УДК 656.2:004.9:004.056:004.8 **DOI: https://doi.org/10.18664/ikszt.v30i4.351514**

СОТНИК В. О., доцент кафедри автоматики та комп'ютерного телекерування рухом поїздів, кандидат технічних наук, Український державний університет залізничного транспорту

ХІСМАТУЛІН В. Ш., професор кафедри автоматики та комп'ютерного телекерування рухом поїздів, кандидат технічних наук, Український державний університет залізничного транспорту

СІРОКЛИН І. М., доцент кафедри автоматики та комп'ютерного телекерування рухом поїздів, кандидат технічних наук, Український державний університет залізничного транспорту

ПРИЛИПКО А. А., доцент кафедри автоматики та комп'ютерного телекерування рухом поїздів, кандидат технічних наук, Український державний університет залізничного транспорту

Створення цифрового двійника залізничної мережі та його інтеграція з автоматизацією реагування на кіберзагрози SOAR на базі штучного інтелекту

Анотація. *У статті обґрунтовано необхідність створення цифрового двійника залізничної мережі (ЦД) і досліджено механізми його інтеграції з передовою системою автоматизації реагування на кіберзагрози (SOAR) на базі штучного інтелекту (ШІ). В умовах тотальної цифровізації, впровадження Інтернету речей (IoT) і АСУ/СЦБ залізнична інфраструктура критично розширює поверхню для кібератак, що потребує переходу від реактивних до проактивних методів захисту.*

ЦД визначено як високоточну віртуальну копію фізичної системи (колії, рухомий склад, енергопостачання, СЦБ, АСУТП і мережева інфраструктура), яка слугує інтелектуальним полігоном для кіберзахисту. Детально розглянуто основні функції ЦД: моделювання руху, моделювання інфраструктури, моделювання систем СЦБ і моделювання енергопостачання і зв'язку. Кожна з цих функцій є критично важливою для симуляції кібератак і оцінювання їхнього реального фізичного впливу на безпеку руху, наприклад спроби несанкціонованої зміни положення стрілки чи порушення зв'язку.

Система SOAR подана як головний інструмент, що забезпечує оркестровку (координацію інструментів безпеки) і автоматизацію (виконання контрзаходів за допомогою «плейбуків»), необхідну для миттєвого реагування на інциденти.

Штучний інтелект виступає в ролі «мозку» для ухвалення рішень, використовуючи ЦД для оцінювання наслідків інциденту і вибору оптимального сценарію реагування SOAR із пріоритетом: Безпека руху – Функціональність – Відновлення. Запропоновано концептуальну архітектуру та алгоритм інтеграції, що дає змогу SOAR/ШІ автоматично тестувати контрзаходи у віртуальному середовищі ЦД перед застосуванням їх у реальній мережі, мінімізуючи операційні ризики.

Наведені практичні приклади застосування елементів ЦД і ШІ на залізницях світу (Deutsche Bahn, Network Rail, Італійська Державна Залізнична Група) що підтверджують перспективність технології.

У висновку зазначено, що інтеграція ЦД, SOAR і ШІ є стратегічною необхідністю для підвищення загальної кіберстійкості та надійності залізничного транспорту, особливо в умовах постійних кібернетичних загроз.

***Ключові слова**: цифровий двійник, кібербезпека, симуляція кібератак, проактивний захист, залізничний транспорт.*

Постановка проблеми

Сучасний залізничний транспорт переживає критичний етап технологічної трансформації – тотальну цифровізацію, що включає масове впровадження Інтернету речей (IoT), а також масштабну інтеграцію автоматизованих систем управління (АСУ) і сучасних систем сигналізації, централізації та блокування (СЦБ). Ці інновації, хоча й обіцяють значне підвищення ефективності та пропускної спроможності, водночас кардинально розширюють поверхню для кібератак. Критична залізнична інфраструктура стає однією з головних мішеней для кіберзагроз, які можуть призвести до катастрофічних наслідків, включаючи порушення графіків, економічні втрати і пряму загрозу безпеці руху пасажирів і персоналу. Традиційні, реактивні методи захисту виявляються недостатньо ефективними та надто повільними у високошвидкісному залізничному середовищі, оскільки сучасні кібератаки є складними і швидко проникають у системи оперативного управління. Це створює гостру необхідність у проактивному, повністю автоматизованому та інтелектуальному захисті.

Аналіз останніх досліджень і публікацій

Аналіз останніх досліджень і публікацій свідчить про те, що основним напрямом у відповідь на ці виклики є використання цифрового двійника (ЦД) залізничної мережі та інтеграція його з передовими системами реагування на кіберзагрози. Цифровий двійник (ЦД), визначений як високоточна віртуальна копія фізичної системи (колії, рухомий склад, енергопостачання, СЦБ, АСУТП і мережева інфраструктура), слугує інтелектуальним полігоном, даючи змогу імітувати кібератаки в безпечному середовищі та оцінювати їхній потенційний фізичний вплив на безпеку руху, наприклад спробу несанкціонованої зміни положення стрілки. Функціями ЦД є моделювання руху, моделювання інфраструктури, моделювання систем СЦБ, енергопостачання та зв'язку, які є найбільш критичними щодо безпеки.

SOAR (Security Orchestration, Automation, and Response) – це технологічний підхід, що забезпечує перехід від ручного оброблення інцидентів до автоматизованого. Система SOAR є головним інструментом, який забезпечує координацію різнорідних інструментів безпеки (брандмауери, SIEM, ЦД) для логічного робочого процесу та виконання контрзаходів за допомогою заздалегідь визначених або динамічно згенерованих сценаріїв, відомих як «плейбуки», для миттєвого реагування на інциденти.

Штучний інтелект (ШІ) використовують у SOAR як «мозок» для ухвалення рішень. ШІ використовує ЦД для оцінювання наслідків інциденту і вибору оптимального сценарію реагування з пріоритетом: Безпека руху → Функціональність → Відновлення. ШІ реалізований через машинне навчання та нейромережі для виявлення аномалій, класифікації інцидентів і автоматичного формування плейбуків.

Світовий досвід підтверджує перспективність технології. Ряд країн, таких як Німеччина, Велика Британія, Італія, ведуть активні розробки та впровадження в цьому напрямі. Створюють фотореалістичні ЦД для навчання ШІ, які аналізують середовище та реагують на нетипові події, а також оптимізують диспетчерське управління. Використовують ЦД також для управління інфраструктурою та складними проєктами модернізації.

Наукова думка і практичний досвід залізничних операторів зосереджені на трьох цих взаємопов'язаних технологічних стовпах для забезпечення кіберстійкості. Основний тренд полягає в синергетичному об'єднанні цих трьох технологій, що допомагає залізничному транспорту перейти до проактивного, інтелектуального кіберзахисту, який може самостійно виявляти, оцінювати і нейтралізувати загрози.

