https://doi.org/10.31891/2219-9365-2025-81-33
УДК 004.8:004.056.53

ТУРОВСЬКИЙ Олександр
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0000-0002-4961-0876
e-mail: s19641011@ukr.net
РИЖАКОВ Микола
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0006-3377-7061
e-mail: nykolay.ryjakov@gmail.com

МЕТОДИЧНИЙ ПІДХІД ДО КОМПЛЕКСНОЇ ІНДЕНТИФІКАЦІЇ ТА АНАЛІЗУ КІБЕРЗАГРОЗ ТРАФІКУ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ 5G/IMT-2020 НА ОСНОВІ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

В роботі проведено аналіз процесу ідентифікації та аналізу кіберзагроз вхідного трафіку в мережах 5G/IMT-2020, побудованих по технології Ultra-reliable and low latency communications, визначені його особливості та напрямки досліджень по підвищенню ефективності та моніторингу трафіку та аналізу кіберзагроз. Для вирішення завдання ідентифікації трафіку та аналізу кіберзагроз мережі 5G/IMT-2020 в роботі розроблена та подана відповідний методичний підхід. Вказаний методичний підхід включає формування масивів метаданих вхідного потоку корисних даних та даних кібератак, модифікацію їх в набір навчальних даних, формування навчального програмно-апаратного комплексу та розбудову структури нейронної мережі, проведення процесу навчання нейронної мережі та втілення її в процес ідентифікації трафіку та аналізу кіберзагроз в телекомунікаційних мережах 5G/IMT-2020.

Оцінка результатів процесу навчання запропонованої нейронної мережі та перевірки її роботи на тестових наборах даних у навченому стані показала, що подана в роботі нейронна мережа здатна провести моніторинг та ідентифікувати згенерований від сервісів Інтернету Речей трафік з ймовірністю до 99,7%. В процесі моніторингу та ідентифікації трафіку від двох та більше сервісів дана ймовірність може знизитися, проте перебуває у допустимих межах 80-90%.

Ключові слова: ідентифікація трафіку, моніторинг інформаційно-комунікаційної мережі 5G/IMT-2020, штучний інтелект, нейронна мережа, аналіз кіберзагроз, кібератаки DDoS, Інтернет речей, високонадійний зв'язок з мінімальними затримками (URLLC)

TUROVSKY Oleksandr, RYZHAKOV Mykola
State University of Information and Communication Technologies

METHODOLOGICAL APPROACH TO COMPREHENSIVE IDENTIFICATION AND ANALYSIS OF CYBERTHREATS IN TRAFFIC IN 5G/IMT-2020 TELECOMMUNICATION NETWORKS BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

The paper analyzes the process of identifying and analyzing cyberthreats of incoming traffic in 5G/IMT-2020 networks built using Ultra-reliable and low latency communications technology, identifies its features and research directions for increasing the efficiency and monitoring of traffic and analyzing cyberthreats. To solve the problem of identifying traffic and analyzing cyberthreats in the 5G/IMT-2020 network, the paper develops and presents an appropriate methodological approach. The specified methodological approach includes formation of metadata arrays of the incoming flow of useful data and cyberattack data, modification of them into a set of training data, formation of a training software and hardware complex and development of the neural network structure, carrying out the process of training the neural network and implementing it in the process of traffic identification and analysis of cyber threats in 5G/IMT-2020 telecommunication networks.

Evaluation of the results of the training process of the proposed neural network and verification of its operation on test data sets in the trained state showed that the neural network presented in the work is able to monitor and identify traffic generated from Internet of Things services with a probability of up to 99.7%. In the process of monitoring and identifying traffic from two or more services, this probability may decrease, but is within the permissible limits of 80-90%.

Keywords: traffic identification, 5G/IMT-2020 information and communication network monitoring, artificial intelligence, neural network, cyber threat analysis, DDoS cyberattacks, Internet of Things, Ultra-reliable and low latency communications (URLLC)

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Інтенсивний розвиток глобальних економічних відноси, посилення ролі інформаційних технологій в процесах накопичення, передачі та обробки корисних даних, вагомі досягнення науки по втіленню нових концепцій управління процесами через глобальні мережі Інтернету вивели на чільне місце необхідність переходу до впровадження перспективних концепцій мереж передачі даних, а саме стандарту 5G/IMT-2020 та, в його розвиток, наступних поколінь таких мереж.

Розбудова сучасних та перспективних концепцій мереж зв'язку, на даному етапі сконцентрована на реалізації трьох основних технологій, на основі яких безпосередньо будується мережа 5G/IMT-2020. А саме [1,2,3]:

1. Глобальні міжапаратні взаємодії – MMC (Massive Machine type Communications);
2. Високоефективний мобільний широкосмуговий зв'язок – eMBB (Enhanced Mobile Broadband);
3. Високонадійний зв'язок з мінімальними затримками – URLLC (Ultra-reliable and low latency communications).

На сьогодні впровадження інформаційно-комунікаційних мереж на основі концепції високонадійного зв'язку з мінімальними затримками (URLLC) є одним із найскладніших завдань для науково-технічної спільноти. Яке посилюється актуальність забезпечення функціонування вказаної мережі в кіберпросторі, який характеризується постійним зростанням та мінливістю методів та процедур та механізмів кібератак як на саму мережі так і на сервіси, що є кінцевим отримувачами корисних даних.

ПОСТАНОВКА ПРОБЛЕМИ

Основна вимога до мереж класу URLLC полягає у забезпеченні високої надійності передавання даних за умов надзвичайно низьких затримок [3].

Такі мережі знаходять застосування у сферах електронної медицини (e-health), автономного транспорту, небезпечних промислових виробництв формату 4.0 та інших галузях. Одними з найвідоміших сервісів, що функціонують на базі URLLC, є Інтернет речей (IoT) та Тактильний Інтернет (Tactile Internet). При розгортанні мереж для забезпечення роботи Tactile Internet ключовим фактором, що визначає архітектуру мережі та її ефективність, є саме досягнення ультранизьких затримок. Їх критичне значення обумовлює необхідність децентралізації мережевої інфраструктури через обмеження відстаней, на яких можливе надання послуг Tactile Internet.

Досягнення надзвичайно малих затримок у мережах Tactile Internet та IoT здатне спричинити децентралізацію економіки й сприяти подоланню цифрової нерівності як усередині окремої держави, так і між регіонами в межах певної соціально-економічної спільноти [1,2].

