy monitorynhu nadzvychainykh sytuatsii v Ukraini: Monohrafiia / V. A. Andronov, M. M. Diviziniuk, V. D. Kaluhin, V. V. Tiutiunyk. – Kh.: NUTsZU, 2016. – 319 s. ISBN 978-617-7474-74-5.

5. Herasymov B. M. Sistemy podderzhky priniatyia reshenyi: proektyrovanye, prymenenye, otsenka effektyvnosty: monohrafyia / B. M. Herasymov, M. M. Dyvyzyniuk, Y. Iu. Subach // Sevastopol: SNYIaEyP, 2004. 318 s.

6. Azarenko E. V Strukturno-lohycheskaia model upravlenyia chrezvychainoi sytuatsyei terrorystycheskoho kharaktera y ee osobennosty, obuslovlennye skrutum эlektromahnytnym vozdeistvyem na operatyvnyi sostav okhraniaemoho obyekta krytycheskoi ynfrastruktury / E. V. Azarenko, Yu. Iu. Honcharenko, M. M. Dyvyzyniuk, V. Y. Myrnenko, Yu. A. Syrytsa // Social development & Security, Vol. 10, No. 1, – 2020. R. 177 – 187.

7. Azarenko O. V. Osoblyvosti upravlinnia nadzvychainoiu sytuatsiieiu na vodnomu transportnomu zasobi / O. V. Azarenko, M. M. Diviziniuk, E. V. Yvanov, V. I. Mirnenko, O. V. Farrakhov // Journal of Scientific Papers “Social development & Security”. 2019. № 9 (3). S. 137–152. https://doi.org/10.33445/sds.2019.9.3.11.

8. Andronov V. A. Naukovo-tekhnichni osnovy syntezu systemy monitorynhu nadzvychainykh sytuatsii na terytorii Ukrainy v ramkakh derzhavnoi polityky v haluzi tsyvilnoho zakhystu / V. A. Andronov, O. V Azarenko, M. M. Diviziniuk, V. D. Kaluhin, V. V. Tiutiunyk // Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl imeni Ivana

Kozheduba. Kharkiv: Kharkivskyi Natsionalnyi universytet Povitrianykh Syl imeni Ivana Kozheduba, 2016. Vyp. 4 (49). S. 150 – 160 http://www.hups.mil.gov.ua /periodic-app/article/17268.

9. Honcharenko Yu. Iu., Strukturno-lohycheskaia model upravlenyia bezopasnostiu krytychesky vazhnoho obъekta / Yu. Iu. Honcharenko, N. V. Kasatkyna, H. V. Kamышentsev, S. V. Lazarenko // Informatsiina bezpeka – naukovyi zhurnal skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia. Severodonetsk: SUNU im. V. Dalia, №1(25), 2017. S. 63 – 69. http://www.lib.nau.edu.ua/ praci/12008Lazarenko.pdf.

10. Honcharenko Yu. Iu. Struktura modely upravlenyia chrezvychainoi sytuatsyei po urovniam y эtapam na okhraniaemykh predpryiatyiakh Ukrayny / Yu. Iu. Honcharenko // Zbirnyk naukovykh prats SNUIaEtaP. Sevastopol: SNUIaEtaP,2011. Vyp. 19. S. 10 – 19.

11. Pampuro V. Y. Optymalnoe upravlenye bezopasnostiu эkolohychesky opasnykh obъektov / V. Y. Pampuro // Kyev: Naukova dumka, 2012, 599s. ISBN 978-9666-00-1155-7.

12. Azarenko E. V. Protsess razvytyia chrezvыchainoi sytuatsyy na okhraniaemom obъekte krytycheskoi ynfrastrukturы / E. V. Azarenko, Yu. Iu. Honcharenko, M. M. Dyvyzyniuk, V. Y. Myrnenko, Yu. A. Syrytsa, V. N. Olyferuk // Journal of Scientific Papers "Social Development and Security". 2019. 9 (6). 132-146.

13. Bezopasnost. Dostup: https://ua.wikipedia.org/wiki/%D0%91%D0%

14. Hykhman Y. Y. Teoryia sluchainykh protsessov, t. I / Y. Y. Hykhman, A. V. Skorokhod // M., «Nauka», 1971. 664 s.

15. Hykhman Y. Y. Teoryia sluchainykh protsessov, t. II / Y. Y. Hykhman, A. V. Skorokhod // M., «Nauka», 1975. 630 s.

16. Hykhman Y. Y. Teoryia veroiatnostei y matematycheskaia statystyka / Y. Y. Hykhman, A. V. Skorokhod, M.Y. Yadrenko // Kyev: Vyshcha shkola, 1979. 408 s.

Elena Azarenko[1], *Doctor of physics and mathematics, professor (ORCID: 0000-0003-2927-5545),*
Yulia Honcharenko[2], *Doctor of technical sciences, docent (ORCID: 0000-0003-2045-0263),*
Mykhailo Divizinyuk[3], *Doctor of technical sciences, professor (ORCID: 0000-0002-5657-2302),*
Oleksandr Tyschenko[4], *Candidate of technical science, professor, (ORCID: 0000-0001-7303-6360)*
Oleh Miroshnyk[4], *Doctor of technical sciences, docent (ORCID: 0000-0001-8951-9498),*
Oleh Zemlianskyi[4], *Candidate of technical science, docent (ORCID: 0000-0002-2728-6972),*
Dmytro Lesechko[4] *(ORCID: 0000-0002-4792-5284)*
[1]National Aviation University,
[2]European univereity,
[3]The Institute of Environmental Geochemistry of National Academy of Sciences of Ukraine,
[4]Cherkassy Institute of Fire Safety Named after Chernobyl Heroes
of National University of Civil Defense in Ukraine

DISTRIBUTING TO THE PROCESS OF MANAGING THE SECURITY OF A CRITICAL INFRASTRUCTURE

The work is devoted to the substantiation of objective contradictions in the process of safety management of a critical infrastructure facility. It is shown that the main goal of managing the safety of a critical infrastructure facility (or managing an emergency of a natural, man-made or terrorist nature at this facility) is to prevent a catastrophic event around which an emergency situation develops, and in the event of its (catastrophic event) occurrence, to minimize damage and possible consequences. To study this goal, the following scientific problems were solved. First, the definition of the term "process of safety management of a critical infrastructure facility" is given. The term process of safety management of a critical infrastructure facility is understood as the activities of the enterprise management and its security system to eliminate external and internal threats to its existence and functioning, caused by potential (predictable) catastrophic events of a natural, man-made and terrorist

nature. Secondly, the main principles of managing the security processes of the enterprise and their mathematical formalization are formulated. It is shown that safety management of a critical infrastructure facility is ultimately reduced to the development of mathematical models of the occurrence of a specific catastrophic event at this facility and its (mathematical model) subsequent use for the development of preventive measures to prevent the onset of this catastrophic event, and in the event of its occurrence - to minimize possible consequences. Thirdly, some systemic contradictions in the process of managing the safety of a critical infrastructure facility have been identified. There are objective contradictions in the two approaches used to manage the safety of critical infrastructure facilities. In the first case, when the time of the onset of a catastrophic event is an unlimited random variable, a theoretical accident occurs in millions of years, which makes the safety management models of facilities incorrect. In the second case, when the time of the onset of a catastrophic event is a limited random value, a theoretical accident occurs one hundred percent during the operation of the facility, which also contradicts common sense and makes incorrect estimates of the probability of the risk of a catastrophic event.

Keywords: *safety, safety management, critical infrastructure object, probability, risk, random variable.*