УДК 004.032+342.951+656.2

С. О. Євдокимов

МОДЕЛЮВАННЯ ЗАГРОЗ І РОЗРОБКА СТРАТЕГІЙ БЕЗПЕКИ ДЛЯ ЗАХИСТУ ЗАЛІЗНИЧНИХ МЕРЕЖ I_OT

У статті досліджуються вразливості та загрози в залізничних мережах IoT (Інтернет речей), які відіграють ключову роль у забезпеченні кібербезпеки в кіберфізичних системах. Залізничні мережі IoT, що складаються з взаємопов'язаних пристроїв, таких як датчики, виконавчі механізми, комунікаційні вузли, хмарні системи та системи керування, забезпечують моніторинг і контроль операцій у реальному часі. Підвищуючи операційну ефективність і безпеку, інтеграція IoT також створює виклики кібербезпеці, включаючи порушення даних, несанкціонований доступ, збої в системі та потенційні ризики для безпеки пасажирів та інфраструктури.

Дослідження висвітлює ключові вразливості в залізничних мережах IoT. Датчики, які відстежують стан колії, швидкість і фактори навколишнього середовища, схильні до відхилень, якщо вони не закріплені належним чином. Приводи, відповідальні за команди керування, можуть невірно відображати дії, що призведе до системних збоїв. Комунікаційні пристрої, такі як маршрутизатори та комутатори, є критичними точками збою, особливо якщо вони неправильно налаштовані або оновлені. Ресурси та системи наглядового контролю, які обробляють конфіденційні дані, також піддаються ризику несанкціонованого доступу та кібервторгнення.

Для захисту від нових загроз наголошується на постійному моніторингу та регулярній оцінці вразливості. Системи виявлення аномалій на основі штучного інтелекту та машинного навчання особливо ефективні для раннього виявлення загроз і проактивного пом'якшення, тоді як адаптивні захисні механізми, що самовідновлюються, підвищують стійкість до нових кіберзагроз.

У статті наголошується на співпраці між транспортними операторами, експертами з кібербезпеки та регуляторами для встановлення єдиних стандартів і скоординованих стратегій. Щоб підвищити безпеку Інтернету речей на залізниці, рекомендовано нормативно-правові рамки для окремих галузей, що передбачають сучасні технології безпеки та гібридні моделі, що поєднують традиційний захист та захист на основі штучного інтелекту. Ці рекомендації спрямовані на забезпечення безпеки пасажирів та захисту від фінансової та репутаційної шкоди. Результати дослідження сприяють вдосконаленню стратегій кібербезпеки для залізничних мереж IoT, сприяючи стійкості до мінливого середовища загроз.

Ключові слова: *кіберфізичні системи, кібербезпека, IoT-пристрій, машинне навчання, залізничні мережі, критична інфраструктура.*

Вступ та постановка проблеми

Залізничний транспорт є критично важливою складовою інфраструктури сучасного суспільства, що забезпечує ефективні та безпечні перевезення пасажирів і вантажів. З впровадженням технологій Інтернету речей (IoT) у цій галузі існує потенціал для значного покращення ефективності, моніторингу та управління залізничними системами. Однак разом із цими перевагами з'являються нові загрози кібербезпеці.

Аналіз останніх досліджень і публікацій

Існує значна кількість літератури, присвяченої вразливостям і загрозам, пов'язаним із залізничними мережами IoT, що відображає критичну важливість кібербезпеки в цій галузі. Наприклад, Чжу, Рігер і Басар досліджують фундаментальні питання безпеки в кіберфізичних системах, наголошуючи на унікальних проблемах, пов'язаних з інтеграцією фізичних і цифрових компонентів. Вони підкреслюють, як взаємопов'язані пристрої в

залізничних мережах можуть стати точками входу для кібератак, що потенційно може призвести до значних збоїв у роботі та загроз безпеці. Ще один важливий внесок зробили Ван, Сю та Ханна (2018), які досліджують використання методів машинного навчання для підвищення безпеки систем Інтернету речей. Їх дослідження демонструє, як алгоритми виявлення аномалій можуть ідентифікувати незвичайні шаблони в мережевому трафіку, що може вказувати на кібератаку. Проте, незважаючи на значні наукові досягнення в цій сфері, залишаються певні прогалини, що потребують додаткового дослідження та розвитку. Одним із найбільших викликів залізничних мереж IoT є висока мобільність їхніх компонентів, що ускладнює захист від атак, особливо у випадку, коли пристрої переміщуються в різні зони з різними рівнями безпеки. Іншим важливим аспектом є критичний характер зв'язку в реальному часі, що ставить додаткові вимоги до забезпечення безперервної роботи систем навіть у разі кібератак.

