ІНСТИТУТ МАТЕМАТИКИ
МНО АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"

УНІВЕРСИТЕТ МІСТА ЖИЛІНА

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей шістнадцятої міжнародної

науково-технічної конференції

29 – 30 квітня 2026 року

Том 5: **секція 6**

Баку – Харків – Жиліна – 2026

УДК 004/681.3 doi: https://doi.org/10.32620/ICT.26.t5

У збірнику подано тези доповідей шістнадцятої міжнародної науково-технічної конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління". Розглянуті питання за такими напрямами: теоретичні та прикладні аспекти систем прийняття рішень, оптимізації та управління системами і процесами; комп'ютерні методи та засоби інформаційно-комунікаційних технологій та управління; безпека функціонування комп'ютерних систем та мереж; інформаційні технології у цивільній безпеці; сучасні інформаційно-вимірювальні системи; інформаційні технології у цивільній безпеці.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Співголови оргкомітету

ГАШИМОВ Ельшан Гіяс огли (*д.н.б.&в.н., проф., ІМ АР, Баку, Азербайджан*);
КОВАЛЕНКО Андрій Анатолійович (*д.т.н., проф., ХНУРЕ, Харків, Україна*);
КУЧУК Георгій Анатолійович (*д.т.н., проф., НТУ «ХПІ», Харків, Україна*);
ЛЕВАШЕНКО Віталій (*к.т.н., проф., Ун-т міста Жиліна, Жиліна, Словаччина*);
ФЕДОРОВИЧ Олег Євгенович (*д.т.н., проф., НАУ «ХАІ», Харків, Україна*).

Члени оргкомітету

ГЛАВЧЕВ Максим Ігорович (*к.е.н., доц., НТУ «ХПІ», Харків, Україна*);
ГЛИВА Валентин Анатолійович (*д.т.н., проф., КНУБА, Київ, Україна*);
ДОРОНІН Євген Володимирович (*к.т.н., доц., ДУ «КАІ», Київ, Україна*);
ЗАЙЦЕВА Єлєна (*к.т.н., проф., Ун-т міста Жиліна, Жиліна, Словаччина*);
КАЛІНІН Євгеній Іванович (*д.т.н., проф., НУ БрПкУ, Київ, Україна*);
КАРПІНСЬКІ Міколай (*д.н., проф., Університет Бельсько-Бяла, Польща*);
КОЛОМІЙЦЕВ Олексій Володимирович (*д.т.н., проф., НТУ «ХПІ», Харків, Україна*);
КОСЕНКО Віктор Васильович (*д.т.н., проф., НУ «ПП», Полтава, Україна*);
ЛЕВЧЕНКО Лариса Олексіївна (*д.т.н., проф., НТУУ «КПІ», Київ, Україна*);
ЛЕЩЕНКО Олександр Борисович (*к.т.н., проф., НАУ «ХАІ». Харків, Україна*);
МОЖАЄВ Олександр Олександрович (*д.т.н., проф., ХНУВС, Харків, Україна*);
ПОДОРОЖНЯК Андрій Олексійович (*к.т.н., доц., НТУ «ХПІ», Харків, Україна*);
РОМАНЕНКОВ Юрій Олександрович (*д.т.н., проф., ХНУРЕ, Харків, Україна*);
РУБАН Ігор Вікторович (*д.т.н., проф., ХНУРЕ, Харків, Україна*);
СЄВЄРІНОВ Олександр Васильович (*к.т.н., доц., ХНУРЕ, Харків, Україна*);
СЕМЕНОВ Сергій Геннадійович (*д.т.н., проф.,УКНО, Краків, Польща*);
СМІРНОВ Олександр Анатолйович (*д.т.н., проф., ЦНТУ, Кропивницький, Україна*);
ТРЕТЬЯКОВ Олег Вальтерович (*д.т.н., проф., ДУ «КАІ», Київ, Україна*);
ШЕФЕР Олександр Віталійович (*д.т.н., проф., НУ «ПП», Полтава, Україна*).

Секретаріат оргкомітету

КУЧУК Ніна Георгіївна (*д.т.н., проф., НТУ «ХПІ», Харків, Україна*);
ЛЯШЕНКО Олексій Сергійович (*к.т.н., доц., ХНУРЕ, Харків, Україна*).

© ІМ АР, НТУ "ХПІ", ХНУРЕ, НАУ «ХАІ», УмЖ, 2026

INSTITUTE OF MATHEMATICS
OF THE MINISTRY OF SCIENCE AND EDUCATION
OF THE REPUBLIC OF AZERBAIJAN

NATIONAL TECHNICAL UNIVERSITY
KHARKIV POLYTECHNIC INSTITUTE

KHARKIV NATIONAL UNIVERSITY
OF RADIO ELECTRONICS

NATIONAL AEROSPACE UNIVERSITY
KHARKIV AVIATION INSTITUTE

UNIVERSITY OF ŽILINA

CURRENT DIRECTIONS IN THE DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES AND CONTROL TOOLS

Proceedings of 16-th International

Scientific and Technical Conference

April 29 – 30, 2026

Volume 5: section 6

Baku – Kharkiv – Žilina – 2026

UDC 004/681.3 doi: https://doi.org/10.32620/ICT.26.t5

Abstracts of reports of the 16-th international scientific and technical conference "Current directions of development of information and communication technologies and control tools" are presented in the collection. Considered issues in the following directions: theoretical and applied aspects of decision-making systems, optimization and control of systems and processes; computer methods and means of information and communication technologies and management; security of functioning of computer systems and networks; information technologies in civil security; modern information and measurement systems; information technologies in civil security.

ORGANIZING COMMITTEE

Co-chairs of the organizing committee:

Elshan Giyas oglu HASHIMOV (Dr. Nat. security and mil. sc., Baku, Azerbaijan);
Andriy KOVALENKO (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Heorhii KUCHUK (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Vitaly LEVASHENKO (Dr. (Comp. Eng.), Prof., Zilina, Slovakia);
Oleg FEDOROVICH (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine).

Members of the organizing committee:

Maksym HLAVCHEV (PhD (Усоп.), Ass. Prof., Kharkiv, Ukraine);
Valentyn GLYVA (Dr. Sc. (Tech.), Prof., Kyiv, Ukraine)
Yevhen DORONIN (*PhD (Tech.), Ass. Prof., Kyiv, Ukraine*);
Elena ZAITSEVA (Dr. (Comp. Eng.), Prof., Zilina, Slovakia);
Yevhen KALININ (Dr. Sc. (Tech.), Prof., Kyiv, Ukraine);
Mikolay KARPINSKI (Dr. Sc. (Tech.), Prof., Bielsko-Biala, Poland);
Oleksii KOLOMIITSEV (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Viktor KOSENKO (Dr. Sc. (Tech.), Prof., Poltava, Ukraine)
Larysa LEVCHENKO (Dr. Sc. (Tech.), Ass. Prof., Kyiv, Ukraine);
Oleksandr LESHCHENKO (PhD (Tech.), Prof., Kharkiv, Ukraine);
Oleksandr MOZHAIEV (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Andrii PODOROZHNIAK (PhD (Tech.), Ass. Prof., Kharkiv, Ukraine);
Yuri ROMANENKOV (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Igor RUBAN (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Oleksandr SIEVIERINOV (PhD (Tech.), Ass. Prof., Kharkiv, Ukraine);
Serhii SEMENOV (Dr. Sc. (Tech.), Prof., Krakow, Poland);
Oleksii SMIRNOV (Dr. Sc. (Tech.), Prof., Kropyvnytskyi, Ukraine);
Oleg TRETYAKOV (*Dr. Sc. (Tech.), Prof., Kyiv, Ukraine*);
Oleksandr SHEFER (Dr. Sc. (Tech.), Prof., Poltava, Ukraine).

Secretariat of the organizing committee:

Nina KUCHUK (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Oleksii LIASHENKO (PhD (Tech.), Ass. Prof., Kharkiv, Ukraine).

Шістнадцята міжнародна науково-технічна конференція “Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління” проводиться 29 та 30 квітня 2026 року в режимі ONLINE. Тези доповідей доступні в INTERNET.

Том 1 (Volume 1)

Секція 1. Теоретичні та прикладні аспекти прийняття рішень, оптимізації та управління системами і процесами

Section 1. Theoretical and Applied Aspects of Decision-Making, Optimization, and Systems and Process Management

Секція 5. Сучасні інформаційно-вимірювальні системи

Section 5. Modern Information and Measurement Systems

Том 2 (Volume 2)

Секція 2. Комп’ютерні методи і засоби інформаційно-комунікаційних технологій та управління

Section 2. Computer Methods and Tools of Information and Communication Technologies and Management

Том 3 (Volume 3)

Секція 3. Методи швидкої та достовірної обробки даних в комп’ютерних системах та мережах

Section 3. Methods for Rapid and Reliable Data Processing in Computer Systems and Networks

Секція 4. Безпека функціонування комп’ютерних систем та мереж

Section 4. Security of Computer Systems and Networks Operation

Томи 4, 5 (Volumes 4, 5)

Секція 6. Інформаційні технології у цивільній безпеці

Section 6. Information Technologies in Civil Security

СЕКЦІЯ 6

Керівник секції: д.т.н. проф. О. В. Третьяков, ДУ «КАІ», Київ
Секретар секції: к.т.н. доц. Є. В. Доронін, ДУ «КАІ», Київ

Підсекція 6.3. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЦИВІЛЬНІЙ БЕЗПЕЦІ

ГІБРИДНА ІНТЕЛЕКТУАЛЬНА СИСТЕМА МОНІТОРИНГУ ПОВЕРХНЕВИХ ВОД ДЛЯ ЗАВДАНЬ ЦИВІЛЬНОЇ БЕЗПЕКИ

Безсонний В.Л.
Харківський національний економічний університет
імені С. Кузнеця, Харків, Україна
Харківський національний університет ім. В. Н. Каразіна,
Харків, Україна
Максименко В.О.
Харківський національний університет імені В. Н. Каразіна,
Харків, Україна

В умовах воєнних дій, техногенних аварій та зростаючого антропогенного навантаження контроль екологічного стану поверхневих вод набуває особливого значення для цивільної безпеки. Руйнування гідротехнічних споруд, забруднення водойм продуктами вибухів, нафтопродуктами та завислими речовинами створюють довготривалі ризики для населення, інфраструктури й екосистем. Традиційні методи моніторингу, що базуються на стаціонарних постах спостереження та лабораторних аналізах, не забезпечують необхідної оперативності, просторового охоплення та безпеки роботи персоналу в небезпечних зонах.

Перспективним напрямом розв'язання цієї проблеми є використання даних дистанційного зондування Землі та методів штучного інтелекту. У доповіді запропоновано концепцію гібридної системи моніторингу поверхневих вод, яка поєднує мультиспектральні супутникові дані Sentinel-2, алгоритми комп'ютерного зору та генеративні мовні моделі. Використання супутникових знімків забезпечує регулярне спостереження за великими територіями без фізичної присутності дослідників, що є критично важливим в умовах мінної небезпеки та обмеженого доступу до постраждалих районів.

Основою кількісної оцінки стану водних об'єктів є спектральні індекси. Для виявлення евтрофікації та зон цвітіння водоростей доцільно застосовувати індекс NDCI, який враховує відбиття у червоному та червоному краї спектра. Для оцінки каламутності води та переміщення завислих частинок використовується індекс NDTI. Особливу роль у підвищенні точності аналізу відіграють канали Red Edge супутника Sentinel-2, чутливі до змін біомаси фітопланктону та оптичних характеристик водного середовища.

Для інтелектуального аналізу супутникових зображень запропоновано використовувати архітектуру Vision Transformer. На відміну від класичних

згорткових нейронних мереж, вона дозволяє враховувати глобальний просторовий контекст зображення, що особливо важливо під час аналізу протяжних річкових систем, водосховищ і зон затоплення. Це підвищує точність сегментації водних поверхонь, виділення меж між водою, сушею, рослинністю та хмарами, а також дає змогу точніше фіксувати аномальні зміни після надзвичайних подій.

Окремим компонентом системи є семантичний модуль на базі великих мовних моделей із застосуванням підходу Retrieval-Augmented Generation. Його призначення полягає не лише у формуванні текстових звітів, а й у поясненні виявлених аномалій із прив'язкою до верифікованих джерел, нормативних документів і попередніх результатів спостережень. Такий підхід знижує ризик фактологічних помилок та робить результати аналізу придатними для підтримки управлінських рішень у сфері цивільної безпеки.

Запропонована система може бути використана для оперативного виявлення екологічних загроз, ранжування територій за рівнем ризику, документування наслідків техногенних катастроф і воєнних дій, а також для підтримки рішень щодо реагування та відновлення. Її практична цінність полягає у поєднанні масштабності супутникового спостереження, точності сучасних моделей глибокого навчання та можливості автоматизованої інтерпретації результатів у зрозумілій для фахівців формі.

Таким чином, впровадження гібридної інтелектуальної системи моніторингу поверхневих вод є перспективним напрямом розвитку інформаційних технологій у цивільній безпеці. Такий підхід дозволяє перейти від фрагментарного спостереження до безперервного, обґрунтованого та безпечного екологічного контролю, що особливо актуально для України в умовах сучасних викликів.

Список літератури

1. Екологічні наслідки руйнування Каховської греблі під час війни в Україні. URL: https://www.nas.gov.ua/news/kahovska-katastrofa-matime-viddaleni-ekologichni-naslidki

2. Policy and technical brief on use of Earth observations to assess ecosystems damage in Ukraine. UNECE. 2024. URL: https://unece.org/sites/default/files/2024-05/Policy%20and%20technical%20brief%20on%20use%20of%20Earth%20observations%20to%20assess%20ecosystems%20damage%20in%20Ukraine.pdf

3. Mishra S., Mishra D. R. Normalized difference chlorophyll index: A novel model for remote estimation of chlorophyll-a concentration in turbid productive waters. *Remote Sensing of Environment*. 2012. Vol. 117. P. 394–406.

4. Dosovitskiy A., Beyer L., Kolesnikov A. et al. An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. *ICLR*. 2021. URL: https://arxiv.org/abs/2010.11929

5. Lewis P., Perez E., Piktus A. et al. Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks. *NeurIPS*. 2020. Vol. 33. P. 9459–9474. URL: https://arxiv.org/abs/2005.11401

РИЗИК-ОРІЄНТОВАНА ОЦІНКА ЯКОСТІ ПОВЕРХНЕВИХ ВОД БАСЕЙНУ ПІВДЕННОГО БУГУ ДЛЯ ПІДТРИМКИ РІШЕНЬ У СФЕРІ ЦИВІЛЬНОЇ БЕЗПЕКИ

Безсонний В.Л.
Харківський національний економічний університет
імені С. Кузнеця, Харків, Україна
Харківський національний університет ім. В. Н. Каразіна,
Харків, Україна
Третьяков О.В., Доронін Є.В.
Державний університет «Київський авіаційний інститут»,
Київ, Україна

Водна безпека є одним із ключових компонентів цивільної безпеки, оскільки стан поверхневих вод безпосередньо впливає на питне водопостачання, зрошення, промислове використання та стійкість водних екосистем.

Для басейнів річок України ризики формуються під впливом як природних чинників, так і антропогенних навантажень, серед яких особливе значення мають комунально-побутові скиди, аграрне освоєння територій, урбанізація та гідротехнічне регулювання русел. У цих умовах актуальним є перехід від описового аналізу якості води до ризик-орієнтованого підходу, що дозволяє оцінювати не лише факт відхилення показників, а й частоту, інтенсивність та просторову локалізацію екологічної небезпеки.

Метою роботи є розробка та апробація відтворюваної методики оцінки ризику погіршення якості води в басейні річки Південний Буг на основі частоти та інтенсивності перевищення нормативних значень. Дослідження виконано за даними державного моніторингу поверхневих вод за 2003–2023 рр., які охоплюють 4766 вимірювань у 77 пунктах спостереження. Для оцінювання використовувалися показники $БСК_5$, розчиненого кисню, завислих речовин, сульфатів, хлоридів, амонію, нітритів, нітратів, фосфатів, СПАР, перманганатної окислюваності та ХСК. Як порогові значення приймалися нормативи ГДК, а інтегральний ризик пункту визначався шляхом агрегування показників перевищення для окремих компонентів.

Методичний підхід базується на поєднанні логіки DPSIR та ймовірнісної інтерпретації гідрохімічних даних. На відміну від традиційних індексів якості води, запропонована схема дає змогу враховувати повторюваність порушень нормативів, а не лише усереднені концентрації. Це є особливо важливим для задач цивільної безпеки, де управлінське рішення повинно спиратися на виявлення стійких зон ризику, пріоритетних для природоохоронного реагування, посиленого контролю або модернізації мережі моніторингу.

Результати розрахунків показали чітко виражену просторову неоднорідність екологічного ризику в межах басейну Південного Бугу. Встановлено, що найвищі значення інтегрального ризику характерні для урбанізованих ділянок, зон впливу очисних споруд, приток із інтенсивним

сільськогосподарським використанням і регульованих відрізків русла. Підвищені значення зафіксовано, зокрема, у пунктах спостереження на р. Кодима в районі м. Балта, у Бузькому лимані поблизу м. Миколаїв, а також на окремих ділянках Південного Бугу, Інгулу та Ташлицького водосховища.

Отриманий рейтинг підтвердив, що основну частину сумарного ризику формує відносно невелика кількість локальних осередків антропогенного впливу.

Аналіз структури ризику показав, що провідними чинниками деградації якості води у масштабі басейну є біогенні елементи — нітрити, фосфати та нітрати, що свідчить про домінування процесів евтрофікації та комунально-побутового забруднення.

Органічні показники, зокрема $БСК_5$ і ХСК, формують підвищений ризик переважно локально, поблизу місць скиду стічних вод. Також встановлено, що екологічна небезпека визначається не стільки окремими екстремальними випадками, скільки систематичними повторюваними перевищеннями нормативів, що підтверджує доцільність використання саме ймовірнісних ризикових метрик у практиці моніторингу.

Запропонована методика є відтворюваною, не потребує складних математичних моделей та може бути реалізована на основі стандартних даних державного моніторингу. Її практична цінність полягає у можливості просторового ранжування ділянок басейну за рівнем екологічної небезпеки, виявлення домінуючих факторів ризику та обґрунтування пріоритетів природоохоронних заходів.

Для сфери цивільної безпеки такий підхід створює аналітичну основу для своєчасного прийняття рішень щодо захисту населення, водокористування та збереження екосистемних функцій річкових басейнів.

Список літератури

1. Song X., Frostell B. The DPSIR framework and a pressure-oriented water quality monitoring approach to ecological river restoration. *Water*. 2012. Vol. 4(3). P. 670–682.

2. Uddin M. G., Nash S., Olbert A. I. A review of water quality index models and their use for assessing surface water quality. *Ecological Indicators*. 2021. Vol. 122. 107218.

3. Liu Y., Zhang X., Chen Y. et al. Combined exceedance probability assessment of water quality indicators based on multivariate joint probability distribution in urban rivers. *Water*. 2018. Vol. 10(8). 971.

4. Brito I., Gonçalves A. M., Pedra A. Risk assessment for the surface water quality evaluation of a hydrological basin. *Stochastic Environmental Research and Risk Assessment*. 2024. Vol. 38. P. 4527–4553.

5. Bezsonnyi V. Use of the entropy approach in water resource monitoring systems. *Visnyk of V. N. Karazin Kharkiv National University, Series "Geology. Geography. Ecology"*. 2023. No. 58. P. 302–320.

6. Bezsonnyi V., Nekos A. Analysis of the environmental risk of water bodies in conditions of military danger. *Monitoring of Geological Processes and Ecological Condition of the Environment, Monitoring 2023*. 2023.

ФІЗИЧНИЙ ЗАХИСТ НАФТОПЕРЕРОБЛЮЮЧИХ КОМПЛЕКСІВ

Буюн Д.О., Доронін Є.В., Макаров В.І.
Державний університет "Київський авіаційний інститут",
Київ, Україна

Для забезпечення безпеки критично важливих для економіки України об'єктів нафтопереробної промисловості:

– нафтопереробні заводи,

– термінали,

– резервуарні парки,

– трубопроводи тощо,

одним з факторів, що забезпечує їх безпеку є система їх фізичного захисту, яка здатна протистояти правопорушникам.

Фізичну безпеку підприємства, установи або організації визначають як сукупність правових норм, організаційних заходів та інженерно-технічних рішень, які здійснені з метою захисту важливих споруд, будівель, земельних ресурсів підприємства, кадрового складу об'єкта від загроз злочинних протиправних дій фізичних осіб незалежно від їх статусу.

Фізична безпека містить комплекс сил служби безпеки і охорони об'єкта, комплекс інженерно-технічних приладів та систем охорони, режим охорони, який встановлений на об'єкті.

