ІННОВАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ ЗАХИСТУ ДОВКІЛЛЯ

УДК 502.58:004.056.5:625.7:629.3
DOI https://doi.org/10.32846/2306-9716/2024.eco.5-56.26

КОМПЛЕКСНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ЕКОЛОГІЧНОЇ БЕЗПЕКИ В СИСТЕМІ «АДС» В УМОВАХ ЦИФРОВІЗАЦІЇ

Адамова Г.В.
Науково-дослідна установа «Український науково-дослідний інститут екологічних проблем»
вул. Бакуліна, 6, 61166, м. Харків
abolmasova@niiep.kharkov.ua

Розвиток інформаційних технологій, що сприяє підвищенню ефективності роботи в системі «Автомобіль-Дорога-Середовище» (АДС), безперечно супроводжується появою все нових ризиків (кіберзагроз), які можуть мати значний вплив на екологічну безпеку. Цей вплив виражається, зокрема, в можливості порушення роботи систем екологічного моніторингу, збільшенні забруднення навколишнього природного середовища, створенні умов для довгострокового впливу на довкілля, використання даних про екологічний стан навколишнього середовища для маніпуляцій, ускладнення прийняття екологічних рішень і т.д. При цьому, більшість досліджень щодо кіберзагроз та кібербезпеки зосереджені на окремих аспектах транспортної інфраструктури, таких як захист окремих компонентів автомобільних систем або інтелектуальних транспортних систем, при цьому не враховуючи екологічний компонент або враховуючи його частково. Але система «АДС» є складним комплексом, в якому, з точки зору кіберзагроз, взаємодіють між собою технічні (автомобілі, дорожня інфраструктура, інженерні споруди), інформаційні (системи збору, передачі та аналізу даних) та екологічні (довкілля, моніторингові системи, екологічні дані) елементи. Тому, для розуміння взаємозв'язків всіх цих елементів та їх компонентів, а також для розуміння щодо потенційного впливу ризиків в системі «Автомобіль-дорога-середовище» на екологічну безпеку, необхідно застосовувати саме комплексний підхід.

Під час дослідження було проаналізовано низку закордонних та вітчизняних робіт з яких виокремлено потенційні види кіберзагроз у системі «АДС» та розподілено їх за спрямуванням на кожний з елементів системи. Також було виділено який вплив можуть чинити розглянуті кіберзагрози в контексті забезпечення екологічної безпеки автомобільних доріг та надані можливі заходи безпеки для підвищення рівня захисту системи «АДС», які необхідно розглядати разом з заходами зі зменшення впливу від експлуатації автомобільної дороги на складові довкілля. *Ключові слова:* система «Автомобіль-Дорога-Середовище», критична інфраструктура, екологічна безпека, кібербезпека, довкілля, загроза, ризик.

A comprehensive approach to ensuring environmental safety in the "CRE" system in the context of digitalization. Adamova H.

The development of information technologies that enhance efficiency in the "Car-Road-Environment" (CRE) system is inevitably accompanied by the emergence of new risks, particularly cyber threats, which can significantly impact environmental safety. This impact is expressed in the potential disruption of environmental monitoring systems, increased environmental pollution, creation of conditions for long-term environmental harm, manipulation of environmental data, and complications in making informed ecological decisions, among other consequences.

Most research on cybersecurity and cyber threats tends to focus on specific aspects, such as protecting individual components of vehicle systems or intelligent transportation systems, while often neglecting or only partially addressing the environmental component. However, the "CRE" system is a complex entity wherein technical (vehicles, road infrastructure, engineering structures), informational (data collection, transmission, and analysis systems), and environmental (natural environment, monitoring systems, environmental data) elements interact in the context of cyber threats. Therefore, a comprehensive approach is needed to systematically analyze risks within the "CRE" system, ensuring a clear understanding of the interconnections between all elements and their potential impacts on environmental safety.

