Міжнародна науково-практична конференція

«Актуальні проблеми та інноваційні технології у сфері гуманітарного розмінування, цивільного захисту, критичної інфраструктури та екологічної безпеки для повоєнного відновлення України»

7 - 8 листопада 2024 року

Науково-дослідна установа
“Український науково-дослідний інститут екологічних проблем”

КІБЕРБЕЗПЕКА ЯК КОМПЛЕКС СКЛАДОВИХ У ЗАХОДАХ ЗАХИСТУ В СИСТЕМІ «АВТОМОБІЛЬ-ДОРОГА-СЕРЕДОВИЩЕ»

Доповідачі:
Адамова Ганна Вячеславівна
Пісня Леонід Андрійович, *канд.техн. наук*

2024

У зв’язку з російською військовою агресією постало вкрай важливе питання щодо всебічного захисту критичної інфраструктури нашої країни.

Транспортне забезпечення належить до життєво важливих послуг, порушення яких призводить до негативних наслідків для національної безпеки України

Відповідно до Закону України «Про критичну інфраструктуру» від 16.11.2021 р. (із змінами, внесеними згідно із Законом № 2684-IX від 18.10.2022 р.) .

Актуальність дослідження

- 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).
- Водночас, 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.

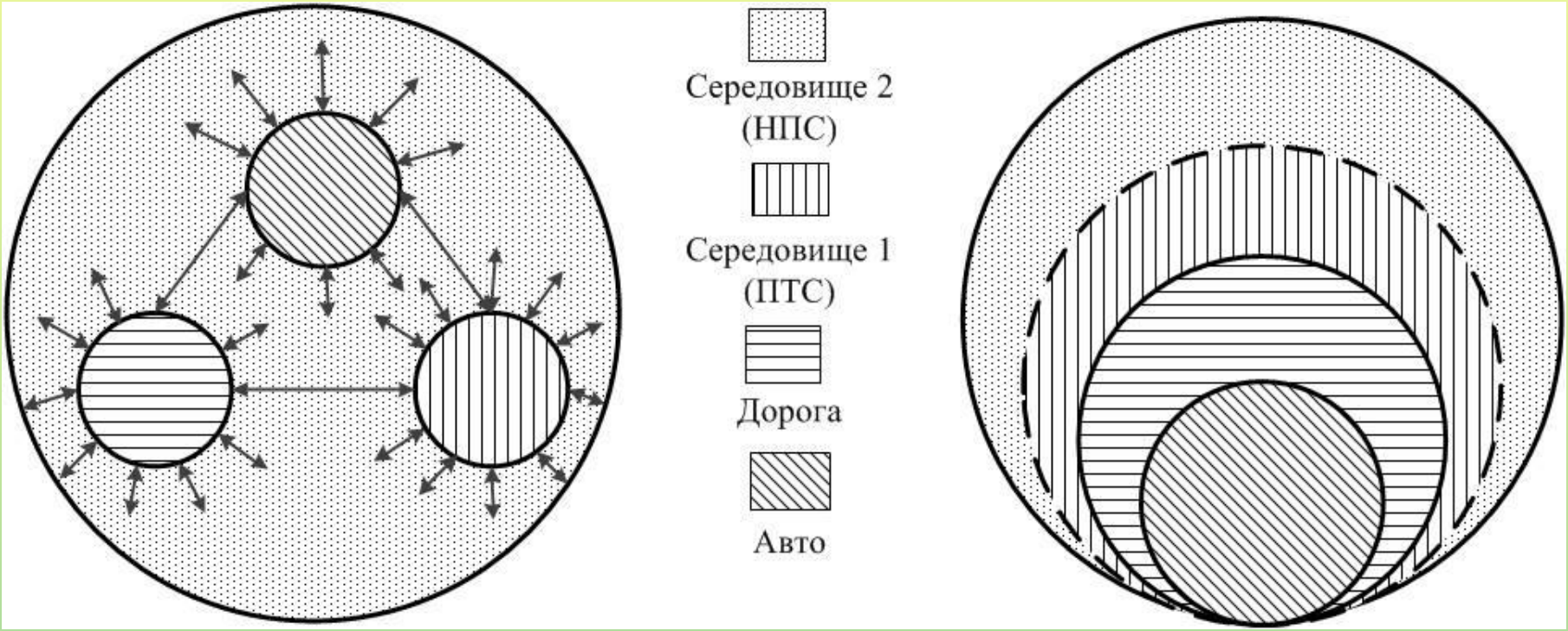
Актуальність дослідження

Кібератаки як елементів так і всієї системи можуть мати суттєві наслідки для життєзабезпечення густонаселених територій, зокрема:

- *порушення роботи управління транспортними системами,*
- *збої руху вантажів та траспортних потоків,*
- *небезпеку для життя людей учасників руху,*
- *збої та втрати даних у моніторингових системах екологічної безпеки.*

- **Мета:** Визначити та дослідити можливі заходи та шляхи підвищення рівня кібербезпеки для системи «АДС», як комплексу складових інтегрованих завдяки системному підходу до забезпечення безпеки всіх комплексних елементів системи "автомобіль-дорога-середовище".

ГРАФІЧНЕ ПОДАННЯ ІСНУЮЧОГО ТА НОВОГО ПІДХОДІВ ДО ОЦІНЮВАННЯ ВПЛИВУ АДС НА ДОВКІЛЛЯ

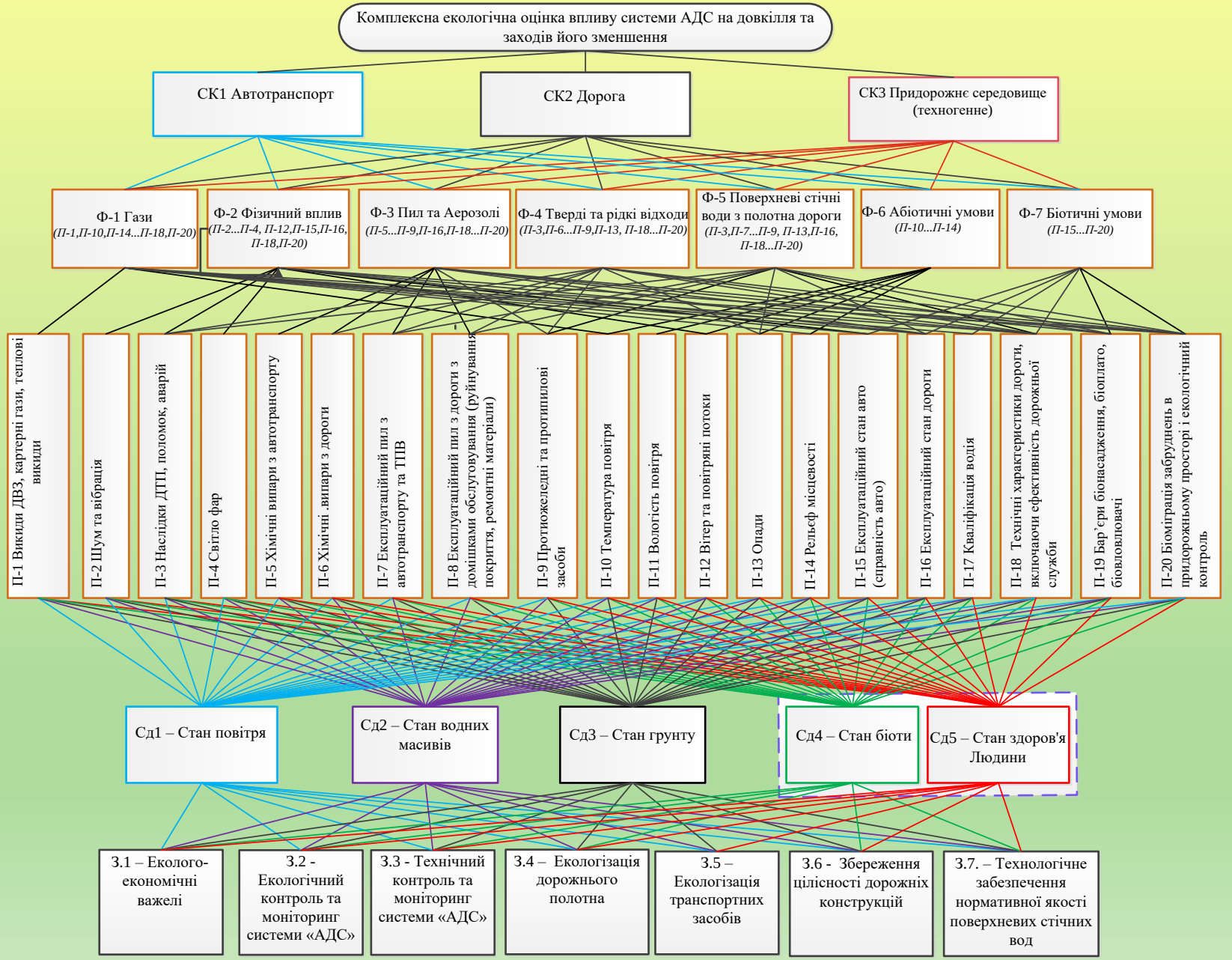