Виділення невирішеної частини загальної проблеми

Загальна проблема полягає в переході до проактивного, інтелектуального захисту критичної залізничної інфраструктури в умовах зростаючих кіберзагроз. Хоча необхідність інтеграції ЦД, SOAR і ШІ визнана як стратегічна, невирішеною частиною залишається детальна, практична реалізація цієї синергії, ураховуючи відсутність загальноприйнятої концептуальної архітектури і алгоритму інтеграції, який би давав змогу системі SOAR/ШІ автоматично тестувати контрзаходи у віртуальному середовищі ЦД перед їх застосуванням у реальній мережі. Існуючі методи потребують розроблення чітких механізмів двостороннього обміну інформацією між ЦД і SOAR, де ЦД надає контекст фізичної безпеки, а SOAR використовує ЦД для симуляційного відтворення інциденту і верифікації плейбуків. Іншою недостатньо розв’язаною проблемою є необхідність розроблення уніфікованих протоколів обміну даними між ЦД і SOAR і вдосконалення моделей ШІ, які були б здатні прогнозувати складні, багатоетапні кібератаки та керувати рішеннями SOAR із пріоритетом «Безпека

руху – Функціональність – Відновлення». Проблемою впровадження ЦД також є високі фінансові інвестиції, потреба у великих обсягах якісних даних і, що особливо складно, точне моделювання логіки систем залізничної автоматики (СЦБ та АСУТП).

Постановка завдання

Мета цієї статті полягає в детальному обґрунтуванні необхідності розроблення концептуальної архітектури створення цифрового двійника залізничної мережі, а також дослідженні та формулюванні механізмів його інтеграції з передовою системою SOAR.

Для досягнення цієї мети необхідно обґрунтувати необхідність створення ЦД для підвищення кіберстійкості залізничної інфраструктури в умовах цифровізації та зростання кіберзагроз і детально розглянути і описати основні функції ЦД, критично важливі для кіберзахисту. Також необхідно дослідити і навести принципи роботи і компоненти системи SOAR (оркестровка та автоматизація) і роль штучного інтелекту в ній, запропонувати концептуальну архітектуру інтеграції ЦД і SOAR на базі ШІ, включаючи механізми двосторонньої взаємодії (ЦД → SOAR: контекст фізичної безпеки; SOAR → ЦД: симуляція для верифікації контрзаходів). Також надзвичайно важливим є розроблення алгоритму, який використовує результати симуляції в ЦД для вибору оптимального сценарію реагування SOAR із пріоритетом: Безпека руху – Функціональність – Відновлення.

1. Вступ

Сучасний залізничний транспорт у всьому світі, зокрема в Україні, знаходиться на критичному етапі технологічної трансформації, відомому як цифровізація. Для цього процесу характерні інтенсивне впровадження передових технологій, таких як Інтернет речей (IoT), який охоплює рухомий склад та інфраструктуру, а також масштабна інтеграція автоматизованих систем управління (АСУ) і сучасних систем сигналізації, централізації та блокування (СЦБ), що гарантують безпеку та ефективність руху поїздів [3]. Ці інновації, хоча й обіцяють значне підвищення пропускної спроможності, оптимізацію витрат і покращення обслуговування, водночас кардинально розширюють поверхню для кібератак [1].

Як наслідок, критична залізнична інфраструктура стає однією з головних мішеней для кіберзагроз, які можуть мати катастрофічні наслідки – від порушення графіків руху та значних економічних втрат до прямої загрози безпеці пасажирів і персоналу. Існуючі традиційні методи захисту, що зазвичай покладені на реактивне виявлення загроз і ручну обробку інцидентів, виявляються недостатньо ефективними та занадто повільними в динамічному, високошвидкісному залізничному середовищі. Сучасні кібератаки є складними, багатоетапними та здатними швидко проникати в системи оперативного управління. Отже, виникає гостра, невідкладна необхідність у проактивному, повністю автоматизованому та інтелектуальному захисті [2].

Ураховуючи ці виклики, основним напрямом розвитку стає створення цифрового двійника залізничної мережі (ЦД). ЦД – це високоточна віртуальна копія реальної фізичної системи, яка включає моделі колії, рухомого складу, енергопостачання, а головне – моделі систем СЦБ, АСУТП і мережевої інфраструктури, які є об'єктами кібератак [2]. Використання ЦД дає змогу імітувати кібератаки в безпечному віртуальному середовищі, оцінювати їхній потенційний вплив на реальні процеси (наприклад на роботу стрілочних переводів чи безпеку руху поїздів), і в такий спосіб тестувати і вдосконалювати контрзаходи для їх застосування на реальній мережі [12].

Мета цієї статті полягає в детальному обґрунтуванні необхідності та розробленні концептуальної архітектури створення такого цифрового двійника залізничної мережі, а також дослідженні механізмів його інтеграції з передовою системою SOAR (Security Orchestration, Automation, and Response). Інтеграція має бути побудована на базі алгоритмів штучного інтелекту (ШІ), що допоможе створити самоналагоджувальну систему, здатну не просто реагувати на інциденти, а й прогнозувати їх, оцінювати ризики через симуляції в ЦД і миттєво застосовувати оптимальні автоматизовані сценарії реагування [4]. Така синергія ЦД, SOAR і ШІ є вирішальною для підвищення загальної кіберстійкості залізничного транспорту.

У статті послідовно розглянуто теоретичні засади ЦД, принципи роботи SOAR, роль ШІ у цьому комплексі, запропоновано архітектуру інтеграції та проаналізовано практичні сценарії її застосування [3].

2. Теоретичні основи цифрового двійника залізничної мережі

В умовах тотальної цифровізації залізничного транспорту концепція цифрового двійника набуває стратегічного значення як фундаментальний інструмент управління, оптимізації та, що особливо важливо, забезпечення кібербезпеки [2]. ЦД являє собою високоточну віртуальну репліку фізичних активів, процесів і систем, що допомагає аналізувати, моделювати і прогнозувати їхню поведінку в реальному часі [7]. Цифровий двійник у контексті залізниці – це динамічна, інтегрована віртуальна модель, яка відображає фізичний стан, функціональність і взаємозв'язки усіх основних елементів залізничної мережі [2]. Розглянемо основні функції ЦД.

Моделювання руху – це процес створення високоточної, динамічної віртуальної симуляції всіх аспектів переміщення рухомого складу та пов'язаних із ним операцій на мережі в реальному часі [10]. Ця функція є багатошаровою і потребує інтеграції даних від усіх підсистем залізниці. Функція охоплює віртуальне відтворення таких основних елементів, як

рухомий склад, інфраструктура, диспетчерські рішення та зовнішні фактори. Ефективність моделювання руху ЦД залежить від постійної синхронізації з фізичною мережею через системи СЦБ, системи позиціонування, системи управління рухомим складом і АСУ диспетчеризації. ЦД використовує ці дані, щоб постійно корегувати свою віртуальну модель, забезпечуючи «живий» двійник руху. Моделювання руху виконує ряд критично важливих завдань, таких як прогноз графіка руху, аналіз сценаріїв, оптимізація енергоспоживання, аналіз пропускної спроможності дільниць та інше [9].

