УДК 681.3 http://doi.org/10.15407/pp2024.02-03.223

О. С. Мостовий

НЕЙРОСИМВОЛЬНИЙ ПІДХІД У ВИЯВЛЕННІ АТАК В СИСТЕМАХ СУПУТНИКОВОГО ЗВ'ЯЗКУ

В умовах зростання кіберзагроз, актуальним завданням стає впровадження нових систем захисту для супутникових комунікацій . Пропонована стаття представляє інноваційний нейросимвольний метод виявлення атак, що інтегрує можливості символьного підходу та нейронних мереж для дієвого протистояння загрозам у сфері супутникового зв'язку. Основа розробки - це синтез сильних сторін символьного штучного інтелекту і глибинного навчання, що уможливлює високоточне розпізнавання та нейтралізацію складних атак. У роботі детально розкривається архітектура запропонованої системи, включно з ключовими компонентами, механізмами роботи та процесом впровадження. Виходячи з аналізу даних з супутникових та наземних мереж, проведено оцінку ефективності системи з використанням методів машинного навчання, що демонструє значні покращення у виявленні вторгнень порівняно з існуючими підходами. Окрему увагу приділено здатності моделі адаптуватися до нових типів атак, що забезпечує її довгострокову ефективність. Архітектура обраної багатошарової нейромережі включає символьний шар, призначений для аналізу вхідних даних мережі на предмет вразливостей чи атак, виходячи з бази знань. Експерименти на наборах даних атак і деяких відомих вразливостей, дозволяють випробувати та підтвердити високу ефективність запропонованого методу. Це дослідження відкриває шляхи до поліпшення систем кібербезпеки у сфері супутникового зв'язку, сприяючи створенню більш захищеного космічного середовища.

Ключові слова: кібербезпека, супутникові системи, нейро-символьний підхід, системи виявлення вторгнень, машинне навчання, багатошаровий перцептрон.

O. S. Mostovyi

NEUROSYMBOLIC APPROACH FOR ATTACK DETECTION IN SATELLITE COMMUNICATION SYSTEMS

Abstract: In the context of increasing cyber threats, the pressing task becomes the implementation of new protection systems for satellite communications. The proposed article presents an innovative neurosymbolic method for attack detection that integrates the capabilities of artificial intelligence and neural networks for effective countermeasures against threats in the domain of satellite communication. The foundation of the development is the synthesis of the strengths of symbolic artificial intelligence and deep learning, enabling highly accurate recognition and neutralization of complex attacks. The architecture of the proposed system is thoroughly detailed, including its key components, mechanisms of operation, and implementation process. Analyzing data from satellite and terrestrial networks, the system's effectiveness is evaluated using machine learning methods, demonstrating significant improvements in intrusion detection compared to existing approaches. Special attention is given to the model's ability to adapt to new types of attacks, ensuring its long-term relevance and efficiency. The architecture of the chosen multilayer neural network includes a symbolic layer, designed for analyzing network input data for vulnerabilities or attacks based on a knowledge base. Experiments on datasets of attacks and vulnerabilities such as CTU-13 and STIN allow for the testing and confirmation of the high efficiency of the proposed method. Thus, this research paves the way for improving cybersecurity systems in the field of satellite communication, contributing to the creation of a more secure space environment.

Keywords: cybersecurity, satellite communication, neurosymbolic AI, attack detection, system architecture, machine learning, ensemble models, random forest, multilayer perceptron, system adaptability.

Вступ

Широкосмугові супутникові мережі мають великий вплив серед бездротових мереж, бо мають переваги в розповсюдженості та доступності зв’язку порівняно з іншими мережами. Можливість використання супутникових мереж у складнодоступних локаціях та умовах як фізичних, так і технологічних мають ключове значення.

Наявність бездротового з'єднання в супутникових системах зв'язку підвищує їхню вразливість від різноманітних загроз безпеки. Можливість несанкціонованого прослуховування або захоплення даних є прикладами потенційних атак. Тому питання безпеки стає критично важливим у розробці архітектури супутникових мереж.