а) існуючий підхід

б) запропонований підхід

*НПС – навколишнє природне середовище
**ПТС – природно-техногенне середовище

ІЄРАРХІЧНА СТРУКТУРА ОЦІНЮВАННЯ КОМПЛЕКСНОГО ВПЛИВУ СИСТЕМИ АДС НА ОБ'ЄКТИ НПС З УРАХУВАННЯ ЗАХОДІВ ПРОТИДІЇ



Вибрана ділянка дороги, що наглядно характеризує максимально-можливий вплив в процесі експлуатації М-29 (20 – 22 км)

Умовні позначення:

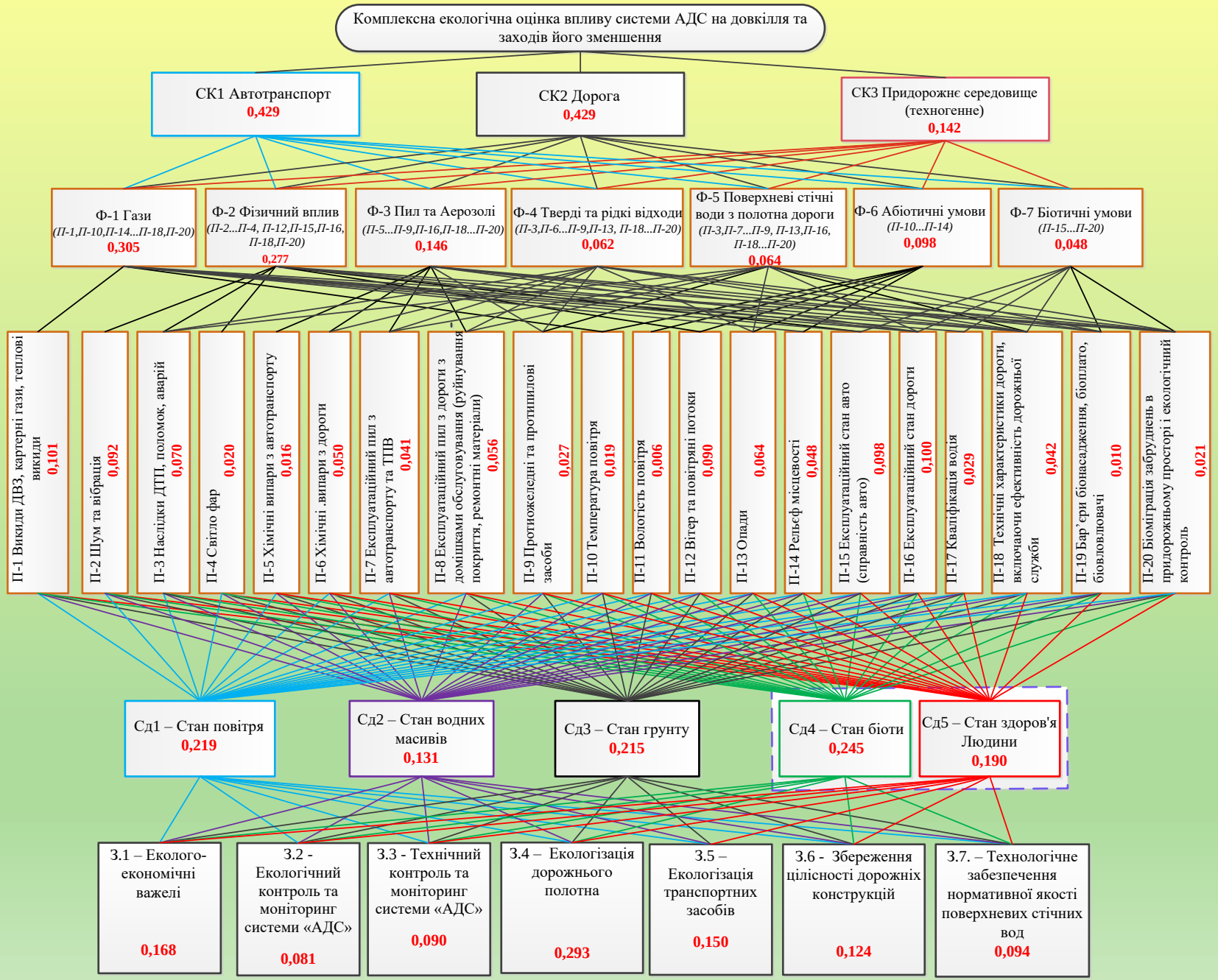
1:5 – точки прямих вимірів стану атмосферного повітря;
1:3,5 – точки відбору проб ґрунту та рослинності;
6 – точка відбору контрольних проб рослинності та ґрунту.