У звіті Міжнародної асоціації залізничної безпеки (IRSA) «Regional Development in The Era of Globalization» (2017) зазначається, що впровадження адаптивних систем захисту є ключовим фактором для підвищення стійкості транспортної інфраструктури. Агентство з кібербезпеки та безпеки інфраструктури (CISA) у своєму звіті «Cybersecurity Best Practices» (2019) наголошує на необхідності інтеграції нових заходів безпеки в наявні системи управління залізницею, щоб уникнути технічних конфліктів і забезпечити сумісність із поточними стандартами безпеки.

Протягом останніх років кіберзагрози для залізничних мереж IoT стали серйозною проблемою. У 2021 році німецька компанія Deutsche Bahn зазнала кібератаки, які спричинили перебої в роботі системи продажу квитків та інформаційних табло на станціях. Атака була здійснена через вразливості в IoT-пристроях, що використовуються для моніторингу та управління операціями. У 2022 році в Австралії було зафіксовано маніпуляцію з даними про швидкість поїздів, що призвело до порушень безпеки руху, завдяки уразливостям в сенсорних мережах IoT. 2023 року в Україні було зафіксовано 1105 кіберінцидентів, що на 62,5 % більше порівняно з попереднім роком, що свідчить про зростаючі кіберзагрози для критичної інфраструктури, зокрема залізничних мереж.

Вищевказані інциденти чітко демонструють серйозні загрози для безпеки залізничних мереж IoT та підкреслюють необхідність розробки ефективніших методів протидії кібератакам у цьому критичному секторі транспорту.

Підсумовуючи, хоча нещодавні дослідження забезпечують міцну основу для розуміння вразливостей і потенційних рішень безпеки для залізничних мереж IoT, залишаються прогалини у вирішенні проблем, унікальних для цього сектору. До них відносяться висока мобільність мережевих компонентів, критичний характер зв'язку в реальному часі та потреба в регуляторних структурах для окремих галузей [1].

Метою статті є дослідження методів виявлення та пом'якшення загроз для залізничних мереж IoT шляхом тестування різних стратегій захисту та оцінки їх ефективності в умовах кіберзагроз.

Для досягнення поставленої мети в статті висуваються наступні завдання:

1. Перегляньте потенційні загрози, які можуть використовувати ці вразливості, зокрема порушення даних, системні збої та фізичний вплив на інфраструктуру та безпеку пасажирів.

2. Оцініть поточні рішення безпеки, такі як шифрування даних, автентифікація пристроїв, моніторинг мережевого трафіку та політики безпеки, шляхом оцінки їх ефективності в контексті залізничних мереж IoT.

Методологія дослідження включає тестування заходів безпеки, моделювання кібератак та оцінку ефективності запропонованих рішень. Для кожного експерименту використовуються топології мережі з різними конфігураціями пристроїв (сенсори, маршрутизатори, виконавчі механізми) та протоколами (TCP/IP, MQTT, HTTP). Тестування включає 50 повторів на кожному сценарії, де оцінюються такі параметри, моніторинг

трафіку, виявлення аномалій за допомогою алгоритмів машинного навчання та моделювання потенційних атак. Критерії оцінки: зменшення кількості успішних атак (рівень нейтралізації атак), час затримки при передачі зашифрованих даних, точність виявлення аномалій, час відновлення після атаки та рівень зниження ризику компрометації.

Виявлення вразливостей в залізничних мережах IoT

Залізничні мережі IoT, які об'єднують різноманітні пов'язані пристрої для управління та моніторингу залізничної інфраструктури, є критично важливим компонентом сучасних транспортних систем [2]. Вони забезпечують ефективність і безпеку роботи залізниці, але також створюють потенційну вразливість до кіберзагроз. Залізничні мережі IoT складаються з численних датчиків, пристроїв керування, мережевих з'єднань і обчислювальних ресурсів, які взаємодіють для моніторингу та управління фізичною інфраструктурою залізниць. Однак така інтеграція технологій створює нові виклики кібербезпеці. Зловмисники можуть отримати доступ до конфіденційних даних, що передаються між пристроями. Атаки можуть призвести до системних збоїв, що впливає на координацію та ефективність залізничних перевезень. Атаки на критичні компоненти можуть мати серйозні наслідки для інфраструктури та пасажирів, у тому числі потенційні аварії.