Моделювання руху є критично важливим для інтеграції з кібербезпекою. Якщо система SOAR виявляє кібератаку на СЦБ (наприклад спробу несанкціонованої зміни положення стрілки), ЦД негайно симулює цю зміну у своєму середовищі [5]. Це дає змогу миттєво оцінити реальний фізичний наслідок атаки (призведе це до зіткнення чи лише затримки, чи зможе система безпеки цьому запобігти) [12]. ШІ, що керує SOAR, використовує дані моделювання руху з ЦД, щоб визначити пріоритет інциденту: атака, що загрожує безпеці руху, отримає найвищий пріоритет і викличе найбільш агресивний автоматичний плейбук SOAR (наприклад аварійне відключення певного сегмента мережі) [3]. Перед тим як SOAR застосує контрзахід (наприклад ізоляцію певного мережевого сегмента), ЦД може швидко промоделювати, як це вплине на графік руху (наприклад чи зупиняться інші поїзди), забезпечуючи, що рішення про кібербезпеку не спричинить значних операційних збоїв, якщо це не необхідно для безпеки [8].

Моделювання інфраструктури. Функція моделювання інфраструктури є основною частиною цифрового двійника залізничної мережі. Вона забезпечує створення статичної та динамічної віртуальних копій всіх фізичних активів, які не є рухомим складом, але критично важливі для функціонування та безпеки руху [11]. Ця функція виходить за рамки простого 3D-моделювання, інтегруючи інженерні, геометричні, експлуатаційні та діагностичні дані. Моделювання інфраструктури охоплює створення детальних віртуальних моделей основних фізичних активів (табл. 1).

Таблиця 1

Фізичні активи моделювання інфраструктури залізничної мережі

Категорія активу	Елемент моделювання	Критичний параметр
Колійне господарство	Колії, земляне полотно, баластна призма, шпали	Геометрія колії (профіль, план), знос рейок, наявність дефектів (тріщини, відколи), допустиме навантаження
Штучні споруди	Мости, шляхопроводи, тунелі, водопропускні труби	Несуча здатність, рівень деформації, вік, результати останніх інспекцій.
Об'єкти СЦБ	Стрілочні переводи, світлофори, колійні датчики, рейкові кола, переїзди	Фактичний технічний стан (нагрів, вібрація), швидкість спрацьовування, логіка керування
Енергопостачання	Контактна мережа, тягові підстанції, трансформатори	Напруга, струм, знос контактного дроту, теплові режими роботи обладнання
Станційні об'єкти	Платформи, вокзали, депо	Розміри, пропускна спроможність, навантаження

Точність і актуальність ЦД залежить від безперервного потоку даних у реальному часі, що надходять від діагностичних систем, сенсорів IoT, системи SCADA, BIM-моделі (використання інформаційних моделей будівель (Building Information Modeling)) [13]. ЦД забезпечує синхронізацію цих різнорідних даних для створення єдиної, цілісної картини стану інфраструктури. Моделювання інфраструктури використано для прогнозного технічного обслуговування, аналізу навантаження та ресурсів, оцінювання впливу змін [9].

Моделювання інфраструктури є життєво необхідним для кібербезпеки. Це дає можливість зрозуміти, як кібератака вплине на логіку керування (наприклад втручання в АСУТП енергопостачання або СЦБ), її фізичну структуру, наприклад призведе атака до перевантаження підстанції чи некоректного спрацьовування стрілочного переводу, що загрожує безпеці руху [12]. ЦД допомагає виявити слабкі місця, де кібератака може завдати максимальної фізичної шкоди, що дає змогу системі SOAR пріоритезувати захист найбільш критичних елементів інфраструктури. Після виявлення атаки ЦД може симулювати сценарії аварійного відновлення чи переконфігурації об'єктів інфраструктури (наприклад перемикання на резервну лінію енергопостачання), забезпечуючи, що дії системи SOAR не спричинять додаткових пошкоджень або ризиків [8].

Моделювання систем СЦБ (сигналізація, централізація, блокування). Ця функція є найбільш критичною з точки зору безпеки та кіберстійкості в цифровому двійнику залізничної мережі, оскільки ці системи безпосередньо контролюють рух поїздів і запобігають їх зіткненням [5]. Це не просто віртуальне відображення обладнання, а точна симуляція логіки, алгоритмів і взаємозалежностей, що забезпечують безвідмовну роботу систем залізничної автоматики. Моделювання СЦБ у ЦД охоплює

віртуальне відтворення чотирьох головних рівнів, що забезпечують безпеку руху (табл. 2).

Таблиця 2

Рівні моделювання СЦБ

Рівень СЦБ	Елемент моделювання	Основна функція в ЦД
Сигналізація	Світлофори, логіка їхніх показань	Симуляція залежності показань від зайнятості колій і встановлених маршрутів
Централізація	Маршрутно-релейна, мікропроцесорна або комп'ютерна централізація	Точне відтворення **логіки блокування** (взаємозалежності між стрілками та світлофорами) і механізму встановлення маршрутів
Блокування	Автоматичне колійне блокування, системи ERTMS/ETCS	Моделювання системи контролю цілісності колії та розмежування рухомого складу на перегонах
Пристрої керування	Стрілочні переводи, рейкові кола, датчики шляху	Моделювання фізичного стану (час переведення стрілки, справність рейкового кола) та електричної взаємодії

Для забезпечення точності ЦД систем СЦБ використовують дані від мікропроцесорних і релейних систем СЦБ (дані про фактичний стан логічних елементів, встановлені маршрути і помилки), діагностичних комплексів (інформація про технічний стан елементів (наприклад струми, напруги, час спрацьовування реле чи стрілочних приводів)), конфігураційних файлів (завантаження фактичної програмної логіки (залежностей) із мікропроцесорних систем СЦБ у віртуальне середовище. ЦД забезпечує динамічну реплікацію: будь-яка зміна в реальній системі СЦБ (наприклад встановлення маршруту диспетчером) миттєво буде відображено у віртуальній моделі) [5].

Моделювання СЦБ є незамінним для тестування нової чи зміненої логіки СЦБ перед її впровадженням у реальну систему. Це допомагає виявити логічні помилки, які можуть призвести до небезпечних ситуацій (наприклад маршрут встановлений на зайняту колію), симуляції відмов обладнання (наприклад несправність рейкового кола, відмова стрілочного привода) та оцінювання реакції резервних систем і оператора та моделювання впливу швидкості спрацьовування СЦБ на пропускну спроможність станції та залізничної дільниці [14].