Метою доповіді є таке: показати та навести основні принципи фізичного захисту нафтопереробляючих комплексів в Україні під час військового стану та в мирний час.

Система фізичного захисту повинна перешкоджати спробам порушення нормального функціонування підприємств, установ та організацій, їх технологічних процесів та роботи загалом.

Завданнями системи фізичного захисту є:

– запобігання здійсненню незаконних дій (або бездіяльності) потенційним правопорушником щодо ядерної установки та ядерних матеріалів;

– виявлення вторгнення правопорушників у зони обмеження доступу;

– затримка просування правопорушників у зонах обмеження доступу;

– реагування на дії правопорушників;

– пом'якшення наслідків незаконних дій щодо ядерної установки та ядерних матеріалів.

За функціональним призначенням в систему фізичного захисту входять пристрої та системи [1]:

– сигналізації виявлення, збору і обробки інформації,

– тривожно викличної сигналізації,

– контролю і управління доступом,

– оптоелектронного спостереження,

– оперативного зв'язку та оповіщення,

– забезпечення електроживлення і електроосвітлення,

– системи забезпечення фізичного захисту ядерних матеріалів при транспортуванні.

Засоби сигналізації поділяються на технічні засоби охоронної, пожежної і тривожної сигналізації [2].

Системи охорони приміщень і контролю прилеглої території на потенційно небезпечних об'єктах, що охороняються, розподіляються по трьох таких зонах:

– внутрішньої,

– охоронюваному периметру,

– зовнішньої (санітарній) зонах.

Основним завданням управління надзвичайної ситуацію є зменшення ступеня небезпеки або загрози, одним з підходів до оцінки якої є концепція ризику.

Одним з перспективних напрямків підвищення ефективності процесу управління надзвичайною ситуацією терористичного характеру на об'єктах критичної інфраструктури держави, що охороняються, є вдосконалення систем фізичного захисту шляхом розробки нових пристроїв і систем акустичного контролю приміщень і територій об'єкта і знімання мовної інформації з використанням параболічних, трубчастих і градієнтних мікрофонів і плоских акустичних фазованіх решіток, які забезпечують прийом акустичних сигналів на видаленні від декольких десятків до кількох сотень метрів і забезпечують повну інформацію про дії та наміри людей, що реєструються в відео системах [3].

В доповіді викладені основні принципи фізичного захисту нафтопереробляючих комплексів та намічені шляхи її подальшого вдосконалення.

Список літератури

1. Олена Азаренко, Юлія Гончаренко, Михайло Дівізінюк, Володимир Мірненко, Валерій Стрілець. Шляхи підвищення ефективності систем візичного захисту об'єктів критичної інфраструктури держави, що охороняються. *Journal of Scientific Papers "Social Development and Security*", Vol. 11, No. 4, – 2021

2.. Третьяков О. В., Доронін Є. В., Халмурадов В. Д.., Зозуля С. В. Основи пожежної безпеки. Київ : Центр учбової літератури. 2024. 356 с.

3. Про затвердження Загальних вимог до систем фізичного захисту ядерних установок та ядерних матеріалів і Загальних вимог до систем фізичного захисту ядерних матеріалів при їх перевезенні. Державний комітет ядерного регулювання України. Наказ № 156 від 28.08.2008.

СИСТЕМИ ПРОТИПОЖЕЖНОГО ЗАХИСТУ ЕНЕРГОГЕНЕРУЮЧИХ ПІДПРИЄМСТВ

Манохін Д., Доронін Є.В.
Державний університет "Київський авіаційний інститут",
Київ, Україна

За минулий рік в Україні за різними причинами виникало більше 97 тис пожеж, вони принесли значні збитки економіці Держави та загиблі люди. Значна кількість пожеж виникла у приватному сектору, але пожежі не забули й про виробничий сектор, який забезпечує економічну безпеку України, до якого відносяться й енергогенеруючі підприємства. Забезпечення їх стабільної роботи є основою сталої роботи усього економічного комплекса нашої Держави.

Тому підвищення й постійна турбота за протипожежний стан енергетичних підприємств є основою забезпечення стійкості роботи енергогенеруючих підприємств.

Основу протипожежного захисту їх забезпечують системи протипожежного захисту, які й є надійною частиною.

Метою доповіді є визначення систем протипожежного захисту, які використовуються у енергетичному комплексі та визначити шляхи вдосконалення протипожежного стану енергогенеруючих комплексів.

Відомо, що до систем протипожеж ного захисту відносяться:

системи пожежної сигналізації;
автоматичні системи пожежогасіння;
автономні системи пожежогасіння;
системи керування евакуацією;
системи протидимного захисту;
системи централізованого пожежного спостерігання;
системи диспетчеризації СПЗ;
системи флегматизації,
системи протипожежного водопроводу тощо [1, 2].

Вдосконалення систем протипожежного захисту може здійснюватися різними шляхами: роброзбкою нових сповіщувачівта приймальних станцій та подальшим хз вдосконаленням.

В доповіді визначена класифікація систем протипожежного захисту та намічені шляхи їх вдосконалення.

Список літератури

1. ДБН В.2.5-56:2014. Системи протипожежного захисту. Київ: Мінрегіонбуд Украхни, 2019. 103 с.

2.. Третьяков О. В., Доронін Є. В., Халмурадов В. Д.., Зозуля С. В. Основи пожежної безпеки:Підручник. 2-ге вид. Київ : Видавництво "SBA Print". 2026. 356 с.

ЗАБЕЗПЕЧЕННЯ ПОЖЕЖНОЇ БЕЗПЕКИ В СУЧАСНИХ БАГАТОПОВЕРХОВИХ БУДІВЛЯХ

Калитчук А., Саньков П.М., Пилипенко О.В.
Навчально-науковий інститут «Придніпровська державна академія будівництва та архітектури» УДУНТ, Дніпро, Україна

Постановка проблеми. Сучасне будівництво характеризується зростанням кількості багатоповерхових будівель, що обумовлює підвищення вимог до рівня їх пожежної безпеки [1, 2].

Використання новітніх будівельних матеріалів, складних інженерних систем і збільшення щільності забудови створює додаткові ризики виникнення та швидкого поширення пожеж.

Мета дослідження. Метою роботи є аналіз сучасних методів забезпечення пожежної безпеки в багатоповерхових будівлях та визначення ефективних заходів щодо її підвищення.

Результати дослідження. Пожежна безпека будівель забезпечується комплексом організаційних і технічних заходів. Важливу роль відіграє правильне проектування евакуаційних шляхів, що дозволяє забезпечити швидке та безпечне виведення людей із будівлі. При цьому враховуються кількість мешканців, поверховість будівлі, її функціональне призначення та можливі сценарії розвитку пожежі [3, 4]. Відповідно до нормативних вимог, евакуаційні виходи повинні бути достатньої ширини, не захараченими та доступними у будь-який час.

Одним із ключових елементів є план евакуації, який містить інформацію про шляхи виходу, місця розташування засобів пожежогасіння та порядок дій у разі виникнення надзвичайної ситуації.

Наявність таких планів сприяє зниженню паніки та підвищує ефективність евакуації.

Особливе значення має правильне розміщення цих планів у доступних для огляду місцях, а також їх відповідність фактичному плануванню будівлі [3].

Сучасні багатоповерхові будівлі оснащуються автоматичними системами пожежної сигналізації, оповіщення та управління евакуацією, системами димовидалення і автоматичного пожежогасіння. Використання таких систем дозволяє своєчасно виявити осередок загоряння, локалізувати його та запобігти поширенню вогню і диму.

Особливо ефективними є спринклерні системи пожежогасіння, які автоматично реагують на підвищення температури та забезпечують гасіння пожежі на початковій стадії [4; 5].

Важливим напрямком є застосування будівельних матеріалів із підвищеною вогнестійкістю. Конструктивні елементи будівель повинні зберігати несучу здатність протягом визначеного часу, що необхідний для евакуації людей та роботи пожежно-рятувальних підрозділів. Використання негорючих матеріалів для оздоблення приміщень також сприяє зниженню швидкості поширення пожежі [4; 5].

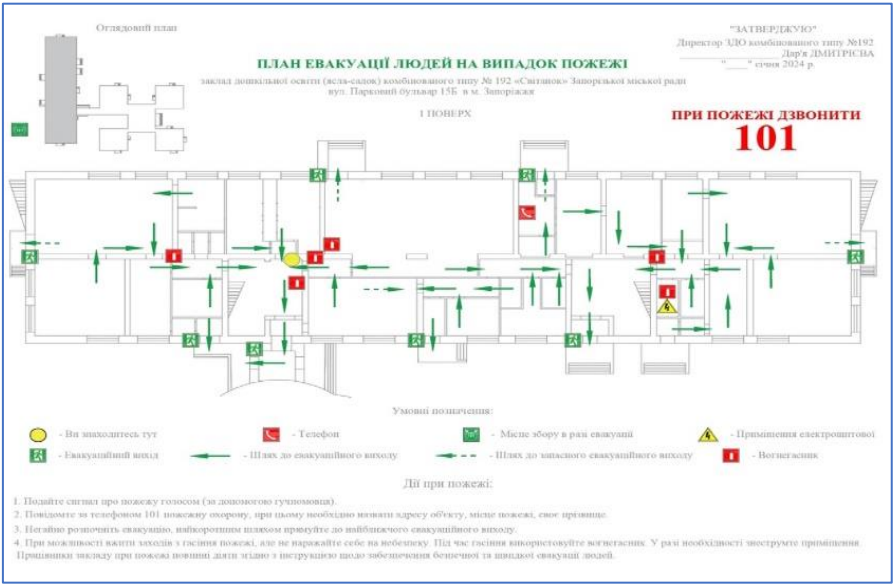

Рисунок 1 – Схема евакуації людей
у багатоповерховій будівлі при пожежі

Висновки. Забезпечення пожежної безпеки в сучасних багатоповерхових будівлях є складним комплексним завданням, що потребує поєднання технічних і організаційних заходів.

Використання сучасних технологій і дотримання нормативних вимог дозволяє значно знизити ризик виникнення пожеж і забезпечити безпеку людей [1, 2].

Список літератури

1. *Пожежна безпека об'єктів будівництва. Загальні вимоги: ДБН В.1.1-7:2016.* — Мінрегіонбуд України, 2017.

2. *Висотні будівлі. Основні положення: ДБН В.2.2-41:2019.* — Мінрегіонбуд України, 2019.

3. Балло Я. В., Голікова С. Ю., Сізіков О. О. *Вимоги пожежної безпеки до висотних будівель* / Науковий вісник: Цивільний захист та пожежна безпека, 2021.

4. Yemelianenko S., Kharchuk A., Miller O. *Аналіз пожежних ризиків для багатоповерхових житлових будинків*. — Пожежна безпека, № 27, 2018.

5. Kodur V., Kumar P., Rafi M. M. *Fire hazard in high-rise buildings: strategies for improving fire safety*. — Applied Sciences, 2021.

УПРАВЛІННЯ РИЗИКАМИ ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННИХ ЗАГРОЗ

Кічата Н.М., Третьяков О.В.
Державний університет «Київський авіаційний інститут»,
Київ, Україна

Стабільне функціонування об'єктів критичної інфраструктури є важливою умовою забезпечення безпеки та життєдіяльності населення. В умовах воєнного періоду об'єкти критичної інфраструктури зазнають значного впливу від різноманітних загроз, зокрема руйнувань унаслідок бойових дій, диверсійних впливів, кібератак та порушення логістичних процесів.

Внаслідок високого рівня взаємозалежності інфраструктурних систем пошкодження окремих елементів може призводити до розвитку каскадних ефектів, що ускладнює процеси оцінювання та управління ризиками [1].

Метою доповіді є розроблення підходу до управління ризиками функціонування об'єктів критичної інфраструктури в умовах воєнних загроз з урахуванням ймовірності виникнення каскадних ефектів.

Запропонований підхід базується на системному аналізі загроз, оцінюванні сценаріїв розвитку небезпечних подій, виділенні ключових загроз, що ініціюють каскадні ефекти, та їх подальшому ранжуванні за рівнем ризику. Реалізація цього підходу дозволяє:

– своєчасно виявляти потенційні джерела каскадних ефектів,
– підвищувати стійкість об'єктів критичної інфраструктури,
– зменшувати негативні наслідки реалізації загроз,
– забезпечувати безперервність їх функціонування.

Підхід створює основу для кількісного оцінювання ймовірностей розвитку каскадних ефектів і визначення рівня стійкості об'єктів на основі аналізу переходів між станами системи. Формалізація процесів розвитку небезпечних подій здійснюється із застосуванням ймовірнісного підходу, що дозволяє описати динаміку зміни станів об'єкта у вигляді сукупності можливих переходів між ними [2].

При цьому враховуються інтенсивності переходів між станами, що характеризують швидкість розвитку небезпечних подій та ймовірність їх ескалації у складніші сценарії.

Такий підхід дає змогу оцінювати взаємозв'язки між окремими подіями, визначати їх комбінований вплив на функціонування об'єкта та ідентифікувати критичні елементи інфраструктури, відмова яких може призвести до виникнення каскадних ефектів.

Практичне застосування запропонованого підходу забезпечує можливість визначення найбільш імовірних сценаріїв розвитку надзвичайних ситуацій, оцінювання часових характеристик їх поширення та встановлення пріоритетності впливу окремих факторів ризику.

Це, у свою чергу, створює передумови для підвищення точності оцінювання рівня стійкості об'єктів критичної інфраструктури та

обґрунтування ефективних заходів щодо запобігання та мінімізації наслідків надзвичайних ситуацій.

Стійкість визначається як здатність систем протистояти негативним впливам, адаптуватися до змін умов функціонування та відновлювати роботу після виникнення надзвичайних ситуацій [2].

Підвищення стійкості досягається шляхом:

– удосконалення системи управління ризиками,

– підвищення рівня фізичного та інформаційного захисту,

– створення резервних систем,

– альтернативних джерел ресурсів,

– впровадження систем моніторингу та раннього виявлення загроз,

– підготовки персоналу до реагування на надзвичайні ситуації [3].

Рівень стійкості доцільно оцінювати за допомогою системи кількісних показників, що відображають імовірності переходів між станами функціонування об'єкта та інтенсивність розвитку небезпечних подій [4].

На відміну від існуючих підходів, запропонований підхід забезпечує формалізацію процесів розвитку каскадних ефектів у вигляді ймовірнісної моделі переходів між станами системи, що дозволяє не лише оцінювати поточний рівень ризику, але й прогнозувати динаміку його зміни в умовах воєнних загроз.

Це дає можливість визначати найбільш критичні сценарії розвитку подій та обґрунтовувати пріоритетні заходи щодо мінімізації ризиків і підвищення стійкості об'єктів критичної інфраструктури.

Запропонований підхід може бути адаптований до різних секторів критичної інфраструктури з урахуванням їх функціональних особливостей та характеру загроз і використаний при розробленні стратегій забезпечення національної стійкості, а також удосконаленні нормативно-методичного забезпечення у сфері захисту критичної інфраструктури.

Список літератури

1. Корченко А.О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями / А.О. Корченко, В.А. Козачок, А.І. Гізун // Захист інформації. 2015. Т. 17, № 1. С. 86-98.

2. Methodology for assessing regional infrastructure resilience (CISA). May 2021. Version 1.0.

3. Zio, E. Challenges in the vulnerability and risk analysis of critical infrastructures, Reliability Engineering and System Safety, 152, 2016. pp. 137-150.

4. Кічата Н.М., Третьяков О.В., Федина В.П., Доронін Є.В. Методологічний підхід до підвищення безпеки та стійкості об'єктів критичної інфраструктури. Науково-технічний журнал «Техногенно-екологічна безпека», №16 (2/2024). 2024. С.3 – 10. DOI: 10.52363/2522-1892.2024.2.1

СТВОРЕННЯ СТІЙКИХ СИСТЕМ ЖИТТЄЗАБЕЗПЕЧЕННЯ У ТЕРИТОРІАЛЬНИХ ГРОМАДАХ

Курська Т.М., Калач І.В.
Національний університет «Одеська політехніка», Одеса, Україна

Системи життєзабезпечення територіальних громад (енергопостачання, водопостачання, теплопостачання, продовольче забезпечення, охорона здоров`я) є основою стабільного функціонування суспільства. В умовах зростання техногенних загроз, змін клімату та воєнних ризиків забезпечення їх стійкості набуває особливої актуальності.

Порушення функціонування цих систем може призвести до значних соціальних і економічних наслідків [1, 2].

Метою доповіді є визначення підходів до створення стійких систем життєзабезпечнення у територіальних громадах в умовах сучасних викликів.

Для вирішення цих достатньо складних питань необхідно:

– проаналізувати основні складові систем життєзабезпечення,

– визначити ключові загрози їх функціонуванню

– обґрунтовано представити напрями їх підвищення.

Міжнародні організації акцентують увагу на концепції “resilience” (стійкості), яка передбачає здатність систем протистояти, адаптуватися та швидко відновлюватися після кризових ситуацій [3–5].

Основні принципи створення стійких систем - це надійність, резервування, адаптивність, відновлюваність та децентралізація. В країнах Європейського Союзу активно впроваджуються концепції сталого розвитку та стійкості громад, що передбачають інтеграцію управління ризиками у всі сфери життєдіяльності.

Основними напрямами вдосконалення стійких систем є:

– підвищення рівня фінансування інфраструктури громад,

– розвиток державно-приватного партнерства,

– впровадження сучасних стандартів управління ризиками,

– цифрова трансформація громад,

– інтеграція з європейськими системами безпеки.

Комплексний підхід, що включає організаційні, технічні та соціальні заходи, дозволить забезпечити безперервність життєдіяльності та підвищити рівень безпеки.

Список літератури

1. Кодекс цивільного захисту України від 02.10.2012 № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17

2. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20

3. ISO 31000:2018 Risk management — Guidelines.

4. ISO 22301:2019 Security and resilience — Business continuity management systems.

5. UNDRR. Sendai Framework for Disaster Risk Reduction 2015–2030.

РОЗРОБКА ІНЖЕНЕРНО-ТЕХНІЧНИХ ЗАХОДІВ ЦИВІЛЬНОГО ЗАХИСТУ ДЛЯ ЗАХИСТУ ПЕРСОНАЛУ

Курська Т.М., Лобяк Т.А.
Національний університет «Одеська політехніка», Одеса, Україна

Забезпечення безпеки персоналу на виробничих об`єктах є одним з ключових завдань системи цивільного захисту.

У сучасних умовах зростання техногенних, природних та військових загроз питання впровадження ефективних інженерно-технічних заходів набуває особливої актуальності. Недостатній рівень захищеності персоналу може призвести до значних людських втрат, порушення виробничих процесів та економічних збитків [1, 2].

Метою доповіді є обґрунтування інженерно-технічних заходів цивільного захисту для забезпечення ефективного захисту персоналу в умовах надзвичайних ситуацій.

Проблеми інженерного захисту населення і персоналу розглядаються у працях фахівців у сфері цивільного захисту та охорони праці, де основна увага приділяється проектуванню захисних споруд, системам оповіщення, а також впровадженню сучасних технологій захисту [3–5].

До основних небезпечних факторів, що впливають на персонал, можна віднести:

– вплив небезпечних виробничих факторів,
– хімічне та радіаційне забруднення,
– обрушення будівель і споруд,
– пожежі та вибухи,
– наслідки військових дій.

Інженерно-технічні заходи цивільного захисту - це комплекс рішень, спрямованих на зниження ризиків впливу небезпечних факторів та забезпечення захисту персоналу шляхом використання технічних засобів і інженерних конструкцій.

В умовах сьогодення необхідно визначити пріритені напрямки вдосконалення вже відомих інженерно-технічних заходів. Для цього необхідним є впровадження, насамперед, міжнародних стандартів безпеки, відповідна модернізація існуючих захисних споруд, а також підвищення рівня автоматизації на об`єктах.

Список літератури

1. Кодекс цивільного захисту України від 02.10.2012 № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17
2. ДБН В.1.2-4:2019 «Інженерно-технічні заходи цивільного захисту».
3. Закон України «Про охорону праці». URL: https://zakon.rada.gov.ua/laws/show/2694-12
4. ISO 45001:2018 Occupational health and safety management systems.
5. ISO 22301:2019 Security and resilience — Business continuity management systems.

ОРГАНІЗАЦІЯ ФУНКЦІОНУВАННЯ ОБ`ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ АВАРІЙНИХ ВІДКЛЮЧЕНЬ

Курська Т.М., Кеня М.А.
Національний університет «Одеська політехніка», Одеса, Україна

Об’єкти критичної інфраструктури забезпечують життєдіяльність держави та суспільства в цілому. Аварійні відключення електроенергії, спричинені техногенними аваріями, природними явищами або військовими діями, можуть призводити до зупинки роботи об’єктів енергетики, транспорту, медицини та зв`язку.

