УДК 656.25:004.056:004.8

КІБЕРБЕЗПЕКА СИСТЕМ ЗАЛІЗНИЧНОЇ АВТОМАТИКИ І ТЕЛЕМЕХАНІКИ. ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ

Канд. техн. наук В. О. Сотник, асп. М. Г. гизи Алмамедова, А. А. Меліхов

CYBER SECURITY OF RAILWAY AUTOMATION AND TELEMECHANICS SYSTEMS. ARTIFICIAL INTELLIGENCE FOR DETECTING AND RESPONDING TO THREATS.

Candidate of Technical Sciences V. O. Sotnyk,
postgraduate student M. H. Almammadova, A. Melikhov

DOI: https://doi.org/10.18664/1994-7852.214.2025.352046

Анотація. *Стаття присвячена дослідженню критичних кіберзагроз, що виникають унаслідок швидкої цифровізації систем залізничної автоматики і телемеханіки, зокрема мікропроцесорної централізації та диспетчерської централізації. Автори обґрунтовують необхідність застосування передових технологій, таких як штучний інтелект, для забезпечення стійкості та безпеки критичної інфраструктури залізниці.*

У статті проаналізовано критичні вразливості систем залізничної автоматики, вектори кібератак на основні системи. Досліджено вразливість систем до атак, типових для COTS-компонентів і стандартних протоколів (TCP/IP), а також загрози впровадження зловмисного ПЗ у прошивку для порушення логіки безпеки руху, що може спричинити зіткнення поїздів. Доведено, що ШІ забезпечує необхідний рівень моніторингу та реагування, який виходить за рамки традиційного сигнатурного захисту. Розглянуто механізми машинного та глибокого навчання, зазначено про критичну роль інтеграції ШІ з платформами SOAR (Security Orchestration, Automation and Response). Зроблено висновки, що штучний інтелект і автоматизовані системи реагування SOAR є основними для перетворення захисту з реактивного на проактивний, превентивний. Запропоновано для подальшого розвитку кіберзахисту систем залізничного транспорту передбачити інтеграцію SOAR із концепцією цифрового двійника залізничної мережі для досягнення повної автономної кібербезпеки.

Ключові слова: *кібербезпека, залізнична автоматика і телемеханіка, штучний інтелект, мікропроцесорна централізація, диспетчерська централізація, критична інфраструктура , безпека руху.*

Abstract. *The article is devoted to the study of critical cyber threats arising from the rapid digitization of railway automation and telemechanics systems, in particular microprocessor centralization and dispatching centralization. The authors justify the need to use advanced technologies, such as artificial intelligence (AI), to ensure the stability and security of critical railway infrastructure.*

The article analyzes critical vulnerabilities of RAAS and provides a detailed analysis of cyberattack vectors on key systems. The vulnerability of systems to attacks typical for COTS components and standard protocols (TCP/IP) is investigated, as well as the threat of introducing malicious software into the firmware to disrupt traffic safety logic, which can cause train collisions. It has been proven that AI provides the necessary level of monitoring and response that goes beyond traditional signature-based protection. Machine and deep learning mechanisms are considered, and the critical role of AI integration with SOAR (Security Orchestration, Automation, and Response) platforms is emphasized. It is concluded that artificial intelligence and automated SOAR response systems are key to transforming protection from reactive to proactive and preventive. It is proposed that the further development of cyber protection for railway transport systems should provide for the integration of SOAR with the concept of a digital twin of the railway network in order to achieve complete autonomous cybersecurity.

Keywords: *cybersecurity, railway automation and telemetry, artificial intelligence, microprocessor centralization, dispatch centralization, critical infrastructure, traffic safety.*

Вступ. Швидкий перехід залізниць до цифрових технологій (ETCS, СЦБ на основі мікропроцесорної техніки, IoT) став джерелом кіберзагроз, у зв’язку з чим важливим став захист критичної інфраструктури. Аналіз сучасних кіберзагроз для систем залізничної автоматики і телемеханіки (СЗАТ) та обґрунтування застосування технологій штучного інтелекту (ШІ) для підвищення їхньої стійкості та безпеки є темою дослідження. Цифровізація залізниці перетворила раніше ізольовані, «повітряно-розділені», релейні системи на мережеві промислові системи управління, значно розширивши їхню поверхню атаки.

Аналіз кіберзагроз у системах залізничної автоматики і телемеханіки. Аналіз кіберзагроз базований на критичності систем і їхніх технологічних вразливостях. Мікропроцесорна централізація (МПЦ) є системою найвищої критичності, оскільки безпосередньо контролює безпеку руху (керування стрілками та сигналами). Злом системи МПЦ може призвести до зіткнень або сходження поїздів. Автоматичне блокування (АБ МП) визначає інтервали руху поїздів на перегонах, і його порушення може призвести до зупинки руху або небезпечного зближення. Диспетчерська централізація (ДЦ) – це центральна точка управління для великого регіону, що робить її єдиним пунктом відмови. Комунікаційні канали є «нервовою системою» СЗАТ і головною мішенню для кібератак, оскільки вони дають змогу здійснювати віддалене втручання. Аналіз вразливостей цих систем від кіберзагроз наведено в табл. 1.