Крім того, моделювання СЦБ є найважливішим компонентом для кіберзахисту критичної залізничної інфраструктури. Якщо кібератака спрямована на зміну логіки СЦБ (наприклад зловмисник намагається змінити показання світлофора або перевести стрілку), ЦД негайно відтворює цю атаку в симуляційному середовищі [12]. Це дає змогу ШІ/SOAR миттєво оцінити, чи призведе ця віртуальна зміна до небезпечного фізичного сценарію (зіткнення, сходження з рейок). Також це допомагає системі SOAR тестувати свої автоматизовані контрзаходи (наприклад ізоляція інфікованого пристрою, переведення системи в безпечний стан) у ЦД, гарантуючи, що ці дії не створять додаткової загрози безпеці руху. ЦД використано для генерації тисяч синтетичних сценаріїв кібератак на СЦБ, які неможливо створити в реальному середовищі. Ці дані використовують для навчання алгоритмів ШІ системи SOAR розпізнавати навіть найменші аномалії в роботі критичної логіки [4]. Крім того, ЦД надає SOAR критичний контекст безпеки руху. Іншими словами, інцидент, пов'язаний із СЦБ, який створює пряму загрозу безпеці, буде автоматично пріоритезований вище, ніж інцидент, що стосується лише офісної мережі, що є основою для ефективного автоматизованого реагування [6].

Моделювання енергопостачання та зв'язку. Моделювання енергопостачання та зв'язку в цифровому двійнику залізничної мережі є критично важливим, оскільки воно відображає життєзабезпечувальні системи, без яких неможливий рух поїздів, робота СЦБ і передавання критичних даних [11]. Ця функція зосереджена на динамічному відтворенні мережевих, електричних і комунікаційних параметрів. Моделювання енергопостачання охоплює всі елементи, що забезпечують живлення рухомого складу і стаціонарних об'єктів: контактну мережу та електрифікацію, тягові підстанції (ТП) і роздільні пункти, енергопостачання непрофільних споживачів. Кібератаки, спрямовані на системи управління

підстанціями (SCADA/АСУ ТП), можуть призвести до відключення живлення критичних ділянок. ЦД симулює цей сценарій, показуючи, як швидко зупиняться поїзди та як відмовлять системи СЦБ [12]. ЦД дає змогу також SOAR/ШІ змоделювати, чи зможе автоматичне перемикання на резервну лінію (як контрзахід проти атаки) бути виконане без збою в електропостачанні, що є необхідним для безпеки [8]. На основі моделювання енергосистеми ШІ може ухвалити рішення: у разі кібератаки краще повністю відключити живлення для локалізації чи перевести навантаження на сусідню підстанцію [4].

Моделювання зв'язку відображає мережеву топологію і трафік, необхідний для роботи всіх критичних систем. У цьому випадку предметом та обсягом моделювання є мережева топологія, протоколи і трафік, бездротовий зв'язок (GSM-R/LTE-R). ЦД допомагає змоделювати кібератаки, спрямовані на порушення комунікацій: DDoS-атаки, сканування мережі, маніпуляція пакетами, компрометація маршрутизаторів [12]. Основним є моделювання того, як втрата зв'язку на певній ділянці (наприклад між пристроєм СЦБ і центром керування) вплине на функціонування (наприклад перейде поїзд у безпечний режим «стоп» чи, навпаки, втратить контроль) [5]. Система SOAR може автоматично генерувати контрзаходи (наприклад застосування правил брандмауера, ізоляція інфікованого сегмента). ЦД моделює, чи не порушить ця ізоляція критичний зв'язок між іншими безпечними системами, гарантуючи, що кіберзахист не призведе до операційного колапсу [3]. ШІ використовує модель нормального трафіку ЦД для виявлення найменших аномалій, що можуть свідчити про початок атаки (наприклад нетиповий обсяг чи тип даних, що передано на пристрої СЦБ) [4]. Отже, моделювання енергопостачання та зв'язку забезпечує контекст життєзабезпечення, даючи змогу системі SOAR на базі ШІ ухвалювати рішення, що є обґрунтованими як із точки зору кібербезпеки, так і операційної цілісності та безпеки руху поїздів [9].

ЦД – це потужна платформа для тестування змін, оптимізації ресурсів та, що є головним для цієї статті, аналізу вразливостей і симуляції кібератак [15].

Складові елементи ЦД залізничної мережі. Для забезпечення комплексної та функціональної реплікації реального середовища, ЦД залізниці має включати кілька взаємопов'язаних рівнів моделей:

1. ***Моделі фізичних активів.*** Ці моделі є фізичними об'єктами, які можна безпосередньо атакувати або вплив на які є критичним для функціонування:

- колії (геометрія, стан);
- рухомий склад (локомотиви, вагони);
- стрілочні переводи та інші виконавчі пристрої [16].

2. ***Моделі систем управління та автоматики.*** Відображають логіку роботи і взаємодію керуючих систем, які забезпечують безпеку та оперативність:

- системи європейської системи управління залізничним рухом (ERTMS/СЦБ);
- автоматизовані системи управління технологічними процесами (АСУТП) [5].

3. ***Моделі кіберпростору.*** Цей рівень є вирішальним для питань кібербезпеки, оскільки він моделює шлях, яким може бути здійснена атака:

- мережева топологія (маршрутизатори, комутатори, мережеві сегменти);
- комунікаційні протоколи, що використані в залізничних системах (наприклад Modbus, OPC UA, протоколи СЦБ) [12].

Інтеграція ЦД є важливим кроком для створення системи проактивної кібербезпеки. Головна перевага полягає в можливості імітації кібератак і оцінювання їхнього впливу на реальні процеси (безпека руху) [12]. Це дає змогу моделювати «що, якщо», виявляти приховані вразливості в системах СЦБ і АСУТП до того, як їх використає зловмисник, тестувати сценарії кібератак, наприклад спробу дистанційного переведення стрілки, та оцінювати реальні фізичні наслідки цього втручання, розробляти і перевіряти контрзаходи та сценарії відновлення в безпечному віртуальному середовищі без жодного ризику для реальної залізничної мережі [8].

Отже, ЦД перетворюється з простого інструменту моделювання на інтелектуальний полігон для кіберзахисту, який є основою для інтеграції з передовими системами реагування [17].

3. Кібербезпека залізничної інфраструктури та концепція SOAR (Security Orchestration, Automation, and Response)

Питання кібербезпеки набуває першочергового значення для залізничного транспорту, який сьогодні є високоавтоматизованою критичною інфраструктурою. Зростання залежності від цифрових технологій потребує переходу від традиційних, реактивних методів захисту до проактивних, інтелектуальних систем реагування [2].

Залізнична інфраструктура є унікальною мішенню, оскільки кібератаки на неї можуть мати прямі фізичні наслідки. Специфіка кіберзагроз на залізниці полягає у спрямованості атак на критичні системи, такі як системи СЦБ, автоматизовані системи управління технологічними процесами (АСУТП), системи диспетчеризації [12]. Отже, потенційний вплив кібератак на залізниці не лише стосується фінансових втрат, але і загрожує безпеці руху та графіка.