During the study, various foreign and domestic works were analyzed to identify potential types of cyber threats within the "CRE" system and classify them according to their focus on specific system elements. Additionally, the study highlighted the possible impacts of these cyber threats in the context of ensuring the environmental safety of road systems. Recommendations for improving the security of the "CRE" system were provided, emphasizing the need to integrate these measures with strategies aimed at reducing the environmental impact of road operations on ecological components. *Key words:* "Car-Road-Environment" system, critical infrastructure, environmental safety, cybersecurity, environment, threat, risk.

Постановка проблеми. Постійний та невпинний розвиток інформаційних технологій (ІТ), зокрема в системі «Автомобіль-Дорога-Середовище» (АДС), сприяє підвищенню ефективності її роботи. Але поряд з цим безперечно зумовлюється поява нових ризиків (кіберзагроз), які можуть мати значний вплив на екологічну безпеку. Серед них, зокрема, вплив на системи екологічного моніторингу та екологічну інфраструктуру, порушення їх роботи, посилення забруднення навколишнього природного

середовища і т.д. Саме тому важливо усвідомлювати взаємозв'язок між екологічною безпекою та кібербезпекою й застосовувати комплексний підхід до забезпечення безпеки та захищеності критично важливої інфраструктури, якою, беззаперечно являються автомобільні дороги.

Актуальність дослідження. Важливу роль в забезпеченні більш ефективної роботи системи «АДС» грають ІТ, насамперед інтелектуальні транспортні системи, автоматизовані системи керування дорожнім рухом і системи екологічного моніторингу. Поряд з перевагами, що вони надають, безперечно зростають і загрози для кібербезпеки, що можуть впливати як на кожну з складових, так і на систему в цілому.

Так, кібератаки як окремих елементів так і всієї системи «АДС» можуть мати суттєві наслідки для життєзабезпечення густонаселених територій, призвести до значних екологічних і соціальних втрат. Зокрема, вони здатні порушувати роботу систем моніторингу забруднення основних складових довкілля (повітря, води, ґрунту), викликати аварійні ситуації, що матимуть екологічні наслідки (розлив небезпечних речовин, забруднення відходами аварій, розливи масел та нафтопродуктів, збільшення рівня викидів), або ж навіть створювати умови для довготривалого впливу на навколишнє природне середовище.

Враховуючи вище наведену інформацію, дослідження зв'язку між екологічною безпекою та кібербезпекою в системі «Автомобіль-Дорога-Середовище» є надзвичайно актуальним.

Зв'язок авторського доробку із важливими науковими та практичними завданнями. В статті підіймаються важливі та актуальні питання, пов'язані із кіберзагрозами в системі «АДС», зокрема в частині впливу їх на екологічну безпеку. Визначено потенційні кіберзагрози, що можуть впливати на систему «АДС», встановлено можливі наслідки для екологічної складової системи, а також запропоновано шляхи підвищення рівня безпеки у системі. Розглянуто механізми дії між технічними, інформаційними та екологічними елементами системи «АДС» з точки зору їх уразливості до кібератак, що підкреслює важливість врахування заходів з кіберзахисту під час розробки комплексних заходів зменшення впливу на довкілля від експлуатації автомобільних доріг.

Аналіз останніх досліджень та публікацій. На сьогодні, системний підхід до забезпечення безпеки всіх комплексних елементів системи «Автомобіль-Дорога-Середовище» є недостатньо дослідженим. Важливим аспектом є інтеграція безпеки на всіх рівнях взаємодії, що охоплює автомобільні системи, дорожню інфраструктуру та навколишнє середовище.

За останні роки було проведено ряд нових досліджень, присвячених питанням кібербезпеки транспортних систем. Однак, більшість з них зосереджені на окремих аспектах, таких як захист окремих компонентів автомобільних систем або інтелектуальних транспортних систем (ITS) [1, 2].