Таблиця 1

Вразливість систем залізничної автоматики і телемеханіки від кіберзагроз

Аспект/об'єкт	Характеристика системи	Вектор кіберзагрози
1	2	3
Мікропроцесорна централізація		
Критичність	Найвища критичність. Безпосередній контроль безпеки руху на станції (керування стрілками та сигналами). Злом системи може призвести до зіткнення/сходження поїздів	
Технології	Використання COTS-компонентів – мікропроцесори, операційні системи, стандартні мережеві протоколи (TCP/IP)	Вектори вразливості, відомі для стандартного IT-середовища (переповнення буфера, відомі експлойти ОС), можуть бути перенесені на МПЦ, якщо не забезпечена належна ізоляція та патчинг
Програмне забезпечення	Складне, великий обсяг коду, що керує логікою безпеки	Загроза полягає в зловмисному програмному забезпеченні (мальваре) або зміні прошивки, спрямовані на обхід або порушення логічних залежностей безпеки
Обслуговування	Потреба у віддаленому моніторингу та оновленні програмного забезпечення	Атаки через ланцюг постачання або компрометація віддалених сервісів/портів для діагностики та обслуговування
Мікропроцесорне автоматичне блокування		
Критичність	Визначає інтервали руху поїздів на перегонах. Порушення призводить до зупинки руху або небезпечного зближення	
Датчики	Сучасні системи використовують лічильники осей, які передають дані про зайнятість блок-ділянки по цифрових каналах	Вектор загроз полягає в компрометації цілісності даних. Наприклад, підміна даних про зайнятість колії, надсилання хибного сигналу про вільність зайнятої блок-ділянки або хибного сигналу про зайнятість вільної ділянки (що спричинить DoS-атаку на рух)
Протоколи	Часто інтегровані з кодовими системами або передають дані через мережу	Загроза полягає в прослуховуванні або втручанні в комунікаційні протоколи, що контролюють передавання сигналів, наприклад кодових сигналів автоматичної локомотивної сигналізації (АЛС)

Продовження табл. 1

1	2	3
Диспетчерська централізація		
Критичність	Центральна точка управління для великого регіону, створення єдиного пункту відмови	
Взаємодія	Тісна інтеграція з корпоративною мережею (IT), включаючи системи планування, графіків руху, бази даних	Міграція загроз – атака на менш захищений IT-периметр (офісні мережі, електронна пошта) може дати змогу зловмиснику отримати плацдарм для проникнення в мережу ДЦ
Інтерфейс	Використання АРМ, які працюють зі стандартними ОС	DoS-атака на диспетчерський центр, яка блокує можливість віддаленого управління, змушуючи переходити на менш ефективне місцеве. Також шпигунство з метою отримання оперативної інформації про рух поїздів
Комунікаційні інтерфейси		
Інтерфейс «Поле – Станція» (виконавчий рівень)	Часто використовує промислові шини (Fieldbus) або спеціалізовані лінії зв'язку, які можуть мати недостатній захист від автентифікації	Підміна команд. Зловмисник, отримавши доступ до виконавчого контролера, може направити команду на переведення стрілки, минаючи логіку безпеки МПЦ. Це класичний сценарій атаки на цілісність системи
Інтерфейс «Станція – диспетчерський центр»	Великий радіус дії, використання стандартизованих телекомунікаційних протоколів	Атака типу «Людина посередині» або прослуховування трафіку. Це дає змогу перехоплювати команди ДЦ до станції та відповіді від станції до ДЦ. Наприклад, ДЦ отримує хибне повідомлення про успішне виконання команди, тоді як насправді команда не була виконана або була змінена
Внутрішній інтерфейс МПЦ (логічний рівень)	Основою безпеки МПЦ є надмірність (резервування), коли два або три незалежні канали обробки даних постійно порівнюють результати	Синхронізація зловмисних станів. Складна кібератака може бути спрямована на одночасне компрометування всіх резервних каналів і примусове узгодження їхніх помилкових результатів. Це дає змогу обійти захист SIL і реалізувати небезпечний стан

Детальний аналіз векторів атак на системи залізничної автоматики і телемеханіки виявляє, що кіберзагрози стосуються всіх рівнів управління – від польового обладнання до центральних диспетчерських пунктів, із фокусуванням на компрометації цілісності даних і доступності систем. Найбільш критичною

мішенню, на нашу думку, є мікропроцесорна централізація, оскільки вона безпосередньо керує стрілками і сигналами, і її компрометація може призвести до зіткнень поїздів, аварій і катастроф. Використання комерційного обладнання (COTS) і стандартних протоколів (TCP/IP, ОС) робить МПЦ вразливою до загроз, типових для звичайного IT-середовища. Зловмисники можуть використовувати відомі експлойти, наприклад переповнення буфера, якщо система не має належної ізоляції та оновлень (патчів). Атака може бути спрямована також на впровадження зловмисного програмного забезпечення або цілісність прошивки з метою обійти чи порушити логічні залежності, які забезпечують безпеку руху [1-3].