Залізничні системи IoT використовують різні мережеві компоненти, такі як маршрутизатори, комутатори, точки доступу та шлюзи. Наприклад, якщо мережеві маршрутизатори або комутатори мають вразливі місця у мікропрограмі або конфігураціях, зловмисники можуть отримати несанкціонований доступ до мережі та її компонентів. Це може дозволити їм перехоплювати або змінювати дані, що передаються через мережу. Наприклад, відсутність належного шифрування трафіку або слабкі паролі можуть бути використані для компрометації системи.

Датчики, які використовуються в залізничних системах IoT (наприклад, для моніторингу стану колії або швидкості поїздів), також можуть бути вразливими до атак. Неналежна автентифікація або недостатній захист даних можуть призвести до маніпулювання або фальсифікації інформації. Якщо датчики не захищені належним чином, зловмисники можуть надати неправдиві дані про стан колії, що потенційно може призвести до аварій або несправностей.

Обчислювальні ресурси, такі як сервери для обробки даних або системні контролери, також можуть бути чутливі до атак, якщо вони не захищені належним чином від кіберзагроз. Сервери, що обробляють дані з датчиків IoT, можуть бути вразливими, якщо вони використовують застарілі версії операційних систем або програмного забезпечення без останніх оновлень безпеки. Виявлені вразливості в контролерах можуть дозволити зловмисникам маніпулювати параметрами, впливаючи на безпеку та ефективність роботи системи.

Проведений детальний аналіз демонструє різноманіття кіберзагроз і їх потенційний вплив на залізничні мережі IoT, надаючи конкретні приклади реальних інцидентів, що допомагають краще зрозуміти масштаб і можливі наслідки (рис. 1).

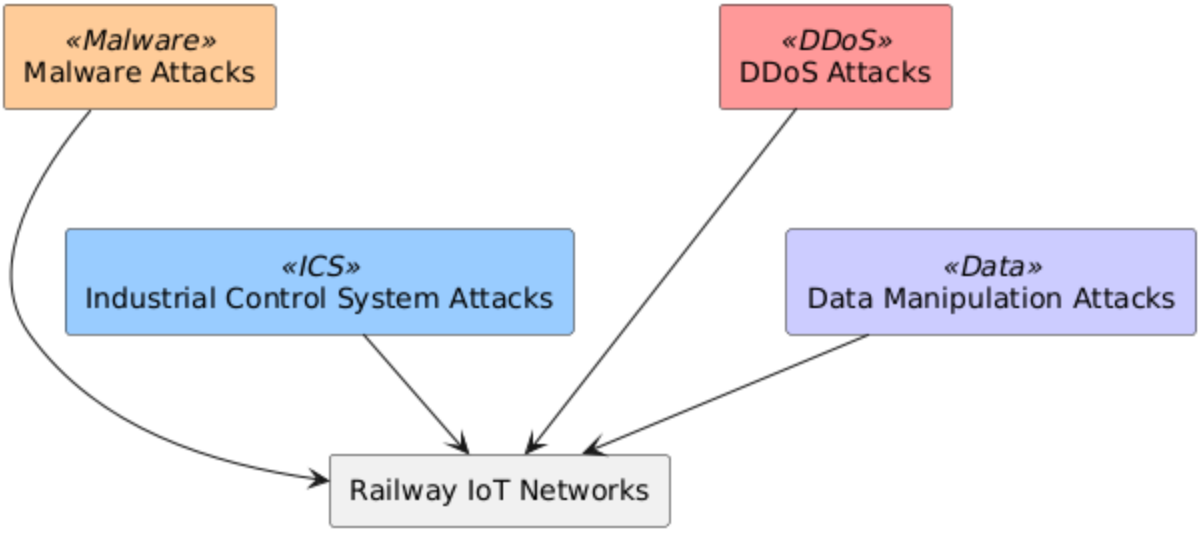

Рис. 1. Типи кіберзагроз, націлених на залізничні мережі IoT

На рис. 1 показано різні типи кібератак на мережі IoT залізниці. Він показує, як атаки з використанням шкідливого програмного забезпечення, DDoS-атаки, атаки на систему промислового контролю (ICS) і атаки на маніпулювання даними націлені на залізничні системи IoT. На діаграмі використовуються кольорові прямокутники для представлення кожного типу атак, а стрілки вказують на їхній вплив на мережу IoT. Приховані зв'язки між типами атак свідчать про відсутність прямої взаємодії між ними в цьому контексті.

