ТЕЗИ СТЕНДОВИХ ДОПОВІДЕЙ ТА ВИСТУПІВ УЧАСНИКІВ КОНФЕРЕНЦІЇ

HIGHLIGHTS OF REPORTS AND PRESENTATIONS OF PARTICIPANTS TO THE CONFERENCE

які к тому ж можуть мати вже вбудовані програми для розрахунків (вводяться тільки величини коефіцієнтів у ПЗП). А серед цих фільтрів найкращій результат дає метод зважування – менша кількість коефіцієнтів.

Цифрові НІХ-фільтри потребували з врахуванням впливу округлення коефіцієнтів на результуючу АЧХ більш дорогих процесорів ЦОС з плаваючою точкою. Крім того, вони можуть бути потенційно нестійкими.

З врахуванням вищевикладеного можна зробити такий висновок: якщо й застосовувати цифрову фільтрацію в існуючій системі локомотивної сигналізації, тоді краще використовувати КІХ-фільтри, а кращій метод розробки такого фільтра – метод зважування з вікном Кайзера.

Джерела інформації

1 Lizhe Tan, Jean Jiang. Digital Signal Processing. Fundamentals, Applications, and Deep Learning. Fourth Edition. Academic Press, 2025. ISBN 978-0-443-27335-3 https://doi.org/10.1016/C2023-0-51030-4

2. Ушенко Ю. О. Основи та методи цифрової обробки сигналів: від теорії до практики [Текст] : навч. посібник / Ю. О. Ушенко, М. С. Гавриляк, М. В. Талах, В. В. Дворжак. – Чернівці : Чернівецький нац. ун-т ім. Ю. Федьковича, 2021. – 308 с

3 Application and Development of Digital Signal Processing Technology in Modern Engineering In book: Proceedings of the 2023 2nd International Conference on Educational Innovation and Multimedia Technology (EIMT 2023) (pp.848-853) DOI:10.2991/978-94-6463-192-0_110

УДК 004.056:656.25

к.т.н. В.О.Сотник, PhD, О.В. Щебликіна
здобувачка гр.103-АКІТР-Д25
М.О. Калашник *Український державний університет залізничного транспорту (м. Харків)*

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

Швидкий перехід залізниць до цифрових технологій (ETCS, СЦБ на мікропроцесорній техніці, IoT) створює нові кіберзагрози, що вимагає захисту критичної інфраструктури. Загрози в першу чергу спрямовані на мережеву інфраструктуру (GSM-R, FRMCS), кінцеві пристрої (контролери, сенсори) та ланцюг постачання програмного/апаратного забезпечення. Типові загрози включають несанкціонований доступ, Man-in-the-Middle (MitM), відмову в обслуговуванні (DoS/DDoS) та Ransomware. Наслідки можуть бути критичними: вплив на безпеку руху (підміна показань сигналів, блокування стрілок, або їх несанкціонований перевід) та значні економічні збитки. Одним із напрямків захисту від цих втручань є жорсткі вимоги до функціональної безпеки (SIL-рівні), які обмежують пряме впровадження комерційних IT-рішень у системах залізничної автоматики і телемеханіки(СЗАТ)[1,2].

Штучний інтелект(ШІ) має великі перспективи застосування в СЗАТ завдяки його здатності до виявлення аномалій, ефективної обробки великих обсягів даних (Big Data) та адаптивності до нових загроз, що є перевагою над традиційними методами [2]. Використання штучним інтелектом таких методів, як навчання з учителем надає можливість для класифікації відомих типів атак, а навчання без учителя можливо використати для виявлення нових, невідомих аномалій у мережевому трафіку СЗАТ. Глибоке навчання (Deep Learning) дозволяє аналізувати складні патерни поведінки систем залізничної автоматики і телемеханіки. Але на зараз існують проблеми з нестачею маркованих даних про кібератаки в реальних залізничних умовах та необхідність балансу між хибнопозитивними та хибнонегативними спрацюваннями[3]. Для їх вирішення і необхідно застосувати функціонал ШІ у виявленні та реагуванні на кіберзагрози. Перш за все це застосування інтелектуального моніторингу- це коли нейромережі застосовуються в системах NIDS/HIDS для аналізу протоколів залізничного обміну (Eurobalise, ДЦ/МПЦ) та ідентифікації нехарактерних команд, а також для прогнозування розвитку атаки. Застосування аналізу поведінки (UEBA)- це коли ШІ створює базові моделі нормальної поведінки пристроїв та користувачів (диспетчерів, контролерів), що дозволяє автоматично ідентифікувати відхилення, які свідчать про компрометацію, а також застосування автоматизованого реагування (SOAR), коли ШІ може приймати рішення про ізоляцію сегментів мережі або блокування підозрілих IP-адрес у режимі реального часу, проте критичним є забезпечення функціональної безпеки при автоматизації реагування. Але впровадження цих засобів має ряд як технічних, так і організаційних труднощів, таких, як складність інтеграції ШІ-рішень у закриті Brownfield-системи , високі вимоги до обчислювальної потужності та необхідність сертифікації ШІ-систем відповідно до міжнародних стандартів, наприклад CENELEC. З точки зору організаційних труднощів- це перш за все кадрова проблема (дефіцит фахівців на стику автоматики, кібербезпеки та ШІ) та відсутність єдиної

нормативної бази для AI-Driven кіберзахисту в СЗАТ[4].

