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].

Список літератури

1. Ковальчук С. І., Лук'яненко Г. П. Захист критичної інфраструктури в умовах кіберзагроз. Сучасні проблеми національної безпеки. 2020. Т. 1, № 2. С. 45–52.
2. Сидоренко П. О., Долінська В. А. Міжнародні стандарти в сфері кібербезпеки. Безпека та кіберзахист. 2021. С. 34–40.
3. Іваненко О. П. Впровадження інновацій у кіберзахист критичних об'єктів. Збірник матеріалів конференції "Безпека майбутнього". Київ, 2023. С. 19–24.
4. Петрова М. В. Аналіз ефективності систем кіберзахисту. Кібербезпека та інформаційні технології. 2022. Т. 3, № 1. С. 12–18.

ЗАХОДИ ІЗ ПОПЕРЕДЖЕННЯ ВИНИКНЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ НА МАГІСТРАЛЬНИХ ТРУБОПРОВІДНИХ КОМУНІКАЦІЯХ

Федина В.П., Якимець І.В., Мартиненко Д.О.
Національний авіаційний університет, Київ, Україна

Трубопровідний транспорт на сьогодні один з найбільших економічних видів транспортування нафти, нафтопродуктів та газів з місць їх виявлення, виробітку та виробництва до ділянок їх переробки та використання. Наразі, магістральні продуктопроводи, аміакопроводи, нафтопроводи і газопроводи транспортують вище перелічені продукти на велику дистанцію короткою ниткою розгалужень з мінімальними втратами. Загальна протяжність усіх магістральних трубопроводів світу, які спроектовані, побудовані, проінспектовані та введені у дію на початок XXI століття, склала приблизно 3500000 км в 120 країнах світу [1].

Головна особливість трубопровідного транспорту — безперервність функціонування. Для забезпечення безперебійної роботи магістральних трубопроводів існує сучасна система моніторингу транспортних трубопровідних комунікацій [2]. Сучасний моніторинг магістральних трубопровідних комунікацій неможливий без застосування авіаційної техніки. В реальних умовах експлуатації важливим є питання вибору засобів моніторингу: пілотовані чи безпілотні повітряні судна (ПС).

Метою доповіді є проведення порівняльного аналізу ефективності застосування авіаційної техніки (пілотованої і безпілотної) для проведення заходів із попередження виникнення надзвичайних ситуацій на об’єктах трубопровідного транспорту. Для проведення такого аналізу розглядались БАС на базі БПЛА «Лелека-100», створений українською компанією DeViRo та багатоцільовим вертоліт МСБ-2 «Надія».

Результати досліджень показують, що йбільш ефективним і економічно вигідним методом моніторингу нафто- і газо - трубопроводів є застосування безпілотних повітряних суден (БПС), які в режимі реального часу (FPV-дрони) надають якісні зображення та дозволяють виявляти нафтові розливи, звалища, врізки, проведення робіт в охоронних зонах і т.д.