Вектори атак можуть бути реалізовані через компрометацію віддалених сервісів/портів, які використовують для діагностики та оновлення програмного забезпечення, а також атаки через ланцюг постачання, вбудовуючи шкідливий код на етапі виробництва чи впровадження.

Вектори атак на перегінному рівні спрямовані на порушення інтервального регулювання руху поїздів. Компрометація цілісності даних – це основний вектор, спрямований на датчики, наприклад лічильники осей. Атака полягає в підміні даних про зайнятість колії: надсилання хибного сигналу про вільність зайнятої блок-ділянки, що спричинить наближення поїздів до небезпечної відстані, або зайнятість вільної ділянки, що спричинить штучну зупинку руху (по суті DoS-атаку на рух). Загроза втручання у протоколи АЛС полягає у прослуховуванні або втручанні в комунікаційні протоколи, які контролюють передавання кодових сигналів автоматичної локомотивної сигналізації.

Диспетчерська централізація є центральною точкою управління, і її компрометація може паралізувати рух на великій дільниці. Через тісну інтеграцію ДЦ (операційні технології, ОТ) із корпоративною мережею (інформаційні технології, IT) можлива міграція загроз. Атака на менш захищений IT-периметр (офісні мережі, електронна пошта) може стати плацдармом для проникнення в мережу ДЦ. DoS-атаки на диспетчерський центр мають на меті порушити доступність системи. DoS-атака на диспетчерський центр блокує можливість віддаленого управління, змушуючи персонал переходити на менш ефективне місцеве керування на станціях. Не менш важливим є шпигунство, яке спрямоване на отримання оперативної інформації про рух поїздів, що може бути використано для подальших фізичних або кібератак.

Комунікаційні канали є «нервовою системою» СЗАТ і головною мішенню для віддаленого втручання.

Отже, усі сучасні СЗАТ, особливо на основі МПЦ і ДЦ, потребують застосування комплексних рішень, що виходять за рамки традиційного IT-захисту. Критичним є захист не лише конфіденційності, а передусім цілісності даних і доступності систем, що безпосередньо впливає на безпеку руху. Саме тут штучний інтелект може забезпечити необхідний рівень моніторингу та реагування, що і є предметом подальшого дослідження в цій статті.

Наслідки кібератак на системи залізничної автоматики і телемеханіки виходять далеко за рамки звичайних IT-інцидентів, безпосередньо загрожуючи безпеці руху, спричиняючи значні економічні збитки та підриваючи суспільну довіру.

Головна небезпека кібератак полягає в можливості зловмисного впливу на основні функції управління поїздами, спрямованого на компрометацію цілісності даних і доступності систем. Атака на мікропроцесорну централізацію або протоколи автоматичного блокування може призвести до підміни даних про зайнятість колії. Це може призвести до надсилання хибного сигналу про вільність зайнятої блок-ділянки, унаслідок чого наступний

поїзд може в'їхати в небезпечну зону і спричинити зіткнення. Через підміну команд на інтерфейсі «Поле-Станція» зловмисник може направити команду на переведення стрілки, минаючи логіку безпеки МПЦ. Це може призвести до сходження поїзда з рейок. У разі компрометації внутрішнього інтерфейсу МПЦ і синхронізації зловмисних станів можна обійти захист SIL, реалізуючи небезпечний стан, який система має блокувати [4-6].

Загроза безпеці руху від кібератак – це головний, але не єдиний аспект. Кібератаки трансформуються у прямі та непрямі збитки для залізничних операторів і держави, а також спричиняють репутаційні наслідки. Порушення безпеки руху через кібератаки підриває довіру суспільства до залізничного транспорту як до найбільш безпечного виду перевезень. Крім того, слід зазначити, що кібератаки на СЗАТ свідчать про вразливість критичної інфраструктури держави, що має стратегічні наслідки для національної безпеки. Отже, кібератаки на СЗАТ є загрозою не лише для технологічної стійкості, але й економічної та соціальної стабільності. Саме тому для виявлення та реагування на ці загрози необхідне застосування передових технологій, таких як штучний інтелект.

1. **Застосування ШІ в гарантуванні кібербезпеки систем залізничної автоматики.** Застосування ШІ в кібербезпеці СЗАТ базовано на його здатності обробляти величезні обсяги даних, виявляти аномалії та ухвалювати рішення зі швидкістю, недоступною людині. Це критично важливо для захисту систем, де порушення цілісності даних і доступності має катастрофічні наслідки. Основою кіберзахисту на базі ШІ є використання алгоритмів машинного навчання, здатних ідентифікувати зловмисну активність без необхідності попереднього знання конкретного вірусу чи експлойту. У табл. 2 наведені механізми та можливі форми застосування ШІ для прогнозування і усунення кіберзагроз у системах ЗАТ.