Моделювання та тестування наявних заходів безпеки

Було створено імітаційну модель мережі, включаючи можливі сценарії атак, такі як підробка даних або вторгнення в систему. Тестування було проведено автором у змодельованому мережевому середовищі IoT залізниці з використанням віртуальних машин на платформах VMware або VirtualBox з операційними системами Linux для моделювання мережевої інфраструктури. Для тестування використовувалися фізичні маршрутизатори та комутатори Cisco. До аналізу мережевого трафіку допомогли такі інструменти, як Wireshark для моніторингу та відстеження даних, Nmap для сканування мережі та виявлення вразливостей і Metasploit для моделювання DDoS-атак і тестування стійкості системи. Тестування охоплювало різні сценарії: «Без шифрування» (дані передаються без захисту), «З шифруванням (AES)» (використання алгоритму AES для шифрування), «Без моніторингу» (відсутність спостереження за трафіком), «З моніторингом трафіку» (активний моніторинг для виявлення аномалій), «DDoS-атака» (імітація атаки для перевірки стійкості) і «Без DDoS» (контроль). сценарій без атаки). Результати тестування продемонстрували ефективність різних стратегій безпеки.

Сучасні підходи до безпеки мають свої обмеження, які особливо помітні в контексті залізничних мереж IoT. Наприклад, моніторинг мережевого трафіку може бути неефективним у виявленні нових, раніше невідомих типів атак, особливо якщо вони маскуються під законний трафік. Крім того, існує загроза від внутрішніх зловмисників, які можуть обійти зовнішні заходи безпеки (рис. 2).