В умовах зростання кількості кіберінцидентів необхідний інструмент, здатний оперативно та ефективно обробляти великі масиви даних і автоматично реагувати на загрози. Цим інструментом є концепція SOAR. Вона являє собою технологічний підхід, що забезпечує перехід від ручного оброблення інцидентів до автоматизованого [3]. Основним компонентом SOAR є **оркестровка.** Це

фундаментальна складова SOAR, що по суті є координаційним центром системи кібербезпеки. Вона забезпечує ефективну взаємодію та управління різнорідними, часто роз'єднаними інструментами безпеки та IT-системами, які функціонують у залізничній мережі. Оркестровка – це технологічний процес, що об'єднує та координує виконання завдань і функцій кількох різних інструментів безпеки (таких як брандмауери, системи виявлення вторгнень (IDS), системи SIEM, антивірусні сканери, системи контролю доступу тощо) для досягнення спільної мети [3]. Ця складова SOAR має головну відмінність порівняно з простою автоматизацією: автоматизація виконує *окремі* завдання, наприклад блокує одну підозрілу IP-адресу, а оркестровка *координує послідовність* цих завдань, забезпечуючи логічний робочий процес.

На залізничному транспорті, де існує величезна кількість критичних систем (від офісної мережі до АСУТП енергопостачання та СЦБ), оркестровка відіграє вирішальну роль, оскільки створює єдиний центр управління, забезпечує контекстуалізацію (збирає інформацію про інцидент з усіх відповідних систем: від SIEM (для даних кіберпростору) до цифрового двійника (для контексту фізичного впливу) і систем управління активами (для визначення важливості пристрою)) і підтримує безпеку руху [12].

Оркестровка як функція реалізована через API-інтерфейси (механізми для зв'язку системи SOAR з іншими системами безпеки та IT-інструментами), робочі процеси (візуальне подання логічних послідовностей дій, які має виконати система у відповідь на інцидент) і централізовану базу знань (зберігання інформації про інструменти, їхні можливості та протоколи взаємодії) [3].

Отже, оркестровка є тим «диригентом», який гарантує, що всі інструменти кібербезпеки в динамічному середовищі залізниці працюють злагоджено, швидко і, найголовніше, з урахуванням безпеки руху.

Автоматизація є другою важливою складовою концепції SOAR і прямим виконавчим механізмом, який реалізує координаційні вказівки, визначені оркестровкою.

Це технологія, що дає змогу виконувати рутинні, повторювані та часто залежні від часу завдання у сфері кібербезпеки без прямої участі людини-аналітика. Вона використовує заздалегідь визначені або динамічно згенеровані сценарії, відомі як «плейбуки», для миттєвого реагування на інциденти. Сутність автоматизації полягає у швидкості та масштабованості. В умовах, коли аналітик витрачає години на збір інформації, аналіз і виконання контрзаходів, автоматизація виконує ті самі дії за секунди або мілісекунди.

Автоматизація в SOAR охоплює два основні типи завдань – автоматизацію збору даних, збагачення контексту і автоматизацію реакції і усунення наслідків. ***На першому етапі*** після виявлення інциденту автоматизація виконує рутинні перевірки: *збір інформації* (автоматичний запит до внутрішніх систем (наприклад SIEM, системи управління активами, цифровий двійник) для отримання повних даних про атакований пристрій), *розвідка загрози* (автоматична перевірка підозрілих IP-адрес, хешів файлів чи доменних імен у зовнішніх базах даних загроз), *перевірка журналів* (автоматичний пошук по журналах (логін) на інших пристроях для визначення масштабу компрометації). ***На другому етапі*** виконувані безпосередні дії, спрямовані на локалізацію та нейтралізацію загрози: *мережеві контрзаходи* (автоматичне блокування трафіку з підозрілих IP-адрес на брандмауерах), *управління кінцевими точками* (віддалений запуск антивірусного сканування, ізоляція інфікованого пристрою в окремий мережевий сегмент), *управління ідентичністю* (автоматичне скидання паролів або блокування облікових записів, які були скомпрометовані), *взаємодія з ЦД* (автоматичне ініціювання симуляції інциденту в цифровому двійнику для оцінювання фізичного ризику) [3, 8].

Хоча терміни часто плутають, вони мають чітке розмежування: оркестровка визначає послідовність дій, які потрібно виконати, і з'єднує необхідні інструменти (*диригент*), а автоматизація виконує самі завдання у визначеній послідовності без втручання людини (*виконавець*). Оркестровка створює логічний потік, а автоматизація наповнює його технічним змістом і швидкістю.

Впровадження автоматизації є життєво необхідним для залізничного транспорту через такі фактори, як необхідність миттєвої реакції, гарантування безпеки руху як пріоритету і зниження людського фактора в технологічному процесі [12]. Завдяки автоматизації SOAR перетворює процес кібербезпеки на ефективну, високошвидкісну та надійну систему, здатну захищати критичну інфраструктуру в режимі 24/7. SOAR допомагає значно скоротити час реагування, підвищити точність рішень і звільнити експертів-аналітиків для вирішення найскладніших, нетипових завдань.

Інтеграція штучного інтелекту в SOAR є необхідною умовою для створення по-справжньому проактивної та інтелектуальної системи безпеки. ШІ забезпечує когнітивні можливості, які дають змогу автоматизації вийти за межі простих, попередньо визначених правил. Роль ШІ в SOAR реалізована через машинне навчання (МН) для виявлення аномалій і прогнозування загроз, нейромережі – для класифікації інцидентів і визначення пріоритетів та автоматичного формування «плейбуків» (сценаріїв реагування) [4]. Використання ШІ перетворює SOAR на адаптивну систему, яка здатна не тільки автоматично реагувати, але й постійно вчитися та самовдосконалюватися [1].

4. Інтеграція цифрового двійника та SOAR на базі ШІ

Інтеграція цифрового двійника залізничної мережі із системою SOAR на базі штучного інтелекту є важливою для підвищення кіберстійкості. Ця синергія дає змогу вийти за межі обмежень існуючих методів захисту, використовуючи ЦД як полігон для імітації кібератак і оцінювання їхнього впливу на безпеку руху без ризику для реальної мережі [2].

Інтеграція цифрового двійника та SOAR на базі ШІ створює комплексний цикл кіберфізичного захисту, що складається з трьох основних елементів (рис. 1) [11].

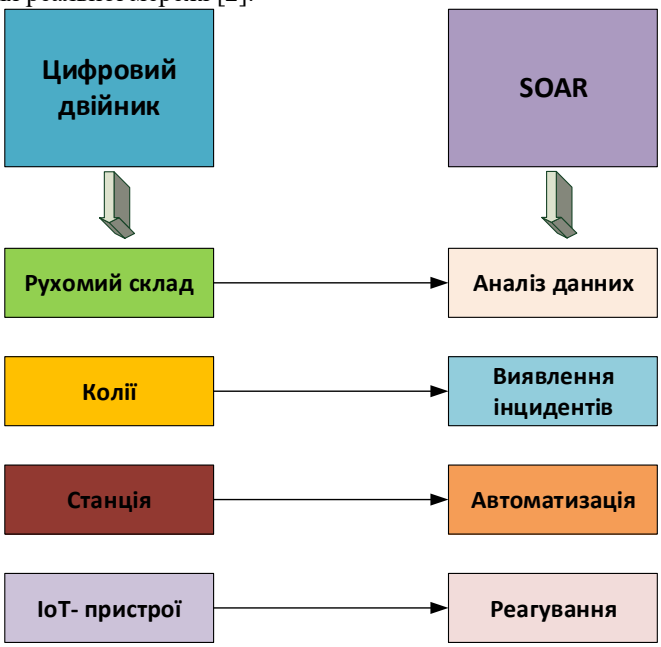

Рис. 1. Архітектура інтеграції цифрового двійника та SOAR на базі ШІ для залізничної мережі

1. **Цифровий двійник** використовують як середовище моделювання та аналізу контексту. Він надає віртуальну копію фізичних активів (колії, рухомий склад, стрілочні переводи), систем управління (ERTMS/СЦБ, АСУТП) і кіберпростору (мережева топологія, протоколи) [7].

