- суміщення на загальній території роздільних пунктів високошвидкісної та звичайної залізничної колії;

- розташування роздільних пунктів високошвидкісної лінії на іншому рівні за принципом віадуків.

Для удосконалення залізничної інфраструктури доцільно використовувати типові схеми основних роздільних пунктів, що дозволить визначити їх основні параметри та показники, які можуть бути використані як на етапі техніко-економічного обґрунтування так і на етапі проектування.

Критерієм доцільності удосконалення залізничної інфраструктури роздільних пунктів при впровадженні швидкісного руху є мінімум приведених витрат на реконструкцію головних колій та перебудову роздільного пункту.

Застосування запропонованого підходу дозволить підвищити швидкість руху та забезпечить необхідний рівень безпеки при впровадженні високошвидкісного руху поїздів, що в теперішній час є досить актуальним. Впровадження високошвидкісного руху дозволить підвищити мобільність населення та його економічну активність. Держава отримує при цьому економічний ефект від інвестицій в інфраструктуру, а також непрямий ефект для економічного розвитку регіону та країни в цілому.

Список використаних джерел

1. Про схвалення Національної транспортної стратегії України на період до 2030 року. Розпорядження Кабінету Міністрів України від 30.05.2018 р. № 430-р.
2. Продащук С.М., Шаповал Г.В., Тоцька О. В., Марченко О.В., Бєлан Д. О. Впровадження інноваційних технологій в пасажирських перевезеннях. *Збірник наукових праць УкрДУЗТ*. 2018. Вип. 178. С. 28-41.
3. Куценко, М. Ю., Шаповал Г.В., Івашкіна А. М., Шкрабуль Є.М. Визначення структури будівельних робіт з реконструкції роздільних пунктів при введенні швидкісного руху. *Збірник наукових праць УкрДУЗТ*. 2017. Вип. 173. С. 29-34.

Жуковицький І. В., д.т.н., професор,
Цикало І. Д., аспірант
(ДНУЗТ ім. академіка В. Лазаряна)

УДК [004.7-047.72]:656.2

ВИКОРИСТАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ВИЯВЛЕННЯ ВТОРГНЕНЬ В КОМП'ЮТЕРНІ МЕРЕЖІ

Ефективність функціонування сучасних інформаційних систем залізничного транспорту в значній мірі пов'язана з проблемою захисту оброблюваної в них інформації. Згідно до звіту Verizon 2018 Data Breach Investigations Report [1] проблема виявлення вторгнень є актуальною. Серед усіх атак 73% здійснено аутсайдерами, 48% хакінгом. Серед усіх інцидентів 68% були виявлення більш ніж через місяць.

Можливості існуючих систем захисту не завжди дозволяють забезпечити безпеку інформаційної системи на достатньому рівні. Причиною цього є те, що процес створення систем виявлення атак пов'язаний з низкою невирішених науково - технічних завдань. Існуючі системи виявлення атак зазвичай використовують найпростіші алгоритми обробки інформації, що надходить, що не дозволяє виявити значну кількість атак на інформаційні системи. До основних методів виявлення атак належать аналіз сигнатур та виявлення аномалій. Аналіз сигнатур був першим методом, застосованим для виявлення вторгнень. Він базується на простому понятті збігу послідовності зі зразком. У вхідному пакеті проглядається байт за байтом і порівнюється з сигнатурою (підписом) — характерним рядком програми, що вказує на характеристику шкідливого трафіку. Такий підпис може містити ключову фразу або команду, яка пов'язана з нападом. Якщо збіг знайдено, оголошується тривога.

Через те що метод виявлення атак на базі сигнатур є статичним, він є вразливим до нових типів атак. Для виявлення нових типів атак необхідно використовувати системи виявлення, що здатні до самонавчання у реальному часі. Створення ефективної системи виявлення атак вимагає застосування якісно нових підходів до обробки інформації, які повинні ґрунтуватися на адаптивних алгоритмах здатних до самонавчання. Найбільш перспективним напрямком у створенні подібних систем виявлення атак є застосування засобів штучного інтелекту [2, 3].

До таких систем належать методи класифікації засновані на алгоритмах машинного навчання (навчання з вчителем). Алгоритми навчання з вчителем використовують набір даних типу «запит – відповідь», де запитом може виступати мережевий пакет та поточний стан мережі або хоста, а відповіддю є значення «0» (нормальний запит) або «1» (вторгнення). Дані системи можуть продовжувати навчання у реальному часі після початкового навчання.

Для виявлення нових типів атак також використовуються системи виявлення вторгнень на основі аномалій. На базі набору запитів формується модель нормальної поведінки, з якою порівняються кожен поточний запит до системи.

Існує велика кількість алгоритмів класифікацій та виявлення аномалій, кожен з яких має свої переваги та недоліки.