Таблиця 2

Механізми та можливі форми застосування ШІ для захисту від кіберзагроз СЗАТ [6, 7]

Концепція ШІ	**Механізм у кібербезпеці**	**Застосування в СЗАТ**
1	2	3
Навчання з учителем (Supervised Learning)	Алгоритми тренують на розмічених даних (відомі атаки vs. нормальний трафік)	Класифікація мережевого трафіку між МПЦ і ДЦ для ідентифікації відомих сигнатур шкідливих програм чи команд
Навчання без учителя (Unsupervised Learning)	Алгоритми виявляють аномалії (відхилення) у нерозмічених даних, будуючи модель нормальної поведінки	Моніторинг внутрішнього трафіку МПЦ/АБ-МП для виявлення несподіваних змін у частоті команд, що свідчить про спробу синхронізації зловмисних станів або SPOOFING
Навчання з підкріпленням (Reinforcement Learning)	Агент навчається ухвалювати рішення (наприклад блокувати чи дозволяти трафік) у динамічному середовищі, отримуючи винагороду за успішний захист	Автоматичне ухвалення рішень на рівні ДЦ про ізоляцію компрометованої станції або автоматичний перехід на резервний канал зв'язку

Продовження табл. 2

1	2	3
Глибоке навчання (Deep Learning) для складних атак	Глибокі нейронні мережі можуть аналізувати сирі мережеві пакети і промислові протоколи (наприклад MODBUS, що можна використовувати у СЗАТ), виявляючи приховані атаки, які неможливо знайти за допомогою традиційних сигнатурних методів	Боротьба з атаками типу «Людина посередині» (MITM) на WAN-інтерфейсі. Виявлення поліморфного та метаморфного шкідливого ПЗ: DL-моделі здатні розпізнавати варіації зловмисного програмного забезпечення, що атакує прошивку МПЦ, оскільки вони вивчають глибинні ознаки коду, а не лише його поверхневі зміни
Автоматизація реагування (SOAR та ШІ)	ШІ трансформує процес реагування, перетворюючи його з реактивного на проактивний. Цього досягають завдяки інтеграції з платформами SOAR	У критичних системах, де рішення необхідно ухвалити за мілісекунди (наприклад блокування команди, що призводить до переведення стрілки), ШІ може автоматично ініціювати ізоляцію скомпрометованого контролера або перенаправити керуючий трафік на безпечний резервний канал. ШІ може точно прогнозувати розвиток атаки та виконувати автоматичний патчинг або відкат конфігурації, мінімізуючи час простою та запобігаючи поширенню загрози, що є основним для доступності системи
Прогнозування та оцінювання ризиків	ШІ забезпечує неперервне оцінювання ризиків на основі комплексного аналізу вхідних даних	ШІ аналізує дані про поточний стан системи, звіти про вразливості COTS-компонентів і зовнішні кібер-інтелектуальні дані для прогнозування наступного вектора атаки на ДЦ або МПЦ, а також постійно оцінює цілісність даних від лічильників осей та іншого польового обладнання, автоматично підвищуючи рівень тривоги, якщо надійність вихідних даних знижується, захищаючи від SPOOFING та Command Injection

2. **Штучний інтелект у системах виявлення та реагування на загрози.** В умовах, коли час реакції на інцидент вимірюваний мілісекундами, штучний інтелект стає необхідною умовою для забезпечення безпеки руху і стійкості транспортної системи.

Традиційні методи захисту, засновані на сигнатурах і жорстких правилах, не здатні протистояти сучасним поліморфним, метаморфним і «нульовим» атакам, які є критичними для систем, що потребують високого рівня цілісності, як-от СЗАТ. ШІ забезпечує цю зміну парадигми завдяки

можливості автоматичного виявлення аномалій. У табл. 3 показана різниця в підходах для кіберзахисту традиційним шляхом і з використанням ШІ.

Таблиця 3

Аспект	Традиційний захист	ШІ-захист
Виявлення	За сигнатурами та відомими правилами	За поведінковими аномаліями та контекстом
Швидкість	Секунди, хвилини (після ідентифікації), іноді дні або тижні	Мілісекунди, секунди
Обробка даних	Обробка агрегованих журналів	Аналіз сирих пакетів (Deep Packet Inspection), промислові протоколи

Світові дослідження підтверджують критичну перевагу ШІ за швидкістю і точністю реагування, що є визначальним фактором для критичної інфраструктури. Для виявлення кібератаки командам безпеки зазвичай потрібні дні або тижні, тоді як рішення на основі ШІ можуть ідентифікувати та ізолювати загрозу практично моментально (рис. 1). Впровадження ШІ у системах безпеки також значно знижує кількість хибних спрацьовувань, одночасно підвищуючи точність виявлення реальних загроз.