Зростаючі обсяги трафіку мережі 5G/IMT-2020, його гетерогенність та різноманітність сервісу Tactile Internet та інших сервісів, у тому числі тих, що належать до URLLC, диктує нові вимоги до оперативності прийнятих рішень щодо забезпечення якості обслуговування (QoS) залежно від умов функціонування всієї системи в цілому. Необхідно врахувати, що однією з таки умов є постійне зростання кіберзагроз процесам передачі корисних даних [2,3].

Слід також зазначити, що у процесі розробки рішень для мереж 5G/IMT-2020, формування відповідних стандартів і проведення супутніх досліджень було зроблено висновки, які свідчать про складність забезпечення вимог URLLC у контексті широкомасштабного впровадження таких послуг [4,6]. Забезпечення сервісів URLLC є можливим лише в межах обмежених географічних зон із використанням виділених мережевих каналів та за умов дотримання низки інших обмежень.

Неоднорідність трафіку, складність ініціалізації потоків, прогнозування їхнього зростання, а також потреба в оперативному виявленні змін профілю трафіку і їх точному аналізі ускладнюють ефективне управління мережею. У зв'язку з цим традиційні «ручні» методи моніторингу, що використовуються в мережах п'ятого покоління (5G/IMT-2020), поступово втрачають свою актуальність і потребують модернізації.

Необхідною умовою функціонування такої мережі є достатньо ефективний її кіберзахист, особливо спрямований на забезпечення цілісності та доступності інформації, що передається та підпадає під целеспрямовані кібератаки.

В умовах глобальної цифровізації питання оцінки рівня захищеності та безпеки мережевого трафіку набуває критичного значення. Зважаючи на різноманіття форматів і значний обсяг даних, що передаються через мережі, слід визнати, що традиційні підходи до кібербезпеки, орієнтовані виключно на технічні засоби захисту, вже не відповідають сучасним викликам [1–4].

У міжнародних стандартах з кібербезпеки, зокрема в Standard ISO/IEC 27032:2023, з урахуванням розвитку глобальної мережі Інтернет, дається визначення понять кіберпростору та кібербезпеки [5,6]. Кіберпростір трактується як середовище (віртуальний простір), що створює умови для комунікацій і соціальних взаємодій, яке виникає в результаті роботи взаємопов'язаних комунікаційних систем і забезпечення електронних зв'язків через Інтернет та/або інші глобальні мережі передачі даних.

Кібербезпека, згідно з цим стандартом, — це стан захищеності життєво важливих інтересів особи, суспільства та держави у процесі використання кіберпростору, що забезпечує сталий розвиток інформаційного суспільства, стабільність цифрового комунікаційного середовища, а також своєчасне виявлення, попередження та нейтралізацію реальних і потенційних загроз національній безпеці України в кіберпросторі [6].

Дані обставини, а саме забезпечення оперативного реагування систем управління мережею на зростання трафіку, зміни гетерогенності в мережах 5G/IMT-2020 (в тому числі періодичного трафіку),

аналізу змін профілю трафіку та вчасної його ідентифікації в умовах впливу кіберзагроз потрібно розробити та втілити відповідну низку механізмів та процедур, пристосованих для ідентифікації трафіка та аналізу на цілісність та доступність інформації.

АНАЛІЗ ЛІТЕРАТУРНИХ ДЖЕРЕЛ ТА ПОСТАНОВКА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Питанням ідентифікації та моніторингу трафіку в інформаційно-комунікаційних мережах останніх поколінь присвячено рад наукових публікацій. Основні підходи та принципі рішення задання ідентифікації та моніторингу подано в наукових роботах [7-10]

На даний момент якість обслуговування в мережах зв'язку забезпечується за допомогою технологій DiffServ (Differential Services), а також інших TE (Traffic Engineering) рішень, наприклад MPLS-TE, що використовує в основі протокол резервування ресурсів RSVP-TE [7,8]. Однак ці рішення мають ряд недоліків для їх застосування в ряді сервісів у мережах п'ятого та наступних поколінь. Основними недоліками є відсутність окремого аналізу та вчасного виявлення ознак кіберзагроз та відсутність динамічного управління трафіком залежно від мінливості його профілю а також обмежений набір класифікаторів трафіку, що в обслуговування сервісів IoT та інших є дуже критичним недоліком.

Необхідний рівень абстрагування від фізичних процесів реалізують концепції SDN (software-defined networking, SDN; програмно-конфігурована мережа) і NFV (Network Functions Virtualization, NFV – концепція віртуалізації мережевої архітектури), що викладені в роботах [9,10]. Відмітимо, що для оперативного реагування систем управління мережі, у разі застосування концепцій SDN та NFV – контролера SDN і Оркестратора, потрібно проводити високоточну ідентифікацію трафіку без безпосереднього втручання у потік на рівні передачі даних та відповідно, без внесення змін до його профілю, а також мінімізації затримок трафіку [9,10]. Механізми такої ідентифікації та процедури моніторингу без втручання в потік даних в поданих роботах не розглянуті, а викладені процедури концепцій SDN і NFV загалом не дозволяють здійснити такий моніторинг при одночасному вирішення покладного на SDN забезпечення кібербезпеки мережі.

Таким чином, завдання по ідентифікації трафіку та подальшого аналізу кіберзагроз в мережах 5G/IMT-2020 при умові ультрамалих затримок та забезпечення цілостності інформації потребує розробки окремого методичного підходу. Виходячи з того, що певні питання моніторінгу трафіку та окремого забезпечення кіберзахисту мереж вже вирішується за допомогою технологій штучного інтелекту, такий методичний підхід повинен бути заснований на вказаних технологіях. Основні вимоги до такого методичного підходу це комплексне рішення, яке дозволить забезпечити вчасне та ефективне виявлення змін трафіку, його розрахунок та оперативне прийняття рішень по управлінню трафіком в умовах наявності кіберзагроз в телекомунікаційних мережах 5G/IMT-2020.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою дослідження є розробка методичного підходу до комплексної ідентифікації та аналізу кіберзагроз трафіку в телекомунікаційних мережах 5G/IMT-2020, які функціонують в межах концепції передачі даних URLLC.