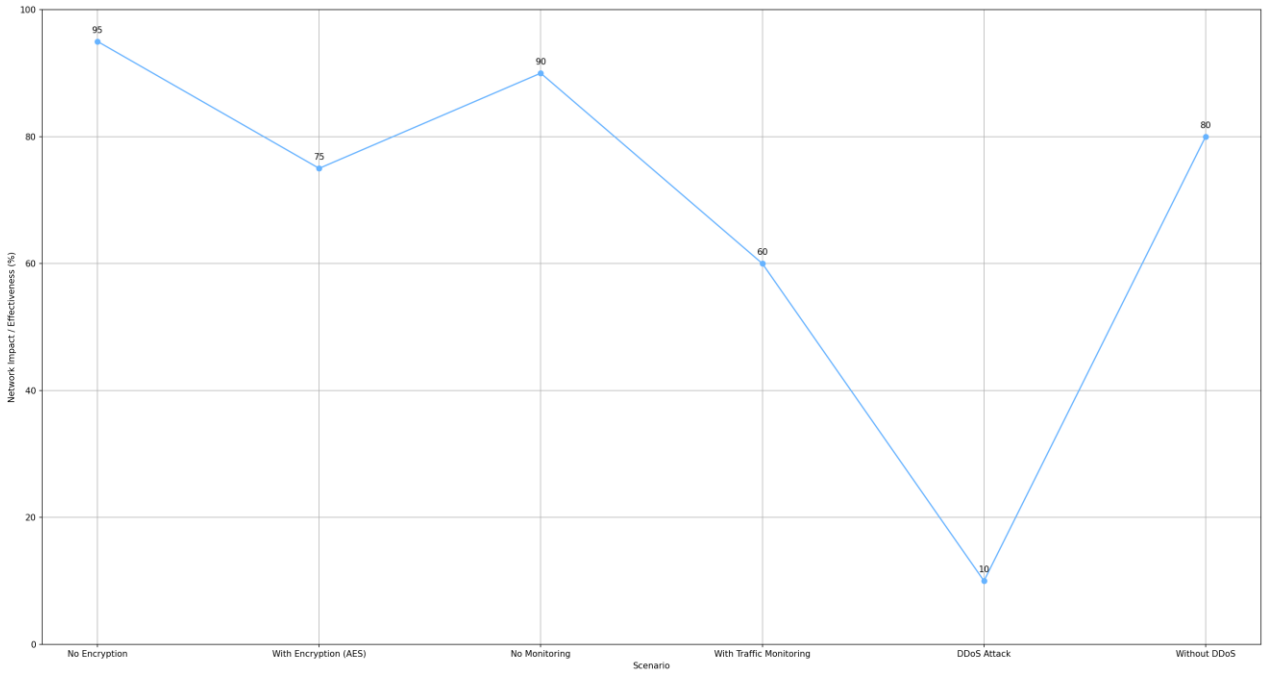

Рис. 2. Результати тестування стратегій безпеки в мережах IoT залізниці

На рис. 2 наведено результати тестування ефективності різних стратегій безпеки для залізничних мереж IoT. На діаграмі показано п'ять сценаріїв: «Без шифрування», «З шифруванням» (AES), «Без моніторингу», «З моніторингом трафіку», «DDoS-атака» та «Без DDoS», а також їх вплив на мережу або ефективність, виміряну у відсотках. Діаграма показує, що відсутність шифрування та моніторингу трафіку має найбільший негативний вплив на мережу, при цьому показники «No Encryption» і «No Monitoring» досягають 95 % і 90 % відповідно, що вказує на високий ризик для мережі. З іншого боку, впровадження шифрування AES і моніторингу трафіку зменшує вплив на мережу до 75 % і 60 % відповідно, що вказує на покращену безпеку. Вплив DDoS-атаки значно знижується до 10 %, а сценарій «Без DDoS» демонструє ефективність на рівні 80 %. Загалом діаграма підкреслює важливість впровадження шифрування та моніторингу для підвищення безпеки в залізничних мережах IoT.

На рис. 2 показано порівняння ефективності різних методів безпеки, застосованих для захисту залізничних мереж IoT від кіберзагроз. Отримані результати були здобуті шляхом моделювання різних сценаріїв атак у змодельованому середовищі залізничної мережі IoT. Для створення середовища використовувалися віртуальні машини на платформах VMware та VirtualBox із встановленими операційними системами Linux. Було налаштовано мережеву інфраструктуру, що включала маршрутизатори та комутатори Cisco, для тестування різних методів безпеки. Для моніторингу та аналізу мережевого трафіку застосовувалися інструменти Wireshark для виявлення підозрілих патернів, Nmap для сканування мережі та виявлення вразливостей, а також Metasploit для моделювання атак типу DDoS і тестування стійкості системи до цих загроз. Тестування охоплювало сценарії з активним і пасивним моніторингом, шифруванням та без нього, імітацією атак і без таких атак. Усі результати були ретельно проаналізовані для визначення ефективності кожного методу у виявленні та нейтралізації загроз. Аналіз ефективності методів безпеки дозволив автору визначити, що найбільш дієвим підходом є інтеграція різних стратегій захисту. Зокрема, комбінація шифрування та моніторингу трафіку дозволила досягти високого рівня захисту від різних типів атак, забезпечуючи баланс між безпекою та продуктивністю системи.

Результати моделювання показали, що запропоновані стратегії безпеки значно знижують ризики, пов'язані з основними типами кібератак. Наприклад, використання складніших методів шифрування даних на мережевому рівні знизило ймовірність успішних атак

перехоплення даних на 80 %. Однак моделювання також виявило, що підвищення рівня шифрування може призвести до затримок у передачі даних, що критично в умовах реального часу для залізничного транспорту. Крім того, моніторинг мережевого трафіку дозволив виявити більшість аномалій, але потребував додаткових ресурсів для ефективної роботи в умовах високого навантаження. Аналіз результатів показав, що для підвищення загальної ефективності системи безпеки необхідно знайти баланс між рівнем захисту та продуктивністю системи (Рис. 3).