Рис. 1. Швидкість реагування на інциденти

MTTD (Mean Time To Detect) – середній час виявлення. Це показник, що показує, скільки в середньому часу проходить від моменту виникнення інциденту/проблеми до її виявлення системою або персоналом. Наприклад, якщо зазвичай на пошук проблеми витрачають 15 хв, то MTTD = 15 хв.

MTTC (Mean Time To Contain) – середній час стримування. Це показник, що відображає, скільки в середньому часу потрібно, щоб локалізувати чи зупинити

поширення інциденту після його виявлення (до повного контролю).

Наприклад, інцидент виявили, і ще через 30 хв його локалізували, отже, MTTC = 30 хв.

Переваги ШІ з виявлення загроз полягають у тому, що він на 99 % дає змогу моментально визначати та ізолювати високошвидкісні атаки, такі як DDoS (критично для ДЦ). Крім того, сучасні ШІ-рішення здатні автоматично вживати захисних заходів для виявлення загроз, суттєво знижуючи навантаження на операторів (рис. 2).

Рис. 2. Ефективність ШІ у виявленні кіберзагроз

Діаграма на рис. 3 демонструє порівняння ефективності виявлення загроз і кількості хибних спрацьовувань у двох підходах: із застосуванням штучного інтелекту і без нього. Аналіз цієї діаграми показує, що системи з ШІ виявляють більше реальних загроз, ніж традиційні системи без ШІ. Штучний інтелект допомагає значно зменшити кількість помилкових тривог, які створюють зайве навантаження на персонал. Отже, діаграма наочно показує, що ШІ одночасно підвищує рівень виявлення справжніх загроз і знижує частоту хибних спрацьовувань, роблячи систему кіберзахисту більш ефективною [7, 9].

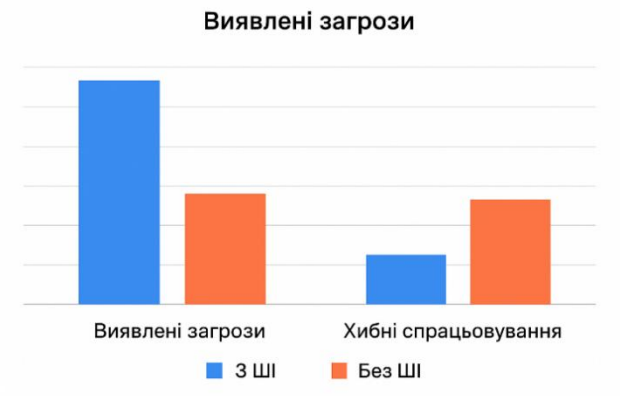

Рис. 3. Порівняння ефективності виявлення загроз і кількості хибних спрацьовувань із застосуванням штучного інтелекту і без нього

3. **Автоматизація реагування (SOAR).** Головна перевага штучного інтелекту в кібербезпеці залізниць полягає не лише у високоточному виявленні аномалій і кібератак, а й у критично важливому компоненті – автоматизації реагування на загрози (Security Orchestration, Automation and Response, SOAR). Саме SOAR забезпечує швидкість, точність і масштабованість захисних дій, що є вирішальним фактором в умовах кіберпротистояння. Швидкість реагування на кібератаку в залізничних системах – це не просто питання фінансових збитків, це питання безпеки руху та життя людей. Людське втручання, навіть висококваліфікованого фахівця, вимірюване хвилинами, тоді як сучасна атака може завдати незворотної шкоди за секунди.

У випадку виявлення атаки, наприклад на інтерфейс зв'язку між центральним сервером диспетчерської централізації і станційним обладнанням, ШІ може миттєво проаналізувати природу аномалії (несанкціонований потік даних, спроба маскування під керуючий протокол), за частки секунди (менше 500 мс) автоматично ініціювати відключення скомпрометованого мережевого сегменту і одночасно перевести зв'язок на резервний, незалежний канал, захищений криптографічно (наприклад VPN із використанням сертифікатів, що не скомпрометовані) (рис. 4).

Рис. 4. Час виявлення загрози

Розрахунок ефективності реагування на загрози (рис. 5) показує, що використання реагування SOAR на базі ШІ знижує час реагування на 99,9 % порівняно з ручним.

Статистичні дані дослідження, проведеного у 2024 році, показало, що впровадження SOAR-систем у критичній інфраструктурі залізниці допомагає скоротити середній час між виявленням і усуненням загрози (MTTR) на 85 %, що є критичним для забезпечення безперервності руху поїздів.

Не менш важливим критерієм доцільності використання автоматизації реагування на загрози (SOAR) на базі ШІ у залізничній галузі є зниження ризику від кіберзагроз і їхніх наслідків. Порівняльна динаміка зниження таких ризиків наведена на рис. 6 [8, 9].