Для захисту супутникової мережі використуваються різні системи виявлення вторгнень (СВВ)[1], які дають можливість ідентифікувати потенційні вразливості, захистити мережу та забезпечити безпеку даних та цілісність роботи всієї мережі. СВВ можуть бути мережевими, як розгорнуті в мережі (МСВВ), або вузловими, тобто розміщені на конкретному вузлі (ВСВВ).
МСВВ аналізують мережевий трафік щодо наявності підозрілих дій або атак, аналізуючи копії пакетів, що проходять через конкретний сегмент мережі. ВСВВ виявляють атаки або зловмисні дії на конкретному вузлі, допомагаючи забезпечити безпеку та захист системи чи об'єкта в реальному часі.

Архітектура сучасних систем виявлення вторгнень часто включає застосування алгоритмів машинного навчання [2][3] та глибинного навчання[4] для підвищення ефективності виявлення та класифікації кібератак. Використання таких алгоритмів дозволяє МСВВ адаптуватися до нових та еволюційних загроз без необхідності ручного оновлення правил або підписів.

Розвиток та адаптація рішень для атак на супутникові мережі є постійним процесом, який включає оновлення та модифікацію атаки для обходу захисних механізмів. Це створює виклики для ідентифікації та протидії новим загрозам, оскільки захисники повинні постійно адаптувати свої системи безпеки для захисту від постійно еволюціонуючих атак. Ефективний захист вимагає комплексного підходу, включно із передовими технологіями розпізнавання, швидким реагуванням на інциденти та регулярним оновленням захисних систем і процедур.

Дана робота пропонує нову структуру для систем виявлення вторгнень, яка базується на інтеграції символьного шару в нейромережі глибокого навчання. Цей інноваційний підхід до поєднання символьного методу та глибокого навчання має на меті підвищити здатність системи виявляти складні та адаптивні кіберзагрози. Інтеграція символьного аналізу дозволяє системі глибше розуміти контекст і логіку потенційних атак, тим самим підвищуючи її ефективність у протидії найновішим загрозам в кіберпросторі.

Огляд супутникових мереж та загроз безпеці

Супутникова мережа представляє собою складну систему, що об'єднує космічні елементи (супутники) та наземні компоненти, включаючи супутникові термінали, шлюзи для зв'язку із земними мережами та центри управління мережею.

Супутникові смуги є частиною електромагнітного спектру, який використовується для супутникового зв'язку. Ці смуги визначаються діапазонами частот, які використовуються для передачі сигналів між космічними супутниками і наземними станціями. Наприклад, L-смуга використовується для мобільного супутникового зв’язку, а C-смуга для дистанційного зондування Землі. Ka-смуга та Ku-смуга використовуються для телебачення та інтернету.

Кожна зі смуг має свої переваги та обмеження залежно від застосування, включаючи чутливість до атмосферних умов, дальність зв'язку та потенціал для перешкод з іншими видами зв'язку. На їх базі створені супутникові системи, найпоширеніші з яких є наступні:

1) SpaceX пропонує послуги інтернет-зв’язку та має глобальне покриття на Ka- та Ku-смугах із затримкою від 20 до 40 мс.

2) Telesat використовує Ka та Ku-смуги для надання послуг інтернет-зв’язку з затримкою близько 50 мс на глобальному рівні.

3) Viasat використовує Ka та Ku-смуги для надання широкого спектру послуг(телебачення, інтернет-зв’язок) з затримкою від 40 до 600 мс

4) Iridium, який використовує L-смугу - та надає послуги інтернет-зв’язку.

5) Inmarsat надає послуги інтернет-зв’язку та телефонного зв’язку. Використо-

вує різні смуги частот, включаючи L-смугу, C-смугу, і в основному Ka-смугу із затримкою від 40 до 800 мс.

6) China Satcom використовує різні смуги частот для надання послуг інтернет-зв'язку такі як: C-смугу , Ka- та Ku-смуги затримкою від 20 до 800 мс.