Для досягнення вказаної мети необхідно:

- визначити механізми ідентифікації та аналізу кіберзагроз трафіка без втручання процес передачі даних та сформувати принципи його функціонування;
- розробити комплексний алгоритм ідентифікації та аналізу кіберзагроз трафіку в телекомунікаційних мережах 5G/IMT-2020, яка повинна функціонувати в межах концепції передачі даних URLLC;
- оцінити можливості застосування поданого алгоритму та створеної на його основі методики для моніторингу навантаження в телекомунікаційних мережах 5G/IMT-2020, які повинні функціонувати в межах концепції передачі даних URLLC.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Як було зазначено раніше, завдання ідентифікації та аналізу кіберзагроз трафіку включає необхідність розпізнавання великої кількості типів сервісів, функціонування яких забезпечується вимогами URLLC. При цьому, така ідентифікація та аналіз кіберзагроз не повинні вносити додаткові затримки у трафік, та забезпечувати можливість розширення та налаштування алгоритму під певне географічне розташування мережі та сервісів [4,6]. Неоднорідність трафіку, складність його ініціалізації та розрахунку його зростання на фоні постійних кібератак, а також складність оперативного розрахунку змінення профілю трафіку призводять до того, що прийняті в даний час для вирішення вказаних завдань «ручні» методи моніторингу та аналізу трафіку втрачають свою актуальність.

В даний час, на основі проведених наукових досліджень прийнята до реалізації та втілюється низка рішень, які забезпечують значне розширення можливості мереж 5G/IMT-2020 по забезпеченню передачі даних відповідно вимог URLLC. А саме [5,7,8]:

1. Зміна технологій передачі даних на фізичному рівні та перехід на "квантові комунікації", які реалізують інший фізичний механізм передачі інформації, заснований на принципі квантової заплутаності. В даний час цей метод знаходиться на стадії ранніх досліджень.

2. Децентралізація мереж зв'язку та децентралізація систем обчислень, гнучке їх управління з імплементацією Штучного інтелекту (ШІ) як системи моніторингу, аналізу та управління.

Виходячи з аналізу поточного рівня мережевих технологій 5G/IMT-2020, які повинні забезпечити процес передачі даних відповідно концепції URLLC та часткових завдань моніторингу, аналізу та управління, в рамках процесу впровадження ШІ в системи управління вказаними мережами найбільш актуальними завданнями для нейромерж будуть наступні [6,9,10]:

– повноцінна ідентифікація трафіку від різних сервісів з подальшим прогнозуванням змін його характеристик;

– аналіз кіберзагроз цілісності та доступності інформації, що передається через мережу;

– ефективний та динамічний розподіл обчислень на інфраструктурі розподілених обчислень характеристик трафіку з залученням окремо визначених механізмів мінімізації кіберзагроз;

– прогнозування та ідентифікація можливих перевантажень керуючих систем, та їх блокування методами кібератак.

При цьому завдання ідентифікації трафіку включає необхідність розпізнавання великої кількості типів сервісів (враховуючи URLLC) та одночасний аналіз кіберзагроз при умові виключення додаткових затримок у трафік та забезпечення можливості адаптації та налаштування алгоритмів ідентифікації та аналізу кіберзагроз під певне географічне розташування мережі та сервісів [4,6].

Поява технологій ШІ та створення на їх основі спеціалізованих систем глибокої інспекції пакетів (DPI, Deep Packet Inspection) відкриває можливість здійснювати моніторинг трафіку на сервісному рівні інфраструктури програмно-конфігурованих мереж [12–14].

У зв’язку з цим, на основі аналізу сучасних можливостей моніторингу трафіку в мережах 5G/IMT-2020, у даній роботі пропонується підхід до вирішення зазначеного завдання, що базується на використанні нейронних мереж спеціальної архітектури. Основною функцією таких мереж є виявлення та ідентифікація певного типу трафіку у загальному обсязі вхідного трафіку визначеної мережі.

Система DPI, як випливає з назви, виконує глибокий аналіз усіх пакетів вхідних даних, що проходять через неї. Під терміном «глибокий» мається на увазі аналіз даних на верхніх рівнях моделі OSI, а не лише на основі стандартних номерів портів. Окрім розпізнавання пакетів за певними стандартними шаблонами — наприклад, за структурою заголовків, портами тощо — DPI-системи також здійснюють поведінковий аналіз трафіку. Такий аналіз дозволяє ідентифікувати додатки, що не використовують стандартних механізмів обміну даними, заздалегідь невідомих або нестандартних [14,15].

Запропонована реалізація DPI як окремої програмно-апаратної системи, яка інтегрується на серверному рівні через REST-інтерфейс, дозволяє створити автономну систему ідентифікації трафіку з мінімальними затримками та спрощеною реалізацією програмно-апаратного комплексу.

Залежно від потреб, така система може бути реалізована як у вигляді апаратно-програмного комплексу, так і як виключно програмне рішення (наприклад, у формі мережевого застосунку).

Принципова архітектура запропонованого рішення з побудови системи ідентифікації трафіку наведена на рис. 1.

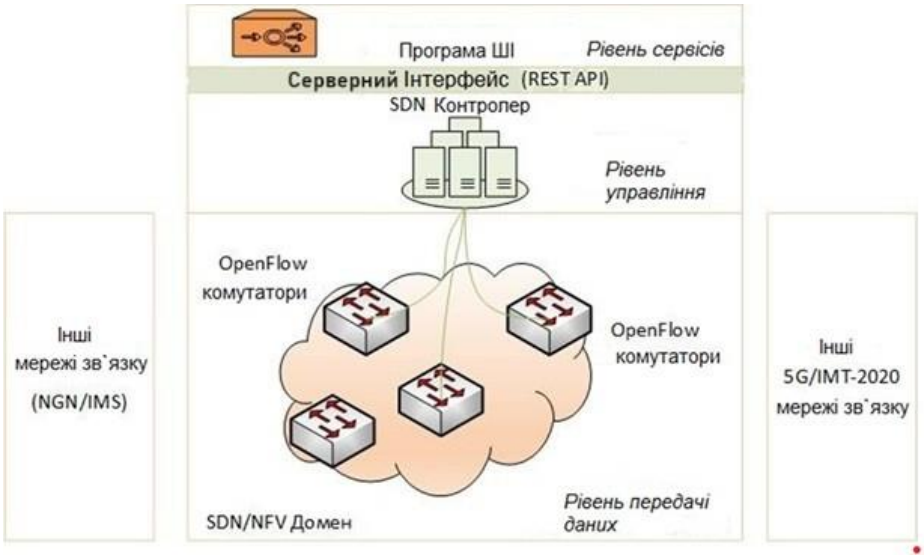

Рис.1 Архітектура системи ідентифікації трафіку на основі технології DPS

Для системи моніторингу трафіку поданого типу на основі технології DPS всі пристрої та потоки є «цифровим об'єктом», що має ряд параметрів та функцій (дій над параметрами), представленим набором методів [14,15].

