контурі управління доставкою запасних частин. Основне положення підходу полягає у розділенні зміни логістичного профілю центру й тимчасової втрати довіри до його даних. Це створює основу для вибору технології доставки та переходу до резервного режиму за цифрових порушень. Подальша робота передбачає параметризацію моделі на даних реальної мережі та сценарну оцінку її результативності.

Список використаних джерел

1. Teunter R. H., Syntetos A. A., Babai M. Z. Intermittent demand: Linking forecasting to inventory obsolescence. European Journal of Operational Research. 2011. Vol. 214, no. 3. P. 606–615. DOI: https://doi.org/10.1016/j.ejor.2011.05.018.
2. Jain A. K. Data clustering: 50 years beyond K-means. Pattern Recognition Letters. 2010. Vol. 31, no. 8. P. 651–666. DOI: https://doi.org/10.1016/j.patrec.2009.09.011.
3. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : National Institute of Standards and Technology, 2024. NIST CSWP 29. DOI: https://doi.org/10.6028/NIST.CSWP.29.

УДК 004.056:004.89:656.05

Гавриленко Аліна Олександрівна,

здобувачка 2 курсу магістратури Харківського національного автомобільно-дорожнього університету

КІБЕРЗАХИСТ ІНФОРМАЦІЇ В ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМАХ

Анотація. У роботі розглянуто питання кіберзахисту інформації в інтелектуальних транспортних системах в умовах цифровізації транспортної галузі. Визначено основні кіберзагрози, пов’язані з використанням інтернету речей, бездротових мереж і взаємопов’язаних інформаційних систем. Розглянуто багаторівневий підхід до захисту інформації, застосування методів автентифікації, шифрування та виявлення аномалій. Особливу увагу приділено використанню математичних моделей для оцінювання ризиків кібератак і своєчасного реагування на потенційні загрози. Обґрунтовано важливість комплексного підходу до забезпечення кібербезпеки для підвищення надійності та стійкості інтелектуальних транспортних систем.

Ключові слова: інтелектуальні транспортні системи, кібербезпека, кіберзахист

інформації, кіберзагрози, DDoS-атаки, машинне навчання, виявлення аномалій, оцінювання ризиків.

Інтелектуальні транспортні системи (ІТС) є складними кіберфізичними системами, у яких взаємодіють транспортні засоби, дорожня інфраструктура, датчики, засоби зв'язку, обчислювальні платформи та центри керування. Архітектура ІТС охоплює фізичний, комунікаційний та обчислювальний рівні, а також рівні аналітичного опрацювання інформації, управління й інтеграції. Фізичний рівень включає дорожні датчики, світлофори, відеокамери та інші пристрої збирання даних. Комунікаційний рівень забезпечує передавання інформації за допомогою бездротових мереж, технологій 5G і V2X, а обчислювальний рівень відповідає за опрацювання даних, прогнозування транспортних потоків та виконання алгоритмів штучного інтелекту [1].

Розвиток інтелектуальних транспортних систем спрямований не лише на автоматизацію управління рухом, а й на підвищення безпеки, комфорту та екологічності перевезень. Збирання й аналіз даних про транспортні потоки, дорожні умови та місцезнаходження транспортних засобів дають змогу прогнозувати час прибуття, планувати оптимальні маршрути, виявляти затори й оперативно інформувати учасників руху. Водночас ефективність таких рішень залежить від узгодженої роботи датчиків, мереж зв'язку, аналітичних систем і належного захисту даних [3].

Взаємозалежність складових ІТС означає, що порушення роботи одного компонента може вплинути на функціонування інших елементів системи. Зокрема, втручання в роботу датчиків або комунікаційних мереж може призвести до отримання недостовірної інформації, помилкових управлінських рішень і порушення регулювання транспортних потоків. Тому кіберзахист має охоплювати не лише окремі пристрої, а й усю інфраструктуру обміну, зберігання та обробки даних.

Окремої уваги потребує кібербезпека автомобільного транспорту,

оскільки сучасні транспортні засоби використовують програмне забезпечення, мережеві інтерфейси та системи геолокації. Уразливості таких компонентів можуть створювати ризики несанкціонованого доступу, витоку персональних даних або втручання в роботу важливих систем автомобіля. Тому захист має охоплювати як програмні засоби – криптографічні алгоритми, захищені протоколи передавання даних і системи виявлення вторгнень, – так і апаратні компоненти транспортного засобу [4].

Серед основних кіберзагроз для ІТС можна виокремити несанкціонований доступ до мережі, розподілені атаки типу «відмова в обслуговуванні» (DDoS), упровадження шкідливого програмного забезпечення, перехоплення або зміну інформації, а також використання вразливостей підключених пристроїв. Збільшення кількості пристроїв IoT розширює потенційні шляхи проникнення зловмисників. Додатковими проблемами є відсутність регулярного оновлення програмного забезпечення на окремих пристроях і недостатня узгодженість стандартів кіберзахисту різних виробників [1, 2].