Проведено дослідження ефективності обраних інтелектуальних засобів у задачі ідентифікації та

класифікації мережевих атак. У якості набору даних мережевого трафіку використовувався набір даних DARPA IDS 1999, що складається майже з 5 мільйонів записів, де кожен представлений не тільки характеристиками IP пакету, а й характеристиками більш високого рівня. Набір даних складається з 5 видів мережевих пакетів: нормальні, атака DoS (Denial of Service), атака Probe, атака R2L (Remote to Local), атака U2R (User to Remote). У якості навчальної вибірки використовувалось приблизно 90% загальної вибірки. Тестова та навчальні вибірки нараховували у собі всі види пакетів, але у навчальній вибірці були відсутні декілька типів атак з кожного класу атак.

Проведено дослідження ефективності моделі логістичної регресії у задачі ідентифікації мережевих атак. Коректність фінальної моделі на тестовий вибірці складає 98.96%, точність – 99.68%, повнота – 99.02%, F1-міра – 99.35%. Коректність на нових типах атак класу DoS – 53%, Probe – 45%, R2L – 100%, U2R – 100%.

Проведено дослідження ефективності моделі штучної нейронної мережі прямого поширення у задачі ідентифікації мережевих атак. У якості моделі було використано ШНМ 119-8-8-1 з функцією активації Leaky-ReLU. Коректність фінальної моделі на тестовий вибірці складає 99.83 %, точність – 99.96 %, повнота – 99.83 %, F1-міра – 99.9 %. Коректність на нових типах атак класу DoS – 98.1 %, Probe –87.4 %, R2L – 50 %, U2R – 100%.

Проведено дослідження ефективності моделі штучної нейронної мережі прямого поширення у задачі класифікації мережевих атак. Коректність фінальної моделі на тестовий вибірці складає 99.55 %, точність – 99.49 %, повнота – 99.83 %, F1-міра – 99.65 %. Коректність на нових типах атак класу DoS – 89.39 %, Probe – 44.15 %, R2L – 0%, U2R – 0 %.

Відповідно до вищезазначених аргументів можна прийти до висновку, що використання технологій машинного навчання є ефективним при їх застосуванні у розв'язку задач виявлення вторгнень у комп'ютерні мережі.

Список використаних джерел

1. Verizon 2018 Data Breach Investigations Report – 2018. – [Електрон. ресурс] – Режим доступу: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

2. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение / пер. с анг. А.А. Слинкина. 2-е изд., испр. М.: ДМК Пресс, 2018. 652 с.

3. Leslie F. Sikos. AI in Cybersecurity. New York : Springer, 2018. 205 p.

Панченко В. В., к.т.н., доцент,
Харін Р. О., аспірант (УкрДУЗТ)

УДК 620.92

МОДЕРНІЗАЦІЯ СИСТЕМ ЕЛЕКТРОПОСТАЧАННЯ ЗАЛІЗНИЦЬ ШЛЯХОМ ЗАСТОСУВАННЯ АЛЬТЕРНАТИВНИХ ДЖЕРЕЛ ЕНЕРГІЇ

Сучасна система електропостачання залізниць потребує удосконалення та модернізації. Опираючись на всесвітній досвід впровадження альтернативних джерел енергії на залізниці, є доцільним впровадити таку практику на залізниці України.

Крім того, необхідно підвищувати ефективність використання наявного устаткування, скорочувати експлуатаційні витрати і переходити на ресурсозберігаючі та енергозберігаючі технології. Також слід відзначити, що впровадження альтернативних джерел енергії при будівництві та експлуатації дозволить розширити залізничне будівництво у віддалених та важкодоступних регіонах. Але навіть поблизу енергомереж застосування альтернативних джерел енергії забезпечить безперебійне енергопостачання, незалежно від поломок і аварій на підстанціях.

У теперішній час спостерігається посилення екологічних вимог у багатьох країнах і це призводить до вирівнювання вартості енергії традиційних та альтернативних джерел. До того ж, завдяки технологічному вдосконаленню устаткування для джерел поновлювальної енергетики знижується їх вартість.

Основними напрямками впровадження альтернативної енергетики на залізниці є:

живлення систем тягового електропостачання від зовнішньої енергетичної системи, в якій разом з традиційними, функціонують в паралельному режимі і альтернативні джерела електричної енергії.

живлення власних потреб тягової підстанції, об'єктів інфраструктури не тягових споживачів як окремо, так і в паралельному режимі роботи.

В результаті проведеного аналізу можливості застосування альтернативних джерел енергії в системах електропостачання залізниць України:

розглянуто можливість розташування фотоелектричних модулів на дахах і території тягової підстанції;

розглянута можливість застосування вітрової енергетики;

зроблено аналіз кількості річного споживання електроенергії на власні потреби тягової підстанції;

встановлено можливість зменшення споживання електроенергії за рахунок застосування сонячної батареї.