Центри керування та управління супутниковою системою відіграють ключову роль у контролі супутникових мереж, об'єднуючи в собі апаратне та програмне забезпечення. Відповідальність за виявлення несанкціонованих доступів та неправильних дій передана до системи управління мережею (Рис 1)

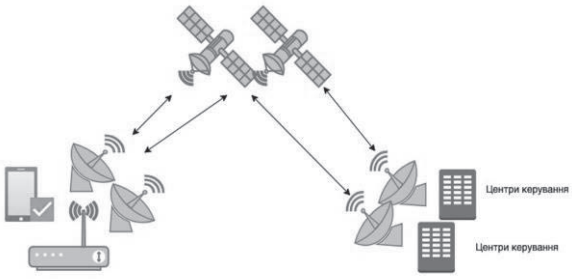

Рис. 1. Супутникова мережа, яка зв'язує супутники з абонентськими терміналами та центрами управління на Землі.

Загрози безпеці

Потенційні загрози та атаки на супутникові мережі можна розділити на пасивні та активні. Пасивні атаки пов'язані з можливістю налаштування на різні частоти та приймання трафіку, призначеного для інших терміналів, використовуючи супутниковий термінал і базові знання комунікаційних протоколів. Така атака може розкрити потенційно чутливі або цінні дані, і її важко виявити, оскільки для її здійснення не потрібно змінювати або вносити альтернації в дані.

Активні атаки:

1) Атаки типу "Відмова в обслуговуванні" (DoS-атаки) відбуваються, коли зловмисник намагається перевантажити, вивести з ладу або зруйнувати ресурс системи, відправляючи величезну кількість трафіку протягом короткого проміжку часу. Загалом, метою є заповнення всієї доступної пропускної спроможності, внаслідок чого легітимні користувачі не можуть отримати доступ до мережевих ресурсів.

2) Атака R2L з віддаленого доступу відбувається, коли нападник намагається отримати доступ до системи як локальний користувач, не будучи легітимним користувачем цієї системи. Для цього зловмисники відправляють нелегальні пакети даних.

3) Атака з метою розвідки (Probe Attack) відбувається, коли нападник намагається отримати інформацію про цільову комп'ютерну мережу. Основна мета - знайти вразливості у цій мережі. Вони відстежують топологію мережі цільової системи та намагаються виявити запущені на ній служби. Для цього можуть використовуватись інструменти атак, такі як Nmap, Ipseewp, Satan.

4) Атака від користувача на адміністратора (U2R-атака) відбувається, коли за допомогою загальних технік, таких як соціальна інженерія, перехоплення паролів, спуфінг, SQL-ін'єкції, крос-сайтові скриптові атаки тощо, хакер намагається отримати права адміністратора цільової системи.

5) Атаки на програмне забезпечення (Exploit Attacks): Використання вразливостей у програмному забезпеченні для виконання шкідливого коду або отримання несанкціонованого доступу

Тренувальні набори даних

Це дослідження аналізує два набори даних для оцінки продуктивності запропонованої мережевої системи виявлення вторгнень. Інформація про набір даних CTU-13[5] описана та представлена в таблиці 1. CTU-13 це мережевий набір даних, призначений для дослідження виявлення мережевих вторгнень і аналізу шкідливого програмного забезпечення. Він був створений Чеським технічним університетом у рамках проєкту CTU (Czech Technical University) і містить реальний мережевий трафік, який включає нормальну активність та різноманітні атаки.

Таблиця 1

Структура набору даних CTU-13

Клас	Опис
Нормальний трафік	Дані, що відображають звичайну поведінку користувачів і служб у мережі без виявлених атак або інших шкідливих дій.
Шкідливий трафік (Ботнети)	Трафік від різних типів ботнетів, мереж інфікованих комп'ютерів, що можуть бути використані для проведення атак, розсилки спаму, крадіжки даних.
Атаки на відмову в обслуговуванні (DoS і DDoS)	Дані про атаки, які мають на меті зробити ресурс недоступним для його користувачів, перевантажуючи мережеву інфраструктуру або сервери.
Сканування портів	Трафік, що вказує на спроби виявити вразливі порти на комп'ютерах в мережі з метою подальшого вторгнення або атак.