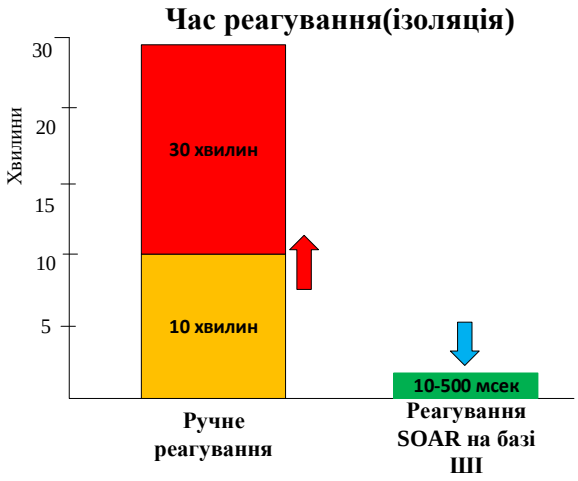

Рис. 5. Час реагування (ізоляція)

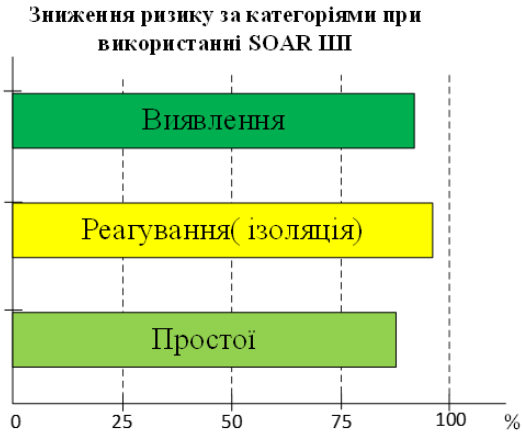

Рис. 6. Зниження ризику за категоріями із використанням SOAR-систем у критичній інфраструктурі залізниці

Однією з найбільш руйнівних тактик кібератак є латеральне переміщення (Lateral Movement). Латеральне переміщення – це техніка кібератаки, під час якої зловмисник, отримавши початковий доступ до одного пристрою або сегменту мережі (зазвичай менш захищеного), використовує його як плацдарм для подальшого просування та міграції в інші, більш критичні сегменти, зокрема OT-сегмент (Operational Technology). На залізничному транспорті це є однією з найнебезпечніших кіберзагроз, оскільки може призвести до прямого впливу на безпеку руху та операційну діяльність. Для розуміння механізму латерального переміщення необхідно чітко розрізняти IT та OT-сегменти на залізничному транспорті.

IT-сегмент (Information Technology) призначений для управління бізнес-процесами, адміністративною діяльністю, плануванням, наприклад корпоративні мережі, поштові сервери, бази даних пасажирів/вантажу, системи продажу квитків, ERP-системи, робочі станції офісних працівників.

OT-сегмент (Operational Technology) призначений для управління фізичними процесами, безпосередньо пов'язаними з

рухом поїздів, безпекою та інфраструктурою, наприклад системи автоматики і телемеханіки на мікропроцесорній базі, системи диспетчерського керування, системи моніторингу та управління об'єктами (стрілками, світлофорами, живленням), системи діагностики рухомого складу та колії і т. д.

Типовий сценарій латерального переміщення з IT в OT-сегмент залізничного транспорту включає такі кроки:

1. Початковий доступ (вхідний вектор атаки в IT). Зловмисник отримує доступ до менш захищеного IT-сегменту.

2. Фішинг. Співробітник офісу відкриває шкідливий файл/посилання на робочому комп'ютері (частина IT-мережі).

3. Компрометація. Використання вразливості у вебсервері, що належить до IT-інфраструктури (наприклад сервер планування чи кадрового обліку).

Наступний вид кіберзагрози – це **скомпрометований підрядник.** Використання облікових даних зовнішнього підрядника, який має доступ до IT-мережі. Той, хто атакує, сканує внутрішню IT-мережу, виявляючи інші підключені пристрої та сервери. При цьому використовують вразливості або техніки Pass-the-Hash для отримання облікових даних із високими привілеями (наприклад обліковий запис доменного адміністратора) або протоколів, які забезпечують зв'язок між IT та OT. Це є безпосередньою міграцією загрози. Зловмисник використовує скомпрометовані IT-облікові дані, які помилково мають довіру або обмежений доступ до мережевого шлюзу чи сегментаційної демілітаризованої зони, що з'єднує IT та OT.

Після успішного проникнення в OT-сегмент зловмисник може внести зміни в логіку мікропроцесорних систем, наприклад хибно встановити стрілку не по маршруту прямування, що може призвести до сходження поїзда чи зіткнення, викликати порушення енергопостачання, відключивши або перевантаживши тягові підстанції через систему SCADA, спричинивши зупинку руху. Також таке втручання дає змогу впровадити шкідливе ПЗ (наприклад вірус-шифрувальник) на серверах АСДК, паралізуючи диспетчерське управління. Наслідками такого втручання є втрата контролю за безпекою руху, параліч операційної діяльності (тривалі затримки, відсутність контролю), значні економічні збитки та погіршення репутації.