Такий підхід дозволяє реалізувати систему моніторингу інфомаційно-комунікаційної мережі, яка працюватиме з даними про потоки (метадані) у режимі «на льоту». Дана система, через свої властивості, дозволяє не вносити додаткові затримки у трафік, а також будь-яким чином змінювати його активність (зміни законів розподілу, інтенсивність тощо). Основою функціонування даної системи є процес «спостереження» за активністю потоків і формування «загальної картини» передачі даних, що відбувається в підконтрольній мережі.

Вхідні дані для поданої системи формуються на основі тих даних, які система може отримати через серверний Інтерфейс контролера і Оркестратора мережі.

Оскільки у цій роботі розглядається аналітика активності потоків і виявлення потоків Інтернету Речей лише на рівні передачі даних, аналітична система має можливість запитати дані таблиць потоків (Flow Tables) з усіх підконтрольних комутаторів SDN у контролера. Аналізуючи дані, що відображаються у двох глобальних частинах таблиці: Match Field і Actions, можна дійти висновку, що на їх основі можна скласти метамодель потоків. Скорочену структуру таблиці потоків комутатора відображено на рис. 2.

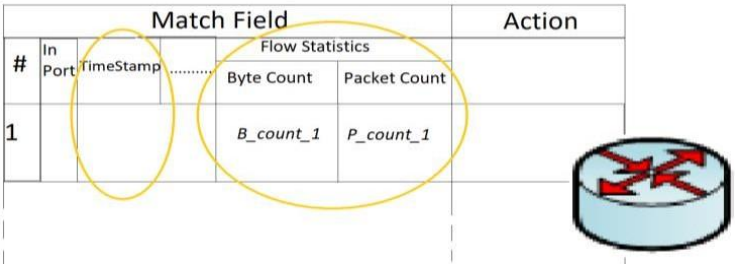

Рис 2. Структура таблиці потоків комутатора S

На рис. 2 жовтими колами виділено ті дані, які використовуються для формування метамоделі про досліджуваний потік у мережі.

Однією з важливих особливостей цих даних є те, що на основі лічильників Byte Count та Packet Count не можна визначити точну довжину пакета в потоці, оскільки за один момент часу лічильники можуть дорівнювати: Byte Count –1500, Packet Count – 2. Відповідно, на основі цих даних не можна точно визначити довжину кожного з пакетів, зареєстрованих у потоці за проміжок часу: $\Delta T = 1$ с.

Варто також відзначити, що лічильники відображають сумарне значення параметрів [Byte Count, Packet Count]. Однак, крім даних лічильників у таблиці потоків існує ще один параметр – Time Stamp, який дозволяє оцінити в кожен момент часу миттєве значення [ByteCount_delta] та [PacketCount_delta]. Таким чином, за довільний період часу ΔT, маючи відліки значень [Byte Count], [Packet Count], [TimeStamp], можливо скласти набір даних з встановленої структурою даних, де кожен відлік відображає миттєве значення [ByteCount_delta] та [PacketCount_delta].

Аналіз низки відомих нейронних мереж, призначених для моніторингу потоків різних типів даних, показав, що одним із ефективних рішень є нейронна мережа, заснована на технології Deep Learning — методі машинного навчання, що використовує багатошарові структури для аналізу даних, автоматичного виокремлення ознак і побудови складних моделей для вирішення завдань ідентифікації, моніторингу та аналізу [16,17].

Нейронні мережі Deep Learning являють собою набір алгоритмів, які дозволяють моделювати високорівневі абстракції у великих масивах даних. У процесі такого моделювання мережа здатна самостійно виявляти приховані закономірності та ознаки, а кількість прихованих шарів у її структурі перевищує два. З огляду на специфіку об’єкта моніторингу — трафік мережі 5G/IMT-2020 — та особливості даних (числові статистичні ряди, що слугують метаданими), було обрано саме цей тип нейронної мережі на основі Deep Learning.

Розробка та навчання нейронної мережі здійснювалися із використанням високорівневої мови програмування Python і спеціалізованих бібліотек та фреймворків. Для реалізації завдання моніторингу трафіку як архітектуру штучної нейронної мережі було обрано рекурентну нейронну мережу (RNN) із додатковими шарами LSTM (Long Short-Term Memory) [18]. Мережа LSTM є універсальною, оскільки, за наявності достатньої кількості нейронів, здатна виконувати будь-які обчислення, що під силу традиційному комп’ютеру.

Інтеграція в архітектуру LSTM-модуля, як складової штучної нейронної мережі, дозволяє виявляти зв’язки між попередніми та поточними даними, навіть за умов великого діапазону значень. Це особливо важливо для розпізнавання закономірностей у трафіку Інтернету речей, який часто характеризується

самоподібністю та періодичністю, що відзначається у багатьох наукових дослідженнях [5,6,19].

Обрана нейронна мережа реалізує підхід «навчання з учителем», що передбачає створення початкового навчального набору даних із маркованими мітками, а також збереження стану навченої моделі для подальшого використання [19].

Для навчання мережі вхідні дані у форматі DataSetML перетворюються на DataSetMLtrain шляхом додавання нового стовпчика з ідентифікаторами статистичних вибірок для кожного рядка. З метою розпізнавання більшої кількості типів трафіку, навчальний набір необхідно розширити, додаючи відповідні мітки — наприклад, для трафіку IoT [17,18].

Архітектура обраної мережі Deep Learning включає два глибинні повнозв'язані шари LSTM та два глибинні шари рекурентної нейронної мережі (RNN), кожен із яких містить по 7 прихованих нейронів. Важливим є побудова алгоритму функціонування вказаної нейромережі в частині аналізу кіберзагроз трафіку. Вказаний алгоритм побудуємо відносно найбільш поширеного виду кібератаки на мережу, а саме, Slow DDoS атаки. Мета яких, порушити доступність до інформації, що передається мережею методом перевантаження мережі [19,20].

Slow DDoS (Slowloris, Slow HTTP POST, Slow Read, R.U.D.Y.) – це атаки, при яких зловмисник навмисне підтримує велику кількість з'єднань з сервером, надсилаючи мінімальні дані, тим самим виснажуючи ресурси сервера.