Окремим викликом є опрацювання великих обсягів даних у реальному часі. Інтелектуальні транспортні системи повинні швидко аналізувати інформацію від датчиків, транспортних засобів і засобів відеоспостереження, водночас забезпечуючи її конфіденційність та цілісність. Використання складних криптографічних механізмів потребує обчислювальних ресурсів, тому під час розроблення засобів захисту необхідно враховувати баланс між безпекою та швидкістю обробки інформації.

Важливим напрямом кіберзахисту є застосування автентифікації, шифрування та контролю цілісності даних. Автентифікація дає змогу перевірити справжність користувачів і пристроїв, а шифрування захищає інформацію від прочитання сторонніми особами. Для обміну

повідомленнями між транспортними засобами та інфраструктурою можуть використовуватися цифрові підписи, сертифікати й інфраструктура відкритих ключів (PKI). Такі засоби допомагають перевіряти походження повідомлень і знижувати ризик підміни даних [1].

Крім криптографічних механізмів, необхідно застосовувати багаторівневий захист. Він передбачає фізичне обмеження доступу до обладнання, використання міжмережевих екранів і VPN, захист каналів зв'язку, контроль доступу до інформації, регулярне оновлення програмного забезпечення та системи виявлення вторгнень (IDS). Важливе значення має моніторинг мережевого трафіку, який дає змогу своєчасно виявляти підозрілу активність і реагувати на можливі атаки [1, 2].

Перспективним підходом до підвищення рівня кібербезпеки є використання математичних моделей оцінювання ризиків. Для моделювання ймовірності кібератак у часі можуть застосовуватися експоненціальний розподіл і розподіл Вейбулла. Експоненціальна модель описує ситуації, у яких інтенсивність атак вважається сталою, тоді як модель Вейбулла дає змогу враховувати її зміну. Накопичення вразливостей без належного оновлення системи може відповідати сценарію зростання ризику, а впровадження регулярних оновлень і додаткових засобів захисту – сценарію його зниження [2].

Для виявлення аномалій у мережевому трафіку можуть використовуватися алгоритми машинного навчання та теорема Байєса. Аналіз таких характеристик, як обсяг переданих даних, час відповіді системи й частота запитів від пристроїв, дає змогу визначати відхилення від звичайного режиму роботи. Наприклад, різке збільшення кількості запитів або затримок у передаванні інформації може свідчити про перевантаження мережі, технічну несправність або потенційну кібератаку. Результати оцінювання можуть використовуватися для блокування підозрілого трафіку, додаткової перевірки мережі та повідомлення операторів [2].

Поєднання моніторингу, математичного оцінювання ризиків і автоматизованого реагування дає змогу створювати адаптивні системи захисту. Водночас ефективність таких рішень залежить від якості вихідних даних, актуальності програмного забезпечення, узгодженості протоколів безпеки та постійного контролю стану транспортної інфраструктури.

Висновки. Кіберзахист інформації є необхідною умовою надійного функціонування інтелектуальних транспортних систем. Основними викликами є збільшення кількості підключених пристроїв, уразливість мережевої інфраструктури, DDoS-атаки, несанкціонований доступ і потреба в оперативному опрацюванні великих обсягів даних. Для протидії цим загрозам доцільно поєднувати шифрування, автентифікацію, контроль доступу, регулярне оновлення програмного забезпечення, системи виявлення вторгнень і моніторинг мережевого трафіку. Додаткові можливості забезпечують математичні моделі оцінювання ймовірності атак та алгоритми машинного навчання для виявлення аномалій. Комплексне застосування цих методів сприяє своєчасному виявленню загроз, підвищенню стійкості ІТС і зменшенню ризиків для транспортної інфраструктури та її користувачів.

Список використаних джерел

1. Mashkina I., Rzaieva S., Kostiuk Y., Mazur N., Brzhevska Z. Cybersecurity in Intelligent Transport Systems: Current Challenges and Solutions. *Cybersecurity Providing in Information and Telecommunication Systems*. 2025. P. 14. URL: https://elibrary.kubg.edu.ua/id/eprint/52531/1/I_Mashkina_S_Rzaieva_Y_Kostiuk_N_Mazur_Z_Brzhevska_CIPTS_2025_3991.pdf.
2. Доля К. В. Основи кібербезпеки та надійності автомобільного транспорту в інтелектуальних транспортних системах : монографія. Харків. 2026. 224 с. DOI: https://doi.org/10.46299/979-8-90553-923-7.
3. Клюєв С. О., Цимбал С. В., Сігонін А. Є. Розвиток інтелектуальних транспортних систем. Вісник машинобудування та транспорту. 2023. № 2(18). С. 80–86. DOI: https://doi.org/10.31649/2413-4503-2023-18-2-80-86.
4. Світличний В. А. Кібербезпека в автомобільному транспорті: виклики та стратегії захисту. Безпека у кіберсфері. Харків, 2025. С. 182–184.