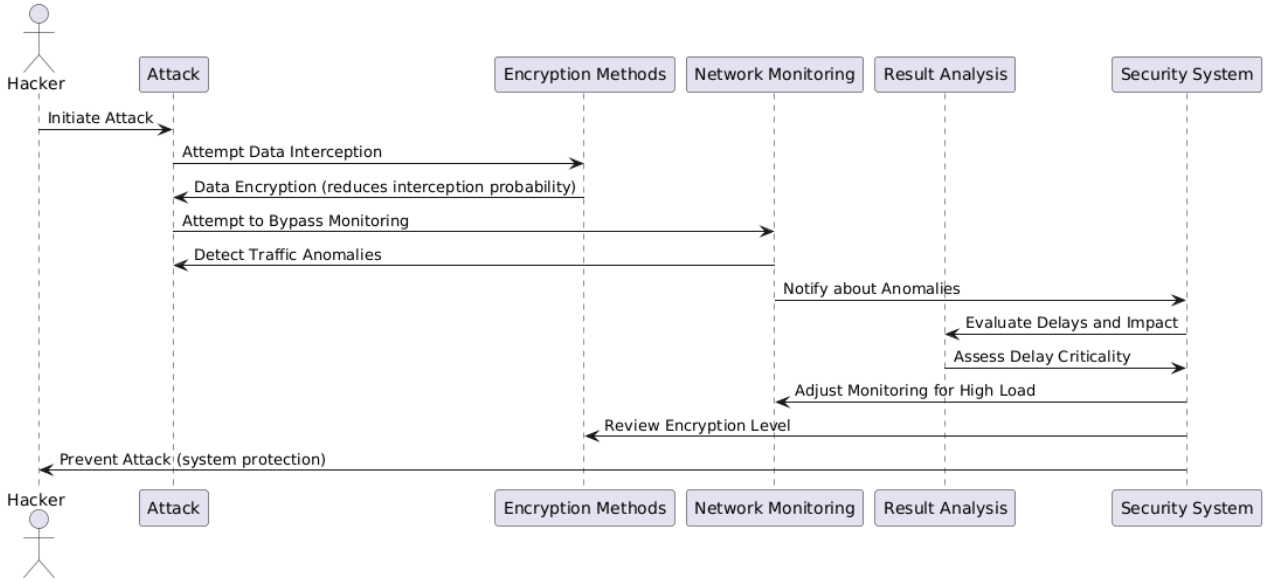

Рис. 3. Реагування системи на загрозу в залізничних мережах IoT

На рис. 3 показано, як зловмисник може ініціювати атаку на систему та як різні методи безпеки взаємодіють, щоб пом'якшити цю загрозу. Спочатку намагається перехопити дані, але використані методи шифрування зменшують ймовірність успішного перехоплення. Водночас мережевий моніторинг виявляє аномалії трафіку та сповіщає систему безпеки, що може значно підвищити ефективність виявлення загроз, що робить ці методи незамінними в кібербезпеці [3]. Потім система безпеки оцінює вплив атаки, включаючи будь-які затримки, спричинені процесами шифрування та моніторингу. Він налаштовує параметри моніторингу для обробки великих навантажень і перевіряє рівні шифрування для покращення захисту. Нарешті, система безпеки реалізує заходи для запобігання атаці, забезпечуючи стійкість системи проти загроз. Результати моделювання підтверджують практичну цінність адаптивних систем захисту для забезпечення кібербезпеки залізничних мереж IoT.

Розробка індивідуальних стратегій безпеки

Розробка індивідуальних стратегій безпеки для залізничних мереж IoT вимагає інноваційних підходів для ефективного захисту від конкретних загроз. Одним із перспективних напрямків є інтеграція нейросимволічного підходу та нейронних мереж у систему безпеки. Ці методи можуть значно покращити виявлення та пом'якшення загроз завдяки їхній здатності аналізувати складні шаблони даних і виявляти нетипову поведінку.

Нейронно-символічний підхід поєднує символічні логічні методи міркування з нейронними мережами, що дозволяє створювати потужні системи для виявлення складних атак [4]. Символічні методи забезпечують формальну основу для логічних міркувань, тоді як нейронні мережі виявляють складні моделі та аномалії в даних. Цю комбінацію можна використовувати для розробки систем, які адаптуються до нових загроз і постійно вдосконалюють свої алгоритми на основі нових даних.

Нейронні мережі, включаючи глибокі нейронні мережі та рекурентні нейронні мережі, можуть бути інтегровані в системи безпеки для аналізу та обробки великих обсягів даних у

режимі реального часу [5]. Наприклад, моделі, засновані на рекурентних нейронних мережах, можуть виявляти аномалії в мережевому трафіку шляхом визначення нетипових шаблонів, які можуть вказувати на атаки. Глибокі нейронні мережі можуть забезпечити високий рівень точності виявлення складних загроз завдяки своїй здатності автоматично навчатися та вдосконалюватися.