В сучасних умовах особливої актуальності набуває питання організації безперервного функціонування таких об’єктів [1, 2].

При розгляданні проблеми забезпечення стійкості критичної інфраструктури основна увага приділяється питанням резервування енергопостачання, управлінню ризиками та впровадженню сучасних технологій забезпечення безперервності діяльності (Business Continuty Management). Разом з тим, в умовах сучасних викликів, зокрема воєнного часу, ці питання потребують додаткового дослідження.

Метою доповіді є аналіз організаційних засад функціонування об`єктів критичної інфраструктури в умовах аварійних відключень та визначення ефективних заходів забезпечення їх стійкості. У країнах ЄС та США широко застосовують стандарти управління безперервністю діяльності (ISO 22301), що дозволяють забезпечити стійкість критичної інфраструктури до надзвичайних ситуацій [3–5].

Організація функціонування об`єктів критичної інфраструктури в умовах аварійних відключень потребує комплексного підходу, що включає організаційні, технічні та управлінські заходи.

Основними напрямами вдосконалення можуть бути: підвищення рівня резервування енергопостачання, цифровізація управління інфраструктурою, інтеграція з європейськими системами безпеки, підготовка кваліфікованих кадрів та розвиток державно-приватного партнерства.

Впровадження сучасних технологій та стандартів дозволить підвищити стійкість систем та мінімізувати наслідки надзвичайних ситуацій.

Список літератури

1. Кодекс цивільного захисту України від 02.10.2012 № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17
2. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20
3. ISO 22301:2019 Security and resilience — Business continuity management systems.
4. ISO 31000:2018 Risk management — Guidelines.
5. OECD. Recommendation on the Governance of Critical Risks. 2014.

ЕКОЛОГІЧНІ ПРОБЛЕМИ УКРАЇНИ В УМОВАХ ВІЙНИ

Новоселя У.Д., Макаренко М.Є., Саньков П.М., Ткач Н.О.
Навчально-науковий інститут «Придніпровська державна академія будівництва та архітектури» УДУНТ, Дніпро, Україна

У теперішньому столітті питання екологічної безпеки набуває особливої актуальності, а в умовах повномасштабної війни в Україні воно перетворюється на одну з ключових складових безпеки життєдіяльності населення.

Військові дії спричиняють масштабні руйнування не лише інфраструктури та економіки, але й довкілля, що має довготривалі та часто незворотні наслідки.

Однією з найсерйозніших екологічних проблем є забруднення атмосферного повітря.

Вибухи, пожежі, руйнування промислових підприємств та нафтобаз супроводжуються викидами великої кількості токсичних речовин [1]. Шум від звуків війни руйнує психіку людини [2]. Це призводить до погіршення якості повітря та негативно впливає на здоров'я населення, зокрема спричиняє респіраторні захворювання та інші хвороби.

Не менш важливою проблемою є забруднення водних ресурсів. Внаслідок руйнування інфраструктури, витоків нафтопродуктів і хімічних речовин відбувається отруєння річок, підземних вод і водосховищ. Це створює загрозу для водопостачання населення.

Суттєвою екологічною загрозою є деградація ґрунтів.

Вибухи боєприпасів, мінування територій та потрапляння важких металів і токсичних речовин призводять до втрати родючості земель. Значна частина ґрунтів зазнала серйозного забруднення, що ускладнює їх подальше використання у сільському господарстві.

Війна також спричиняє значні втрати біорізноманіття.

Руйнування природних екосистем, пожежі в лісах, знищення місць існування тварин і рослин призводять до скорочення чисельності багатьох видів і навіть загрози їх зникнення.

Частина територій природно-заповідного фонду опинилася під окупацією або зазнала значних пошкоджень.

Окремо слід відзначити проблему накопичення відходів війни. Зруйновані будівлі, військова техніка, залишки боєприпасів формують величезні обсяги небезпечних відходів, які містять токсичні речовини та потребують спеціальної утилізації.

Загалом масштаби екологічних збитків є колосальними [3–5].

За даними Міністерства захисту довкілля, зафіксовано тисячі випадків шкоди довкіллю внаслідок збройної агресії рф, а загальні збитки обчислюються трильйонами гривень (рис. 1).

Крім того, війна спричиняє значний вуглецевий слід, що посилює глобальні кліматичні зміни.

Рисунок 1 – Збитки довкіллю внаслідок збройної агресії рф

Таким чином, війна в Україні призвела до комплексної екологічної кризи, яка охоплює всі компоненти довкілля: повітря, воду, ґрунти та біорізноманіття. Подолання цих наслідків потребує значних ресурсів, міжнародної підтримки та впровадження ефективної екологічної політики. Відновлення довкілля стане важливим етапом післявоєнної відбудови України та запорукою безпеки майбутніх поколінь.

Список літератури

1. Вплив війни на екологію - ТОВ «Автоекоприлад». https://eco.aep.kiev.ua/novini/vpliv-vijni-na-ekologiyu/

2. Капленко Д.Д. (АРХ-23мн), Макаренко М.Є.(АРХ-23-1) «Вплив війни на сучасне архітектурне середовище» (керівники: проф. Саньков П.М., доц. Ткач Н.О., ст.викл. Палагіна Л.П.)/ Наука і сталий розвиток транспорту 2024. Т.І: зб. тез доп. Всеукр. наук.-техн. конф. студентів і молодих учених, Дніпро, 27 листоп. 2024р.- Дніпро: УДУНТ, 2028.- 228с. С. 196

3. Міністерство захисту довкілля та природних ресурсів України. Збитки довкіллю від війни. https://mepr.gov.ua/topics/novyny/zbytky-dovkillyu-vid-vijny/

4. Екологічні наслідки війни в Україні: аналітичний огляд (2024–2025). https://mepr.gov.ua/wp-content/uploads/2023/05/DP-Harkivskyj-zavod-spetsialnyh-mashyn.pdf

5. Екологічні наслідки війни: масштаби збитків зростають. https://dei.gov.ua/post/3072

ЗАХОДИ НЕОБХІДНІ ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ ЕНЕРГЕТИЧНОЇ СИСТЕМИ РЕГІОНАЛЬНИХ АЕРОПОРТІВ

Паращанов В.Г., Доронін Є.В.
Державний університет "Київський авіаційний інститут",
Київ, Україна

Для забезпечення стійкості критичної інфраструктури аеропорту в умовах техногенних ризиків і надзвичайних ситуацій необхідно впроваджувати стратегію розвитку енергетичного сектору, засновану на принципах гнучкості, мобільності та резистентності.

У разі виникнення криз система повинна дозволяти швидке перемикання на резервні джерела, а також функціонувати в режимі обмежених ресурсів і непередбачуваних перебоїв.

Метою доповіді є забезпечення стійкості роботи об'єктів критичної інфраструктури в умовах нештатних ситуацій в процесі живлення підприємств.

Когенерація є ефективною технологією одночасного виробництва електричної та теплової енергії в єдиному процесі (зазвичай на базі газових турбін або двигунів).

Коефіцієнт корисної дії таких установок сягає 80–90 %, що значно перевищує показники окремих традиційних електростанцій (близько 35–40 % для електроенергії).

Перехід до когенераційного постачання дозволяє суттєво підвищити автономність, надійність і стійкість енергозабезпечення аеропорту.

Основним рішенням є створення децентралізованих енергетичних «островів» — незалежних модульних систем, здатних працювати автономно від центральної мережі.

Концепція когенерації передбачає розміщення джерел генерації ближче до споживача.

Це зменшує втрати на транспортування енергії, підвищує загальну ефективність і знижує залежність від зовнішніх мереж.

Додаткові заходи для підвищення стійкості є такими:

– встановлення мобільних когенераційних установок, які можна швидко розгортати в кризових ситуаціях.

– інтеграція систем акумулювання енергії (батареї, теплові накопичувачі) для компенсації пікових навантажень і перебоїв.

– комбінування з відновлюваними джерелами (сонячні панелі на дахах терміналів, геотермальні теплові насоси) для гібридних рішень.

– автоматизовані системи управління (SCADA з елементами «розумних» мереж) для моніторингу та швидкого перерозподілу енергії.

– регулярні тренування персоналу та тестування режимів «острівної» роботи.

– впровадження цих заходів не тільки мінімізує ризики блекаутів, але й знижує експлуатаційні витрати, зменшує викиди та підвищує загальну

резистентність аеропорту як об'єкта критичної інфраструктури. У довгостроковій перспективі це сприяє енергетичній незалежності та відповідності міжнародним стандартам безпеки авіаційного транспорту.

Для досягнення стратегічної мети – надійного енергозабезпечення аеропорту в кризових умовах – необхідно реалізувати комплекс тактичних кроків:

- забезпечення технологічної модернізації когенераційних установок та залучення інвестицій для підвищення їхньої ефективності;
- розробка сучасної системи управління та моніторингу енергоспоживання, що дозволить оптимізувати використання ресурсів і зменшити енергоємність;
- створення механізму оцінки та постійного моніторингу ризиків для когенераційних систем, включаючи щоденний контроль ситуації в зоні їх розташування;
- формування резерву електроенергії, палива та води для безперервної роботи установок і мінімізації ймовірності відмов;
- організація тісної співпраці з місцевими органами влади та енергетичними компаніями;
- підготовка до оперативного реагування на будь-які збої чи загрози для когенераційного обладнання.

Реалізація цих заходів гарантує створення стабільної та ефективної системи когенерації в аеропорту.

З економічного погляду впровадження когенерації принесе наступні переваги:

✓ зростання прибутковості завдяки децентралізації системи та кращому контролю витрат на виробництво тепла;

✓ зниження витрат на енергоносії через ефективніше використання ресурсів і зменшення споживання палива;

✓ покращення роботи теплових мереж за рахунок адаптації до потреб окремих зон;

✓ підвищення резистентності критичної інфраструктури аеропорту до різних загроз;

✓ збільшення надійності електро- та теплопостачання, запобігання аварійним ситуаціям.

Критичними вузлами електричного навантаження є:

1. Термінали, технічні споруди, насосні станції та приміщення обслуговування — об'єкти, життєво важливі для функціонування аеропорту.
2. Вузли видачі потужності в розподільчі або транзитні мережі.
3. Зони з потенційним дефіцитом потужності.

Підключення когенераційних установок до системи аеропорту не повинно порушувати стабільну роботу електроспоживачів, насосних станцій чи очисних споруд.

Схема, наведена на рис. 1, показує процес електропостачання та роботи насосної станції.

Спочатку електроенергія виробляється за допомогою розділеної когенерації. Далі вона передається через лінії електропередач (ЛЕП). Після цього електроенергія надходить на знижувальну підстанцію ДТЕК.

На підстанції напруга зменшується до потрібного рівня для споживання. Потім електроенергія подається на насосну станцію.

На станції використовується перетворювач частоти струму для керування обладнанням. Насосна станція забезпечує подачу води населенню та відведення стоків.

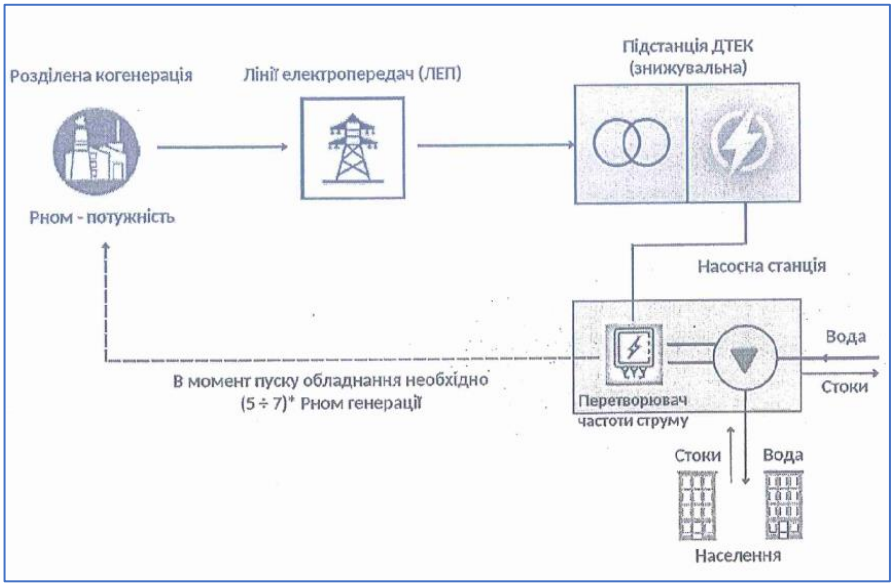

Рисунок 1 – Схема електроживлення від когенераційних установок

Для зменшення споживання електроенергії з центральної мережі пропонується встановлювати альтернативні джерела на найбільш енергоємних об’єктах.

Список літератури

1. Малишев В. В. Альтернативна енергетика / Конспект лекцій / Університет Україна. - Київ. 2022.

2. Паращанов В.Г., Доронін Є.В. Забезпечення стійкості об'єктів критичної інфраструктури з використанням альтернативних джерел енергопостачання. Проблеми інформатизації : матеріали XIII Міжнар. наук.-техніч. конф., м. Харків, 27 – 28 листопада 2025 р. Харків, 2025. С. 140–141.

МЕТОДОЛОГІЯ ОЦІНКИ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Паращанов В.Г., Доронін Є.В.
Державний університет "Київський авіаційний інститут",
Київ, Україна

Процес оцінки стійкості критичної інфраструктури розпочинається з виявлення проблеми та продовжується через створення плану оцінювання, збір необхідних даних, їх аналіз, документування результатів, презентацію висновків і стимулювання зацікавлених сторін до практичних кроків для підвищення стійкості.

Кожен етап передбачає активну співпрацю з партнерами, що допомагає визначити спільні виклики, забезпечити підтримку, обмін даними, обговорення попередніх висновків та реалізацію рекомендацій, отриманих за підсумками оцінки.

Якісний аналіз ризиків базується переважно на суб'єктивній оцінці, яка враховує характеристики загроз, їхній потенційний вплив та ймовірність виникнення.

Цей підхід застосовується, коли даних недостатньо або потрібна оперативна попередня оцінка. Для класифікації ризиків використовуються описові шкали, наприклад, «низький», «середній» чи «високий». Зазвичай якісний аналіз включає такі етапи:

Ідентифікація ризиків: визначення потенційних загроз, здатних вплинути на об'єкт, процес чи мету.

Оцінка ризиків: аналіз їхнього можливого впливу та ймовірності на основі експертних думок, історичного досвіду та іншої якісної інформації.

Ранжування ризиків: встановлення пріоритетів залежно від ступеня серйозності, з урахуванням наслідків і ймовірності.

Реагування на ризики: призначення відповідних стратегій – уникнення, пом'якшення, передача чи прийняття [1, 2].

Метою доповіді є визначення методології оцінки стійкості об'єктів критичної інфраструктури.

Для системного виявлення та вирішення проблем стійкості регіональної інфраструктури рекомендується дотримуватися шести основних етапів.

Перший етап – «Ідентифікація проблеми».

Він починається з чіткого формулювання проблеми та розробки концепції, яку партнери мають вирішувати спільно. Громади в різних регіонах часто стикаються з подібними прогалинами в розумінні та забезпеченні стійкості інфраструктури.

Визначивши ці прогалини, регіональні партнери можуть використовувати їх як основу для подальших оцінок.

Ефективна концепція оцінки ґрунтується на точно сформульованому питанні чи проблемі. Часто ініціатива виникає від зацікавлених сторін на основі практичного досвіду чи попередніх досліджень.

Оскільки проекти підвищення стійкості спрямовані на заповнення прогалин у знаннях, важливо визначити, якої саме інформації бракує та які дослідження допоможуть її отримати.

Другий етап – «Проектування оцінки».

На цьому кроці формулюються ключові дослідницькі питання, визначається географічний масштаб, обираються інфраструктурні системи для аналізу та плануються конкретні дії для отримання відповідей.

Третій етап – «Збір даних».

Він включає використання відкритих джерел, міжвідомчу співпрацю, інтерв'ю з експертами, фокус-групи, обстеження об'єктів та інші методи для отримання необхідної інформації. Дані для оцінки стійкості можуть бути різноманітними:

– якісними та кількісними,

– зібраними різними способами.

Четвертий етап – «Аналіз».

Тут застосовуються аналітичні методи (наприклад, просторовий аналіз, моделювання чи симуляція) для оцінки обраних інфраструктурних систем. Після збору даних основна увага приділяється пошуку відповідей на дослідницькі питання.

П'ятий етап – «Документування та презентація результатів».

Основний акцент робиться на фіксації виявлених проблем, викликів і можливостей, а також на формулюванні потенційних напрямів дій для усунення прогалин у стійкості.

Шостий етап – «Сприяння діям».

Фінальний крок передбачає створення умов для практичної реалізації висновків через:

– інвестиції,

– планування,

– навчання

– тренування.

Збір даних і аналіз є важливими, але не завершальними.

Результати оцінки мають інтегруватися в довгостроковий процес управління ризиками, стимулюючи спільні дії для досягнення реального прогресу в підвищенні стійкості.

В доповіді визначена методологія оцінки стійкості об'єктів критичної інфраструктури та визначені етапи вирішення проблем стійкості регіональної інфраструктури

Список літератури

1. Атлас енергетичного потенціалу відновлюваних джерел енергії України / За ред. С.О. Кудрі. Київ.: ТОВ "Віол Принт",– 2008. 55 с.

2. Кудря С.О. Електроенергетичний потенціал відновлюваних джерел енергії України / Матеріали XXI-ої міжнародної конференції "Відновлювана енергетика та енергоефективність XXI століття", м. Київ, 14-15 травня 2020 р. − С. 26-33.

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ОСНОВИ ПРОВЕДЕННЯ ВИПРОБУВАНЬ НА ВОДОВІДДАЧУ ПРОТИПОЖЕЖНОГО ВОДОПРОВОДУ

Петухова О.А., Трипольська К.С.
Національний університет цивільного захисту України, Черкаси, Україна

Випробування на водовіддачу систем протипожежного водопостачання є важливою складовою підтримання в працездатному стані елементів комплексу протипожежного захисту об'єктів.

Під час випробувань визначається фактична кількість води, яку можна забрати з мережі для цілей пожежогасіння.

Для одержання достовірного результату випробувань необхідно виконання наступних вимог:

- вибір місця та часу проведення випробувань повинні відповідати найгіршим умовам роботи мережі з точки зору її водозабезпечення;
- вибір типу та кількості приладів для проведення вимірювань повинні враховувати особливості мережі (зовнішня або внутрішня, параметри тиску та витрат води, діаметр труб);
- перерахунок та оцінювання результатів вимірювань та загальні результати випробувань необхідно порівнювати з нормативними витратами води на пожежогасіння для того об'єкта, який захищається мережею.

Якісне виконання кожного етапу проведення випробувань забезпечується багатьма показниками, одним з яких є якісна підготовка тих, хто безпосередньо приймає участь у випробуваннях.

Покращення цього процесу на сьогодні забезпечується використанням інформаційних технологій.

Для підготовки до проведення випробувань викладачами НУЦЗ України підготовлені дистанційні курси, навчально-тестові симулятори, навчальні відеофільми, а для самоконтролю - контрольні питання та тестові завдання. Навчання та контроль засвоєння може проходити самостійно та під керівництвом викладачів, також завдяки використанню гугл-класів можлива дистанційна робота в режимі "питання-відповідь". Аналіз якості вивчення питань проведення випробувань на водовіддачу із використанням запропонованих теоретичних та прикладних можливостей показав, що за умови зацікавленості того, хто навчається, в результативності навчання, використання одержаних знань виключає помилки при проведенні випробувань, а це означає, що кількість води, яку визначено при випробуваннях, є фактичною витратою, що реально можна забрати з водопровідної мережі в будь-яку пору року та будь-яку годину доби на пожежогасіння.

Важливим питанням при проведенні випробувань на водовіддачу є правильне використання приладів при проведенні вимірювань. Це пов'язано з тим, що кількість крапок, де підключаються прилади, залежить від нормативних витрат води на пожежогасіння.

Для зовнішньої мережі кількість $n_{\text{прил}}$ приладів визначається:

$$n_{\text{прил}} = \frac{Q_{\text{пож}}}{5},$$

де $Q_{\text{пож}}$ – нормативні витрати води на пожежогасіння, л/с;

5 – середня пропускна здатність однієї рукавної лінії, яка задіяна при випробуваннях, л/с.

Для внутрішньої мережі кількість $n_{\text{прил}}$ приладів визначається:

$$n_{\text{прил}} = n_{\text{струм}},$$

де $n_{\text{струм}}$ - нормативна кількість струменів для захисту кожної крапки приміщення, що захищається.