Запобігти таким атакам можна через сегментацію мережі: жорстке фізичне та логічне розділення IT та OT з мінімальною кількістю дозволених точок доступу, використання «принципу найменших привілеїв» і багатофакторної автентифікації навіть для внутрішніх переходів. Дуже важливим також є постійний моніторинг трафіку: впровадження систем IDS/IPS і Network Monitoring для виявлення аномальної активності (наприклад незвичних команд на контролери СЦБ) у точках стику, а також регулярне оновлення IT-систем, оскільки вони є найчастішим початковим вектором атаки.

Отже, латеральне переміщення є головним етапом у ланцюгу кібератак на критичну залізничну інфраструктуру. Воно перетворює типову офісну кіберзагрозу в пряму загрозу безпеці та життю людей, що потребує впровадження спеціалізованих захисних механізмів, орієнтованих на OT-безпеку [6-9].

4. **Можливості прогнозування кібератак за допомогою ШІ.** Штучний інтелект, використовуючи алгоритми графових нейромереж (GNNs) і глибокого навчання, може аналізувати:

- поведінкові патерни, нетипові запити від IT-мережі (наприклад із робочих місць офісного персоналу ДЦ) до OT-серверів (серверів МПЦ);

- індикатори компрометації (IoC): файли, хеші, IP-адреси, пов'язані з відомими кампаніями APT-груп;

- траєкторію потенційної міграції: аналіз відкритих мережевих портів, прав

доступу і маршрутів зв'язку між IT та OT-мережею.

На основі прогнозу ШІ система SOAR не чекає, поки загроза досягне мети, а автоматично ізолює потенційно заражені елементи. Наприклад, робоча станція (АРМ) диспетчера, яка демонструє аномальну поведінку (надмірні спроби підключення до OT-мережі), може бути автоматично виведена з мережевого сегменту або її мережевий доступ обмежений до мінімально необхідного; автоматичне оновлення правил міжмережевого екрана на міжсегментному шлюзі, що з'єднує IT та OT-мережі, для блокування підозрілих протоколів або джерел.

Збиток від кіберзагрози можна розрахувати за формулою

$$D = T + V, \quad (1)$$

де T – час;

V – швидкість поширення.

Що показує діаграма? Без SOAR (синя лінія): загроза поширюється експоненціально, збитки зростають катастрофічно швидко; із SOAR (червона лінія): автоматична ізоляція миттєво зупиняє атаку, збитки мінімальні. Якщо SOAR → T ≈ 0, то Збиток → min (рис. 7).

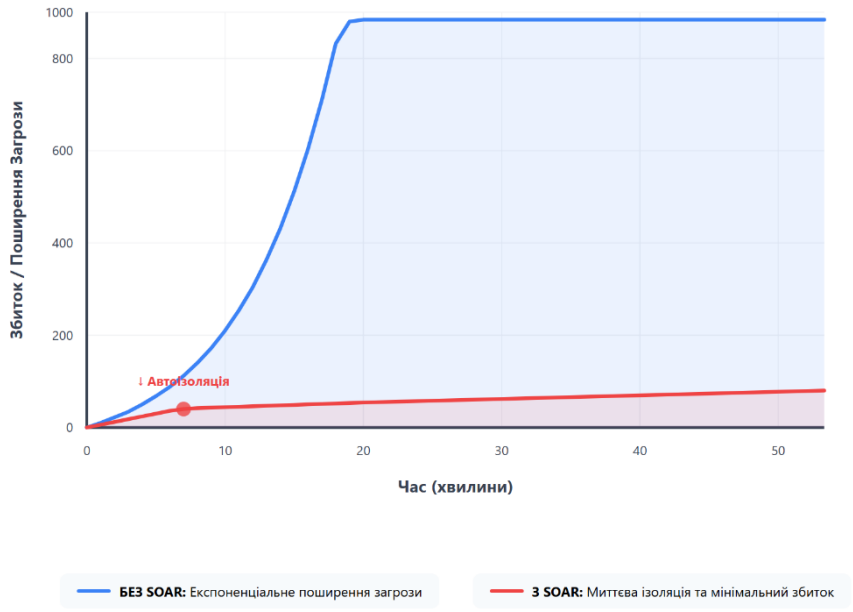

Рис. 7. Діаграма поширення загрози та реакція SOAR

Отже, SOAR допомагає обробляти тисячі інцидентів на день, чого не може зробити жоден центр безпеки, забезпечуючи захист мереж, що постійно зростають. Автоматичне реагування усуває «людський фактор» і забезпечує стабільну, швидку реакцію. Здатність ШІ до прогнозування перетворює реагування з пасивного на активний, превентивний захист.

Висновок. Подальші дослідження необхідно зосередити на інтеграції SOAR з елементами цифрового двійника залізничної мережі, що дасть змогу ШІ «тренувати» сценарії реагування у віртуальному середовищі, доводячи дії до ідеальної автоматичної послідовності. Це відкриє шлях до повної автономної кібербезпеки залізничного транспорту [10].