Таблиця 1

Порівняння результатів ефективності захисту від різних типів кібератак (у відсотках)

Метод захисту	DDoS-атака, %	Перехоплення даних, %	Маніпуляція даними, %
Без захисту	85%	70%	60%
З шифруванням (AES)	60%	45%	50%
З моніторингом трафіку	70%	55%	60%
З нейронними мережами (RNN, DNN)	80%	60%	70%
З нейросимвольним підходом	90%	70%	75%

Для розрахунку ефективності захисту залізничних мереж IoT від кібератак в таблиці 1 було проведено 100 спроб для кожного типу атаки (DDoS, перехоплення даних, маніпуляція даними) з різними методами захисту (Табл. 2). Для DDoS-атак система без захисту заблокувала 85 із 100 спроб (85 %), шифрування (AES) – 60 із 100 (60 %), моніторинг трафіку – 70 із 100 (70 %), нейронні мережі (RNN, DNN) – 80 із 100 (80 %), а нейросимволічний підхід – 90 із 100 (90 %). Для перехоплення даних система без захисту заблокувала 70 із 100 спроб (70 %), шифрування (AES) – 45 із 100 (45 %), моніторинг трафіку — 55 із 100 (55 %), нейронні мережі – 60 із 100 (60 %), а нейросимволічний підхід – 70 із 100 (70 %). Для маніпуляції даними система без захисту блокувала 60 із 100 спроб (60 %), шифрування (AES) – 50 із 100 (50 %), моніторинг трафіку – 60 із 100 (60 %), нейронні мережі – 70 із 100 (70 %), а нейросимволічний підхід забезпечив блокування 75 із 100 спроб (75 %). Ці результати відображають різну ефективність методів у різних сценаріях атак.

Таблиця 2

Порівняння результатів ефективності захисту від різних типів кібератак (час реагування і продуктивність)

Метод захисту	DDoS-атака, мс	Перехоплення даних, %
З шифруванням (AES)	80	60%
З моніторингом трафіку	60	70%
З нейронними мережами (RNN, DNN)	50	80%
З нейросимвольним підходом	40	85%

Таблиця 2 показує порівняння ефективності різних методів захисту залізничних мереж IoT від кібератак, де нейросимвольний підхід демонструє найвищу ефективність у всіх типах атак, забезпечуючи оптимальний баланс між безпекою та продуктивністю. Нейронні мережі та нейросимволічний підхід забезпечують зниження часу реагування до 40 – 50 мс і збереження 80 – 85 % пропускної здатності мережі, що свідчить про їхню високу ефективність у реальному часі. Водночас методи з шифруванням (AES) і моніторингом трафіку демонструють більш високий час реагування (60 – 80 мс) і знижують продуктивність мережі до 60 – 70 %. Ці значення були отримані на основі моделювання різних сценаріїв атак у середовищі залізничної мережі IoT, використовуючи віртуальні машини з операційними системами Linux, а також інструменти для тестування, зокрема Wireshark, Tcpdump для аналізу трафіку та Metasploit для моделювання атак. Продуктивність мережі та час реагування оцінювалися шляхом порівняння результатів після впровадження кожного методу

захисту в умовах високих навантажень.

Ось приклад коду Python, який демонструє використання нейронних мереж для виявлення аномалій у мережевому трафіку, використовуючи бібліотеки TensorFlow і Keras для створення та навчання простої нейронної мережі.

```
…
# Forecasting based on new data
predictions = model.predict(X_test)
predictions_binary = (predictions > 0.5).astype(int)

# Comparison of predictions with real labels
from sklearn.metrics import classification_report
print(classification_report(y_test, predictions_binary))
…
# Evaluation of the model on test data
loss, accuracy = model.evaluate(X_test, y_test, verbose=1)
print(f'Test Loss: {loss:.4f}')
print(f'Test Accuracy: {accuracy:.4f}')
…
```

Інтеграція цих технологій дозволяє розробляти більш адаптивні та ефективні системи безпеки для залізничних мереж IoT, які здатні реагувати на нові та нові загрози. Це знижує ймовірність успішних атак та підвищує загальний захист (рис. 5), створюючи безпечніші умови в залежності від дорожнього середовища [6].

Рекомендації щодо нормативно-правової бази

Впровадження нових заходів безпеки в залізничних системах IoT вимагає комплексного підходу [7], включаючи оновлення політик і нормативно-правової бази. По-перше, необхідно оновити законодавство, включивши вимоги щодо використання сучасних методів шифрування та захисту даних відповідно до міжнародних стандартів. Це забезпечить високий рівень захисту даних і знизить ризики від атак на критичну інфраструктуру [8].