В [3] розглядаються екологічні ризики, що можуть бути викликані кіберзагрозами, зокрема, зазначено, що для транспортних систем впливи можуть бути на камери, що знаходяться на дорогах, на сигнали та системи моніторингу/контролю. Однак у роботі відсутній розширений аналіз щодо того, як саме це вплине на екологічну безпеку доріг і відсутні пропозиції щодо шляхів підвищення рівня безпеки захисту**.**

В Україні існують кілька нормативних документів [4-6], які регулюють питання кібербезпеки та опосередковано торкаються екологічної безпеки, зокрема через захист критичної інфраструктури. Так, у [4] визначено основи кібербезпеки, включаючи захист критичної інфраструктури, до якої належать також і елементи, що можуть впливати на навколишнє середовище, наприклад, транспортні та дорожні системи [7]. Однак чіткої інформації щодо зв'язку між екологічною безпекою та кібербезпекою автомобільних доріг немає.

Виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття та новизна.

Кібербезпека автомобільних доріг, як об'єкта критичної інфраструктури, потребує інформації не лише про будівництво, утримання та експлуатацію автомобільних доріг, а й про планування та організацію впровадження заходів із забезпечення екологічної безпеки.

Більшість досліджень на цю тему зосереджені або на автомобільних системах, або ж на дорожній інфраструктурі, при цьому дуже часто екологічний компонент у них не враховується. Ці дослідження окреслюють загальні питання пов'язані з кіберзагрозами в транспортних системах і пропонують технічні рішення для їх мінімізації. Але ж вразливими для кібератак можуть бути зокрема і дорожні об'єкти дистанційного відстеження змін та параметрів стану та умов навколишнього середовища в районі проходження автомобільної дороги, де використовуються датчики або інші системи моніторингу. Це означає, що заходи екологічної безпеки також повинні враховувати необхідність захисту кібербезпеки для запобігання потенційним атакам, які можуть порушити роботу цих систем або поставити їх роботу під загрозу.

Тому необхідно застосовувати комплексний підхід, який охоплюватиме всі аспекти системи «АДС», та враховуватиме як екологічну безпеку так і кібербезпеку цієї системи.

Мета дослідження: визначити можливі кіберзагрози в системі «АДС», зокрема з точки зору їх впливу на екологічну безпеку та надати пропозиції щодо можливих заходів безпеки для підвищення рівня захисту системи.

Методологічне або загальнонаукове значення. Дослідження проводилися на основі опрацювання наукових, нормативних та методологічних літературних джерел за тематикою статті.

Викладення основного матеріалу.

Для забезпечення екологічної безпеки автомобільних доріг оптимальним є використання комплексного експертно-аналітичного підходу із застосуванням MAI. Для цього була розроблена ієрархічна структура комплексної оцінки впливу експлуатації автомобільної дороги на довкілля (рис. 1). Детальний опис декомпозиції проблеми, самої структури, постановок завдання експертам для попарного порівняння елементів та аналіз результатів еколого-експертно-аналітичного дослідження (ЕЕАД) надані в [8].

Система «АДС» є складним комплексом, в якому, з точки зору кібербезпеки, взаємодіють між собою технічні (автомобілі, дорожня інфраструктура, інженерні споруди), інформаційні (системи збору, передачі та аналізу даних) та екологічні (довкілля, моніторингові системи, екологічні дані) елементи. Розгляд системи «АДС» в такому ключі дозволить виокремити «слабкі місця» кожного з елементів та його компонентів, а також розробити комплексні заходи захисту для кожного з них. Окрім цього це надасть змогу зрозуміти так званий «каскадний ефект» кіберзагроз, коли порушення роботи одного елемента системи може мати серйозні наслідки для інших, включаючи вплив на екологічну безпеку.

У контексті екологічної безпеки кіберзагрози, націлені на систему «АДС», можуть мати шкідливий вплив на складові екосистеми. Так, встановлення датчиків, камер та інших систем моніторингу вздовж автомобільних доріг може створити нові вразливі місця та додаткові цілі для кібератак. Кібератаки можуть пошкодити системи управління дорожнім рухом, спричинити затори та аварії, а також мати негативний економічний та соціальний вплив як на учасників дорожнього руху, так і на навколишнє середовище [9].