Для ідентифікації таких атак пропонується наступний алгоритм роботи нейронної мережі [17,18,21]:

Крок 1: Збір та підготовка даних

• **Збір мережевого трафіку** у вигляді журналів взаємодії клієнтів із сервером (IP-адреси, методи HTTP-запитів, інтервали між пакетами, час сесій).

• Виділяються ознаки, які особливо характерні саме для повільних атак:

• Частота надсилання пакетів (надзвичайно низька швидкість передачі)

• Тривалий час відкритих сесій з мінімальною кількістю даних

• Наявність великої кількості відкритих, але неактивних підключень до сервера

Крок 2: Попередня обробка

• Дані нормалізуються, приводяться до числових значень, очищаються від шумів і випадкових сплесків трафіку.

• IP-адреси кодуються у числові значення або у вектори ознак (наприклад, one-hot encoding).

• Дані агрегуються за певними часовими інтервалами (наприклад, хвилина, 30 секунд).

Крок 3: Архітектура нейронної мережі

Найкраще підходять архітектури, що працюють із послідовностями (наприклад, LSTM або GRU):

• **Вхідний шар**:

• Отримує набір підготовлених послідовностей трафіку.

• Кожен елемент послідовності містить параметри (час між пакетами, довжина пакету, активність сесії).

• **Прихований рекурентний шар (LSTM/GRU)**:

• Вивчає тимчасові залежності, патерни поведінки клієнта.

• Враховує як частоту запитів, так і тривалість відкритих сесій.

• **Вихідний шар**:

• Визначає ймовірність того, що поточна поведінка є аномальною (атака) або нормальною (звичайна активність).

Крок 4: Навчання нейронної мережі

• Використовується навчання з учителем (supervised learning):

• Позначаються дані як «slow DDoS» та «нормальний трафік».

• Використовується оптимізатор Adam із функцією втрат binary_crossentropy.

• Нейромережа навчається розпізнавати патерни, типові для slow DDoS-атак:

• довготривалі сесії з дуже низькою активністю

• велика кількість відкритих TCP-з'єднань

• низька швидкість передачі даних з одного джерела

Крок 5: Робота нейронної мережі у реальному часі

• Нейромережа в реальному режимі аналізує трафік:

• Отримує поточні параметри з'єднань.

• Подає ці дані у модель, яка обчислює ймовірність slow DDoS.

• Якщо ймовірність перевищує певний пороговий рівень (наприклад, 85-90%), система автоматично спрацьовує:

• генерується тривога для адміністраторів

• активуються механізми блокування IP-адрес або з'єднань

Крок 6: Оцінка та покращення

• Регулярно здійснюється оцінка ефективності моделі за допомогою метрик (Accuracy, Precision, Recall, F1-score).

• Проводиться періодичне перенавчання моделі на нових даних, щоб адаптуватись до змін поведінки атакувальників.

Запропонований метод ідентифікації та аналізу кіберзагроз трафіку мережі 5G/IMT-2020 пропонується реалізуватиу вигляді програмного модуля мовою програмування Python версії 2.7 для аналітичної системи, реалізованої на основі MVC патерну.

Дане програмне забезпечення, відповідного обраного підходу до ідентифікації та аналізу трафіку, схематично поданого на рис.3 втіленням відповідної функції, реалізованої через програмний застосунок, вкладений поверх серверного програмного інтерфейсу API контролера програмно-конфігурованої мережі та Оркестратора мережі лабораторії.

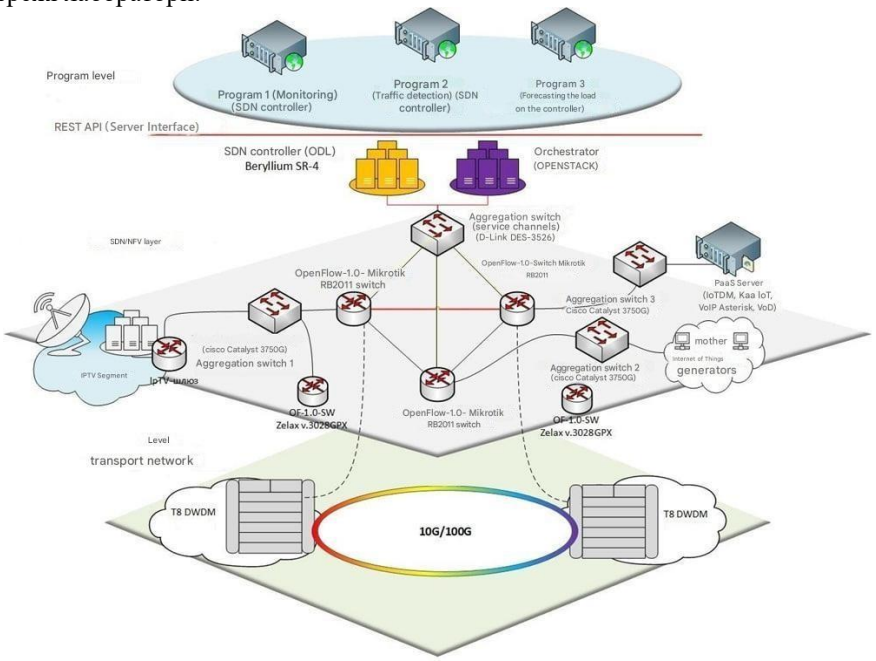

Рис. 3. Схема функціонування програмно апаратного комплекснейронної мережі

В результаті експериментального дослідження за допомогою запропонованого програмно-апаратного комплексу, схематично поданого на рис.3 отримано масив даних $DataSet_{MLtrain}$, який сформований з двох маркованих наборів даних (IoT, Video).

Далі $DataSet_{MLtrain}$ подається на вхід нейронної мережі, конфігурація якої відображена вище.

За отриманим масивом $DataSet_{MLtrain}$ побудована діаграма розкиду значень. Діаграма наведена на рис. 4.