Набір даних STIN[6] (Satellite and Terrestrial Integrated Networks) – це спеціалізований набір даних, розроблений для дослідження та аналізу безпеки в інтегрованих супутникових та наземних мережах. Він був створений з метою допомогти в розробці та вдосконаленні систем виявлення атак, які можуть виникати в таких складних мережевих середовищах. STIN містить дані про різні типи атак, зібраних або симульованих в умовах, які імітують реальне мережеве середовище, що об'єднує супутникові та наземні технології. У таблиці 2. наведена структура набору даних STIN, де атаки розділені на дві категорії:

1) Наземні атаки – це атаки на сервіси центру управління

2) Супутникові атаки – це атаки на супутники

Таблиця 2

Структура набору даних STIN

Домен	Тип Атаки
Наземні атаки	Botnet
	Web attack
	Backdoor
	LDAP DDoS
	MSSQL DDoS
	NetBIO DDoS
	Portmap DDoS
Супутникові атаки	Syn DDoS
	UDP DDoS

Архітектура СВВ із використанням глибокого навчання та символьного підходу

Архітектура систем виявлення вторгнень із застосуванням нейромереж глибокого навчання та нейромереж із символьним вхідним шаром в СВВ є багатообіцяючим підходом у сфері кібербезпеки . Цей підхід дозволяє аналізувати та ідентифікувати потенційні загрози та атаки на мережеву інфраструктуру, використовуючи синергію нейромереж та символьних методів. Розглянемо архітектуру такої системи.

Нейромережа глибокого навчання. Нейромережі глибокого навчання стають важливим інструментом у виявленні кібератак та аномалій у мережевому трафіку, дозволяючи аналізувати великі набори даних і автоматично ідентифікувати складні статистичні залежності. Вони використовуються для виявлення прихованих властивостей даних, що робить їх ефективними проти нових і невідомих загроз. Системи на основі глибокого навчання включають вхідний шар, який приймає дані; один або кілька прихованих шарів, що виявляють залежності, і вихідний шар, який генерує прогнози моделі. Вони застосовують різноманітні функції активації, такі як ReLU та сігмоїд, і використовують методи зворотного поширення помилки та градієнтного спуску для оптимізації ваги. Оглядова

стаття[7] детально описує ці процеси, надає порівняльний аналіз різних підходів та визначає майбутні напрямки досліджень у цій галузі.

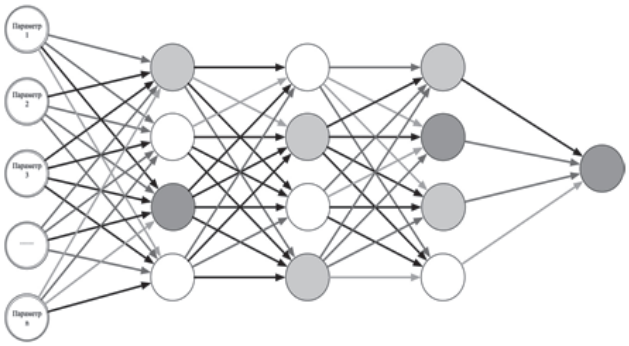

Рис. 2. Структура нейромережі глибокого навчання

Нейромережа із символьним вхідним шаром. Нейромережі використовують символьний вхідний шар для трансформації категоріальних та текстових даних мережевого трафіку в чисельні параметри, які потім можуть бути аналізовані за допомогою символьних правил. Ці правила вбудовуються в нейромережі як центр знань, дозволяючи не лише обробляти вхідні дані на основі їхніх чисельних характеристик, а й використовувати логічні або символьні правила для виведення та інтерпретації даних. Такий підхід дозволяє ефективно об'єднувати переваги символьного мислення (наприклад, можливість роботи з абстрактними концепціями та виконання логічного виведення) з потужністю нейромережевих моделей глибокого навчання.

Символьний шар. Даний шар є першим, що приймає вхідні дані. Кожен нейрон у цьому шарі відповідає одному вхідному параметру. На даному етапі вбудовуються символьні обмеження, які представляють алгоритми класифікатори, що аналізують параметри для виявлення вразливості чи атаки. В дослідженні використано набір алгоритмів, які аналізують вхідні параметри і повертають відповідь як число з плаваючою точкою , яке слугує штрафом для оновлення ваги.