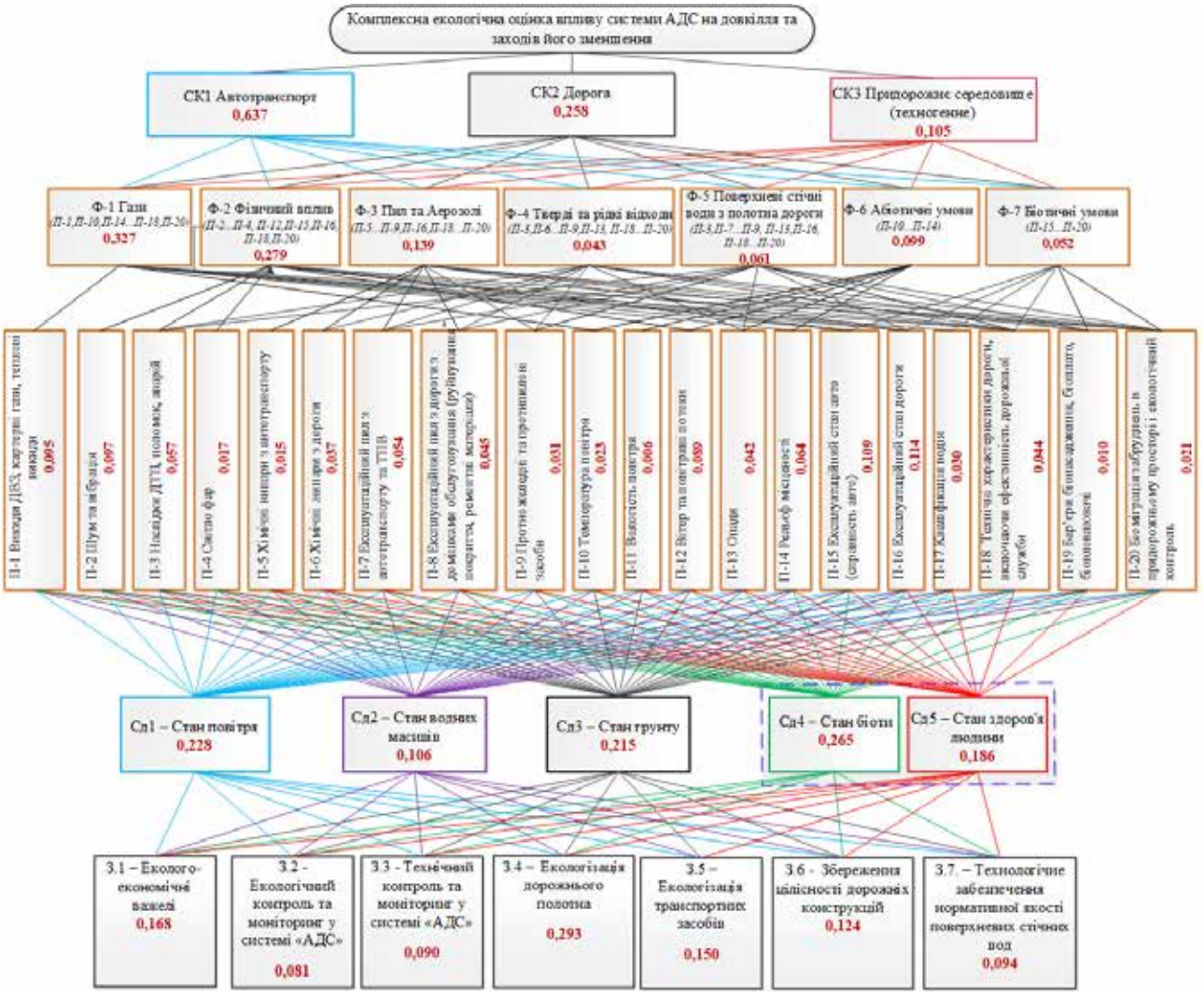

Рис. 1. Ієрархічна структура комплексної оцінки впливу експлуатації автомобільної дороги на довкілля з результатами ЕЕАД [8]

Розподіл кіберзагроз за елементами системи «АДС» дозволить краще зрозуміти, на які елемени та/або їх компоненти слід звернути особливу увагу для забезпечення їх безпеки. Тому, проаналізувавши дослідження, які стосуються питань кібербезпеки, зокрема [1-3, 10, 11], було виділено можливі кіберзагрози і вразливості до кібератак у системі «АДС» та згруповано їх за спрямованістю на кожний з елементів системи (рис. 2).