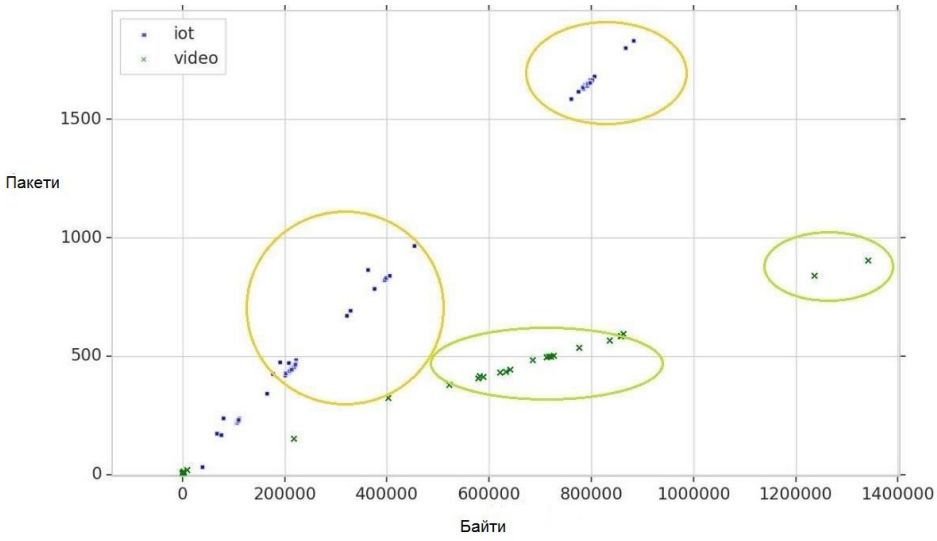

Рис. 4. Діаграма розкиду значень DataSetML*train*

Після того, як навчальний набір даних сформований, згідно з алгоритмом, викладеним вище в цій статті, програмний модуль розробленого додатка, що реалізує штучну нейронну мережу (ШНМ), переходить до процесу навчання нейронної мережі.

Протягом процесу навчання нейронної мережі розробленим додатком контролюються та фіксуються значення наступних параметрів [23,24]:

- Train Accurancy (Точність навчання);
- Test Accurancy (Точність проходження тесту ШНМ);
- Train loss (Помилки під час навчання);
- Test loss (Помилки під час проходження тесту ШНМ);

Графік, що відображає дані параметри у процесі проходження епох навчання, наведено на рис.5.

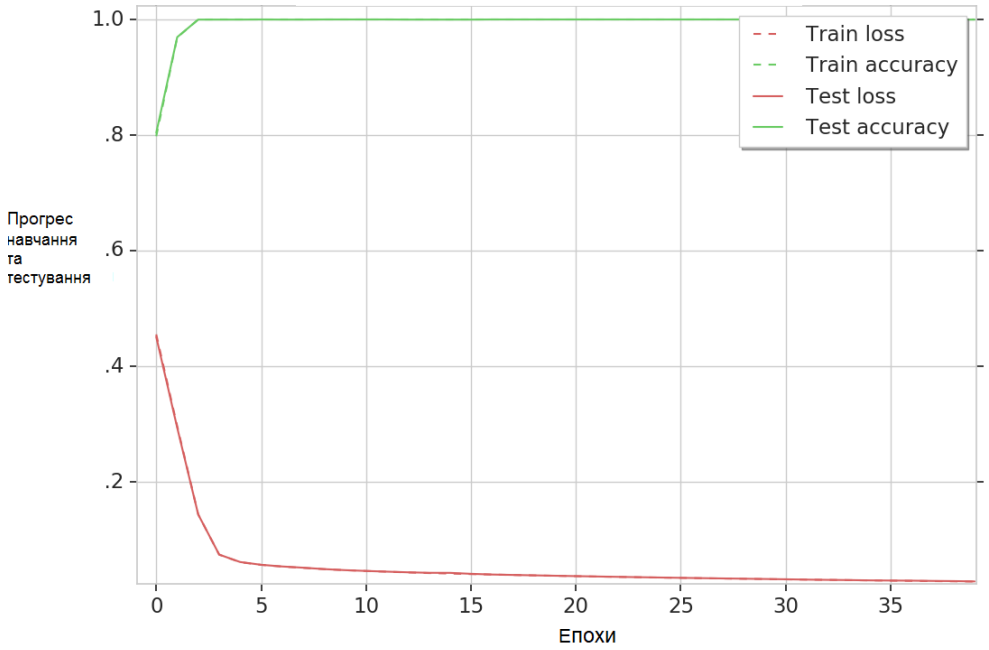

Рис. 5. Графік навчання та тестування штучної нейронної мережі

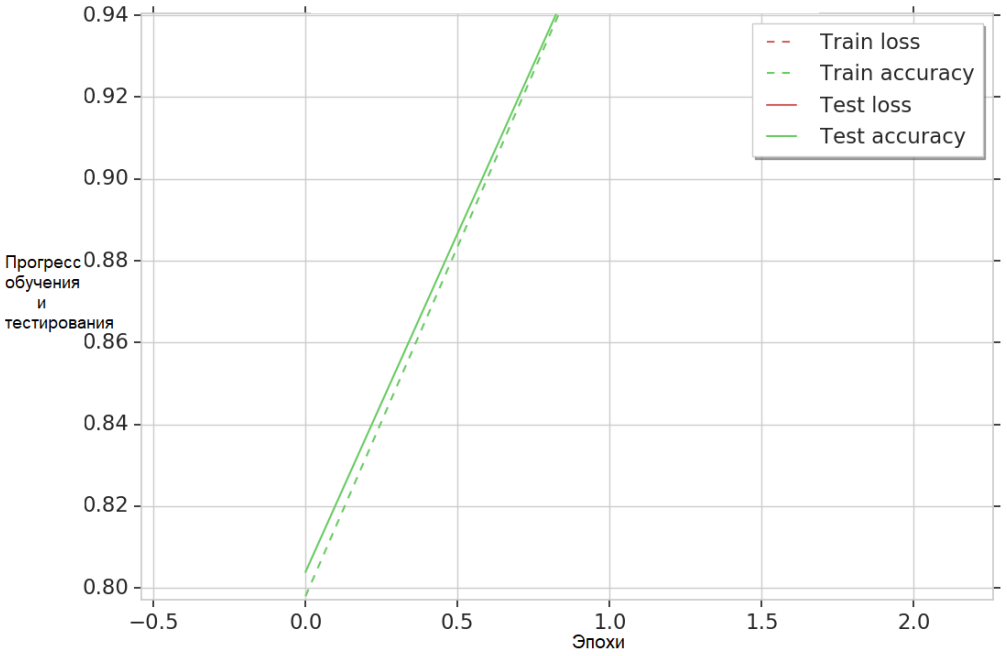

Рис. 6. Масштабований графік навчання та тестування штучної нейронної мережі

Аналіз залежностей, поданих на рис.5, рис.6, де відображено процес навчання мережі, показав, що для поставленого завдання моніторингу трафіку розроблена штучна нейронна мережа успішно пройшла процес навчання. В результаті процесу навчання нейронної мережі та перевірки її роботи на тестових наборах даних у навченому стані розроблена нейронна мережа може ідентифікувати потік Інтернету Речей, що генерується, з ймовірністю 99,7%.