Нехай X_i буде вхідними даними для і-го шару, тоді вихід Y_i перед застосуванням символьного обмеження можна визначити як:

$$Y_i = \sigma(X_i W_i + B_i)$$

де
W_i і B_i - ваги та зміщення для i-го шару відповідно,σ – функція активації

Для застосування символьного обмеження, запропоновано новий параметр P , який є вектором штрафних балів з розмірами, відповідними до кількості вибірок даних в X_i, де кожен елемент вказує штрафний бал для відповідної вибірки, індукуючи імовірність того, що вибірка є частиною трафіку атаки. Тоді скоригований вихід $Y_i{}'$ можна визначити як:

$$Y_i^{'} = Y_i \cdot (1 - P)$$

Ця формула дозволяє адоптивно коригувати вихід нейронного шару на основі оцінки трафіку атаки, зменшуючи вплив кожної вибірки, які ідентифіковані як атаки, на подальшу обробку мережею.

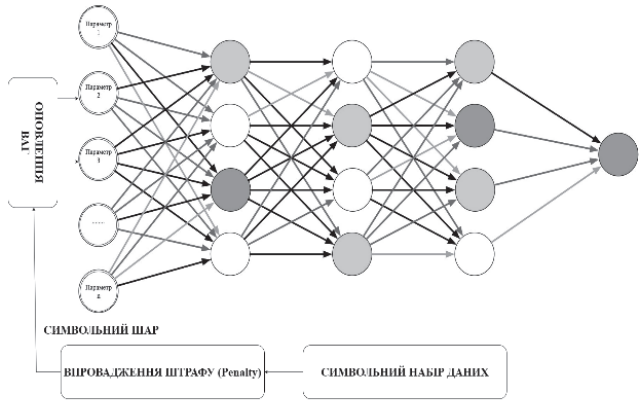

Рис. 3. Структура нейромережі глибокого навчання із символьним вхідним шаром

Оцінка ефективності та метрики

Для оцінки ефективності та порівняння алгоритмів використовувались такі метрики, як влучність (Accuracy), точність (Precision), повнота (Recall) та метрика F1-бал (F1). Ці метрики оцінюються з викори-

станням матриці помилок, де TP позначає істинно позитивні випадки, TN - істинно негативні, FP - хибно позитивні, а FN - хибно негативні випадки та визначаються наступним чином

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

$$\text{Precision} = \frac{TP}{TP+FP}$$

$$\text{Recall} = \frac{TP}{TP+FN}$$

$$\text{F1} = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Результати експерименту

Запропоновані нейромережі були протестовані на двох наборах даних - CTU-13 і STIN з метою оцінки їхньої ефективності та здатності до виявлення та класифікації атак у мережі.

Налаштування експерименту

Набір даних, які використовуються в експерименті, розділений на набір тренувань і набір тестів у співвідношенні 0,6 і 0,4 відповідно. Запропоновані нейромережі оцінюються з точки зору точності, влучності та оцінки F1. Експерименти проводяться з використанням графічного процесора Radeon Pro 555X на 4 ГБ на 2,2 GHz 6-ядерний процесор Intel Core i7 машини з 16Гб DDR4 оперативної пам'яті (RAM). Нейромережі розроблені на основі мови програмування Python 3.9.

Продуктивність нейромереж

Результати використання декількох нейромереж у класифікації трафіку показано в Табл. 3 . Для ідентифікації звичайного трафіку стандартна нейромережа показує точність 96.1%, тоді як покращена символьна нейромережа демонструє вищу точність — 98.7%. У разі виявлення шкідливого трафіку від ботнетів стандартна нейромережа досягає точності 96.3%, тоді як символьна нейромережа знову ж таки показує кращі результати з точністю 98.9%. Під час ідентифікації атак на відмову в обслуговуванні, включно із DoS та DDoS, стандартна нейромережа має точність 97.5%, тоді як символьна нейромережа досягає навіть вищої точності — 99.2%. Нарешті для виявлення сканування портів стандартна нейромережа показує точність 96.8% у порівнянні з 99.1% точності символьної нейромережі.