Нижче наведено перелік деяких наслідків, що можуть бути спричинені переліченими загрозами [2, 10, 11]:

– Збільшення заторів на дорогах і викидів забруднюючих речовин.

– Вплив на енергоефективність і додаткові викиди CO_2.

– Підробка та/або втрата даних моніторингу якості повітря та інших екологічних показників.

– Ускладнення прийняття екологічних рішень.

– Порушення роботи обладнання систем контролю стану НС.

– Негативний вплив на флору та фауну.

– Порушення роботи інфраструктури збереження біорізноманіття.

– Вплив на екологічні параметри через використання даних про транспортні потоки.

– Втрата координації автомобіля та підвищення вірогідності ДТП.

– Ускладнення моніторингу дорожньої ситуації та реагування на екологічні та транспортні аварії.

– Зростання ризику екологічних катастроф.

– Використання даних про екологічний стан НС для маніпуляцій.

– Зміни транспортних маршрутів (збої в навігації), що призведе до збільшення часу в дорозі, споживання палива та викидів ЗР.

Виходячи з вищенаведеної інформації можна зробити висновок, що ризики кіберзагроз є для кожної складової системи «АДС». Саме тому заходи з підвищення екологічної безпеки у системі «АДС» повинні також враховувати кібербезпеку задля запобігання потенційним атакам, які можуть порушити роботу системи і призвести до негативних впливів на довкілля.

Проаналізувавши вітчизняні та закордонні роботи щодо захисту критичної інфраструктури [12-14], було виділено заходи безпеки для підвищення рівня