Варто відзначити, що отримана ймовірність розпізнавання потоків даних (трафік даних від мережі Інтернету Речей та трафік Відео) має досить високі значення і при збільшенні кількості типів трафіку, що розпізнаються, дана ймовірність може знизитися, проте перебуває у допустимих межах (80-90%) [21,22].

Таким чином, запропоновано методичний підхід до комплексної індентифікації та аналізу кіберзагроз трафіку в телекомунікаційних мережах 5G/IMT-2020 на основі технологій штучного інтелекту включає:

– процес формування метамоделі потоків вхідних даних в мережу 5G/IMT-2020: DataSetML = ([Byte Count], [Packet Count], [TimeStamp]);

– модифікація DataSetML в навчальний набір DataSetMLtrain шляхом включення в набір даних ідентифікаторів статистичної вибірки;

– формування програмно-апаратного комплексу навчання та оцінки ефективності застосування нейронної мережі для ідентифікації та аналізу кіберзагроз трафіку мережі 5G/IMT-2020;

– побудову структури нейронної мережі Deep Learning з додатковими шарами LSTM відповідно задань ідентифікації та аналіху кіберхагроз трафіку мережі 5G/IMT-2020;

– реалізацію процесу навчання нейронної мережі та підготовка її до функціонування за призначенням;

– втілення запропонованого методу та програмно – апаратного комплексу в процес ідентифікації та аналізу трафіку в телекомунікаційних мережах 5G/IMT-2020.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

1. В роботі проведено аналіз процесу ідентифікації та аналізу кіберзагроз вхідного трафіку в мережах 5G/IMT-2020, побудованих по технології Ultra-reliable and low latency communications, визначені його особливості та напрямки досліджень по підвищенню ефективності та моніторингу трафіку та аналізу кіберзагроз.

2. Для вирішення завдання ідентифікації трафіку та аналізу кіберзагроз мережі 5G/IMT-2020 в роботі розроблена та подана відповідний методичний підхід.

Вказаний методичний підхід включає формування масивів метаданих вхідного потоку корисних даних та даних кібератак, модифікацію їх в набір навчальних даних, формування навчального програмно-апаратного комплексу та розбудову структури нейронної мережі, проведення процесу навчання нейронної мережі та втілення її в процес ідентифікації трафіку та аналізу кіберзагроз в телекомунікаційних мережах 5G/IMT-2020.

3. Оцінка результатів процесу навчання запропонованої нейронної мережі та перевірки її роботи на тестових наборах даних у навченому стані показала, що подана в роботі нейронна мережа здатна провести моніторинг та ідентифікувати згенерований від сервісів Інтернету Речей трафік з ймовірністю до 99,7%.

В процесі моніторингу та ідентифікації трафіку від двох та більше сервісів дана ймовірність може знизитися, проте перебуває у допустимих межах 80-90%.

Література

1. В.С. Шуста, А.І. Сусла, В.Ю. Біганич, «Трансформація мережевих технологій: від 4G до 5G», Вчені записки ТНУ імені В.І. Вернадського, Серія: Технічні науки, 2024, 3, С.94-99

2. Technical Report ITU-T GSTP-TN5G: Transport network support of IMT-2020/5G. –SG15-TD338/PLEN, October 2018.

3. Draft Recommendation Characteristics of transport networks to support IMT-2020/5G (G.ctn5g). – SG15-TD295/PLEN, October 2018

4. S. Hendaoui, F. Hendaoui, N. Zangar, «Dynamic proactive–reactive scheduling for URLLC in 5G: Leveraging XGBoost and network virtualization», Physical Communication, 68, art. no. 102553. 2025.

5. X. Shen, W. Liao, Q.Yin, «A Novel Wireless Resource Management for the 6G-Enabled High-Density Internet of Things», IEEE Wirel. Commun, 2022, 29, p.32–39.

6. X. Li, L.D. Xu, «A Review of Internet of Things—Resource Allocation», IEEE Internet Things J., 2021, 8, p.8657–8666.

7. the Internet of Things: A Survey», J. Netw. Comput. Appl. 2022, 206, 103464.

8. A.A. Ateya, S. Bushelenkov, A. Muthanna, A. Paramonov, «Multipath Routing Scheme for Optimum Data Transmission in Dense Internet of Things», Mathematics. 2023; 11(19):4168.

9. Yongho Seok, Youngseok Lee, Yanghee Choi and Changhoon Kim, "Dynamic constrained multipath routing for MPLS networks", Proceedings Tenth International Conference on Computer Communications and Networks (Cat. No.01EX495), Scottsdale, AZ, USA, 2001, pp. 348-353.

10. W.A. Aljoby, X. Wang, D.M. Divakaran, T.Z.J. Fu, «DiffPerf: Toward Performance Differentiation and Optimization With SDN Implementation», IEEE Transactions on Network and Service Management, 2024, 21(1), pp. 1012 – 1031.

11. L. Brown, «Advanced Techniques in NFV and SDN for Scalable Networks», International Journal of Communications Technology, 2022, 12(4), з.78-92.

12. L.-H. Chang, Tsung-Han Lee, Hung-Chi Chu, and Cheng-Wei Su, "Application-Based Online Traffic Classification with Deep Learning Models on SDN Networks", Adv. technol. innov., Sep. 2020, 5(4), pp. 216–229.

13. P.K.R. Maddikunta, Q.-V. Pham, D.C. Nguyen, (eds), «Incentive Techniques for the Internet of Things: A Survey», J. Netw. Comput. Appl. 2022, 206, 103464.