Наступним кроком, де можливі похибки при проведенні випробувань, є точність самих приладів.

Найчастіше використовуються прилади, до складу яких входить манометр, встановлений на корпусі приладу. Як показала практика, при підключенні такого приладу до мережі, при вимірюваннях, відбувається коливання стрілки манометра, що призводить до того, що необхідно випробування подовжувати у часі, що збільшує витрати води та вартість самого процесу випробування.

В Національному університеті цивільного захисту України запропоновано вдосконалення, що виключає таку похибку при вимірюваннях та розроблений математичних апарат для оцінювання результатів вимірювань та загальних результатів випробувань.

Таким чином, реалізація теоретичних та практичних пропозицій, спрямованих на покращення процесів підготовки до проведення випробувань, роботи з приладами під час вимірювань, оцінювання результатів випробувань, забезпечить якісне виконання повного комплексу робіт з визначення фактичної кількості води з внутрішньої або зовнішньої мережі для пожежогасіння та відповідно і успішну ліквідацію пожежі.

Список літератури

1. Петухова О. А. Особливості перевірки протипожежного водопроводу. *Захист населення, територій та об'єктів критичної інфраструктури: освіта, наука, практика*: матеріали II Міжнар. наук.-метод. конф. Київ: ДУ КАІ, 2025. С. 34. http://repositsc.nuczu.edu.ua/handle/123456789/26057

2. Петухова О.А., Білаш Є.А., Швед А.В. Інформаційні технології при вивченні дисципліни “Протипожежне водопостачання*”. Free and Open Source Software*: матеріали XVI Міжнародної науково-практичної конференції. Харків: Харківський національний економічний університет імені Семена Кузнеця, 2025. С. 175-176. http://repositsc.nuczu.edu.ua/handle/123456789/24696

ЕВОЛЮЦІЯ ЗМІН РЕКОМЕНДАЦІЙ МКРЗ

Пилипенко О.В., Тимченко П.О.
Навчально-науковий інститут «Придніпровська державна академія будівництва та архітектури» УДУНТ, Дніпро, Україна
Доронін Є.В.
Державний університет "Київський авіаційний інститут",
Київ, Україна

Вступ. Міжнародна комісія з радіологічного захисту (МКРЗ), заснована у 1928 році, є головним міжнародним органом, що формує наукові рекомендації у сфері захисту від іонізуючого випромінювання.

Публікації МКРЗ покладено в основу національних норм більшості країн світу, включаючи:

– українські Норми радіаційної безпеки (НРБУ-97, ОСПУ-2005),

– Basic Safety Standards МАГАТЕ (GSR Part 3, 2014),

– Директиву EURATOM 2013/59.

Еволюція рекомендацій Міжнародної комісії з радіологічного захисту є поступальним науковим обґрунтованим процесом, де кожна базова публікація спирається на нові епідеміологічні та медичні дані, вдосконалені біокінетичні моделі та досвід великих ядерних аварій – Чорнобиля (1986) та Фукусіми (2011).

Мета і завдання дослідження. Метою даної роботи є систематичний аналіз ключових публікацій МКРЗ від Публікації № 9 (1966) до Публікації № 152 (2022), що охоплює понад п'ять десятиліть розвитку системи [1].

Основна частина. Розглянуто ключові публікації, що визначили сучасну систему радіологічного захисту:

Публікація № 60 (формування ефективної дози опромінення),

Публікація № 103 (три ситуації опромінення людини в умовах впливу радіонуклідів), серію OIR (Публікації № 130, № 134, № 137, № 141, № 151),

Публікація № 152 (методологія радіаційного опромінення та розрахунок дози опромінення).

Визначено вплив на нормативну базу України (НРБУ-97, ОСПУ-2005).

Публікація 9 (1966) стала першою базовою рекомендацією МКРЗ формування стохастичних ефектів: Вперше визначено поняття стохастичних ефектів (рак, спадкові наслідки) без безпечного порогу дози та сформульовано прообраз принципу ALARA – підтримувати дози «якомога нижчими». Граничні дози встановлено на рівні 50 мЗв/рік для працівників та 5 мЗв/рік для населення [2].

Публікація 60 (1991) здійснила фундаментальну реформу системи:

– введено сучасне поняття ефективної дози $E = \Sigma_T w_T \times H_T$,

– нові тканинні вагові коефіцієнти w_T (гонади = 0,20; легені, шлунок, кістковий мозок = 0,12),

– знижено граничну дозу для працівників до 20 мЗв/рік (середнє за 5 років).

Radiation detriment уперше оцінено на рівні ~7,3 × 10^{-2} Зв$^{-1}$. Pub 60 лягла в основу НРБУ-97 [3].

Публікація 103 (2007) замінила Публікація 60, модернізувавши систему на концептуальному рівні:

– запроваджено три ситуації опромінення (planned, emergency, existing) замість дихотомії «практики/втручання»;

– суттєво переглянуто w_T:

– гонади знижено з 0,20 до 0,08 (менша вага спадкових ефектів),

– молочну залозу підвищено з 0,05 до 0,12 (нові епідеміологічні дані).

– Radiation detriment оновлено до 5,7 × 10^{-2} Зв$^{-1}$;

– публікація 103 стала основою Норм радіаційної безпеки України, наведених у [4].

Серія OIR: оновлення внутрішньої дозиметрії

Серія Occupational Intakes of Radionuclides (OIR) – найбільший технічний проєкт МКРЗ за останні три десятиліття, що замінив застарілі Публікація 30 (1979÷1988) та Публікація 68 (1994).

Серія базується на оновлених фізіологічних моделях: Human Respiratory Tract Model (HRTM) та Human Alimentary Tract Model (HATM, Pub 100), що забезпечують фізіологічно реалістичне моделювання поглинання, розподілу та виведення радіонуклідів [5].

Публікація 130 (2015) – методологічна основа серії: описано переглянуту HRTM з фракційним осадженням для аерозолів від 0,0006 до 20 мкм, методологію біоаналізу та стандартні параметри моделей.

Публікація 134 (2016) – перший поелементний документ серії, що охоплює 14 елементів: H, C, P, S, Ca, Fe, Co, Zn, Sr, Y, Zr, Nb, Mo, Tc.

Ключовою особливістю є перехід від емпіричних ретенційних моделей до фізіологічно обґрунтованих системних моделей.

Для більшості нуклідів нові коефіцієнти дещо нижчі, проте для окремих форм (^{60}Co тип S, ^{90}Sr тип S, ^{59}Fe тип F) коефіцієнти зросли через уточнення моделей тканинного утримання [4].

Публікація 137 (2017) – найоб'ємніша публікація серії, що охоплює 14 радіологічно найзначущіших елементів: Ru, Sb, Te, I, Cs, Ba, Ir, Pb, Bi, Po, Rn, Ra, Th, U.

Серед ключових змін:

– для урану UO_2 та U_3O_8 перекласифіковано з типу S на тип M/S (відношення $e(50)_{OIR}/e(50)_{ICRP119}$ = 0,23÷0,84);

– для радону нові коефіцієнти – 3 мЗв/(мДж·год·м$^{-3}$) (~10 мЗв/WLM);

– для цезію та йоду – уточнені моделі утримання 48].

Публікація 141 (2019) та **Публікація 151 (2022)** завершили серію OIR, охопивши лантаноїди, актиноїди (^{239}Pu, ^{241}Am – основні дозоформуючі нукліди паливного циклу) та решту елементів.

З виходом Публікація 151 завершено майже 40-річний процес оновлення Публікація 30 [5].

Публікація 152 (2022) – методологічний документ, що формалізує процедуру розрахунку radiation detriment:

– від номінального ризику (lifetime attributable risk, моделі ERR/EAR, DDREF = 2) до корекції на тяжкість (lethality fraction, quality of life, years of life lost).

Документ визначив пріоритети для наступних базових рекомендацій (після 2025÷2030 рр.):

– диференціація шкоди за статтю та віком,

– оновлені популяційні дані,

– відкритий програмний інструмент [5].

Висновки.

1. Еволюція рекомендацій МКРЗ від Публікація 9 до Публікація 152 є послідовним науковим процесом, де три принципи:

– обґрунтування,

– оптимізація,

– обмеження доз,

залишаються незмінними від 1977 року, тоді як кількісні параметри та моделі постійно вдосконалюються.

2. Серія OIR (Публікації №№ 130÷151) реалізувала Публікація 103 на практичному рівні, забезпечивши фізіологічно обґрунтовані дозові коефіцієнти для всіх радіонуклідів, що зустрічаються на виробництві. Публікації № 134 та № 137 охопили найважливіші елементи для ядерної енергетики та медицини.

3. Для України рекомендації МКРЗ є обов'язковими через НРБУ-97, ОСПУ-2005 та імплементацію IAEA GSR Part 3. Дані серії OIR є критичними для дозиметричного контролю на об'єктах СхідГЗК, АЕС та в медичних установах.

Список літератури

1. The effect of external radiation exposure per person depending on his position and anthropometric indicators Pylypenko O., Shalomov V., Strezhekurov Y., Rudenko V., & Tymchenko P. International Scientific and Practical Conference Innovations in Construction and Smart Building Technologies for Comfortable, Energy Efficient and Sustainable Lifestyle (ICSBT 2024) 10 June 2024 E3S Web of Conferences Volume 534, 2024 – 01016. Режим доступу: https://doi.org/10.1051/e3sconf/202453401016.

2. ICRP 1966. Publication 9. Recommendations of the ICRP.

3. ICRP, 1991. 1990 Recommendations of the International Commission on Radiological Protection. ICRP Publication 60. Ann. ICRP 21 (1-3).

4. ICRP, 2007. The 2007 Recommendations of the International Commission on Radiological Protection. Publication 103. Ann. ICRP 37(2–4).

5. ICRP, 2015. Publication 130. Ann. ICRP 44(2).

ДО МОЖЛИВОСТІ ВИКОРИСТАННЯ МОБІЛЬНИХ МАЛОГАБАРИТНИХ ВОГНЕГАСНИКІВ ПРИ ГАСІННІ ПОЖЕЖІ

Савченко М.Ф., Лагутін М.І., Савченко М.М.
Харківський національний економічний університет імені С. Кузнеця,
Харків, Україна

Надзвичайно великі витрати вогнегасних речовин, як показує, на жаль, оцінка результатів ліквідації пожежі, а також виділення супутніх шкідливих газів, сприяють не лише забрудненню навколишнього середовища шкідливими речовинами.

Великою проблемою стають умови покращення доступності застосування вогнегасників, наприклад, у таких місцях, як під вагонами метро або через певні обмеження банківських установ, де надзвичайно важливе значення набуває саме мінімальне використання вогнегасних рідин [1, 2].

Наразі наявні різноманітні засоби пожежогасіння, їх умовно поділяють на три типи:

– переносні,

– пересувні

– стаціонарні.

Метою доповіді є розробка малогабаритного переносного типу вогнегасників, які можуть у надзвичайних ситуаціях застосовуватись при мінімальних навичках та при необхідності випадковими людьми.

В доповіді наводяться результати розробки можливих конструкцій такого типу вогнегасників, які можуть легко прикріплятись до небезпечних місць або вкидатись та утримуватись певних час.

Особливістю будови є використання двох основних за призначенням секцій:

– одна для створення (завчасно або безпосередньо при застосуванні) підвищеного тиску,

– друга – для розміщення вогнегасної речовини (желеподібної, порошку або суміші, наприклад, в ампулі).

При застосуванні можуть бути передбачені попередні елементи для локально точного розміщення вогнегасників такого типу в місцях, наближених до місця джерела пожежі.

Список літератури

1. Звітні матеріали Державної служби України з надзвичайних ситуацій URL: https://dsns.gov.ua/uk/operational-information/nadzvicaini-situaciyi-v-ukrayini-2/dovidka-zarik (дата звернення: 24.10.2023)

2. В. В. Присяжнюк, Б. О. Алімов, Ю. А. Пух, О. В. Куртов, М. В. Осадчук. Застосування переносних .технічних засобів пожежогасіння для гасіння пожеж. Матеріали VIII Міжнародної науково-практичної конференції «Теорія і практика гасіння пожеж та ліквідації надзвичайних ситуацій» 18-19 травня 2017 р., с.144-145.

ENSURING THE TECHNOLOGICAL SAFETY OF THE HELICOPTER SITE FOR DISASTER MEDICINE DURING AIR RAIDS

Serikov Y.
O. M. Beketov National University of Urban Economics in Kharkiv,
Kharkiv, Ukraine

Introduction

Aviation medicine is an extremely important component of the system of providing emergency assistance to victims.

It is a structural specialized element of emergency medicine and disaster medicine.

In this structural element, aircraft (helicopters, airplanes) are used to solve the following specific tasks:

1 - emergency transportation of persons who have suffered as a result of emergencies, man-made disasters, accidents, natural disasters, road accidents, fires, etc.;

2 - emergency evacuation of patients who are in such a critical condition that the intervention of doctors of certain qualifications is required;

3 - urgent transportation of patients in case of need for specialized treatment;

4 - urgent transportation, delivery of medical personnel, medical equipment to the place of an emergency, disaster, etc.

This type of medical care is widely used in countries such as the:

– USA [1],

– Great Britain [2],

– Australia [3].

Based on the military emergency situation that exists in Ukraine, it is necessary to actively develop aviation medicine in our country.

But in addition to the intensification of the development of this area in disaster medicine, in the conditions of Ukraine it is also necessary to ensure the technogenic safety of the site where helicopters take off, land, load patients, etc.

Purpose and objectives of the study.

The helicopter pad is located on the roof of the medical complex (Fig. 1). During air raids, there is a risk of damage to medical personnel, pilots, the helicopter, and the structure of the pad itself by unmanned aerial vehicles, debris, including ammunition, formed during such emergency situations.

The purpose of the study is to ensure the technogenic safety of the helicopter pad, which is involved in the structure of aviation medicine for disasters.

The task of the study is to minimize such a danger. When solving the problem, it is necessary to take into account the following specific requirements:

- rapid transformation of the pad from the regular operation mode to the protection mode;

- the specifics of medical aviation and the requirements for ensuring flight safety, taking into account the structure intended for protection.

Such requirements can be ensured in the case of using a mobile protective net (anti-drone) [4].

Figure 1 – Disaster medicine aviation helipad,
located on the roof of the medical complex

Research methods

To solve the problem, the method of statistical analysis of published applied solutions for the protection of critical infrastructure facilities was used to determine an effective design direction.

Research results

The object of protection is a medical aviation helicopter pad located on the roof of a medical complex. The size of the pad is 25×25 m.

Objects of impact of the pad: UAV fragments, fragments of ammunition, concrete, metal, glass, etc.

That is, the mobile protective net is not intended to protect against a direct hit by a missile or other combat elements, but serves as a structural element of a comprehensive protection system in emergency situations of the considered nature to minimize the risk:

- injury to medical personnel and pilots;
- damage to the pad (its coating) and the upper floor of the medical complex building:

According to the operating mode, the protective net should operate in two modes:

1 - the operating mode of the pad in which the protective net should be removed;

2 - alarm mode in which the protective net should automatically move over the site.

Design: Structurally, the entire system of the designed protective mobile net is 4 corner arches with telescopic supports 6 m high. We provide for the upper connection of the arches with guide rails. As the material for the net, we choose a steel cable with a cross section of 8 mm.

The size of the mesh cell is 30 mm. This type of mesh material will provide proper reliability of protection.

For laying the net in the normal operation mode of the site, we provide cassette modules with a design for its automatic laying in the modules and fixing its fastening.

When an alarm signal is received, we provide a device for automatically resetting the latch and deploying the net over the site territory.

Conclusions.

1. Based on the review of the development of medical aviation in the USA, Great Britain, Australia, as well as taking into account the current state of war in our country, the need for the development of medical aviation in Ukraine as a structural element in the disaster medicine system was identified.

2. An analysis of constructive solutions for the protection systems of critical infrastructure facilities, which include medical aviation sites as part of disaster medicine, was conducted, and the need for their mobile protection in the event of air raids was identified.

3. Research into constructive solutions used to protect the sites of aviation medical facilities (helicopters) from damage by unmanned aerial vehicles, fragments of missiles, shells, etc., identified the direction of design as a protective mobile grid.

4. The results obtained form a scientific and practical basis for activating the further development of medical aviation in Ukraine, taking into account the emergency situation of a military nature.

5. A pilot project has been developed, representing a system of comprehensive mobile protection of a helipad, which includes the following stages: - selection of material and design parameters of a protective mobile grid; - layout and composition of the structural elements of the system; - use of an electric drive and automation system to ensure the solution of the task.

References

1. Urgent medical evacuation to the USA. URL: https://www.statmedevac.com/

2. Jet Air Ambulance - Air ambulance - 24/7 Air Ambulance in UK. URL: https://247aviation.co.uk/medical-repatriation/?gad_source=1&gad_campaignid=18703031892&gbraid=0AAAACMfC29kKY1jHKBD-bOMAFU0CRNQZ&gclid=CjwKCAjw1tLOBhAMEiwAiPkRHswtAGKqYFrUuAj_L0DeS-394WJ7Ls1tkI6xI0Ok79O2aHt1ZArxyhoCZNUQAvD_BwE

3. Royal Australian Air Ambulance Service. URL: https://www.flyingdoctor.org.au/#

4. Heliport Safety Equipment. URL: https://fecheliports.com/about-helipad-equipment/

RISK ASSESSMENT OF INJURY TO PERSONNEL DURING INSTALLATION OF ARTIFICIAL LIGHTING SYSTEM OF A HELICOPTER LANDING ON THE ROOF OF A MEDICAL COMPLEX

Serikov Ya.O., Gerasimenko V.A.
O. M. Beketov National University of Urban Economics in Kharkiv,
Kharkiv, Ukraine

Introduction. The helipad, located on the roof of a medical complex, is part of the aviation medicine system and is actually a critical infrastructure facility that operates 24/7.

The urgency of providing and installing an artificial lighting system for a medical helipad is due to the fact that, based on the cases and emergencies of its use, the lighting system is necessary not only in the dark, but also in conditions of limited visibility, for example, in fog, precipitation.

That is, in case of urgent calls, for example, during hostilities, accidents, catastrophes, when emergency medical assistance is needed for victims or patients.

According to statistics, about 25–30% of accidents with helicopters occur due to poor-quality lighting in conditions of insufficient visibility due to meteorological conditions or in the dark [1].

It is obvious that the quality of lighting, the reliability of the lighting system depends not only on design solutions, but also on the quality of electrical installation work, in which the human factor is important - the attitude of the installation organization's management to ensuring the safety of their implementation, that is, in fact, to preserving human health during the work process. Moreover, the analyzed installation process refers to work of increased danger [2, 3].

Purpose and objectives of the study. The purpose and objectives of the study are to ensure the proper level of safety of installation personnel when installing the artificial lighting system of the helipad, which is located on the roof of the medical complex.

Research methods. The research methods are a risk-oriented method in identifying and ranking hazards and a systematic approach in achieving the set goal.

Research results. The installation of the artificial lighting system of the helipad, located on the roof of the medical complex, is characterized by the following main features:

- performance of work at height;
- influence of unsatisfactory meteorological factors (increased or decreased air temperature, inflated air speed);
- installation, electrical installation operations;
- work in the area of the operating medical complex, which determines increased requirements for noise and safety.

The use of a risk-oriented methodology made it possible to identify the main hazards, perform their ranking and develop directions for preventing the implementation of hazards (Table 1).

Table 1 – Risk-based hazard assessment based on the matrix method

Negative factor	Severity of injury (S)	Proba-bility of occurrence (P)	Risk (R)	Risk charac-teristics	Measures to prevent the realization of risk
Fall from height	5	4	20	Critical	Protective fencing around the perimeter of the roof
Electrotrau ma	5	3	15	High	Grounding system and RCD
Increased air velocity	4	3	12	High	Prohibition of work at wind speeds > 10–12 m/s
Falling objects	4	3	12	High	Installing the protective net, fixing the tool
Slippery surface	4	3	12	High	Anti-slip surface of the site

Conclusions.

Based on the application of risk-based methodology, an analysis, definition and ranking of risks was carried out during the installation of a system of artificial uniform lighting of a helicopter pad, which belongs to the medical aviation system, disaster medicine. The platform is located on the roof of a medical complex.

Studies have shown that this feature, the conditions of work have determined that the risks are multifactorial in nature. This nature of the hazards requires thorough development, a systematic approach to preserving the health of installation personnel.

References

1. Human Factors Analysis of Helicopter Air Ambulance Accidents, Incidents, and Events (2013-2023) / DOT/FAA/AM- 24/22 Office of Aerospace Medicine. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.faa.gov/data_research/research/med_humanfacs/oamtechreports/media/202422.pdf

2. NPAOP 0.00-4.12-2005. List of works with increased danger.

3. Serikov Ya.O. Industrial safety and social protection of employees of industrial enterprises, companies and corporations. Kharkiv: KhNUMG named after. Beketov - corp. SHELL. FPP Andreev, 2015. - 247 p.

