

структурних викликів, пов'язаних із удосконаленням системи охорони праці. Незважаючи на виконану роботу, ключові аспекти охорони праці залишаються недостатньо розвиненими та потребують подальшої адаптації до європейських стандартів [1]. Основні проблеми та шляхи їх вирішення:

1. Фінансування: Одним із найголовніших викликів є обмежене фінансування, що стримує реалізацію широкомасштабних реформ. З метою покращення умов праці держава має сприяти залученню інвестицій та надавати субсидії на модернізацію обладнання, особливо у високоризикових галузях.

2. Підготовка кадрів: Нестача кваліфікованих фахівців у галузі охорони праці потребує створення нових освітніх програм і курсів для підвищення кваліфікації спеціалістів. Варто розробити спільні програми з європейськими партнерами для обміну досвідом та знаннями.

3. Права обізнаність роботодавців: Значна частина роботодавців не до кінця усвідомлює важливість відповідності європейським нормам. Це вимагає організації спеціальних інформаційних кампаній, тренінгів та підвищення відповідальності за порушення правил охорони праці.

Перспективи та очікувані результати: Впровадження європейських стандартів охорони праці в Україні забезпечить значні соціально-економічні переваги: підвищення продуктивності праці, зменшення кількості нещасних випадків на виробництві, покращення здоров'я працівників і, як наслідок, зниження витрат на соціальне забезпечення та медичне страхування. Це також сприятиме підвищенню інвестиційної привабливості країни та інтеграції української економіки в європейський ринок.

Список літератури

1. Впровадження європейських стандартів охорони праці в діяльність українських підприємств. <http://www.economy.nayka.com.ua>

ОЦІНКА СТІЙКОСТІ ТРАНСПОРТНОЇ ІНФРАСТРУКТУРИ ДО НАДЗВИЧАЙНИХ СИТУАЦІЙ

Карпенко О.О.

Національний авіаційний університет, Київ, Україна

Транспортна інфраструктура є важливим елементом національної економіки, а її стійкість до надзвичайних ситуацій є ключовою для зменшення ризиків та збереження безпеки населення [1]. **Метою доповіді є оцінка стійкості об'єктів транспортної інфраструктури до надзвичайних ситуацій та аналіз методів підвищення їхньої надійності в умовах кризових ситуацій.**

Одним із дієвих підходів є системи раннього попередження та використання датчиків для моніторингу стану конструкцій, що дозволяє вчасно виявляти можливі пошкодження через природні катастрофи або перевантаження [2]. Аналітика великих даних і штучний інтелект також сприяють прогнозуванню ризиків та впровадженню оперативних заходів

безпеки, таких як захист доріг та мостів у разі повеней [3]. Регулярна оцінка стану інфраструктури та її модернізація за міжнародними стандартами є важливими факторами стійкості. Показовим є досвід Японії, де тестування інфраструктури на стійкість до землетрусів є пріоритетом, що суттєво знижує ризики внаслідок катастроф [4]. Забезпечення стійкості транспортної інфраструктури вимагає комплексного підходу, що включає технічні, організаційні та інформаційні заходи, які сприяють захисту критичних об'єктів та мінімізації можливих збитків у разі надзвичайних подій.

Список літератури

1. Тихоненко С. П., Литвиненко Р. М. Розвиток транспортної інфраструктури в умовах підвищених ризиків. Транспорт та безпека. 2022. Т. 5, № 3. С. 29–34.
2. Коваленко Ю. О., Смирнов А. В. Аналітика великих даних у транспортній безпеці. Наукові записки з транспортної інженерії. 2021. Т. 4, № 2. С. 15–20.
3. Смирнов А. В. Методи оцінки стійкості транспортних об'єктів. Практика безпеки на транспорті. 2023. Т. 2, № 1. С. 10–15.
4. Ямашита Т. Підвищення безпеки мостів та тунелів під час землетрусів. Японський журнал безпеки інфраструктури. 2020. Т. 12, № 4. С. 45–49.

СТРАТЕГІЇ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРЗАГРОЗ

Карпенко О.О.

Національний авіаційний університет, Київ, Україна

Захист критичної інфраструктури від кіберзагроз є одним із найважливіших аспектів національної безпеки в сучасному світі. Розвиток інформаційних технологій і зростання числа кібератак підвищують ризики для стратегічних об'єктів, таких як електростанції, транспортні системи, фінансові установи та водопостачання [1]. Застосування комплексного підходу до кіберзахисту включає аналіз ризиків, впровадження сучасних засобів кібербезпеки та розробку планів дій на випадок надзвичайних ситуацій.

Метою доповіді є аналіз сучасних стратегій захисту критичної інфраструктури від кіберзагроз та дослідження інноваційних підходів до забезпечення кібербезпеки.

Ключовими елементами кіберзахисту є застосування систем раннього попередження, адаптивних систем захисту та використання штучного інтелекту для виявлення аномальних активностей. На додаток, міжнародне співробітництво сприяє розробці єдиних стандартів і спільних заходів захисту критичних інфраструктур [2].

Згідно з дослідженнями, систематичний підхід до захисту критичної інфраструктури від кібератак дозволяє знизити ризики та забезпечити більш ефективне реагування на потенційні загрози [3]. Це забезпечує надійність об'єктів критичної інфраструктури навіть у випадках серйозних надзвичайних ситуацій [4].