Таблиця 3

Влучність класифікатор ів на наборі даних CTU-13

Тип Атаки	Нейромережа	Нейромережа з символьним шаром
Нормальний трафік	96.1	98.7
Шкідливий трафік (Ботнети)	96.3	98.9
Атаки на відмову в обслуговуванні (DoS і DDoS)	97.5	99.2

Таблиця 4 показує результати для набору супутникових даних STIN. У випадку атак типу UDP Dos, стандартна нейромережа показує точність 93.12%, тоді як нейромережа з символьним шаром має вищу точність — 96.73%. Для атак типу Syn DDoS, точність стандартної нейромережа складає 89.17%, а символьна DNN значно ефективніша з результатом 95.16%.

Таблиця 4

Влучність класифікаторів на наборі даних супутникових даних STIN

Тип Атаки	Нейромережа	Нейромережа з символьним шаром
UDP_Dos	93.12	96.73
Syn_DDoS	89.17	95.16

Результати ефективності, які показані в Таблиці 5, свідчать, що нейромережа із символьною компонентою постійно демонструє кращі результати порівняно зі стандартною нейромережою. Наприклад, для виявлення атак типу "Backdoor" нейромережа має точність 94.22%, тоді як символьна нейромережа підвищує цей показник до 96.72%. Схожа тенденція спостерігається і для інших типів атак: символьна нейромережа покращує результати з 89.13% до 95.14% для LDAP DDoS, з 92.54% до 96.31% для MSSQL DDoS, і так далі за списком. Найбільше поліпшення точності відзначено під час виявлення атаки Syn DDoS, де точність зросла з 93.14% до майже ідеальних 98.95%.

Таблиця 5

Влучність класифікаторів на наборі даних супутникових даних STIN

Тип Атаки	Нейромережа	Нейромережа з символьним шаром
Backdoor	94.22	96.72
LDAP DDoS	89.13	95.14
MSSQL DDoS	92.54	96.31
NetBIO DDoS	90.25	95.74
Portmap DDoS	91.45	97.29
Syn DDoS	93.14	98.95
UDP DDoS	91.81	94.67
Backdoor	94.22	96.72

У табл. 6 показано середнє значення результатів нейромереж на наборах даних CTU-13 та STIN. На основі впровадження символьного шару в нейромережу збільшують ефективність усіх запропонованих метрик та покращують здатність моделі до класифікації та виявлення шкідливої поведінки.

Таблиця 6

Середнє значення класифікаторів на наборі даних CTU-13 та супутникових даних STIN

Тип нейромержи	Влучість	Точність	Повнота	F1- бал
Нейромережа	93.00	92.68	91.60	92.14
Нейромережа з символьним шаром	96.94	96.56	96.93	96.75

Висновки

Інноваційний нейросимвольний метод, запропонований у дослідженні, успішно інтегрує символьний штучний інтелект та технології глибинного навчання, створюючи потужну систему для виявлення та нейтралізації атак у сфері супутникового зв'язку. Експериментальні результати підтверджують, що представлена модель перевершує традиційні підходи, забезпечуючи високу точність виявлення навіть у складних умовах. Важливою є здатність системи адаптуватися до нових та раніше невідомих типів загроз, що робить її не лише актуальною, а й перспективною. Основою для такої ефективності стає вдосконалена архітектура, в тому числі символьний шар, що аналізує мережеві дані на основі розгорнутої бази знань про вразливості та атаки. Результати, отримані на таких наборах даних, як CTU-13 та супутниковий набір STIN, не лише демонструють високу ефективність методу, а й відкривають нові можливості для покращення кіберзахисту у сфері супутникового зв'язку, що важливо для забезпечення безпеки сучасного космічного середовища.