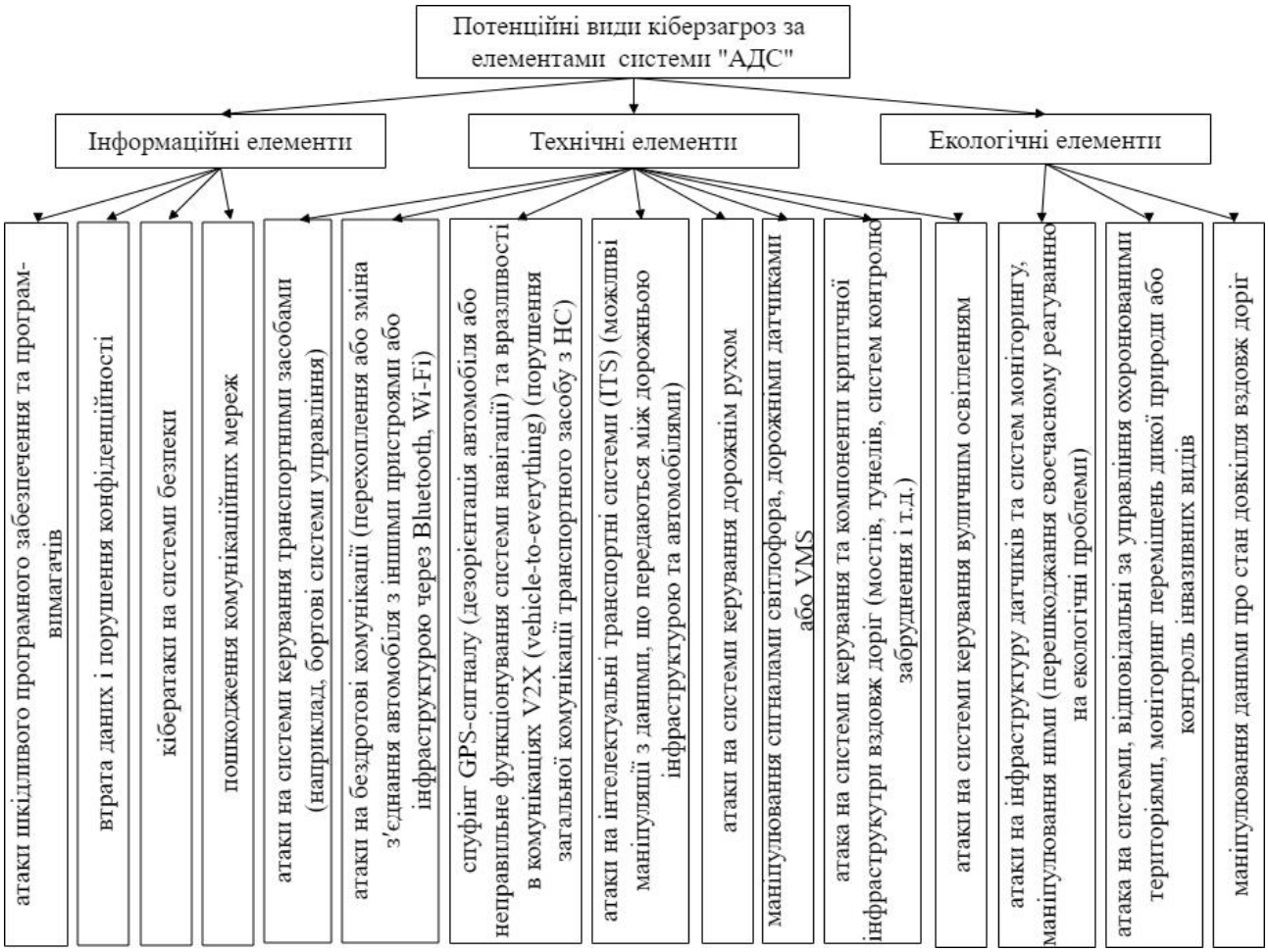

Рис. 2. Потенційні види кіберзагроз в системі «АДС» за спрямуванням на кожний з елементів системи

Джерело: розроблено автором за [1-3, 10, 11]

захисту системи «АДС» та згруповано їх в окремі блоки (Табл. 1). Як видно з таблиці, запропоновані заходи безпеки включають як технічні, так і організаційні рішення, що дозволяють підвищити рівень захисту у системі.

Головні висновки. В сьогоднішніх умовах стрімкого і невпинного росту цифрових технологій важливим є усвідомлення взаємозв'язку між екологічною безпекою та кібербезпекою системи «АДС» та застосування комплексного підходу, що враховує технічні, інформаційні та екологічні аспекти системи.

В роботі визначено можливі кіберзагрози в системі «АДС», зокрема з точки зору їх впливу на екологічну безпеку та надано пропозиції щодо можливих заходів безпеки для підвищення рівня захисту системи.

Підкреслено важливість та необхідність врахування заходів із забезпечення кібербезпеки цифрових систем і мереж під час реалізації заходів із захисту довкілля в системі «АДС». Реалізація таких комплексних заходів сприятиме, зокрема, створенню умов для безпечної та екологічно відповідальної експлуатації автомобільних доріг та всебічного захисту навколишнього природного середовища.

Перспективи використання результатів дослідження. Результати дослідження можуть бути використані:

– для вдосконалення проведення екологічного моніторингу та впровадження комплексних заходів захисту системи «АДС», що включатимуть заходи з кібербезпеки.

– як додаткові матеріали для розробки рекомендацій та нових стандартів з кібербезпеки, для комплексного захисту системи «АДС» та забезпечення екологічної безпеки;

– як інформаційні матеріали при підготовці фахівців з кіберзахисту критичної інфраструктури в системі «АДС».

Таблиця 1

Можливі заходи безпеки для підвищення рівня захисту системи «АДС»