Технічна характеристика дороги:

Тип дороги – магістральна а/д;
Тип покриття – асфальт;
Ширина земляного полотна – 26,5 м.;
Ширина проїзної частини – 16 м (4 смуги руху);
Ширина центральної розділової смуги – 8 м.;
Ширина смуги для зупинки – 2,5 м.;
Інтенсивність руху: 2 680 авт./добу;
Середня швидкість руху – 110 км/год;

Склад руху (Р, %):
легкі вантажні автомобілі (до 2,5 т) - 21,6 %,
середні вантажні автомобілі (до 5 т) - 13,4 %,
важкі вантажні автомобілі (більше 8 т) - 6,0%,
мікроавтобуси - 17,2 %,
автобуси - 1,5 %,
легкові автомобілі - 40,3 %.

ІЄРАРХІЧНА СТРУКТУРА КОМПЛЕКСНОГО ВПЛИВУ СИСТЕМИ «АДС» НА ДОВКІЛЛЯ ТА ЗАХОДИ ЩОДО ЙОГО ЗНИЖЕННЯ (з результатами еколого-аналітичної оцінки)



КІБЕРЗАГРОЗИ В СИСТЕМІ АДС

Потенційні види кіберзагроз

- Кібератаки на системи безпеки
- Атаки на бездротові комунікації
- Атаки на інтелектуальні транспортні системи (ITS)
- Атаки на системи керування та компоненти критичної інфраструктури вздовж магістралей
- Атаки на системи керування вуличним освітленням
- Атаки на інфраструктуру датчиків та систем моніторингу, маніпулювання ними
- Пошкодження комунікаційних мереж
- Атака на системи, відповідальні за управління охоронюваними територіями, моніторинг переміщень дикої природи або контроль інвазивних видів
- Маніпулювання даними про стан навколишнього середовища вздовж доріг
- Атаки на системи керування дорожнім рухом
- Маніпулювання сигналами світлофора, дорожніми датчиками або системами VMS
- Атаки на системи керування транспортними засобами
- Спуфінг GPS-сигналу та вразливості в комунікаціях V2X
- Втрата даних і порушення конфіденційності
- Атаки шкідливого програмного забезпечення та програм-вимагачів

МОЖЛИВІ НАСЛІДКИ КІБЕРАТАК НА СИСТЕМУ «АДС»