2. **Система SOAR** діє як система реагування, що відповідає за оркестровку, автоматизацію та виконання контрзаходів [3].

3. **Штучний інтелект** виконує функцію «мозку» для ухвалення рішень, забезпечуючи інтелектуальну ланку між ЦД та SOAR [4].

Ефективність системи залежить від двостороннього обміну інформацією між ЦД та SOAR (рис. 2).

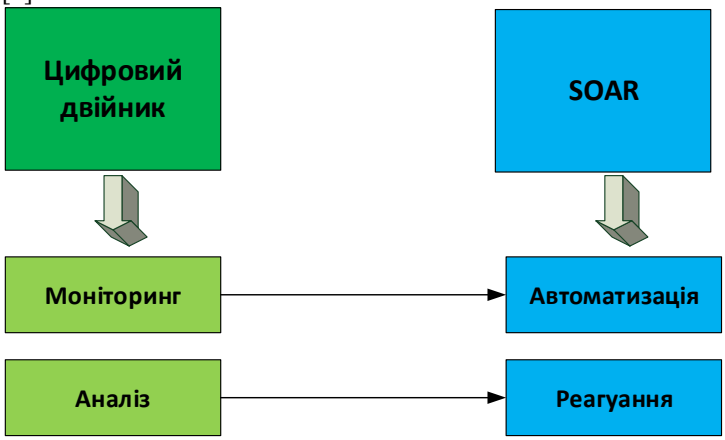

Рис. 2. Механізми взаємодії цифрового двійника та SOAR на базі ШІ для залізничної мережі

ЦД → SOAR: контекст фізичної системи. На цьому етапі ЦД надає SOAR точний, життєво важливий контекст про поточний стан фізичних систем. У разі виявлення кіберінциденту SOAR звертається до ЦД, щоб оцінити фізичні наслідки. Наприклад, ЦД може відповісти на запитання «чи вплине відключення комутатора X на безпеку руху поїзда Y?». Ця інформація допомагає SOAR, керованому ШІ, коректно класифікувати інцидент і визначити його реальний пріоритет: кібератака на офісну мережу має менший пріоритет, ніж атака на СЦБ, яка загрожує зіткненням [12].

SOAR → ЦД: симуляційне відтворення інциденту. Цей механізм використовують для верифікації та тестування контрзаходів. SOAR передає дані про виявлені інциденти для їхнього симуляційного відтворення в безпечному середовищі ЦД. Це дає змогу імітувати наслідки кібератаки, наприклад спробу несанкціонованої зміни сигналу чи переведення стрілки. Перед застосуванням будь-яких автоматизованих контрзаходів (плейбуків) (наприклад ізоляція мережевого сегмента) їх спочатку тестують у ЦД. Це гарантує, що дія SOAR не призведе до небажаних операційних чи безпекових наслідків [8].

Штучний інтелект є «мостом», що забезпечує розумну взаємодію між віртуальним середовищем цифрового двійника залізничної мережі та системою автоматизованого реагування SOAR. Цей інтегрований підхід створює адаптивну систему, здатну як автоматично реагувати на загрози, так і проактивно їх прогнозувати, використовуючи ЦД як віртуальний полігон для ухвалення оптимальних рішень у режимі реального часу [15].

Сам алгоритм реалізовано через етапи, зображені на рис. 3.

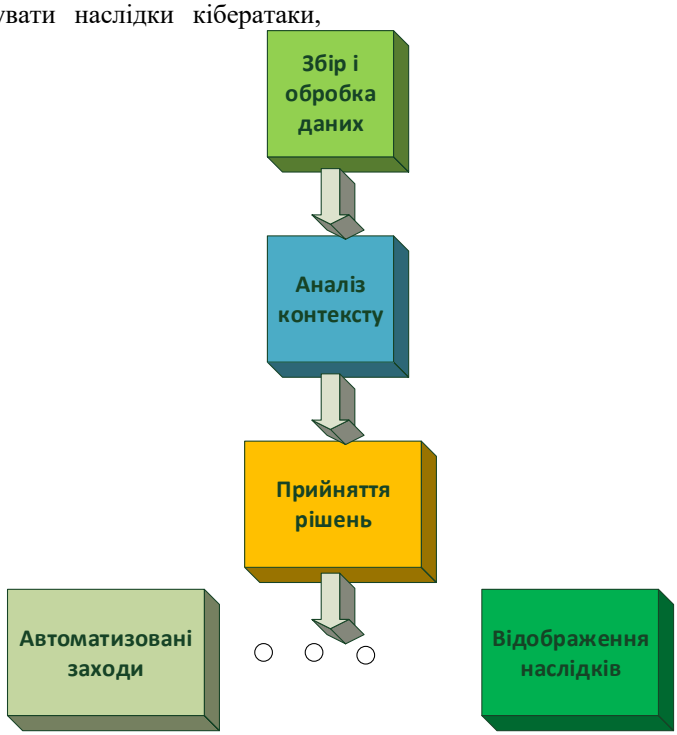

Рис. 3. Алгоритм ШІ для інтеграції ЦД та SOAR у залізничну інфраструктуру

Етап 1. Збір і обробка даних. На цьому початковому етапі збирають дані з реальної залізничної мережі, що необхідні для симуляції та аналізу [6].

Етап 2. Аналіз контексту. Зібрані дані аналізують для визначення контексту інциденту чи ситуації. Нейромережі допомагають на цьому етапі, класифікуючи інциденти і визначаючи їхні пріоритети [4].

Етап 3. Ухвалення рішення. Це критичний етап, який ґрунтований на симуляції в ЦД. На цьому етапі ШІ використовують для оцінювання наслідків інциденту, який був промодельований у віртуальному середовищі ЦД. На основі цього ШІ вибирає оптимальний сценарій реагування SOAR. При цьому вибір завжди керований чітким пріоритетом: ***Безпека руху – Функціональність – Відновлення*** [12].

Після ухвалення рішення відбувається реалізація **автоматизованих заходів** (запускають відповідні сценарії реагування SOAR, вибрані ШІ, для усунення загрози чи інциденту) і **відображення наслідків (**результати виконання заходів фіксують і аналізують) [3].