Назва заходу	Шляхи підвищення рівня безпеки захисту системи «АДС»
Посилення кіберзахисту системи	Встановлення систем виявлення та запобігання вторгненням; впровадження системи контролю цілісності (виявлення несанкціонованих змін у програмне забезпечення чи налаштування системи); застосування шифрування даних.
Авторизація та автенти-фікація	Використання механізмів багатофакторної автентифікації (запобігання несанкціонованому доступу до систем керування дорожнім рухом та ін.). Впровадження політики паролів і контролю доступу.
Оновлення та патчі	Виправлення вразливостей у програмному забезпеченні, операційних системах та інших системних компонентах, оцінка та застосування патчів безпеки, тощо.
Сегментація мережі	Поділ мережевої інфраструктури на ізольовані сегменти за допомогою віртуальних приватних мереж.
Навчання персоналу	Проведення навчальних програм з кібербезпеки для співробітників, які працюють в системі «АДС» (підвищення обізнаності про кіберзагрози та методи запобігання). Навчання персоналу розпізнавати та реагувати на підозрілу активність, фішингові атаки або незвичну поведінку системи.
Вдосконалення політик безпеки	Розробка та впровадження політик і процедур, які регулюють використання інформаційних систем для складових системи «АДС».
Резервне копіювання та відновлення	Дотримання протоколів створення резервних копіювання даних (відновлення систем після кібератаки/ інциденту). Тестування ефективності процедур відновлення та розробка планів реагування на інциденти.
Співпраця та обмін інформацією	Участь у національних та міжнародних ініціативах з обміну інформацією про кіберзагрози, вразливості та нові методи захисту. Співпраця між урядовими установами, експертами з кібербезпеки, екологічними організаціями та операторами інфраструктури автомобільних доріг.
Регулярний аудит безпеки	Проведення регулярних аудитів безпеки системи «АДС» (виявлення вразливостей, оцінка ефективності заходів безпеки та визначення шляхів покращення).
Постійний моніторинг і реагування на інциденти	Моніторинг мережевого трафіку, відстеження підозрілої активності, системні журнали та механізми виявлення аномалій. Можливість застосування штучного інтелекту для аналізу великих обсягів даних і виявлення аномалій, які можуть вказувати на кіберзагрози.
Використання інерціальних систем навігації	Використання інерційних систем (у разі атаки на GPS можуть працювати самостійно і видавати точне місцезнаходження). Використання технологій, що можуть виявляти спроби підробити сигнал GPS, запобігати їм, і перемикати на альтернативні джерела даних для навігації.

Література

1. Положий Д. С., Орєхов О. О. Інтелектуальні системи автомобільної безпеки на основі хмарних архітектур. Системи управління навігації та зв'язку Збірник наукових праць 4(74):91-95. DOI:10.26906/SUNZ.2023.4.091
2. Мигаль В.Д. Інтелектуальні системи в технічній експлуатації автомобілів: монографія. Харків: Майдан, 2018. 262 с. URL: https://api.dspace.khadi.kharkov.ua/server/api/core/bitstreams/ecbc039f-13a5-46ac-ac96-6236761e3aec/content
3. Environmental risks: cyber security andcritical industries. An environmental white paper. Environmental Risk Consulting team. URL: https://axaxl.com
4. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398
6. Постанова КМУ від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
7. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки».* 2024. Том 11, № 1(41). С. 314-320. URL:https://doi.org/10.23939/law2024.41.314
8. Адамова Г.В. Можливості еколого-експертно-аналітичних досліджень системи «АДС». Екологічні науки : науково-практичний журнал 2024. – № 2(53). С. 16-22. URL: https://doi.org/10.32846/2306-9716/2024.eco.2-53.2
9. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. *Державне управління: удосконалення та розвиток*. 2022. № 1. – URL: http://www.dy.nayka.com.ua/?op=1&z=2610
10. What is Environmental Risk in Cyber Security? [Електронний ресурс]. – https://cyberinsight.co/what-is-environmental-in-cyber-security/
11. Safeguarding the environment: Cybersecurity in environmental protection URL: https://cybersecurityguide.org/industries/environmental-protection/
12. Road infrastructure operational technology cyber security primer. Prepared by Transport Canada. 2022. URL: https://tc.canada.ca/sites/default/files/2022-12/Road_Infrastructure_Operational_Technology_Cyber_Security_Primer-ENG.pdf
13. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.
14. Safeguarding Critical Infrastructure In The Transportation Sector. URL: https://www.forbes.com/councils/forbestechcouncil/2024/02/02/safeguarding-critical-infrastructure-in-the-transportation-sector/