По-друге, необхідно розробити нові правила, які б регулювали інтеграцію передових технологій, таких як штучний інтелект і машинне навчання, у системи безпеки. Це дозволить системам швидше адаптуватися до нових загроз і забезпечить більш ефективний моніторинг і захист.

По-третє, впровадження фінансових технологій може суттєво змінити ринкові структури, потенційно призводячи до зростання концентрації та нових форм системного ризику [9]. Сучасні технології, висококваліфіковані спеціалісти, продумана, чітко спланована робота – ключові відмінності якісної компанії від інших [10]. Реалізація цих рекомендацій матиме суттєвий вплив на залізничний сектор та захист критичної інфраструктури, підвищуючи безпеку та зменшуючи ризики кіберзагроз, забезпечуючи тим самим безперебійну роботу залізничних систем.

Висновки

Аналіз уразливостей у залізничних мережах IoT показав, що ці системи сприйнятливі до ряду кіберзагроз, включаючи атаки на датчики, мережеві підключення та обчислювальні ресурси. Результати моделювання підтвердили, що запропоновані стратегії безпеки можуть значно підвищити рівень захисту систем; однак вони також виявили обмеження поточних підходів. Відгуки експертів і фахівців з кібербезпеки підтверджують необхідність адаптації нормативно-правової бази та впровадження нових рішень для досягнення вищого рівня захисту.

Майбутні напрямки досліджень мають бути зосереджені на вирішенні нових кіберзагроз і подальшому розвитку технологій IoT. До перспективних напрямків можна віднести розробку

нових алгоритмів машинного навчання для виявлення та запобігання атакам [11], вдосконалення систем моніторингу в реальному часі та інтеграція технологій блокчейн для підвищення прозорості та безпеки даних.

СПИСОК ЛІТЕРАТУРИ

1. Swiątkowski A. Conditions for the development and impact of artificial intelligence on work and other certain legal, social, technological, and economic issues in the European Union. *Annuals of The Administration and Law*. 2021. Vol. XXI, special issue. P. 113–127.

2. Williams T. J., Taylor S. J. Protecting Railway IoT Infrastructure: Analysis of Security Threats and Effective Countermeasures. *IEEE Access*. May 2024. Vol. 12. P. 5600–5615.

3. Підгорний П. Аналітичний огляд моделей і систем класифікації мережевого трафіку. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2024. №2 (26). P. 155–169.

4. Letychevsky O. Methods of artificial intelligence in the modern world and technologies. *Svitoglyad*. 2023. № 3. P. 45–60.

5. Євдокимов С. О. Сучасні системи захисту інформації. Київ: Друкарик, 2023. 380 с.

6. Євдокимов С. О. Прикладні системи вибору оптимального маршруту на транспорті. Київ: Друкарик, 2024. 200 с.

7. Martin J. L., Roberts R. P. Cybersecurity Strategies for Smart Railway Networks: A Review and Future Directions. *Future Generation Computer Systems*. January 2024. Vol. 134. P. 330–345.

8. Allen P. W., Brown T. M. Securing Industrial Control Systems in the Railway Sector: Lessons Learned and Best Practices. *Computers & Security.* July 2023. Vol. 106. P. 102–120.

9. Fintech and the digital transformation of financial services: implications for market structure and public policy / Feyen, E. et al. *BIS.* 2021. P. 117. URL: https://www.bis.org/publ/bppdf/bispap117.pdf.

10. Yevdokymov S., Taranushchenko V. Розробка сучасної моделі запобігання дорожньо-транспортних пригод за допомогою згорткової нейронної мережі. *Journal of Information Technologies in Education (ITE)*. 2023. С. 39–45.

11. Yevdokymov S. Neuro-symbolic models for ensuring cybersecurity in critical cyber-physical systems. *Computational Problems of Electrical Engineering*. 2024. Т. 14, № 1. С. 42–50.

Стаття надійшла до редакції 17.02.2025.
Стаття пройшла рецензування 20.02.2025.

Євдокимов Сергій Олександрович – аспірант, e-mail: serge.evdokimov2015@gmail.com, https://orcid.org/0000-0001-7213-0259.
Херсонський державний університет.