4. Serikov Ya.O. Methodology for reducing the level of occupational injuries in the electric power industry of Ukraine / NTZ "Communal economy of cities", Ser.: Technical sciences and architecture. - 2022. Vol. 3 No. 170. P. 302-306.

ЗАЛЕЖНІСТЬ ЗАХВОРЮВАНЬ ДИХАЛЬНОЇ СИСТЕМИ ЛЮДИНИ ВІД РУЙНАЦІЇ ІНФРАСТРУКТУРИ ТА ЕНЕРГЕТИКИ

Синило К.В., Якимець І.В.
Державний університет «Київський авіаційний інститут»,
Київ, Україна

Нові масштабні екологічні катастрофи, такі як руйнування електростанцій, об’єктів газової інфраструктури та нафтобаз під час збройних конфліктів, є терміновим і значною мірою маловивченим джерелом комплексного забруднення повітря. Вони спричиняють викиди сумішей твердих часток, важких металів, вуглеводнів та побічних продуктів горіння у середовище проживання цивільного населення. Ці випадки забруднення не є короткочасними. Вони можуть зберігатися протягом тривалих періодів, створюючи сценарії хронічного впливу, які сильно уражують вразливі верстви населення.

Основними екологічними факторами ризику, пов'язаними з енергетичними об'єктами, є забруднення повітря, води та ґрунту; хімічні домішки та тверді частки тощо. Епідеміологічні та експериментальні дослідження вказують на стійкий зв'язок між забрудненням довкілля та неврологічними захворюваннями та захворюваннями дихальної сисеми, що підтверджується спостереженнями на тваринах та моделях in vitro.

Проте причинно-наслідкові зв'язки та механістичні шляхи залишаються недостатньо визначеними, переважно через брак прогностичних та фізіологічно релевантних експериментальних систем людини.

У цьому матеріалі розглянемо більш детально вплив на дихальну систему людини.

Коли через військові дії страждає інфраструктура та енергетика, легені людини опиняються під впливом відразу з кількох сторін:

- токсичний смог та продукти горіння,
- відсутність опалення та «пічне» забруднення,
- холод і вологість (цвіль),
- стрес та дефіцит ресурсів.

Легені виконують одну з ключових функцій в організмі людини. Одним з важливих захисних природних механізмів легень слугує сурфактант.

Сурфактант – це поверхнево-активна речовина, яка має складний ліпопротеїновий комплекс, що вкриває тонкою плівкою внутрішню поверхню легеневих альвеол.

Сурфактант знижує поверхневий натяг, запобігаючи злипанню альвеол при видиху та забезпечуючи стабільність легень.

Було розглянуто вплив негативних чинників на легені людини.

1. Токсичний смог та продукти горіння

Руйнування енергетичних об'єктів (ТЕЦ, нафтобаз, підстанцій, тепломереж) та промислових підприємств, призводить до викиду в повітря

величезної кількості дрібнодисперсних часток, важких металів та хімікатів. Токсичні гази та сажа викликають окислювальний стрес, який буквально «роз'їдає» сурфактант. Без нього легені стають жорсткими і дихати стає набагато важче.

2. Відсутність опалення та «пічне» забруднення

Коли зруйновано енергосистему, люди переходять на альтернативне опалення: «буржуйки», генератори, неякісне паливо. При цьому можливі наступні наслідки: постійне вдихання продуктів неповного згоряння та чадного газу в закритих приміщеннях призводить до хронічного запалення дихальних шляхів. Це вдруге пригнічує синтез сурфактанту клітинами легень.

3. Холод, вологість та цвіль

Руйнування оздоблення будівель та відсутність тепла ведуть до високої вологості, що при тривалій дії може призвести до появи грибків. У легені потрапляють спори плісняви. Імунна система у спробі боротьби з ними пошкоджує власні тканини. Сурфактант втрачає свої захисні антибактеріальні властивості, що може призвести до важких форм пневмоній, а також до проявів симптомів астми.

4. Стрес та дефіцит ресурсів

Постійний стрес та погане харчування заважають організму відновлювати ліпідні компоненти сурфактанту. В умовах війни навіть звичайний бронхіт швидше переходить у хронічну форму через те, що природне «мастило» легень не встигає регенерувати.

Руйнування цивілізованих умов життя перетворює повітря на агресивне середовище, яке руйнує захисний бар'єр легень - сурфактант, роблячи легені беззахисними перед інфекціями, пневмоніями, астмами та фіброзом.

Тому вирішення проблеми забруднення довкілля, пов'язаного з війною, є як науковим, так і суспільним імперативом. Існує критична потреба у впровадженні інноваційних систем, здатних моделювати складні суміші забруднювачів та їхній довготривалий вплив на здоров'я людини.

В доповіді викладені проблеми забруднення довкілля, пов'язаного з війною, вплив його на здоров'я людини.

В результаті дослідження встановлено, що основними чинниками негативного впливу на легені людини є:

токсичний смог та продукти горіння;

відсутність опалення та «пічне» забруднення;

холод, вологість та цвіль;

стрес та дефіцит ресурсів.

З метою покращання умов проживання людини при усіх негараздах війни намічені шляхи ліквідації негатиних наслідків та розроблені заходи, здатні поліпшити стан здоров'я людини.

ОЦІНКА СТІЙКОСТІ ОБ'ЄКТІВ ЗАЛІЗНИЧНОЇ ІНФРАСТРУКТУРИ

Третьяков О.В., Давиденко Я.Ф.
Національний університет «Київський авіаційний інститут»,
Київ, Україна

Вступ. Залізничний транспорт упродовж багатьох десятиліть залишається одним із ключових елементів транспортної системи України. Він забезпечує значну частку вантажних та пасажирських перевезень, формує логістичний потенціал держави та є критично важливою складовою національної безпеки.

Мета і завдання дослідження. Аналіз стану та функціональної ролі об'єктів залізничної інфраструктури, оцінка їх стійкості до різних типів загроз та обґрунтування заходів щодо підвищення живучості й безпеки залізничної транспортної системи..

Результати дослідження. Проведена систематизація понять загроз, ризиків та вразливості інфраструктури, а також проаналізовано основні чинники, що впливають на безпеку та стійкість роботи об'єктів залізничного транспорту. Встановлено, що залізнична інфраструктура є складною багаторівневою системою, уразливість якої зумовлена як фізичним зношенням елементів, так і впливом зовнішніх факторів, включаючи аварійні та кризові ситуації, особливо у воєнний час.

Розглянуто наслідки порушення функціонування залізничних об'єктів, зокрема втрати пропускної спроможності, зниження пасажиропотоку, ускладнення логістичних процесів та економічні збитки, в разі реалізації загроз різного типу.

Аналіз показав, що відсутність резервних маршрутів суттєво знижує стійкість транспортних вузлів і призводить до значних втрат навіть у разі локальних пошкоджень наземної інфраструктури.

Визначена необхідність переходу від суто реактивного підходу до управління інфраструктурою до превентивного, який передбачає завчасне проєктування альтернативних та резервних рішень. Зроблено висновок, що впровадження підземних елементів транспортної мережі є одним із найбільш ефективних способів підвищення стійкості та живучості залізничної системи в цілому.

Розроблена концепція підземної резервної тунельної лінії в районі станції Дарниця з розгалуженням у напрямках Ніжина та Яготина.

Запропоноване рішення передбачає створення багатофункціонального підземного об'єкта, який може виконувати роль резервної лінії у разі пошкодження наземної інфраструктури, використовуватися для оптимізації графіків руху, а також забезпечувати можливість організації швидкісного та спеціалізованого руху.

ВПЛИВ ВНУТРІШНІХ ЗАГРОЗ НА ПРОЯВ ІНШИХ ЗАГРОЗ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Третьяков О.В., Халмурадов Б.Д., Кічата Н.М., Федина В.П.
Державний університет «Київський авіаційний інститут»,
Київ, Україна

Вступ. До того, як внутрішні загрози мають прояв, вони є ризиками. Ризик визначається як можливість навмисного або ненавмисного заподіяння шкоди організації шляхом неналежного використання її ресурсів особою, яка має до них авторизований доступ. Під доступом мається на увазі як фізичний, так і віртуальний доступ, а ресурси включають інформацію, процеси, системи та обладнання. Інсайдер – це довірена особа, якій надано доступ до будь-яких ресурсів, даних або систем компанії, її бази знань, або яка володіє інформацією про них. Ресурси можуть бути як загальнодоступні, так і не загальнодоступні. В умовах воєнного стану вплив внутрішніх загроз на безпеку і стійкість об'єктів критичної інфраструктури (ОКІ) набуває ще більшої значущості та їх прояв може посилювати негативні наслідки реалізації природних, воєнних, техногенних загроз і кібератак [1].

Для об'єктивного врахування впливу внутрішніх загроз на прояв інших загроз неохідно створення методу розрахунку ризику внутрішніх (інсайдерських) загроз на ОКІ, який би дозволял проводити кількісну його оцінку, спираючись на вимоги групи стандартів ДСТУ ISO 31000:2018 [2].

Мета і завдання дослідження. Розроблення методу розрахунку ризику прояву внутрішніх (інсайдерських) загроз на ОКІ на основі поєднання організаційно-технічних та психологічних аспектів безпеки та оцінка впливу внутрішніх загроз на прояв інших загроз для ОКІ.

Результати дослідження. Інсайдер – це довірена особа, якій надано доступ до будь-яких ресурсів, даних або систем компанії, її бази знань, або яка володіє інформацією про них. Ресурси можуть бути як загальнодоступні, так і не загальнодоступні. Інсайдерами можуть бути наступні категорії користувачів.

Внутрішні ризики важче виявляти, ніж зовнішні, оскільки в першому випадку зловмисники вже мають доступ до ресурсів організації і знають про її заходи безпеки.

Знання типів внутрішніх ризиків допомагає організаціям у посиленні захисту цінних ресурсів.

Розроблений підхід оцінки ризику інсайдерських загроз зосереджений на поєднанні двох підходів – реалізації організаційно-технічного методу та психологічного. При цьому проводиться аналіз нетипової поведінки при виконанні службових обов'язків, в інформаційних системах, у спілкуванні з колегами, в режимі реального часу на основі інформації, зібраної за допомогою системи виявлення вторгнень та системних сигналів.

Крім того проводиться аналіз такого компоненту як психологічне профілювання – визначення рівня стресу працівників та ін.

Керівництво ОКІ повинно мати змогу передбачити потенційну загрозу інсайдерів, виявляти взаємозв'язок між усіма параметрами, зібраними з джерел психологічної профілактики та технічного контролю, за трьома факторами: мотивацією, можливостями та здібностями, де кожен фактор отримує ймовірнісну оцінку в діапазоні (від 0 до 1), що дає змогу кількісної оцінки ризику внутрішніх загроз.

Мотивація працівника M_i оцінюється за трьома параметрами: ймовірність схильності до зловмисної поведінки P_i, ймовірний рівень стресу S_i та ймовірність наявності вміння (навичок) V_i. Спираючись на теорію ймовірності [3], ймовірність формування мотивації користувача можна визначити за формулою:

$$\mathrm{M}_i f(P_i, S_i, V_i) = 1 - (1 - P_i) \cdot (1 - S_i) \cdot (1 - V_i). \quad (1)$$

Наявність можливості для працівника O_i визначається за трьома параметрами: ймовірність зміни робочої поведінки B_i, ймовірність доступу до матеріальних або інформаційних активів R_i та ймовірність благоприємних обставин для здійснення злочинних дій H_i, з урахуванням встановлення в організації Правила двох осіб – принципу, що ґрунтується на спостереженні однієї особи за діями іншої з метою недопущення несанкціонованих дій, які вже впроваджені на окремих ОКІ [4, 5]. Ймовірність можливості для працівника [3], може бути визначена за наступною формулою:

$$O_i f(B_i, R_i, Y_i) = 1 - (1 - B_i) \cdot (1 - R_i) \cdot (1 - H_i). \quad (2)$$

Зміна робочої поведінки, визначається під час взаємодії з усіма елементами інфраструктури при виконанні службових обов'язків, і може свідчити про те, що працівник знаходиться в процесі пошуку можливої цілі (вразливості) в тій, чи іншій системі. Другим важливим показником, який потрібно оцінювати, є рівень доступу до матеріальних або інформаційних активів, який визначається позицією організаційної структури підприємства та посадовою інструкцією. Благоприємні обставини для здійснення злочинних дій визначаються з урахуванням загальної системи безпеки ОКІ, наявності і дотримування працівниками прийнятої політики безпеки в організації.

Здатність працівника C_i до здійснення зловмисних дій оцінюється за двома параметрами: продемонстрована спроможність D_i та вишуканість користувача S_i (ймовірний рівень стресу) за наступною формулою

$$C_i f(B_i, R_i, Y_i) = 1 - (1 - D_i) \cdot (1 - S_i). \quad (3)$$

Продемонстрована здатність вимірюється за допомогою психометричного тесту, який пристосований для умов підприємства і посадових обов'язків відповідних категорій працівників.

Оцінка ймовірність реалізації загрози P_{i3} визначається з урахуванням усіх наведених вище ймовірностей.

$$P_{i3} f(M_i, O_i, C_i) = 1 - (1 - M_i) \cdot (1 - O_i) \cdot (1 - C_i). \quad (4)$$

Запропонований метод характеризується простотою і зручністю у використанні. Оцінки базуються, в де яких випадках, на думці експертів, що дає можливість уникнути певного формалізму у порівнянні з машинним оцінюванням.

Але, разом з тим, у такому підході є деякі обмеження, він потребує проведення попереднього психометричного тестування усіх співробітників і, в подальшому проводити його періодично.

Розроблений підхід визначення ймовірності прояву внутрішніх (інсайдерських) загроз необхідно враховувати при розрахунках ризику небезпечної події для об'єктів критичної інфраструктури статистичним методом, що ґрунтується на використанні історичних даних для оцінки ймовірності виникнення цих подій і пов'язаних із ними ризиків з урахуванням каскадних ефектів, який широко застосовується останні роки для багатьох ОКІ [1].

Перевірка запропонованого методу проводилась для Комплекса водопідготовки (КВ), розташованому в прифронтовій зоні України, який є важливим об'єктом КІ, що забезпечує питною водою велике місто. Його функції включають як подачу води, так й її очищення.

Попереній аналіз можливого прояву внутрішніх (інсайдерських) загроз в додаток до означених найбільш небезпечних при реалізації сценаріїв хакерська атака на засоби автоматизації комплексу (S_3) с подальшою відмовою системи подачі електроенергії (S_2) $S_3 \rightarrow S_2$ (зупинка роботи аварійного електроживлення зловмисником) – ймовірність прояву по запропонованому підходу становить для комплексе водопідготовки $P_{э2} = 0{,}25$ та атака БПЛА (S_5) с подальшою відмовою системи подачі електроенергії (S_2) $S_5 \rightarrow S_2$ (позначення найбільш важливих вразливих технологічних елементів спеціальними мітками) ймовірність прояву становить для комплексу водопідготовки $P_{э5} = 0{,}20$. В цих випадках значення ймовірностей реалізації сценаріїв суттєво збільшується (таблиця).

Таблиця – Ймовірності реалізації сценаріїв загроз на КВ з урахуванням ймовірності прояву внутрішніх (інсайдерських) загроз

Сценарії	Значення ймовірності реалізації					
$S_3 \rightarrow S_2$	P_6	$P_{э2}$	P'_6	P_7	$P_{э2}$	P'_7
	0,3499	0,25	0,5124	0,4355	0,25	0,5766
$S_5 \rightarrow S_2$	P_{10}		$P_{э5}$		P'_{10}	
	0,676		0,20		0,7408	

Таким чином, при проведенні оцінки ризику безпеки об'єктів критичної інфраструктури надзвичайно важливо визначати внутрішні загрози, які можуть мати прояв збільшувати ймовірності інших загроз. Реалізація такого підходу дозволить підвищити достовірність оцінки ризиків прояву усіх можливих

загроз для активів ОКІ, забезпечити їх вірне ранжування для обґрунтування заходів підвищення безпеки і стійкості об'єкту критичної інфраструктури.

Висновки.

В запропонованому підході кількісної оцінки ймовірності прояву внутрішніх (інсайдерських) загроз проводиться через аналіз нетипової поведінки при виконанні службових обов'язків, в інформаційних системах, у спілкуванні з колегами, в режимі реального часу на основі інформації, зібраної за допомогою системи виявлення вторгнень та системних сигналів та аналіз психологічного профілювання і визначення рівня стресу працівників.

Оцінка загрози зловмисника проводиться з урахуванням ймовірності мотивації інсайдера, ймовірностей його можливостей і здатностей.

Запропонований підхід визначення ймовірності прояву внутрішніх (інсайдерських) загроз повинен бути врахований при розрахунках ризику небезпечної події для об'єктів критичної інфраструктури статистичним методом, що ґрунтується на використанні історичних даних для оцінки ймовірності виникнення небезпечних подій і пов'язаних із ними ризиків з урахуванням каскадних ефектів, який широко застосовується останні роки для об'єктів критичної інфраструктури.

Врахування ймовірності прояву внутрішніх (інсайдерських) загроз при розрахунках ризику небезпечної події для об'єкту критичної інфраструктури створює можливість отримати більш достовірні значення ризику, провести вірне їх ранжування і більш точне визначення пріоритетних заходів захисту.

Розроблено метод розрахунку ризику прояву внутрішніх (інсайдерськіх) загроз для об'єктів критичної інфраструктури дозволяє отримувати кількісні значення ймовірності їх прояву, враховувати ці значення при визначенні рівня ризику впливу воєнних, природніх, техногенних загроз, кіберзагроз та інших на ОКІ. Застосування такого підходу дозволяє підвищити достовірність оцінки ризиків прояву усіх можливих загроз для активів ОКІ, забезпечити їх вірне ранжування для обґрунтування рішень з підвищення безпеки і стійкості об'єкту критичної інфраструктури.

Список літератури

1. Кічата Н. М., Третьяков О. В. Оцінка реалізації загроз на об'єктах критичної інфраструктури. Old and new technologies of learning development in modern conditions: proceedings of the VI International scientific and practical conference. (February 13-16, 2024). Berlin, Germany, 2024. С.319-321. DOI: 10.46299/ISG.2024.1.6.
2. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та керівні вказівки.
3. Теорія ймовірностей та математична статистика: навчальний посібник / О. І. Огірко, Н. В. Галайко. – Львів: ЛьвДУВС, 2017. – 292 с.
4. Правила фізичного захисту ядерних установок та ядерних матеріалів. Наказ Державного комітету ядерного регулювання України від 04.08.2006 № 116.
5. Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки. Наказ Державної інспекції ядерного регулювання України від 22.03.2022 № 223.

ІНТЕЛЕКТУАЛЬНА МОДЕЛЬ ОЦІНКИ ПОЖЕЖНИХ РИЗИКІВ НА ПІДПРИЄМСТВАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Третьяков О.В., Лінчевський І.В.
Державний університет «Київський авіаційний інститут»,
Київ, Україна

Вступ. Сучасні умови розвитку України характеризуються підвищенням рівня техногенних і природних загроз, що супроводжуються зростанням частоти пожеж на промислових, транспортних та енергетичних об'єктах. Особливо гостро ця проблема постала після початку повномасштабної воєнної агресії російської федерації проти України, яка призвела до масового руйнування енергетичної, транспортної, комунікаційної та оборонної інфраструктури. Унаслідок цього значно збільшилася кількість пожеж, вибухів, вторинних уражень критичних об'єктів.

Мета дослідження. Розробка інтелектуальної моделі оцінки пожежних ризиків для підприємств критичної інфраструктури з урахуванням умов воєнного часу задля підвищення рівня їхньої пожежної безпеки та забезпечення стійкості функціонування.

Результати дослідження. Проведено комплексний аналіз існуючих методів оцінювання пожежних ризиків та сучасних систем пожежогасіння, що дозволило виявити недоліки традиційних підходів, зокрема їхню нечутливість до слабовиражених ознак тління, неспроможність прогнозувати розвиток небезпечних ситуацій та високу вірогідність хибних спрацювань.

Розроблено гібридну інтелектуальну модель, яка поєднує методи нечіткої логіки (Fuzzy Logic) та штучних нейронних мереж (ANN). Такий підхід забезпечує як експертну інтерпретацію параметрів, так і можливість машинного навчання на реальних експлуатаційних даних, що значно підвищує точність і надійність оцінювання ризиків.

Сформовано математичний апарат та алгоритм роботи моделі, включаючи: систему нечітких множин, базу правил, архітектуру нейронної мережі, нормалізацію вхідних параметрів, метод гібридної інтеграції та формування підсумкового показника ризику R_Hybrid.