Література

1. Ляо, Х.Дж.; Lin, C.H.R.; Лін, Y.C.; Тунг, К.Й. Система виявлення вторгнень: комплексний огляд. J. Netw. обчис. апл. 2013, 36, 16–24

2. Хусейн, Дж.; Лалмуанавма, С.; Чхакчхуак, Л. Двоетапна гібридна техніка класифікації для системи виявлення вторгнень у мережу. Міжн. Ж. Обчисл. Intell. сист. 2016, 9, 863–875.
3. Ахмад, М. Башері, М. Дж. Ікбал, А. Рахім, Порівняння продуктивності векторної машини підтримки, випадкового лісу та екстремальної навчальної машини для виявлення вторгнень. IEEE Access 6, 33789–33795 (2018). https://doi.org/10.1109/access.2018.2841987
4. Чжун, В.; Ю, Н.; Ai, С. Застосування системи глибокого навчання на основі великих даних для виявлення вторгнень. Великі дані Мін. анальний 2020, 3, 181-195. https://ieeexplore.ieee.org/document/9142151
5. Себастьян Гарсія, Мартін Ґрілл, Ян Стіборек і Алехандро Зуніно "Емпіричне порівняння методів виявлення ботнетів. Журнал комп'ютерів і безпеки, Elsevier. 2014. Том 45, стор. 100-123. http://dx.doi.org/10.1016/j.cose.2014.05.011
6. Лі, К.; Чжоу, Х.; Ту, З.; Ван, В.; Чжан, Х. Розподілена мережева система виявлення вторгнень у супутниково-наземних інтегрованих мережах з використанням федеративного навчання. IEEE Access 2020, 8, 214852–214865.
7. Ланскі, Джан і Алі, Сакіб і Мохаммаді, Мохтар і Маджід, Мохаммед і Карім, Сархель і Рашиді, Шима і Хоссейнзаде, Мехді і Рахмані, Амір. (2021). Системи виявлення вторгнень на основі глибокого навчання: систематичний огляд 9. 101574-101599. 10.1109/ACCESS.2021.3097247

References

1. Liao, H.J.; Lin, C.H.R.; Lin, Y.C.; Tung, K.Y. Intrusion detection system: A comprehensive review. J. Netw. Comput. Appl. 2013, 36, 16–24.
2. Hussain, J.; Lalmuanawma, S.; Chhakchhuak, L. A two-stage hybrid classification technique for network intrusion detection system. Int. J. Comput. Intell. Syst. 2016, 9, 863–875
3. Ahmad, M. Basheri, M.J. Iqbal, A. Rahim, Performance comparison of support vectormachine, random forest, and extreme learning machine for intrusion detection. IEEE Access 6, 33789–33795 (2018). https://doi.org/10.1109/access.2018.2841987
4. Zhong, W.; Yu, N.; Ai, C. Applying big data based deep learning system to intrusion detection. Big Data Min. Anal. 2020,3, 181–195. https://ieeexplore.ieee.org/document/9142151
5. "An empirical comparison of botnet detection methods" Sebastian Garcia, Martin Grill, Jan Stiborek and Alejandro Zunino. Computers and Security Journal, Elsevier. 2014. Vol 45, pp 100-123. http://dx.doi.org/10.1016/j.cose.2014.05.011
6. Li, K.; Zhou, H.; Tu, Z.; Wang, W.; Zhang, H. Distributed Network Intrusion Detection System in Satellite-Terrestrial Integrated Networks Using Federated Learning. IEEE Access 2020, 8, 214852–214865
7. Li, K.; Zhou, H.; Tu, Z.; Wang, W.; Zhang, H. Distributed Network Intrusion Detection System in Satellite-Terrestrial Integrated Networks Using Federated Learning. IEEE Access 2020, 8, 214852–214865

Одержано: 06.03.2024
Внутрішня рецензія отримана:21.03.2024
Зовнішня рецензія отримана:27.03.2024

Про автора:

[1]*Мостовий Олександр Сергійович*,
аспірант першого курсу .
https://orcid.org/0009-0006-6687-866X

Місце роботи автора:
Інститут кібернетики НАН України,
Тел. (+38) (096) 822-70-78
E-mail: adsmander@gmail.com