Для підтримки актуальності та ефективності алгоритму необхідне ***динамічне оновлення ЦД.*** Застосування машинного навчання є критично важливим для постійного корегування та вдосконалення моделей ЦД. Корегують моделі ЦД на основі даних реального часу та фактичних кіберінцидентів. Машинне навчання також використовують для виявлення аномалій і

прогнозування загроз, що забезпечує актуальність віртуального середовища ЦД для симуляції [4]. Цей інтегрований підхід створює адаптивну систему, здатну не лише автоматично реагувати на загрози, але й проактивно прогнозувати їх, використовуючи віртуальний полігон ЦД для ухвалення оптимальних рішень у режимі реального часу [15].

5. Практичні аспекти застосування та перспективи розвитку цифрового двійника залізничної мережі

Цифровий двійник залізничної мережі є передовою технологією, що створює віртуальну копію реальної інфраструктури, даючи змогу моделювати, аналізувати і прогнозувати її стан [2]. Впровадження ЦД має вирішальне значення для підвищення стійкості, безпеки та ефективності залізничного транспорту [9]. Його використання відкриває нові можливості для кібербезпеки та операційної стійкості залізничної мережі. ЦД слугує безпечним полігоном для тестування нових плейбуків (сценаріїв автоматизованого реагування) SOAR-систем. Це допомагає перевіряти ефективність автоматизованих дій перед їх застосуванням у реальній мережі. Через симуляцію різних кібератак і загроз у віртуальному середовищі ЦД фахівці можуть **виявляти вразливості** інфраструктури, які залишаються непоміченими традиційними засобами захисту [8]. У разі успішної атаки ЦД може бути використаний для **автоматизованої переконфігурації мережі**. Рішення про відновлення попередньо перевіряють і відпрацьовують у двійнику, забезпечуючи мінімальний час простою [10].

Однак, незважаючи на значні переваги, впровадження ЦД залізничної мережі стикається з низкою серйозних проблем. Розроблення та підтримка повноцінного цифрового двійника потребує значних фінансових інвестицій. Крім того, для точного моделювання необхідні великі обсяги якісних, актуальних даних із реальної мережі. Особливу складність становить моделювання систем залізничної автоматики, таких як системи СЦБ та АСУТП (автоматизовані системи управління технологічними процесами). Також існують питання, пов'язані з розробленням єдиних стандартів і регуляторної бази для застосування ЦД [2, 5].

Багато країн світу, зокрема Європа, Азія та США, уже мають приклади впровадження окремих елементів ЦД і SOAR на своїх залізницях. Так, німецький залізничний оператор Deutsche Bahn (DB) є одним із лідерів у впровадженні ЦД і штучного інтелекту. У рамках проєкту Digitale Schiene Deutschland (DSD) DB спільно з NVIDIA створює фотореалістичного цифрового двійника залізничних ліній і станцій (наприклад для S-Bahn Гамбурга), щоб повністю симулювати автоматичне обслуговування поїздів у всій мережі. Двійника використовують для навчання ШІ, який має безперервно аналізувати навколишнє середовище та оптимально реагувати на нетипові події (наприклад падіння предметів на колію або поява людини біля краю платформи) [1]. Це допомагає розробляти і тестувати системи сприйняття та управління без ризику для реальної інфраструктури. DB активно впроваджує ШІ, який спирається на цифрову копію мережі, для вирішення конфліктів між поїздами в системах диспетчерського управління (зокрема на міських залізницях Штутгарта, Мюнхена та Берліна). Моделювання сценаріїв розвитку ситуації дає змогу диспетчеру отримувати оптимізовані варіанти регулюючих заходів і уникати затримок ще до виникнення серйозних проблем [4].

У Великій Британії компанія Network Rail використовує ЦД для управління інфраструктурою та складними проєктами, серед них такі, як модернізація інфраструктури. Під час модернізації важливого вузла Carstairs Junction ЦД відіграв головну роль у мінімізації збоїв і прискоренні виконання робіт. Динамічна, насичена даними модель дала змогу точно координувати проєктування та будівельні заходи, симулюючи реальні умови та інтегруючи різні джерела даних для ухвалення рішень у режимі реального часу [13].

У 2022 році інжинірингова фірма Італійської Державної Залізничної Групи застосувала технологію ЦД для проєкту високошвидкісної залізничної лінії Неаполь-Барі. ЦД був підготовлений із використанням цифрової BIM-бібліотеки (Building Information Modelling), що налічувала близько 1500 параметричних компонентів, що значно покращило управління проєктом та оцінювання його життєвого циклу [7].

В Австралії було продемонстровано, що ЦД, поєднаний із глибоким навчанням, може надавати детальніші дані про вплив збоїв на пасажирів у режимі реального часу. Метою цього дослідження було дати змогу операційним центрам краще пом'якшувати наслідки збоїв та оптимізувати обслуговування пасажирів [9].

Ці приклади ілюструють, що ЦД використовують не лише для прогнозування технічних відмов та управління активами, але й оптимізації руху, навчання систем ШІ/SOAR і підвищення кіберстійкості залізничних мереж [15]. Цей міжнародний досвід підтверджує перспективність технології.

Для України впровадження ЦД має особливе значення. Технологія є критично важливою для модернізації залізничної інфраструктури та підвищення стійкості української залізниці, що є життєво необхідним в умовах воєнних і постійних кібернетичних загроз [12].

Інтеграція ЦД залізниці та SOAR на базі ШІ є наступним етапом еволюції кібербезпеки залізничного транспорту, що дає змогу перейти від реактивного до контекстно-залежного проактивного реагування. Розроблення уніфікованих протоколів обміну даними між ЦД і SOAR, удосконалення

моделей ШІ для прогнозування складних, нинішньому етапі розвитку цих технологій [4]. Загалом цифровий двійник залізничної мережі є не лише інструментом для оптимізації, але й стратегічною необхідністю для гарантування її надійності та безпеки в сучасному цифровому середовищі [17].