Розроблено Python-реалізацію моделі з демонстраційними прикладами та можливістю розширення під реальні промислові сценарії. Код моделі придатний для інтеграції у SCADA, OPC-UA/MQTT системи та мікросервісні архітектури контролерів безпеки.

Проведено апробацію моделі на тестових сценаріях, що відображають реальні умови експлуатації систем GAMMA-108SAT та Brand-3: тління, різкий температурний стрибок, масове задимлення, механічні вібровпливи та зниження тиску в модулі.

Результати показали високу чутливість моделі до різних типів загроз, можливість раннього прогнозування та стійкість до завад.

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ КІБЕРЗАГРОЗ: ОЦІНКА ТА АНАЛІЗ РИЗИКІВ

Демченко І.О., Вальченко О.І.
Державний університет «Київський авіаційний інститут»,
Київ, Україна

Сучасна критична інфраструктура України, зокрема енергетичний та транспортний сектори, перебуває у стані цифрової трансформації. Впровадження систем складного моніторингу та автоматизованих систем керування технологічними процесами (SCADA) підвищує ефективність управління, але водночас створює нові вектори вразливості. В умовах гібридної агресії кіберзагрози перестали бути лише проблемою IT-сектору, перетворившись на реальний фактор екологічної небезпеки.

Специфіка об'єктів енергетики та транспорту полягає у їхній високій потенційній небезпеці для довкілля.

Кібератака, спрямована на зміну алгоритмів роботи систем охолодження на АЕС, тиску в нафтогазопроводах або систем диспетчеризації небезпечних вантажів на залізниці, може спровокувати викиди токсичних речовин, пожежі або розливи палива.

Таким чином, аналіз кіберризиків є невід'ємною частиною оцінки екологічної стійкості держави [1, 2].

Досвід атак на енергосистему України (наприклад, Black Energy) продемонстрував можливість дистанційного відключення підстанцій.

Проте найбільш критичними з точки зору екології є атаки типу *Stuxnet* або *Triton*, що втручаються в роботу систем протиаварійного захисту (SIS). У транспортній галузі вразливість систем керування рухом суден чи потягів із хімічними речовинами створює ризики масштабного забруднення акваторій та ґрунтів.

Метою доповіді є аналіз взаємозв'язку між кіберстійкістю об'єктів енергетики і транспорту та рівнем екологічної безпеки, аналіз ризиків виникнення техногенних аварій внаслідок кібератак на автоматизовані системи керування

Методологія оцінки ризиків. Для аналізу стійкості критичної інфраструктури пропонується комплексний підхід, що базується на моделі NIST Cybersecurity Framework з інтеграцією параметрів екологічної шкоди. [3].

1. Ідентифікація активів: Визначення критичних вузлів, вихід з ладу яких спричинить екологічне лихо.

2. Моделювання загроз: Аналіз ймовірності злому через вразливості нульового дня (0-day) або соціальну інженерію.

3. Оцінка наслідків: Розрахунок потенційного обсягу викидів шкідливих речовин та вартості рекультивації територій у разі успішної кібератаки.

Аналіз стійкості критичної інфраструктури на основі запропонованого комплексного підходу свідчить, що стійкість критичної інфраструктури залежить не лише від наявності засобів мережевого захисту, а й від здатності

системи підтримувати безпечний стан навіть при втраті цифрового управління. Ключовим ризиком визнано каскадний ефект: кібератака на електромережу призводить до зупинки очисних споруд або систем вентиляції на хімічних підприємствах, що спричиняє вторинну екологічну шкоду.

Кібербезпека об'єктів енергетики та транспорту має розглядатись як базовий елемент екологічної безпеки країни.

Необхідно впроваджувати концепцію «Security by Design», де екологічні ризики враховуються ще на етапі проектування цифрових систем управління. Стійкість критичної інфраструктури в умовах кіберзагроз вимагає створення ізольованих резервних контурів управління та регулярного стрес-тестування персоналу на випадок техногенних інцидентів, спричинених втручанням у мережу. [3].

Додатково важливим елементом підвищення стійкості критичної інфраструктури є впровадження систем раннього виявлення кіберінцидентів та постійного моніторингу стану технологічних процесів.

Використання інтелектуальних систем аналізу даних дозволяє своєчасно ідентифікувати аномалії у роботі обладнання, що можуть свідчити про втручання у систему керування, та запобігати розвитку аварійних ситуацій ще на початкових етапах.

Окрім технічних заходів, значну роль відіграє підвищення рівня підготовки персоналу, який обслуговує об'єкти критичної інфраструктури. Проведення регулярних навчань, моделювання кризових ситуацій та відпрацювання алгоритмів дій у разі кібератак сприяють зниженню ймовірності помилок та мінімізації наслідків потенційних інцидентів. Таким чином, поєднання технологічних рішень і людського фактору є ключовою умовою забезпечення кіберстійкості та екологічної безпеки держави.

Водночас доцільним є впровадження принципу резервування та автономності систем управління, що дозволяє забезпечити їх безпечне функціонування навіть у разі часткового або повного порушення цифрової інфраструктури. Застосування ізольованих контурів управління, а також регулярне тестування стійкості систем до кіберзагроз підвищує рівень їх надійності.

У сукупності такі заходи сприяють формуванню комплексної моделі захисту, орієнтованої не лише на запобігання атакам, але й на мінімізацію їх потенційних наслідків для довкілля та суспільства.

Список літератури

1. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19.06.2019 № 518 : станом на 20 листоп. 2025 р.

2. World Economic Forum. Global Risks Report 2023. – Geneva: WEF, 2023.

3. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. – Gaithersburg: National Institute of Standards and Technology, 2018.

ОЦІНКА РИЗИКІВ ПОВТОРНОГО РАДІАЦІЙНОГО ЗАБРУДНЕННЯ ТЕРИТОРІЙ У ЗОНІ ВІДЧУЖЕННЯ ЧОРНОБИЛЬСЬКОЇ АЕС

Сошко І.С., Вальченко О.І.
Державний університет «Київський авіаційний інститут»,
Київ, Україна

Оцінка ризиків повторного радіаційного забруднення територій у зоні відчуження Чорнобильської АЕС залишається надзвичайно актуальною проблемою навіть через десятиліття після аварії.

Незважаючи на поступове зниження рівня радіаційного фону, на території зони відчуження зберігається значна кількість довгоживучих радіонуклідів, таких як цезій-137, стронцій-90 та ізотопи плутонію [1, 5].

Одним із головних джерел повторного радіаційного забруднення є лісові пожежі в зоні відчуження, під час яких радіонукліди з ґрунту та рослинності потрапляють у повітря у вигляді аерозолів і можуть переноситися на значні відстані.

Значний ризик також пов’язаний із порушенням ґрунтового покриву внаслідок діяльності людини, що спричиняє підняття радіоактивного пилу [2, 3].

Окрему увагу слід приділити гідрологічним процесам, які можуть сприяти перенесенню радіонуклідів через водні системи.

Під час повеней або інтенсивних опадів забруднені частинки можуть потрапляти до річок і підземних вод, що створює ризик їх поширення на значні території.

Не менш важливим чинником є поступова деградація інженерних захисних споруд, зокрема об’єкта «Укриття» та інших бар’єрів, які стримують поширення радіоактивних матеріалів [2, 5].

Оцінка рівня ризику повторного радіаційного забруднення базується на такому:

– комплексному аналізі радіаційного фону,

– моделюванні можливих сценаріїв поширення радіонуклідів,

– врахуванні кліматичних і погодних умов.

Важливу роль відіграє також оцінка ймовірності виникнення надзвичайних ситуацій, таких як пожежі або повені [3, 5].

Не менш важливою складовою є оцінка ймовірності виникнення надзвичайних ситуацій, таких як лісові пожежі, повені або техногенні аварії, які можуть спричинити повторне підняття та перенесення радіонуклідів у навколишнє середовище.

Наприклад, під час пожеж радіоактивні частинки можуть знову потрапляти в атмосферу та переноситися на значні відстані, а під час паводків — поширюватися через водні системи. У зв’язку з цим проводиться постійний моніторинг потенційно небезпечних зон і розробляються превентивні заходи для мінімізації ризиків.

Наслідки повторного радіаційного забруднення можуть бути досить серйозними як для довкілля, так і для населення.

Серед них варто виділити погіршення екологічного стану територій, підвищення рівня радіаційного навантаження на людину, забруднення продуктів харчування та водних ресурсів, а також обмеження господарської діяльності.

Крім того, радіонукліди негативно впливають на флору і фауну, що призводить до змін у біорізноманітті регіону [4, 5].

З метою мінімізації ризиків повторного радіаційного забруднення необхідно впроваджувати комплекс заходів, серед яких ключове значення має постійний радіаційний моніторинг території. Важливо забезпечити ефективну систему виявлення та гасіння лісових пожеж, обмежити доступ до найбільш небезпечних ділянок, а також підтримувати належний технічний стан захисних споруд.

Додатково доцільно здійснювати рекультивацію забруднених земель та проводити інформаційно-роз'яснювальну роботу серед населення щодо потенційних ризиків [2, 3].

Таким чином, ризик повторного радіаційного забруднення у зоні відчуження Чорнобильської АЕС залишається реальним і потребує постійного контролю та ефективного управління.

Найбільшу загрозу становлять природні фактори, зокрема лісові пожежі, які можуть спричиняти повторне підняття радіонуклідів у повітря та їх подальше поширення на значні території, а також антропогенний вплив, пов'язаний із діяльністю людини.

Додатковим ризиком є зміни клімату, що можуть збільшувати частоту екстремальних погодних явищ і, відповідно, підвищувати ймовірність повторного забруднення.

Тому важливим є впровадження сучасних систем моніторингу та швидкого реагування для мінімізації можливих наслідків [1, 2, 5].

Список літератури

1. Закон України «Про правовий режим території, що зазнала радіоактивного забруднення внаслідок Чорнобильської катастрофи» від 27.02.1991 № 791а-XII.

2. Державне агентство України з управління зоною відчуження. Офіційний сайт. – Режим доступу: https://dazv.gov.ua

3. Державна служба України з надзвичайних ситуацій. Аналітичні матеріали та звіти. – Режим доступу: https://dsns.gov.ua

4. Всесвітня організація охорони здоров'я (WHO). Health effects of the Chernobyl accident and special health care programmes. – Женева, 2006.

5. Міжнародне агентство з атомної енергії (IAEA). Environmental Consequences of the Chernobyl Accident and Their Remediation: Twenty Years of Experience. – Vienna, 2006.

UNMANNED MINE DETECTION SYSTEM USING AN OPTIMIZED YOLO26 MODEL FOR EDGE COMPUTING ON STM32

Podorozhniak A., Liubchenko N., Skorlupin O., Oleksiienko D.
National Technical University “Kharkiv Polytechnic Institute”,
Kharkiv, Ukraine

The relevance of autonomous unmanned systems for humanitarian demining is driven by critical risks to sappers' lives and the urgent need for reliable, safe technologies that minimize human involvement. Modern breakthroughs in artificial intelligence (AI), particularly deep learning, combined with the rapid development of edge AI, enable the full implementation of intelligent algorithms directly on onboard microcontrollers.

This eliminates dependence on cloud services or powerful computers, ensuring high autonomy, energy efficiency, low latency, and real-time data processing. In the context of humanitarian demining in Ukraine, the adoption of unmanned platforms is recognized as a strategic priority to enhance operational safety.

Key challenges include maintaining stable video links under active electronic warfare, complex terrain, and dense vegetation.

Additionally, prolonged video stream monitoring leads to physical and cognitive operator fatigue, resulting in misses of explosive ordnance (EO) and unexploded ordnance (UXO), such as mines or unexploded munitions.

The optimal solution involves offloading computational tasks to the unmanned autonomous vehicle: instead of transmitting "heavy" full video, only coordinates of detected objects, their photos, and metadata are sent, drastically reducing bandwidth and risks.

The objective of this study is to develop, programmatically optimize, and integrate an onboard module for EO and UXO detection based on the STM32 microcontroller platform using the AI model YOLO26, adapted for real-world field operation conditions.

The foundation relies on computer vision methods based on convolutional neural networks, which reliably analyze visual data in challenging scenarios:

– background noise,

– lighting fluctuations,

– weather changes,

varied target positioning.

– For detection, the YOLO architecture was selected, renowned for its high inference speed and efficiency in continuous monitoring modes. A specialized version of YOLO26, optimized for low-power unmanned aerial and ground vehicles, was employed, enabling operation under constrained computational power, memory, and energy resources.

A dedicated training dataset was curated from thousands of EO and UXO images, covering diverse viewing angles, lighting conditions, partial occlusion by

background, soil, or landscape elements, as well as typical Ukrainian terrains. Additional data preprocessing (normalization, filtering) and augmentation (rotation, brightness adjustment, noise simulation) were applied to significantly enhance the model's generalization capability.

The proposed methodology is flexibly adaptable for detecting other hazardous objects (e.g., wire traps or improvised explosive devices), paving the way for universal monitoring systems across various security tasks. The development of an Edge AI system for mine recognition based on STM32 microcontrollers and the YOLO26 AI model is described; these were chosen for their high energy efficiency and peripheral integration.

Video processing is handled via interfaces in STM32CubeMX, allowing direct transfer of camera frames to memory without CPU overhead, thereby freeing resources for AI model inference.

To overcome Flash memory limitations, the YOLO26 model was quantized to INT8 format, reducing its size while preserving accuracy and enabling real-time object detection.

During the software implementation, the following key tasks were addressed:

– training dataset of EO and UXO images was curated and annotated considering real-world conditions (varied angles, lighting, occlusion), on which the YOLO26 model was trained and validated using test data;

– AI model was programmatically optimized through quantization, dataflow compilation, and vectorization, ensuring stable YOLO26 performance on unmanned aerial and ground vehicles in real-time mode;

– entire software stack was adapted to the STM32 platform, which is affordable, low-resource, and widely available, facilitating scalable production of cost-effective solutions for humanitarian demining.

System debugging and comprehensive testing were conducted in the Renode emulator, simulating real operational conditions without a physical prototype. The proposed approach convincingly demonstrates the potential of Edge AI on low-resource chips, enabling affordable mass-produced solutions for demining.

Development prospects include integration with multisensor complexes, further optimization for serial production, and enhancement of national security. Planned further research focuses on dataset expansion and integration of multispectral cameras for operations under limited visibility (night, fog, smoke), as well as model adaptation to diverse microprocessor platforms in autonomous robotic systems for humanitarian demining.

References

1. Podorozhniak A., Liubchenko N., Skorlupin O., Korolenko S., Stas A. Mobile explosive object detection system for humanitarian demining needs. 2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek), pp. 1-6. DOI: https://doi.org/10.1109/KhPIWeek61436.2025.11288620.

2. Ultralytics YOLO26 Documentation. – URI: https://docs.ultralytics.com/ru/models/yolo26/.

3. Levchenko D., Podorozhniak A., Liubchenko N. Tools and methods for explosive objects detection using artificial intelligence and computer vision. Control, Navigation and Communication Systems. 2025. No. 3 (81). Pp. 117–121. DOI: https://doi.org/10.26906/SUNZ.2025.3.117

4. Oleksiienko D., Liubchenko N., Podorozhniak A. Mine detection AI system. Problems of informatization: Proceedings of 13-th International Scientific and Technical Conference, November 27-28, 2025, Baku, Kharkiv, Bielsko-Biala. – Kharkiv: NTU "KhPI", 2025. – P. 145. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/97699.

5. Podorozhniak A., Skorlupin O. Mobile explosive detection system for civil defense needs. Proceedings of 25-th International Scientific and Technical Conference, September 25-28, 2025, Kharkiv. – Kharkiv: NTU "KhPI", 2025. – P. 89. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95085.

DEVELOPMENT OF AN AUTONOMOUS ANTI-SPAM PROTECTION SYSTEM FOR MESSENGERS

Podorozhniak A., Liubchenko N., Heiko H., Frolov D.
National Technical University “Kharkiv Polytechnic Institute”,
Kharkiv, Ukraine

In today's era of rapid digitalization, combating spam in instant messengers and social media has become a critical challenge [1].

The massive influx of unsolicited messages not only hinders productive communication but also poses significant threats, ranging from the spread of phishing links and fraudulent schemes to the distribution of malicious software.

This erodes trust in online platforms and carries a risk of financial loss. Implementing intelligent automated moderation systems significantly enhances security, reduces the cognitive load on users, and minimizes risks associated with human error.

This study presents an autonomous anti-spam system based on machine learning (ML) and natural language processing (NLP) techniques [2]. The system is designed to function without constant administrative oversight, analyzing incoming content in real-time.

Algorithms accurately assess spam probability while dynamically adapting to evolving malicious tactics [3, 4].

This approach automates the moderation process, substantially increasing processing speed and overall cybersecurity [4, 5].

The development process involved several key stages: thorough text preprocessing (noise reduction, removing emojis and URLs, lemmatization, and stemming), followed by vectorization (TF-IDF method).

The classification model, based on the Naive Bayes algorithm, demonstrated high efficiency in distinguishing spam from legitimate messages.

The system was integrated into a Telegram bot for seamless interaction, automatically analyzing input and providing a report with a spam probability score. The implementation utilized Python (pandas, scikit-learn, python-telegram-bot, joblib) and the SMSSpamCollection dataset (over 5,000 samples). Testing confirmed the stability and reliability of the proposed solution under real-world conditions.

References

1. Social Big Data Analytics: Practices, Techniques, and Applications / B. Abu Salih, P. Wongthongtham, D. Zhu, K. Y. Chan, A. Rudra. – Springer Nature. – 2021. – 218 p. DOI: https://doi.org/10.1007/978-981-33-6652-7.

2. Natural Language Processing Fundamental for Developers / O. Campesato. – Mercury Learning and Information. – 2021. – 364 p. DOI: https://doi.org/10.1515/9781683926566.

3. Research application of the spam filtering and spammer detection algorithms on social media and messengers / A. Podorozhniak, N. Liubchenko, V. Oliinyk, V. Roh // Advanced Information Systems. – 2023. – Vol. 7. – Iss. 3. – P. 60-66. DOI: https://doi.org/10.20998/2522-9052.2023.3.09.

4. Research Application of the Spam Filtering and Spammer Detection Algorithms on Social Media / N. Liubchenko, A. Podorozhniak, V. Oliinyk // CEUR Workshop Proceedings 3171, pp. 116-126, 2022. URI: https://ceur-ws.org/Vol-3171/paper13.pdf.

5. Strategies for Filtering Unwanted Comments in Social Media / A. Podorozhniak, V. Oliinyk, N. Liubchenko // 2024 IEEE 5th KhPI Week Kharkiv, Ukraine, pp. 1-4. DOI: https://doi.org/10.1109/KhPIWeek61434.2024.10877962.

COMPUTER MODELING OF COMPLEX PROCESSES USING A ONE-DIMENSIONAL APPROACH

Dymertsov D.O.
Simon Kuznets Kharkiv National University of Economics
Kharkiv, Ukraine

The relevance of the study is determined by the need to develop efficient information technologies and software tools for modeling gas-dynamic processes in technical systems.

Full-scale multidimensional models are limited by high computational costs and implementation complexity, which reduces their practical applicability. In this context, one-dimensional models provide an optimal balance between accuracy, computational efficiency, and algorithmic simplicity, and also support the development of integrated information and analytical systems with databases for storing and updating operational parameters.

The aim of the study is to develop, implement, and verify a one-dimensional mathematical and computational model for thermogas-dynamic processes in flow elements of technical systems using modern numerical methods.

The research focuses on constructing efficient and stable algorithms that account for key physical phenomena such as gas flow, heat and mass transfer, energy

transformations, turbulence, and hydraulic losses. The object of the study is numerical modeling of gas-dynamic processes in technical systems, while the subject is methods based on a generalized one-dimensional mathematical model for their calculation and analysis.

A relevant direction in Computer Science is the development of algorithmically efficient software tools for modeling gas-dynamic processes. Modern numerical methods and computational approaches enable the creation of software systems capable of accurately reproducing complex unsteady phenomena in technical systems.

Mathematical modeling plays a fundamental role in Computer Science, as it formalizes physical processes into computational models suitable for software implementation.

Under current conditions, the development of efficient numerical methods and algorithms for technical and energy systems is especially important [1], since it requires high accuracy under limited computational resources. This leads to the need for optimized, scalable, and performance-oriented computational models integrated into applied software systems.

In this work, within the framework of developing a software complex for calculating gas-dynamic processes in gas-jet acoustic generators, a unified computational model is proposed, focused on filling and emptying processes in closed technical volumes.

The model development emphasizes algorithmic formulation, selection of discretization methods, and implementation of efficient numerical procedures. The proposed model was verified by comparison with experimental and reference computational data, confirming its correctness and suitability for engineering applications.