Список використаних джерел

1. ENISA (European Union Agency for Cybersecurity) / UIC (International Union of Railways). *Cyber Security in Railways: State of Play and Recommendations*. URL: https://www.enisa.europa.eu/publications/railway-cybersecurity (дата звернення: 16.10.2025).

2. Ali Strategies & Zafer Bilal. (2024). Advanced Persistent Threats (APTs): Analysis, Detection, and Mitigation. URL: https://www.researchgate.net/publication/377382446_ Advanced_Persistent_Threats_APTs_Analysis_Detection_and_Mitigation.

3. ДСТУ EN IEC 62443-3-2:2022. Безпека систем промислової автоматизації та управління. Частина 3-2. Оцінювання ризиків безпеки для проєктування системи (EN IEC 62443-3-2:2020, IDT; IEC 62443-3-2:2020, IDT). Чинний 2023-12-31. URL: https://online.budstandart.com.

4. Alam K., Fahad Monir M., Junayed Hossain M., Shorif Uddin M. and Habib M. T. Adaptive Defense: Zero-Day Attack Detection in NIDS With Deep Reinforcement Learning. *IEEE Access*. 2025. Vol. 13. P. 116345-116361. doi: 10.1109/ACCESS.2025.3585445.

5. Almedires M. A., Elkhalil A. & Amin M. Adversarial Attack Detection in Industrial Control Systems Using LSTM-Based Intrusion Detection and Black-Box Defense Strategies. *Journal of Cyber Security and Risk Auditing*. 2025. 3. 4–22. https://doi.org/10.63180/jcsra.thestap.2025.3.2.

6. Чуньвей Се. Ai-DRIVEN advanced persistent threat (apt) attack detection system. Faculty of Cyber Security, Software Engineering, and Computer Science International Humanitarian University. *International scientific journal «Internauka»*. 2025. № 3 (170). P. 129. DOI: 10.25313/2520-2057-2025-3-10815.

7. Використання штучного інтелекту для прогнозування, зупинки та відновлення після інциденту з програмами-вимагачами. *Інтернет-журнал «Кібербез».* URL: https://cybersec.net.ua/statti/858-vykorystannia-shtuchnoho-intelektu-dlia-prohnozuvannia-zupynky-ta-vidnovlennia-pislia-intsydentu-z-prohramamy-vymahachamy.html (дата звернення: 16.10.2025).

8. Veeam Software. *2025. Gartner® Magic Quadrant™ for Backup & Data Protection Platforms.* URL: https://www.veeam.com/gartner-magic-quadrant.html (дата звернення: 26.10.2025).

9. IBM (and Ponemon Institute). *Cost of a Data Breach Report 2025: The AI Oversight Gap.* URL: https://www.bakerdonelson.com/webfiles/Publications/20250822_Cost-of-a-Data-Breach-Report-2025.pdf (дата звернення: 28.10.2025).

10. Deutsche Bahn співпрацюють з NVIDIA для створення цифрового двійника залізниць. *Railway Supply*. 2022. URL: https://www.railway.supply/uk/db-spivpraczyuyut-z-nvidia-dlya-storennya-czifrovogo-dvijnika-zaliznicz/.

Сотник Василь Олександрович, кандидат технічних наук, доцент кафедри автоматики та комп'ютерного телекерування рухом поїздів, Український державний університет залізничного транспорту, Харків, Україна. https://orcid.org/0000-0002-8039-1392. Тел.: +38(057) 730-10-32. E-mail: sotnyk.va@kart.edu.ua.
Алмамедова Мехрібан Гусейнага гизи, аспірантка кафедри автоматики та комп'ютерного телекерування рухом поїздів, Український державний університет залізничного транспорту, Харків, Україна. https://orcid.org/0000-0001-8324-3697. Тел.: +994505378748. E-mail: almamedovamehriban@gmail.com.
Меліхов Анатолій Анатолійович, MIPRO OY, Таллінн, Естонія. ttps://orcid.org/0009-0005-4436-3780. Тел.: +37256711666. E-mail: melikhov.anatoliy@gmail.com.

Sotnyk V. O., Associate Professor of the Department of Automation and Computerized Train Control, Cand. tech. Sciences, Ukrainian State University of Railway Transport. https://orcid.org/0000-0002-8039-1392. Tel.: +38(057) 730-10-32. E-mail: sotnyk.va@kart.edu.ua.

Almammadova Mehriban, graduate student of the Department of Automation and Computerized Train Control, Cand. tech. Sciences, Ukrainian State University of Railway Transport. https://orcid.org/0000-0001-8324-3697.
Tel.: +994505378748. E-mail: almamedovamehriban@gmail.com.
Melikhov Anatolii, Mipro OY, Tallinn, Estonia. https://orcid.org/0009-0005-4436-3780. Tel.: +37256711666.
E-mail: melikhov.anatoliy@gmail.com.

Статтю прийнято 01.12.2025 р.