Список використаних джерел

1. Ficzere P. The role of artificial intelligence in the development of rail transport. *Cognitive Sustainability*. 2023. Vol. 2, No. 4. Article 81. DOI: https://doi.org/10.55343/cogsust.81.
2. Ghaboura S., Ferdousi R., Laamarti F., Yang C. and Saddik A. E. Digital Twin for Railway: A Comprehensive Survey. *IEEE Access*. 2023. Vol. 11. P. 120237-120257. doi: 10.1109/ACCESS.2023.33270423.
3. Ngai E., Chen C., Tolba A. M., Obaidat M. S. and Wang F. IEEE Access Special Section Editorial: Artificial Intelligence (AI)-Empowered Intelligent Transportation Systems. *IEEE Access*. 2021. Vol. 9. P. 69492-69497. doi: 10.1109/ACCESS.2021.3074996.
4. FICZEREP. (2023). The role of artificial intelligence in the development of rail transport. *Cognitive Sustainability*. *2*(4). https://doi.org/10.55343/CogSust.81.
5. Mirabadi A. & YAZDI Mohammad. (2009). Automatic generation and verification of railway interlocking control tables using FSM and NuSMV. *Transport Problems : an International Scientific Journal*.
6. Pappaterra M. J., Flammini F., Vittorini V., Bešinović N. A Systematic Review of Artificial Intelligence Public Datasets for Railway Applications. *Infrastructures.* 2021. *6.* 136. https://doi.org/10.3390/infrastructures6100136.
7. Dirnfeld Ruth. (2022). Digital Twins in Railways. 10.13140/RG.2.2.32690.68804. Chelsea Finn. 2018. Learning to Learn with Gradients. PhD Thesis, EECS Department, University of Berkeley.
8. Ariyachandra Mahendrini & Wen Ya & Yu Jiadong. (2025). Advancing Rail Infrastructure: Integrating Digita Twins and Cyber-Physical Systems for Predictive Maintenance. 10.35490/EC3.2025.272.
9. Al-Nasser N. & Chen D. (2025). Smart Railways: Predictive Maintenance, Digital Twins, and Energy-Aware Operations. *Multidisciplinary Engineering Science Open*. 2. 1-11. https://jmesopen.com/index.php/jmesopen/article/view/16.
10. Werbińska-Wojciechowska S., Giel R., Winiarska K. Digital Twin Approach for Operation and Maintenance of Transportation System—Systematic Review. *Sensors.* 2024. *24*. 6069. https://doi.org/10.3390/s24186069.
11. Thaduri A., Verma A. K., Kumar U. Maintenance of Railway Infrastructure Using Cyber-Physical Systems. *Decision Analytics Applications in Industry*. 2020. P.521-540. DOI:10.1007/978-981-15-3643-4_41.
12. Zezhou Wang, Xiang Liu. Cyber security of railway cyber-physical system (CPS) – A risk management methodology. December 2022. 100078. https://www.sciencedirect.com/science/article/pii/S2772424722000282.
13. Ariyachandra M. R. F., Wen Y., Yu J. Advancing Rail Infrastructure: Integrating Digital Twins and Cyber-Physical Systems for Predictive Maintenance. *Proceedings of the 2025 European Conference on Computing in Construction (EC3), Porto, Portugal.* URL: https://discovery.ucl.ac.uk/id/eprint/10211557. DOI: 10.35490/EC3.2025.272 ResearchGate.
14. Yang J., Sun Y., Cao Y., Hu X. Predictive Maintenance for Switch Machine Based on Digital Twins. *Information.* **2021**. *12*. 485. https://doi.org/10.3390/info12110485.
15. Thompson Emmanuel Anu & Lu Pan & Alimo Philip & Atuobi Herman & Akoto Evans Tetteh & Abbew Cephas. (2025). Revolutionizing Railway Systems: A Systematic Review of Digital Twin Technologies. *High-speed Railway*. September 2025. Vol. 3, Iss. 3. P. 238-250. https://doi.org/0.1016/j.hspr.2025.05.005.
16. Kampczyk A., Dybeł K. The Fundamental Approach of the Digital Twin Application in Railway Turnouts with Innovative Monitoring of Weather Conditions. *Sensors.* **2021**. *21*. 5757. https://doi.org/10.3390/s21175757.
17. Dimitrova E. and Tomov S. Digital Twins: An Advanced technology for Railways Maintenance Transformation. *2021 13th Electrical Engineering Faculty Conference (BulEF)*, Varna, Bulgaria. 2021. P. 1-5. doi: 10.1109/BulEF53491.2021.9690822.

CREATION OF A DIGITAL DOUBLE OF THE RAILWAY NETWORK AND ITS INTEGRATION WITH AI-BASED SOAR CYBER THREAT RESPONSE AUTOMATION

Abstract

The article substantiates the need to create a digital duplicate of the railway network (CD) and explores the mechanisms of its integration with an

advanced system of automating response to cyber threats conditions of total digitalization, introduction of the Internet of Things (IoT) and ACS/CSS, the railway infrastructure critically expands the surface for cyber attacks, which requires a transition from reactive to proactive methods of protection.

CD is defined as a high-precision virtual copy of the physical system (tracks, rolling stock, power supply, control system, automatic control system and network infrastructure), which serves as an intellectual training ground for cyber protection. The main functions of the CD are considered in detail: traffic modeling, infrastructure modeling, SBS systems modeling, and energy supply and communication modeling. Each of these functions is critical for simulating cyber-attacks and assessing their real-world physical impact on traffic safety, such as attempted unauthorized changes to the arrow's position or communication disruption.

The SOAR system is presented as a key tool that provides the orchestration (coordination of security tools) and automation (implementation of countermeasures using «playbooks») necessary for immediate incident response.

Artificial intelligence acts as a «brain» for decision-making, using the CD to assess the consequences of an incident and choose the optimal SOAR response scenario with the priority: Traffic safety - Functionality - Recovery. A conceptual architecture and integration algorithm are proposed that allow SOAR/AI to automatically test countermeasures in a virtual CD environment before deploying them in a real network, minimizing operational risks.

Practical examples of the application of CD and AI elements on the world's railways (Deutsche Bahn, Network Rail, Italian State Railway Group) are given, which confirm the promising nature of the technology. The conclusion emphasizes that the integration of CD, SOAR and AI is a strategic necessity to increase the overall cyber resilience and reliability of rail transport, especially in the face of constant cyber threats.

***Keywords**: digital twin, cybersecurity, cyberattack simulation, proactive protection, rail transport.*

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.

Хісматулін Володимир Шайдуллович, кандидат технічних наук, професор кафедри автоматики та комп'ютерного телекерування рухом поїздів, кандидат технічних наук, Український державний університет залізничного транспорту, Харків, Україна. https://orcid.org/0000-0001-7578-1217. Тел.: +38(057) 730-10-32. E-mail: khisvs@kart.edu.ua.

Сіроклин Іван Миколайович, доцент кафедри автоматики та комп'ютерного телекерування рухом поїздів, кандидат технічних наук, Український державний університет залізничного транспорту, Харків, Україна. https://orcid.org/0000-0001-9978-8261. Тел.: +38(057) 730-10-32. E-mail: seroklin@kart.edu.ua.

Прилипко Андрій Андрійович, доцент кафедри автоматики та комп'ютерного телекерування рухом поїздів, кандидат технічних наук, Український державний університет залізничного транспорту, Харків, Україна. https://orcid.org/0000-0001-6126-1085. Тел.: +38(057) 730-10-32. E-mail: prilipkoaa@kart.edu.ua.

Sotnyk V., 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.

Khismatulin V., Professor of the Department of Automation and Computerized Train Control, Cand. tech. Sciences, Ukrainian State University of Railway Transport. https://orcid.org/0000-0001-7578-1217. Tel.: +38(057) 730-10-32. E-mail: khisvs@kart.edu.ua.

Siroklyn I. Associate Professor of the Department of Automation and Computerized Train Control, Cand. tech. Sciences, Ukrainian State University of Railway Transport. https://orcid.org/0000-0001-9978-8261. Tel.: +38(057) 730-10-32. E-mail: seroklin@kart.edu.ua.

Prylypko A. Associate Professor of the Department of Automation and Computerized Train Control, Cand. tech. Sciences, Ukrainian State University of Railway Transport. https://orcid.org/0000-0001-6126-1085. Tel.: +38(057) 730-10-32. E-mail: prilipkoaa@kart.edu.ua.