The results demonstrate the potential of the approach for building intelligent decision-support systems, optimizing parameters, and automating the analysis of complex energy processes.

The aim of the study is to develop a generalized mathematical and computational model of thermogas-dynamic processes in gas-jet cooling-heating acoustic generators with further software implementation, focusing on an efficient numerical algorithm that describes the interaction of wave, thermal, and hydrodynamic phenomena.

The final goal is the creation of a software-oriented system for numerical experiments, analysis of operating modes, and optimization of gas-jet acoustic generator parameters, which improves energy efficiency, enables adaptive control of operating regimes, and expands practical applications in modern information-controlled systems.

The developed software complex also allows the formation of a database of operational characteristics and simulation results for further analysis and systematization.

In modern Computer Science research, mathematical modeling is a key tool for analyzing complex dynamic systems, particularly physical and gas-dynamic

processes, as it enables the representation of governing equations as computational algorithms implemented in software systems [2].

Numerical models are based on methods for solving nonlinear differential equations, including the finite difference method, finite volume method, and other approximation schemes [3, 4]. Multidimensional (2D and 3D) models provide detailed spatial-temporal resolution of processes but are computationally expensive and require significant optimization of implementation algorithms [5]. In contrast, one-dimensional models reduce complexity, simplify algorithmic structure, and improve computational efficiency while maintaining acceptable accuracy for engineering analysis and system behavior evaluation [6].

Modern computational approaches increasingly include hybrid and adaptive models that combine different numerical methods to improve stability and efficiency. These methods allow dynamic adaptation of discretization depending on the complexity of the simulated process, which is particularly important for nonlinear and unsteady physical systems [4, 5].

A crucial role in these approaches is played by algorithm design, numerical method selection, and optimization of computational procedures. Implementation typically involves methods such as finite differences and finite volumes, solvers for hyperbolic systems, and integration into programming environments using languages and tools like Python, C++, and Lazarus. As a result, flexible software systems are developed that support simulation, visualization, and analysis of complex dynamic processes.

The analysis of modern scientific literature shows that computational modeling methods are a core component of information technologies in engineering and scientific applications, as they combine accuracy, algorithmic efficiency, and automation capabilities. These approaches enable the construction of formalized mathematical and computational models of complex physical processes, forming a foundation for the development of effective simulation and optimization software systems.

The developed unified one-dimensional computational model was implemented using the Lazarus and Free Pascal as a software complex for numerical calculation of operating parameters of gas-jet acoustic generators. The selected programming environment provides high computational performance, flexibility in implementing numerical algorithms, and the ability to create an intuitive graphical user interface.

The developed software enables numerical simulation of thermogas-dynamic processes occurring in the working elements of the system. In particular, it allows the study of wave phenomena associated with the propagation of shock and expansion waves, as well as thermal processes involving heat exchange between the working medium and the walls of the receiving tube. This approach makes it possible to integrate the computational model into software systems for analysis, optimization, and verification of gas-jet acoustic generator operation.

As a result of the study, a unified one-dimensional computational model of gas-dynamic processes was developed. It accounts for key physical mechanisms,

including gas flow, energy conversion, heat and mass transfer, turbulence effects, and local hydraulic losses, and enables software implementation of numerical algorithms for engineering simulations. The model is based on fundamental conservation laws of mass, momentum, and energy, ensuring its physical validity and applicability to a wide range of gas-dynamic problems. During development, the model structure, initial and boundary conditions, and discretization approach were defined, ensuring numerical stability, convergence, and computational efficiency.

The proposed model was implemented as a software system for engineering calculations, operating режим analysis, and parameter optimization of gas-dynamic systems. Validation against experimental and literature data confirmed good agreement (error within 5%), demonstrating the correctness of assumptions and practical applicability of the approach.

The model can also be integrated into information systems supporting the life cycle of technical objects, enabling data storage, processing, and updating through databases or data warehouses.

Such integration allows recalculation of operational parameters based on updated input data, supporting prediction of equipment condition, degradation analysis, and maintenance planning.

The obtained results confirm the feasibility of using one-dimensional models as part of modern information technologies for engineering analysis and lifecycle management of technical systems. The proposed approach can be used to develop integrated software-information systems for decision support and optimization of gas-dynamic installations.

References

1. Potapov, V., Dymertsov, D. (2025), “Prospects for the Application of Gas-Jet Acoustic Generators as Secondary Energy Sources”, Refrigeration Engineering and Technology, 61(2), pp. 128–137, DOI: https://doi.org/10.15673/ret.v61i2.3178.
2. Vyslouch, S. P., Voloshko, O. V., Tymchyk, H. S., Filippova, M. V. (2021), Computer Modeling of Processes and Systems. Numerical Methods, Kyiv: Igor Sikorsky Kyiv Polytechnic Institute.
3. Dymertsov, D. (2025), “Modeling of Gas-Dynamic Processes of Wave Low-Temperature Heat Generators Dynamic Gas Distribution”, In: Tonkonogyi, V., Ivanov, V., Trojanowska, J., Oborskyi, G. (eds) Advanced Manufacturing Processes VI. Interpartner 2024. Lecture Notes in Mechanical Engineering. Springer, Cham. DOI: https://doi.org/10.1007/978-3-031-82746-4_68.
4. Zeidan, D., Hidalgo, A., Zhang, L. T., Goncalves Da Silva, E. (2025), Computational Fluid Dynamics: Novel Numerical and Computational Approaches, Springer Nature, DOI: https://doi.org/10.1007/978-981-97-8152-2.
5. Nadamani, M. N., Shadloo, M. S., Dbouk, T. (2025), “A Review: Theoretical and Computational Fluid Dynamics Modeling of Coupled Heat and Mass Transfer”, Energies, Vol. 18, No. 24, Article 6418, DOI: https://doi.org/10.3390/en18246418.
6. Anderson, J. D. (2003), Modern Compressible Flow: Modern Compressible Flow with Historical Perspective, McGraw-Hill.

A STUDY OF METHODS FOR IMPROVING THE STABILITY OF RADIO RELAY COMMUNICATIONS THROUGH SPATIAL-POLARIZATION SIGNAL PROCESSING

Kuznietsov O.L., Katunin A.M., Koval K.O.
Ivan Kozhedub Kharkiv National Air Force University,
Kharkiv, Ukraine
Kolomiitsev O.V.
National Technical University "Kharkiv Polytechnic Institute",
Kharkiv, Ukraine

Radio relay communication enables the transmission and reception of data messages between subscribers, typically within line-of-sight range.

The reliability of radio relay communication is enhanced through the implementation of modern technical solutions in these systems. Such technical solutions include the use of digital antenna arrays, the incorporation of dual polarization in these arrays, and the implementation of optimal algorithms for frequency-domain and time-domain signal processing.

The implementation of these solutions allows for the compensation of signal fading, the reduction of interpolarization interference, and the improvement of the radio relay communication system's noise immunity [1, 2].

However, the stability of radio relay communication is significantly affected by the composition and characteristics of the terrain.

Therefore, when setting up radio relay communication, it is essential to carefully select the route of the communication line or to implement technical measures to minimize the impact of interference from direct waves and waves reflected from the ground.

Thus, the effects of the terrain can be accounted for either by optimally routing the transmission path prior to deploying the communication line or by taking into account the distortions of the radio signal's phase front during its spatial processing.

The aim of the report is to presentation of the results of a comparative analysis of route selection methods and methods for accounting for fluctuations in the phase front of a radio signal wave caused by its multipath propagation.

The report reveals the Methods have been proposed to enhance the resilience of radio-relay communications, based both on optimizing the route selection method and on optimizing the algorithm for spatial processing of the radio signal.

Список літератури

1. A. Martynchuk, V. Vasylyshyn, Wu Lixiang, O. Martynchuk Research efficiency use of orthogonal double polarization MIMO antennas in drone communication. *Information Processing Systems.* – 2021. – 2 (165) – P. 40-47. https://doi.org/10.30748/soi.2021.165.05.

2. Barton D.K. Radar Equations for Modern Radar / D.K. Barton. London: Artech House, 2012.264 p.

A SAAS PLATFORM FOR REAL-TIME SOCIAL-PSYCHOLOGICAL GAMES

Kolomiitsev O.V., Kasianov A.S.
National Technical University “Kharkiv Polytechnic Institute”,
Kharkiv, Ukraine

The current stage of development of the information society is characterized by the transition of traditional forms of group leisure into the digital space.

Social-psychological games (such as “Mafia” and “Bunker”) have ceased to be mere entertainment, transforming into tools for developing emotional intelligence, critical thinking, and negotiation skills.

However, existing solutions often fail to provide the necessary level of “presence” due to technical limitations: high latency in game state transmission, poor video quality when zooming, and a lack of flexible mechanisms for managing gaming sessions.

Therefore, there is a need to develop the “Nightroom” web platform based on an event-driven architecture, which will enable us to address these challenges and combine the high speed of event processing via WebSockets with the benefits of media stream broadcasting using the SFU architecture.

Thus, the development of a SaaS platform for real-time social-psychological games is a pressing scientific challenge.

The aim of the report is to minimal synchronization delay and operational stability of the service's business model.

The report reveals the an analysis of the technical requirements for real-time systems was conducted.

The choice of an event-driven architecture for gaming platforms was justified. A game state model based on a finite state machine was designed and implemented to automate complex game scenarios.

A real-time session and status management system has been developed using Redis to ensure fault tolerance and efficiency.

The paper details the integration of a WebRTC-based media infrastructure to ensure stable group communication at low infrastructure costs. An assessment of the economic efficiency of the developed platform business model as a SaaS solution for the private and corporate sectors is presented.

The “Nightroom” platform has been proposed, whose social value lies in creating a tool for cognitive development and socialization. The project's business model is based on a freemium approach and the provision of the platform as a service to corporate clients, which, thanks to the low cost of processing traffic, makes the project economically attractive.

Thus, the project addresses the pressing social need for high-quality tools for remote socialization and professional training in the context of global digitalization.

МЕТОД ОБРОБКИ ВЕЛИКИХ ДАНИХ У ХМАРНОМУ СЕРЕДОВИЩІ З ВИКОРИСТАННЯМ ГІБРИДНИХ СТРУКТУР І АВТОМАТИЧНО МАСШТАБОВАНОЇ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

Кравченко П.О., Бобро В.Є., Почуєнков В.І.
Харківський національний університет радіоелектроніки,
Харків, Україна

Сучасні інформаційні системи функціонують в умовах безперервного зростання обсягів і швидкості надходження даних, що висуває підвищені вимоги до продуктивності та гнучкості обчислювальної інфраструктури.

Традиційні централізовані підходи до обробки великих даних дедалі частіше виявляються недостатньо ефективними для навантажень, що поєднують потокову обробку, аналітичні запити та масштабування у реальному часі.

Актуальним є поєднання хмарних обчислень, гібридних структур зберігання та мікросервісної архітектури з автоматичним масштабуванням [1].

Сучасні дослідження підтверджують, що архітектури типу data lakehouse є перспективною основою для таких рішень.

Метою доповіді є розробка методу обробки великих даних у хмарному середовищі на основі гібридних структур зберігання та автоматично масштабованої мікросервісної архітектури.

Запропонований підхід орієнтований на:

– забезпечення високої пропускної здатності, адаптивного керування ресурсами,

–зниження затримок

–підтримку пакетного, потокового та гібридного режимів обробки даних.

На рівні зберігання використовуються гібридні структури, що об'єднують властивості підходів data lake, data warehouse та lakehouse [1, 2]. Це дає змогу розмежувати «сирі» дані, аналітичні набори та структуровані агрегати без надлишкового дублювання.

Відкриті формати та об'єктне зберігання разом із кешуванням забезпечують масштабованість і переносність між хмарними провайдерами. На рівні надходження даних метод передбачає керування конвеєрами типу metadata-driven: метадані описують джерела, правила трансформації та маршрутизацію, що спрощує підключення нових джерел і зменшує операційну складність.

Функціональні компоненти системи реалізуються у вигляді мікросервісів, кожен з яких відповідає за окрему стадію обробки: приймання, валідацію, трансформацію, маршрутизацію, індексацію та надання результатів.

Така декомпозиція підвищує модульність, спрощує масштабування вузьких місць і забезпечує стійкість до відмов.

Для оркестрації використовується cloud-native середовище з автоматичним масштабуванням і балансуванням навантаження, що підтверджено практикою побудови сучасних платформ даних на основі Kubernetes і lakehouse-архітектури [3].

Ключовою особливістю методу є автоматичне масштабування мікросервісів на основі комплексного аналізу навантаження.

На відміну від простих порогових схем, масштабування враховує взаємозв'язки між сервісами, затримку обробки, показники SLO/SLA та динаміку потоку запитів.

Додатково поєднуються реактивний механізм (швидка відповідь на поточні перевантаження) та проактивний (прогнозування на основі історичних метрик). Дослідження підтверджують, що такі підходи дозволяють досягати вимог SLO при помітно нижчих витратах ресурсів порівняно зі стандартними механізмами [4– 6].

Запропонований метод поєднує переваги гібридних структур зберігання, керування типу metadata-driven та автоматично масштабованої мікросервісної архітектури. Його застосування підвищує адаптивність системи до змінного навантаження, покращує ефективність використання ресурсів і знижує затримки обробки.

Практична цінність методу полягає в можливості використання як у корпоративних системах підтримки рішень, так і в сервісах реального часу, де необхідна одночасна обробка великих розподілених наборів даних.

Список літератури

1. Harby A. A., Zulkernine F. Data Lakehouse: A survey and experimental study. Information Systems. 2025. Vol. 127. Article 102460. DOI: 10.1016/j.is.2024.102460

2. Rucco C., Longo A., Saad M. Enhancing Data Ingestion Efficiency in Cloud-Based Systems: A Design Pattern Approach. Data Science and Engineering. 2025. DOI: 10.1007/s41019-025-00300-2

3. AbouZaid A., Barclay P. J., Chrysoulas C., Pitropakis N. Building a modern data platform based on the data lakehouse architecture and cloud-native ecosystem. Discover Applied Sciences. 2025. Vol. 7. Article 166. DOI: 10.1007/s42452-025-06545-w

4. ZargarAzad M., Ashtiani M. An Auto-Scaling Approach for Microservices in Cloud Computing Environments. Journal of Grid Computing. 2023. Vol. 21. Article 73. DOI: 10.1007/s10723-023-09713-7

5. Nunes J. P. K. S., Nejati S., Sabetzadeh M., Nakagawa E. Y. Self-adaptive, Requirements-driven Autoscaling of Microservices. Proceedings of the 19th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS '24). 2024. P. 168–174. DOI: 10.1145/3643915.3644094

6. Shafi N., Abdullah M., Iqbal W., Bukhari F. CEMA: Cost Effective Multi-Layered Autoscaling for Microservice based Applications. Journal of Network and Computer Applications. 2025. Vol. 242. Article 104266. DOI: 10.1016/j.jnca.2025.104266

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СТРАТЕГІЙ КЕШУВАННЯ ТА СИНХРОНІЗАЦІЇ ДАНИХ У ПРОГРЕСИВНИХ ВЕБЗАСТОСУНКАХ

Фомічов О.О., Кутній О.С., Росінський Д.М.
Харківський національний університет радіоелектроніки,
Харків, Україна

Прогресивні вебзастосунки (PWA) відображають перспективний підхід до створення кросплатформних систем, що поєднують доступність вебтехнологій із частиною можливостей нативних застосунків. Ключову роль у їхній ефективності відіграють service workers, які перехоплюють мережеві запити, організовують локальне кешування та забезпечують роботу в умовах нестабільного з'єднання.

Водночас застосування кешування породжує нову задачу – підтримання актуальності й узгодженості даних у динамічних мережевих умовах, а його вплив поширюється й на енергоефективність застосунку на мобільних пристроях [1, 2].

Метою доповіді є оцінювання ефективності стратегій кешування та синхронізації даних у PWA за критеріями продуктивності, офлайн-доступності, економії трафіку та актуальності даних.

Актуальність проблеми зумовлена відсутністю універсального рішення: підхід, оптимальний для статичних ресурсів, може бути неприйнятним для динамічних даних [3].

Систематичні огляди підтверджують, що серед практичних переваг PWA найчастіше виокремлюють офлайн-підтримку та швидке повторне завантаження, тоді як серед труднощів – складність оптимального кешування і синхронізацію стану.

У дослідженні розглянуто три базові стратегії кешування [1, 4].

Cache First забезпечує мінімальний час доступу до збережених ресурсів і є оптимальною для статичних елементів інтерфейсу. Network First орієнтована на отримання актуальної версії з сервера, проте знижує швидкість реакції за слабкого з'єднання.

Stale-While-Revalidate повертає кешовану версію з паралельним оновленням у фоновому режимі.

Емпіричні результати показують, що кешування суттєво покращує продуктивність і зменшує енергоспоживання, однак ефект залежить від типу навантаження й структури застосунку.

Для PWA з офлайн-режимом природним є локальне накопичення змін із подальшою передачею на сервер. Однак цей підхід підвищує ризик конфліктів між локально зміненими та дистанційно оновленими даними [5]. Для їх вирішення дедалі частіше розглядаються структури CRDT, що гарантують збіжність реплік за одночасних незалежних змін, а також механізми Background Sync, які забезпечують контрольовану синхронізацію після відновлення з'єднання [6].

Система критеріїв ефективності охоплює:

– час першого та повторного завантаження;

– швидкість реакції інтерфейсу;

– доступність в офлайн-режимі;

– обсяг трафіку;

– затримку оновлення даних;

– стабільність за погіршення мережі.

Окремо враховується відповідність даних очікуванням користувача, адже висока швидкодія не забезпечує корисності, якщо відображається застаріла або суперечлива інформація.

Таким чином, найефективнішим є не ізольоване використання однієї стратегії, а їх комбінування:

– Cache First – для статики,

– мережево-орієнтовані або гібридні схеми – для чутливих до актуальності даних,

– локальне накопичення з контрольованою синхронізацією – для офлайн-редагування.

Це формує підґрунтя для розробки адаптивних моделей керування даними у PWA, що змінюють поведінку залежно від типу контенту та мережевого контексту.

Список літератури

1. Malavolta I., Chinnappan K., Jasmontas L., Gupta S., Soltany K. A. K. Evaluating the Impact of Caching on the Energy Consumption and Performance of Progressive Web Apps. Proceedings of the IEEE/ACM 7th International Conference on Mobile Software Engineering and Systems (MOBILESoft). 2020. P. 109–119. DOI: 10.1145/3387905.3388593.

2. Huber S., Mittermeir R. T., Kaufman R. et al. A Comparative Study on the Energy Consumption of Progressive Web Apps. Information and Software Technology. 2022. Vol. 146. Article 106865. DOI: 10.1016/j.infsof.2022.106865.

3. Fauzan R., Wibowo D. A., Rochimah S. A Systematic Literature Review on Progressive Web Application Practice and Challenges. Jurnal Teknik ITS. 2022. Vol. 11, No. 2. P. A309–A314.

4. Correia F., Ribeiro O., Silva J. C. Progressive Web Apps Development: Study of Caching Mechanisms. 21st Int. Conf. on Computational Science and Its Applications (ICCSA). 2021. P. 181–187. DOI: 10.1109/ICCSA54496.2021.00033.

5. Sirigiri K., Narra A., Sirumalla A. Offline-First PWA: Case Study on Efficient Data Handling and Synchronization. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023. Vol. 9, No. 3. P. 747–754. DOI: 10.32628/CSEIT25112782.

6. Josephe A. O., Chrysoulas C., Peng T., El Boudani B., Iatropoulos I., Pitropakis N. Progressive Web Apps to Support (Critical) Systems in Low or No Connectivity Areas. 2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET). 2023. P. 1–6. DOI: 10.1109/GlobConET56858.2023.10235946.

ANALYSIS AND COMPARATIVE STUDY OF METHODS FOR ENHANCING UAV CYBERSECURITY UNDER CONDITIONS OF VISUAL INFORMATION DEFICIENCY

Yu Jian., He Jiang
National Technical University "Kharkiv Polytechnic Institute",
Kharkiv, Ukraine

Modern unmanned aerial vehicles (UAVs) are widely used in monitoring, reconnaissance, and control tasks; however, their operation strongly depends on the quality of visual information [1–3].

Under conditions of limited or degraded visual data (nighttime, environmental interference, adverse weather, or intentional jamming), UAVs become significantly more vulnerable to cyber threats, which necessitates the development of specialized protection methods.

The aim of this study is to analyze and compare modern approaches to enhancing UAV cybersecurity in scenarios with insufficient or distorted visual information.

Particular attention is given to methods based on behavioral system analysis, multisensor data fusion, and machine learning algorithms for anomaly detection.