Затори та збільшення викидів шкідливих речовин

Аварії та екологічні наслідки через неконтрольоване пересування транспорту

Ускладнення прийняття екологічних рішень

Зупинка або зміна роботи сенсорів та обладнання

Негативний вплив на місцеву фауну та флору

Вплив на екологічні параметри

Збої в системах звязку, втрата координації та підвищення аварійності

Збої руху вантажів та траспортних потоків

Влив на безпеку руху та енергоефективність

Порушення роботи управління транспортними системами

Збої та втрати даних у моніторингових системах екологічної безпеки

Вплив на екологічні ініціативи щодо переходу на екологічно чистий транспорт

Небезпеку для життя людей та учасників руху

Ускладненн/порушення моніторингу дорожньої ситуації

Маніпуляції у системах збору і відведення стічних вод

Перешкоди евакуації або мобілізації аварійних служб

Спотворення/прихування реальної екологічної ситуації

ЗАХОДИ ТА ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ КІБЕРЗАХИСТУ ДЛЯ СИСТЕМИ «АДС»

НАЗВА ЗАХОДУ	ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ЗАХИСТУ СИСТЕМИ «АДС»
Посилення кіберзахисту системи	Встановлення та регулярне оновлення брандмауерів, систем виявлення вторгнень та систем запобігання вторгненням. Впровадження системи контролю цілісності для виявлення внесення несанкціонованих змін у програмне забезпечення чи налаштування системи. Застосування шифрування даних при їх передачі через мережу для захисту від перехоплення та несанкціонованого доступу до конфіденційної інформації.
Авторизація та автентифікація	Використання механізмів багатофакторної автентифікації для запобігання несанкціонованому доступу до систем керування дорожнім рухом та іншими критичними компонентами. Реалізація суворих політик паролів та управління доступом, включаючи багатофакторну автентифікацію та регулярне оновлення паролів.
Оновлення та патчі	Регулярне оновлення програмного забезпечення, операційних систем, прошивки та інших компонентів системи для виправлення вразливостей. Оцінка та застосування патчів безпеки для оновлення вразливих компонентів системи..
Сегментація мережі	Поділ мережевої інфраструктури на ізольовані сегменти за допомогою віртуальних приватних мереж (VPN), VLAN або мережевих фільтрів. Це допомагає запобігти розповсюдженню атаки по всій мережі.

ЗАХОДИ ТА ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ КІБЕРЗАХИСТУ ДЛЯ СИСТЕМИ «АДС»

НАЗВА ЗАХОДУ	ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ЗАХИСТУ СИСТЕМИ «АДС»
Регулярний аудит безпеки	Проведення регулярних аудитів безпеки системи «АДС» для виявлення вразливостей, оцінки ефективності заходів безпеки та визначення шляхів для покращення.
Постійний моніторинг і реагування на інциденти	Безперервний моніторинг і оперативне реагування на інциденти у системі магістралей дозволять вчасно виявити та пом'якшити кіберзагрози (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 свідчити про кіберзагрози
Загально-національний чи колективний підхід	Співпраця між урядовими установами, експертами з кібербезпеки, екологічними організаціями та операторами інфраструктури на магістралях. Обмін інформацією, передовим досвідом і проведення спільних навчань можуть підвищити готовність і можливості реагування.
Використання інерціальних систем навігації	Інерціальні системи можуть працювати незалежно від GPS і забезпечувати точне позиціонування навіть у випадку атаки на GPS. Використання технологій, що можуть виявляти спроби спуфінгу (підробки) сигналу GPS, і переключення на альтернативні джерела даних для навігації та запобігання GPS-спуфінгу/GPS-спуфінг детекції.