Одним із перспективних напрямків досліджень в цьому напрямку є включення ШІ для тестування на проникнення та його застосування у поєднанні з квантовою криптографією[4].

Таким чином необхідний поетапний план впровадження, починаючи з некритичних систем моніторингу, з фінальною метою інтелектуального захисту централізованих систем керування рухом, а також співпраця між науковими установами та експлуатаційними службами для розробки галузевих рішень.

Використана література.

1. Cybersecurity challenges for the railway sector. https://www.railway-cybersecurity.com/
2. Artificial Intelligence in Railway Signalling: Case Studies, Automation and Savings from 42 %. https://exceltic.com/en/artificial-intelligence-in-railway-signalling-real-cases-automation-and-savings-of-42/
3. 3. Anomaly Detection for ICS Based on Deep Learning: A Use Case for Aeronautical Radar Data. January 2022annals of telecommunications - annales des télécommunications 77(3). DOI:10.1007/s12243-021-00902-7 https://www.researchgate.net/publication/357991662_Anomaly_Detection_for_ICS_Based_on_Deep_Learning_A_Use_Case_for_Aeronautical_Radar_Data
4. Applying Penetration Testing Techniques to Strengthen ERTMS Communication Security. https://www.era.europa.eu/system/files/2024-10/session%200-4%20-%20applying%20pentest%20to%20ertms%20-%20yasmine%20benghename.pdf?t=1750977732
5. Нормативно-Правові та Стандарти.
   -EN 50126 (IEC 62278): Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
   -EN 50128 (IEC 62279): Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems.
   -EN 50129 (IEC 62425): Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling.
   -IEC 62443 (Серія стандартів): Security for industrial automation and control systems (IACS).

к.т.н. **А.Л. Сумцов**
Український державний університет залізничного транспорту

КЛАСИФІКАЦІЯ СПОЖИВАННЯ ЕНЕРГІЇ ПРИ ВИЗНАЧЕННІ ЕНЕРГЕТИЧНОГО БАЛАНСУ МОТОРВАГОННОГО РУХОМОГО СКЛАДУ

Моторвагонний рухомий склад (МВРС) посідає вагоме місце у системі пасажирських перевезень України. Однак його нинішній технічний стан, що зумовлений тривалим строком експлуатації та впливом низки несприятливих чинників, не в повній мірі відповідає сучасним вимогам конкурентоспроможності на ринку транспортних послуг, особливо у порівнянні з автомобільним транспортом. Водночас стабільність перевезень протягом року та нижчий рівень залежності від погодних умов зумовлюють збереження попиту й актуальності цього виду транспорту.

У цих умовах одним із пріоритетних завдань є підвищення рівня енергоефективності та скорочення втрат енергії, що має безпосереднє значення для забезпечення економічної доцільності та екологічної стійкості функціонування транспортної галузі. Визначення енергетичного балансу виступає ключовим інструментом у даному процесі, оскільки воно дозволяє ідентифікувати основні напрями використання та втрат енергоресурсів, сформувати цілісне уявлення про характер енергетичних потоків та забезпечити більш обґрунтовану інтерпретацію результатів енергетичного аудиту. Це, у свою чергу, створює наукову й практичну основу для розроблення та впровадження ефективних заходів з оптимізації енергоспоживання моторвагонного рухомого складу.

В літературних джерелах [1] загально прийнятим є поділ споживання енергії на два: на тягу та на власні потреби. Така класифікація не дозволяє аналізувати весь спектр систем на борту МВРС. В той самий час аналізувати кожну систему є невиправдано трудомістким процесом, якщо ефект від оптимізації буде знаходитися в межах статистичної похибки вимірювання витрат енергії.

Аналізуючи процедуру складання енергетичного балансу [2, 3] необхідно скористатися функціональним призначенням споживачів енергії на борту МВРС. Застосовуючи принцип уніфікації застосування класифікації для різних типів МВРС та різних джерел енергії, які можуть використовуватися пропонується використати наступну класифікацію споживання енергії:

- На тягу;