The paper considers several approaches, including the use of alternative sensors (inertial, radar, telemetry-based), algorithms for reconstruction or compensation of missing information, and cybersecurity techniques based on the analysis of system dynamics.

The comparative analysis demonstrates that hybrid approaches combining signal-level and behavioral models provide the highest robustness, enabling effective protection even under significant degradation of visual data.

The obtained results can be applied in the design of intelligent UAV protection systems capable of operating under uncertainty and limited information conditions.

References

1. Semenov, S., Krupska-Klimczak, M., Frontczak, M., Yu, J., He, J. & Chernykh, O. "Adaptive stochastic GERT modeling of UAV video transmission for urban monitoring systems".Applied Sciences.2025;15 (17):9277.DOI: https://doi.org/10.3390/app15179277.

2. Semenov, S., Jian, Y., Jiang, H., Chernykh, O. &Binkovska, A. "Mathematical model of intelligent UAV flight pathplanning". Advanced Information Systems.2025;9 (1):49–61.DOI: https://doi.org/10.20998/2522-9052.2025.1.06.

3. Semenov, S.; Karlov, D.; Solecki, M.; Ruban, I.; Kovalenko, A.; Piskarov, O. Integrated Model for Intelligent Monitoring and Diagnostics of Animal Health Based on IoT Technology for the Digital Farm. Sustainability 2025, 17, 8507. https://doi.org/10.3390/su17188507

ЗАДАЧА ІНТЕЛЕКТУАЛЬНОГО МОНІТОРИНГУ ТА ДІАГНОСТИКИ СТАНУ ЗДОРОВ'Я ТВАРИН

Семенов С.Г.
Краків, Університет комісії національної освіти, Польща
Карлов Д.С.
Харківський національний університет радіоелектроніки,
Харків, Україна

У наукових працях [1, 2] було розглянуто реалізацію системи інтелектуального моніторингу стану здоров'я тварин на основі технології IoT, яка включає архітектуру збору даних, їх обробку та формування інтегрального показника стану. Запропонована модель продемонструвала ефективність у задачах оцінки поведінкових та фізіологічних характеристик тварин, однак її опис має прикладний характер і орієнтований на конкретну реалізацію системи.

Разом з тим, використання лише прикладної моделі не дозволяє у повній мірі формалізувати загальний процес інтелектуального моніторингу та діагностики, забезпечити перенесення підходу на інші IoT-платформи, а також дослідити властивості системи незалежно від конкретних технічних рішень. Зокрема, залишаються недостатньо визначеними формальні зв'язки між потоковими даними, поведінковими ознаками, індивідуальними характеристиками тварин та процедурами прийняття діагностичних рішень.

У зв'язку з цим виникає необхідність розробки узагальненого методу інтелектуального моніторингу та діагностики стану здоров'я тварин, який^

– визначає формальну структуру обробки IoT-даних,

– забезпечує інтеграцію індивідуальних і групових характеристик поведінки,

– дозволяє виконувати оцінку стану в умовах потокового надходження даних.

Авторами запропоновано метод, що узагальнює підхід, реалізований у [1, 2], та визначає його математичну і алгоритмічну основу незалежно від конкретної архітектури системи.

Список літератури

1. Semenov, S.; Karlov, D.; Solecki, M.; Ruban, I.; Kovalenko, A.; Piskarov, O. Integrated Model for Intelligent Monitoring and Diagnostics of Animal Health Based on IoT Technology for the Digital Farm. Sustainability 2025, 17, 8507. https://doi.org/10.3390/su17188507

2. Семенов С. Карлов Д. Кібербезпека та стандартизація в iot-системах моніторингу тварин на основі протоколу LORAWAN. Матеріали XVII-ої Міжнародної науково-практичної конференції «Free and Open Source Software», Харків, 11-12 лютого 2026 р. – Харків: Харківський національний економічний університет імені Семена Кузнеця, 2026. – 180 с. https://foss.kn-it.info/

СИСТЕМА ПОКАЗНИКІВ ЕФЕКТИВНОСТІ АНСАМБЛІВ РІЗНОЕНЕРГЕТИЧНИХ СКЛАДНИХ СИГНАЛІВ ДЛЯ НАДШИРОКОСМУГОВИХ СИСТЕМ МНОЖИННОГО ДОСТУПУ З КОДОВИМ РОЗДІЛЕННЯМ

Лисечко В.П.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба, Харків, Україна
Жученко О.С., Індик С.В.
Український державний університет залізничного транспорту,
Харків, Україна

Сучасний розвиток бездротових електронних комунікаційних систем та мереж зумовив активний розвиток надширокосмугових систем доступу для малопотужних застосувань, спільною рисою яких є можливість застосування імпульсних складних сигналів. Сигнали такого типу дають змогу одночасно забезпечити вимоги щодо енергоефективності та практичної реалізації високочастотних трактів передавання, приймання та обробки у виділених для надширокосмугових систем доступу діапазонах частот. Подальший перехід до систем множинного доступу з кодовим розділенням дає змогу забезпечити гарантований одночасний доступ певної кількості користувачів. У роботах з формування ансамблів коротких відеоімпульсів з низьким рівнем взаємної кореляції цей напрям пов'язано з послідовностями з мінімальною енергетичною взаємодією [1]; такі послідовності пропонується називати часорозділювальними складними сигналами з періодичною структурою. Характерною особливістю таких ансамблів є конструктивна різноенергетичність сигналів через різну кількість імпульсів при їх однаковій тривалості.

Одним з основних показників ефективності системи множинного доступу з кодовим розділенням є відношення енергії корисного сигналу до сумарної енергії завад множинного доступу та шуму SINR (Signal-to-Interference-plus-Noise Ratio). Складовою SINR, що безпосередньо визначається ансамблем складних сигналів, є енергія завад множинного доступу. Для рівноенергетичних ансамблів складних сигналів оцінка зверху нормованої величини сумарної енергії завад множинного доступу, яку доцільно розглядати як показник структурної ефективності ансамблю, визначається добутком нормованої величини сумарної енергії заважаючих сигналів (енергетична складова), яку наближено можна прийняти такою, що дорівнює об'єму ансамблю, та найбільшим по ансамблю квадратом взаємної кореляції (кореляційна складова). У цьому випадку показник структурної ефективності є добутком двох скалярних величин, що забезпечує зручну для практичного використання форму показника. Для різноенергетичних ансамблів складних сигналів така форма показника не зберігається через різні енергії сигналів.

Можливим шляхом застосування форми показника структурної ефективності у виді добутку двох скалярних складових є застосування наближення, яке полягає у роздільному врахуванні структурних та

енергетичних властивостей ансамблів різноенергетичних складних сигналів. Для реалізації такого наближення запропоновано виконати зведення сукупності енергій сигналів різноенергетичного ансамблю до скалярної величини, результатом чого є фактична заміна різноенергетичного ансамблю умовним рівноенергетичним, яку визначено як еквівалентне перетворення [2, 3]. Два взаємопов'язані варіанти такого зведення визначають структурний еквівалентний об'єм, що відображає вплив нерівномірності розподілу енергій сигналів на завади множинного доступу, та енергетичний еквівалентний об'єм, що відображає зосередження сумарної енергії ансамблю в меншій умовній кількості сигналів. Ці величини мають протилежний характер зміни і задають дві різні інтерпретації впливу завад множинного доступу на користувачів з найменшими і найбільшими енергіями сигналів, що відповідає різному ступеню прояву ефекту домінування сигналів.

Отже, структурний еквівалентний об'єм $L_{\text{eq}}^{(+)}$ і енергетичний еквівалентний об'єм $L_{\text{eq}}^{(-)}$ утворюють взаємообернену пару характеристик одного різноенергетичного ансамблю. Через ці величини задаються показник структурної ефективності $\gamma_{\text{str}}^{(+)}$ та показник енергетичної справедливості $\gamma_{\text{en}}^{(-)}$. Для ансамблю об'ємом L з енергіями сигналів $E_i, i = 1,2, \dots, L$, та найбільшим по ансамблю квадратом взаємної кореляції R_{max}^2 система показників ефективності має:

$$L_{\text{eq}}^{(+)} = L^2 \sum_{i=1}^{L} E_i^2 \Big/ \left(\sum_{i=1}^{L} E_i \right)^2,$$

$$L_{\text{eq}}^{(-)} = \left(\sum_{i=1}^{L} E_i \right)^2 \Big/ \sum_{i=1}^{L} E_i^2,$$

$$L_{\text{eq}}^{(+)} L_{\text{eq}}^{(-)} = L^2,$$

$$\gamma_{\text{str}}^{(+)} = L_{\text{eq}}^{(+)} R_{max}^2,$$

$$\gamma_{\text{en}}^{(-)} = L_{\text{eq}}^{(-)} / L.$$

Застосування показника структурної ефективності у виді добутку величин структурного еквівалентного об'єму та максимального значення взаємної кореляції в ансамблі дозволило удосконалити метод оцінки структурної ефективності ансамблів складних сигналів на основі кореляційних функціоналів та забезпечити збіг з результатами оцінки для ансамблів рівноенергетичних складних сигналів, вищу частоту збігу з результатами точного порівняння ансамблів та меншу обчислювальну складність при його поширенні на ансамблі різноенергетичних складних сигналів.

У разі спільного застосування вищезазначені показники набувають значення взаємопов'язаних складових єдиного інструменту, який може бути застосовано в задачах синтезу, вибору, порівняння та ранжування ансамблів

складних сигналів. Двовимірне представлення ансамблів у просторі показників ефективності або у просторі еквівалентних об'ємів забезпечує врахування структурних і енергетичних властивостей і не може бути еквівалентно замінене однією скалярною величиною без втрати змісту кожної зі складових. Сформульовано загальну задачу вибору ансамблів-кандидатів у вигляді трьохетапної процедури у вибраному двовимірному просторі, що включає формування множини кандидатів, перевірку допустимості як належності точки допустимій області та застосування правила вибору серед допустимих точок. Наведено типові задачі вибору, які охоплюють випадок заданого об'єму ансамблю, випадок вибору ансамблю максимально можливого об'єму в межах заданих енергетичних обмежень, а також випадок вибору сигналу для допуску нового користувача у робочому стані системи множинного доступу за наявності підмножин зайнятих і вільних сигналів. Практичне значення системи показників ефективності полягає у тому, що вона може бути використана для узагальненого порівняння різних ансамблів складних сигналів з одночасним урахуванням об'єму ансамблю, кореляційних властивостей та нерівномірності енергетичного розподілу. Геометричне представлення множини ансамблів-кандидатів у площині показників ефективності або у площині еквівалентних об'ємів дозволяє будувати процедури перевірки допустимості та вибору ансамблю за заданими обмеженнями на завади множинного доступу.

Введені показники ефективності поставлено у відповідність рівням запропонованої багаторівневої функціональної моделі показників ефективності системи множинного доступу з кодовим розділенням [4], а саме: показник енергетичної справедливості $\gamma_{\text{en}}^{(-)}$ - енергетичному рівню; показник структурної ефективності $\gamma_{\text{str}}^{(+)}$ - структурному рівню. Потужнісно-канальному рівню відповідає SINR, який є композицією функціоналів енергетичного та структурного рівнів, системному рівню - функціонал, що визначає узагальнений показник ефективності системи множинного доступу відповідно до поставленої задачі і є композицією функціоналів енергетичного, структурного та потужнісно-канального рівнів. Багаторівнева модель визначається такими співвідношеннями:

$$P_{\text{EN}} = \gamma_{\text{en}}^{(-)};\ P_{\text{STR}} = \gamma_{\text{str}}^{(+)};\ P_{\text{CHP}} = F_{\text{CHP}}\left(\gamma_{\text{str}}^{(+)}, N\right) = \text{SINR};$$

$$P_{\text{SYS}} = F_{\text{SYS}}(P_{\text{CHP}}, C_{\text{SYS}}),$$

де P_{EN}, P_{STR}, P_{CHP}, P_{SYS} - показники ефективності відповідно енергетичного, структурного, потужнісно-канального та системного рівнів; N - параметр потужнісно-канального рівня, що визначається моделлю каналу зв'язку; C_{SYS} - множина параметрів системного рівня, що визначається постановкою задачі оцінки або вибору.

Запропонована багаторівнева функціональна модель разом з алгоритмом функціональної редукції дає змогу будувати узгоджені за рівнями показники ефективності та порівнювати варіанти побудови системи множинного доступу

з кодовим розділенням за мінімально необхідним складом рівнів, що забезпечує використання лише тих рівневих функціоналів, які впливають на результат розв'язання поставленої задачі.

Список літератури

1. Indyk S. V., Lysechko V. P., Zhuchenko O. S., Kitov V. S. The Formation Method of Complex Signals Ensembles by Frequency Filtration of Pseudo-Random Sequences with Low Interaction in the Time Domain. Radio Electronics, Computer Science, Control. 2020. No. 4. P. 7–14. DOI: https://doi.org/10.15588/1607-3274-2020-4-1. URL: https://ric.zp.edu.ua/article/view/217986.

2. Zhuchenko O., Panchenko S., Lysechko V., Indyk S. Methodology of Equivalent Transformations of Unequal-Energy Complex Signal Ensembles in Code-Division Multiple Access Systems. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2026. Вип. 62. С. 337–345. DOI: https://doi.org/10.36910/6775-2524-0560-2026-62-38

3. Жученко О. С., Індик С. В. Методологія оцінювання ефективності ансамблів різноенергетичних складних сигналів у надширокосмугових системах множинного доступу з кодовим розділенням. Застосування інформаційних технологій у підготовці та діяльності сил безпеки і оборони : збірник тез доповідей Міжнародної науково-практичної конференції, 17 березня 2026 р., м. Харків. Харків : Нац. акад. НГУ, 2026. С. 368–370.

4. Panchenko S. V., Lysechko V. P., Zhuchenko O. S., Indyk S. V. Multi-Level Functional Model of Performance Indicators for Ultra-Wideband Code Division Multiple Access Systems. Сучасні наукові парадигми: інтеграція знань і технологій : матеріали науково-практичної конференції, м. Вінниця, 26–27 грудня 2025 р. Одеса : «Молодий вчений», 2025. С. 121–123.
https://molodyivchenyi.ua/omp/index.php/conference/catalog/view/164/2843/5903-1

УЧАСНИКИ КОНФЕРЕНЦІЇ (секція 6, підсекція 6.3)

Dymertsov D.O. 53
Frolov D. 52
Gerasimenko V.A. 36
He Jiang 63
Heiko H. 52
Kasianov A.S. 58
Katunin A.M. 57
Kolomiitsev O.V. .. 57
..... 58
Koval K.O. 57
Kuznietsov O.L. 57
Liubchenko N. 50
Liubchenko N. 52
Oleksiienko D. 50
Podorozhniak A. ... 50
..... 52
Serikov Y. 33
..... 36
Skorlupin O. 50
Yu Jian 63
Безсонний В.Л. 6
..... 8
Бобро В.Є. 59
Буюн Д.О. 10
Вальченко О.І. 46
..... 48
Давиденко Я.Ф. ... 40
Демченко І.О. 46
Доронін Є.В. 8
..... 10
..... 12
..... 22
..... 25
..... 29
Жученко О.С. 65
Індик С.В. 65
Калач І.В. 17
Калитчук А. 13
Карлов Д.С. 64
Кеня М.А. 19
Кічата Н.М. 15
..... 41
Кравченко П.О. ... 59
Курська Т.М. 17
..... 18
..... 19
Кутній О.С. 61
Лагутін М.І. 32
Лисечко В.П. 65
Лінчевський І.В. . 45
Лобяк Т.А. 18
Макаренко М.Є. .. 20
Макаров В.І. 10
Максименко В.О. 6
Манохін Д. 12
Новоселя У.Д. 20
Паращанов В.Г. .. 22
..... 25
Петухова О.А. 27
Пилипенко О.В. .. 13
..... 29
Почуєнков В.І. 59
Росінський Д.М. . 61
Савченко М.М. ... 32
Савченко М.Ф. 32
Саньков П.М. 13
..... 20
Семенов С.Г. 64
Синило К.В. 38
Сошко І.С. 48
Тимченко П.О. 29
Ткач Н.О. 20
Третьяков О.В. ... 15
..... 40
..... 41
..... 45
..... 8
Трипольська К.С. 27
Федина В.П. 41
Фомічов О.О. 61
Халмурадов Б.Д. . 41
Якимець І.В. 38

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Азербайджанський державний економічний університет, Баку, Азербайджан
Азербайджанський технічний університет, Баку, Азербайджан
Азербайджанський університет будівництва та архітектури, Баку, Азербайджан
Академія Державної прикордонної служби, Баку, Азербайджан
Акціонерне товариство «Інститут інформаційних технологій», Харків, Україна
Алматинський технологічний університет, Алмати, Казахстан
Бакинський інженерний університет, Баку, Азербайджан
Військова академія Університету оборони, Белград, Сербія
Військовий науково-дослідний інститут, Баку, Азербайджан
Військовий інститут імені Гейдара Алієва, Баку, Азербайджан
Гянджинський технологічний університет, Гянджа, Азербайджан
Державний біотехнологічний університет, Харків, Україна
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
Інститут географії, Баку, Азербайджан
Інститут математики, Баку, Азербайджан
Інститут освіти Республіки Азербайджан, Баку, Азербайджан
Інститут системної інженерії, Пекін, Китай
Карачинський університет, Карачі, Пакистан
Київський національний університет будівництва і архітектури, Київ, Україна
Національне аерокосмічне агентство, Баку, Азербайджан
Національний аерокосмічний університет "Харківський авіаційний інститут", Харків, Україна
Національний технічний університет "Харківський політехнічний інститут", Харків, Україна
Національний університет «Київський авіаційний інститут», Київ, Україна
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
Національний університет оборони Азербайджанської республіки, Баку, Азербайджан
Національний університет "Одеська політехніка", Одеса, Україна
Національний університет цивільного захисту України, Київ, Харків, Черкаси, Україна
Педагогічний університет імені Комісії Національної Освіти в Кракові, Краків, Польща
Придніпровська державна академія будівництва та архітектури» УДУНТ, Дніпро, Україна
Республіканський центр сейсморозвідки, Баку, Азербайджан
Сумгаїтський державний університет. Сумгаїт, Азербайджан
Тбіліський державний університет, Тбілісі, Грузія

Технічний університет Клуж-Напоки, Клуж-Напока, Румунія
ТОВ «Праймкор», Харків, Україна
Український науково-дослідний інститут екологічних проблем», Харків, Україна
Університет Ель-Манар, Туніс, Туніс
Університет Заказік, Заказік, Єгипет
Університет міста Жиліна, Жиліна, Словаччина
Університет національної оборони Туреччини, Стамбул, Туреччина
Університет нафти і мінералів імені короля Фахда, Дахран, Саудівська Аравія
Університет Сол Плаат'є, Кімберлі, Південно-Африканська Республіка
Університет технологій Гянджі, Гянджа, Азербайджан
Університет технологій імені Нетаджі Субхаса, Нью-Делі, Індія
Університет технології і гуманітарних наук, Бельсько-Бяла, Польща
Управління метрології та стандартизації, Київ, Україна
Харківський національний автомобільно-дорожній університет, Харків, Україна
Харківський національний економічний університет імені Саймона Кузнеця, Харків, Україна
Харківський національний університет імені В.Н. Каразіна, Харків, Україна
Харківський національний університет міського господарства імені О.М. Бекетова, Харків, Україна
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна
Харківський національний університет радіоелектроніки, Харків, Україна
Черкаський державний технологічний університет, Черкаси, Україна

Affiliation of conference participants

ЗМІСТ

Том 1: секції 1, 5

Том 2: секція 2

Том 3: секції 3, 4

Том 4: секція 6

Том 5: секція 6

Секція 6 (підсекція 6.3) Інформаційні технології у цивільній безпеці 6

Учасники конференції (секція 6, підсекція 6.3) 69

Організації, які прийняли участь у конференції 70

НАУКОВЕ ВИДАННЯ

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей
шістнадцятої міжнародної науково-технічної конференції
(29 – 30 квітня 2026 року)
Том 5: секція 6

Відповідальний за випуск *Г. А. Кучук*
Технічний редактор *І. А. Лєбедева*
Коректор *В. В. Богомаз*
Комп'ютерне складання та верстання *Н. Г. Кучук*

Адреса оргкомітету: вул. Кирпичова, 2, Харків, 61002, Україна
Вечірній корпус, кімната 314
тел. +38 (057) 707 61 65

Підписано до друку 22.04.2026 Формат 60 × 84/16
Ум.-вид. арк. 4,5. Тираж 40 пр. Зам. 422/5-26

Віддруковано з готових оригінал-макетів у цифровій друкарні Impress
61002, м. Харків, вул. Пушкінська, 56, тел. **+ 38 (057) 714-52-11**
e-mail: **irina@impress.biz.ua**