ЗАХОДИ ТА ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ КІБЕРЗАХИСТУ ДЛЯ СИСТЕМИ «АДС»

НАЗВА ЗАХОДУ	ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ЗАХИСТУ СИСТЕМИ «АДС»
Навчання персоналу	Проведення навчальних програм з кібербезпеки для співробітників, які працюють в системі «АДС», для підвищення обізнаності про кіберзагрози та методи запобігання. Навчання персоналу розпізнавати та реагувати на підозрілу активність, фішингові атаки чи незвичайну поведінку системи.
Вдосконалення політик безпеки	Розробити та впровадити політики та процедури, що регулюють необхідність використання інформаційних систем для авто та складових системи «АДС».
Резервне копіювання та відновлення	Дотримання протоколів створення резервних копій даних для забезпечення можливості відновлення систем після кібератаки чи інцидентів. Тестування ефективності процедур відновлення та розроблених планів реагування на інциденти.
Співпраця та обмін інформацією	Участь у загальнонаціональних та міжнародних ініціативах щодо обміну інформацією про кіберзагрози, вразливості та нові методи захисту. Співпраця з правоохоронними та органами кібербезпеки для аналізу виявлення та розслідування кібератак.

ВИСНОВКИ

- Аналіз публікацій дозволив визначити основні кіберзагрози та вразливості в системі "автомобіль-дорога-середовище" (АДС) та запропонувати можливі заходи безпеки для підвищення рівня захисту.
- Встановлено, що ризики кіберзагроз стосуються кожної складової системи «АДС», що вимагає комплексного підходу до розробки заходів кібербезпеки. Тобто, заходи повинні охоплювати як автомобільні системи, так і дорожню інфраструктуру, а також враховувати вплив на зовнішнє середовище, забезпечуючи надійний захист від потенційних загроз.
- Визначено доцільність та нагальність інтегрувати заходи кібербезпеки в системи управління та моніторингу екологічних показників з метою запобігання загрозам та забезпечення більш надійний захист системи АДС та довкілля.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. 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

3. Мигаль В.Д. Інтелектуальні системи в технічній експлуатації автомобілів: монографія. Харків: Майдан, 2018.262 с. URL: http://surl.li/vfatxk

4. Adamova G.V., Pisnya L.A. Environmental safety of operation of motor roads of Ukraine. Assessment methods and tools and cyber security. Challenges and threats to critical infrastructure. Collective monograph – NGO Institute for Cyberspace Research (Detroit, Michigan, USA), 2023. P. 284–302. URL: http://surl.li/mhuka. ISBN-10/979-8-218-22315-1 (дата звернення: 01.11.2024).

5. Адамова Г.В. Комплексне еколого-аналітичне оцінювання впливу системи «АДС» на складники довкілля в процедурі ОВД. / Вісник Харківського національного автомобільно-дорожнього університету, Т.1, №102, – 2023.
С. 37-47. DOI: https://doi.org/10.30977/BUL.2219-5548.2023.102.1.37

6. Комп'ютерна програма «PROGRAM OF ANALYTICAL SYSTEM OF STRATEGIC ENVIRONMENTAL ASSESSMENT. ANALYTIC HIERARCHY/NETWORK PROCESS» / Л.А. Пісня, Л.Я. Аніщенко, Б.С. Свердлов, С.Б. Свердлов. Номер свідоцтва про реєстрацію авторського права на твір: 121616, Дата реєстрації авторського права: 06.12.2023, Об'єкт авторського права, до якого належить твір: 16. Комп'ютерні програми, Дата публікації: 29.12.2023, Номер бюлетеня: 78. https://ukrpatent.org/uk/articles/bulletin-copyright.

7. Автомобільна кібербезпека: нові обов'язкові правила з липня 2024 року. – [Електронний ресурс]. – URL: http://surl.li/vsfbwr

8. Road infrastructure operational technology cyber security primer. Prepared by Transport Canada. 2022. URL: http://surl.li/qjiupp

9. 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. URL: http://surl.li/snddyj

10. 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 DOI: 10.32702/2307-2156-2022.1.38

11. Transportation sector report cyber security for road, rail, air, and sea. ECSO Publications, WG 3. 2020. URL: https://ecs-org.eu/ecso-uploads/2022/10/5fdb2791553ac.pdf

12. Safeguarding Critical Infrastructure In The Transportation Sector. [Електронний ресурс]. – URL: http://surl.li/dbsgey


ДЯКУЮ ЗА УВАГУ !