14. Foreman, Justin, Waters, Willie L., Kamhoua, Charles A., Hemida, Ahmed H. Anwar, Acosta (2024) Detection of Hacker Intention Using Deep Packet Inspection? Journal of Cybersecurity and Privacy, 4 (4), pp. 794 – 804. DOI: 10.3390/jcp4040037

15. Parra G. D. L. T., Rad P., Choo K. K. R., Beebe N. Detecting internet of things attacks using distributed deep learning. Journal of Network and Computer Applications, 2020, vol. 163, pp. 102662. doi:10.1016/ j.jnca.2020.102662

16. Al-Garadi M. A., Mohamed A., Al-Ali A., Du X., Guizani M. A Survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 2020, vol. 22, no. 3, pp. 1646–1685. doi:10.1109/COMST.2020.2988293

17. Pacheco, Fannia & Exposito, Ernesto & Gineste, Mathieu & Baudoin, Cédric & Aguilar, Jose. (2018). Towards the Deployment of Machine Learning Solutions in Network Traffic Classification: A Systematic Survey. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2018.2883147.

18. Hochreiter, Sepp & Schmidhuber, Jürgen. (1997). Long Short-Term Memory. Neural Computation. 9. 1735-1780. 10.1162/neco.1997.9.8.1735.

19. Кондакова, А., & Корецький, О. (2024). Моделі побудови мереж інтернету речей для управління інфраструктурою міста. *Smart Technologies*, 2(15), 124–132. DOI: https://doi.org/10.32347/st.2024.2.1901

20. Oleksandr Koretskyi, Rodion Khvorostianyi, Yevhen Bondarenko Hardware and software complex for the functioning of a neural network for identification and traffic management in 5G/IMT-2020 networks. *The IV International Conference «Emerging Technology Trends on the Smart Industry and the Internet of Things «TTSIIT»*, м. Київ, Україна, 21-22 січня 2025 р., Київ, КНУБА. С.44-49. https://drive.google.com/file/d/145aOtud0A7zl4N9RKXiFyt9iMLKYsMt_/view

21. J.Yao, Y. Wang, Q. Li, Mao, «An Efficient Routing Protocol for Quantum Key Distribution Networks», Entropy, 2022, 24, 911.

22. Study on Scenarios and Requirements for Next Generation Access Technologies (3GPP TR 38.913 version 14.2.0 Release 14). https://www.etsi.org/deliver/etsi_tr/138900_138999/138913/14.02.00_60/tr_138913v140200p.pdf

References

1. V.S. Shusta, A.I. Susla, V.Yu. Biganych, "Transformation of Network Technologies: From 4G to 5G", Scientific Papers of V.I. Vernadsky TNU, Series: Technical Sciences, 2024, 3, P.94-99

2. Technical Report ITU-T GSTP-TN5G: Transport network support of IMT-2020/5G. –SG15- TD338/PLEN, October 2018.

3. Draft Recommendation Characteristics of transport networks to support IMT-2020/5G (G.ctn5g). – SG15-TD295/PLEN, October 2018

4. S. Hendaoui, F. Hendaoui, N. Zangar, "Dynamic proactive–reactive scheduling for URLLC in 5G: Leveraging XGBoost and network virtualization", Physical Communication, 68, art. no. 102553. 2025.

5. X. Shen, W. Liao, Q. Yin, "A Novel Wireless Resource Management for the 6G-Enabled High-Density Internet of Things", IEEE Wirel. Commun, 2022, 29, pp. 32–39.

6. X. Li, L.D. Xu, "A Review of Internet of Things—Resource Allocation", IEEE Internet Things J., 2021, 8, pp. 8657–8666.

7. the Internet of Things: A Survey", J. Netw. Comput. Appl. 2022, 206, 103464.

8. A.A. Ateya, S. Bushelenkov, A. Muthanna, A. Paramonov, "Multipath Routing Scheme for Optimum Data Transmission in Dense Internet of Things", Mathematics. 2023; 11(19):4168.

9. Yongho Seok, Youngseok Lee, Yanghee Choi and Changhoon Kim, "Dynamic constrained multipath routing for MPLS networks", Proceedings Tenth International Conference on Computer Communications and Networks (Cat. No.01EX495), Scottsdale, AZ, USA, 2001, pp. 348-353.

10. W.A. Aljoby, X. Wang, D.M. Divakaran, T.Z.J. Fu, "DiffPerf: Toward Performance Differentiation and Optimization With SDN Implementation," IEEE Transactions on Network and Service Management, 2024, 21(1), pp. 1012 - 1031.

11. L. Brown, "Advanced Techniques in NFV and SDN for Scalable Networks", International Journal of Communications Technology, 2022, 12(4), pp. 78-92.

12. L.-H. Chang, Tsung-Han Lee, Hung-Chi Chu, and Cheng-Wei Su, "Application-Based Online Traffic Classification with Deep Learning Models on SDN Networks", Adv. technology innov., Sep. 2020, 5(4), pp. 216–229.

13. P.K.R. Maddikunta, Q.-V. Pham, D.C. Nguyen, (eds), "Incentive Techniques for the Internet of Things: A Survey", J. Netw. Comput. Appl. 2022, 206, 103464.

14. Foreman, Justin, Waters, Willie L., Kamhoua, Charles A., Hemida, Ahmed H. Anwar, Acosta (2024) Detection of Hacker Intention Using Deep Packet Inspection? Journal of Cybersecurity and Privacy, 4 (4), pp. 794 – 804. DOI: 10.3390/jcp4040037

15. Parra G. D. L. T., Rad P., Choo K. K. R., Beebe N. Detecting internet of things attacks using distributed deep learning. Journal of Network and Computer Applications, 2020, vol. 163, pp. 102662. doi:10.1016/ j.jnca.2020.102662

16. Al-Garadi M. A., Mohamed A., Al-Ali A., Du X., Guizani M. A Survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 2020, vol. 22, no. 3, pp. 1646–1685. doi:10.1109/COMST.2020.2988293

17. Pacheco, Fannia & Exposito, Ernesto & Gineste, Mathieu & Baudoin, Cédric & Aguilar, Jose. (2018). Towards the Deployment of Machine Learning Solutions in Network Traffic Classification: A Systematic Survey. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2018.2883147.

18. Hochreiter, Sepp & Schmidhuber, Jürgen. (1997). Long Short-Term Memory. Neural Computation. 9. 1735-1780. 10.1162/neco.1997.9.8.1735.

19. 2. Kondakova, A., & Koretsky, O. (2024). Models for building Internet of Things networks for city infrastructure management. Smart Technologies, 2(15), 124–132. DOI: https://doi.org/10.32347/st.2024.2.1901

20. Oleksandr Koretskyi, Rodion Khvorostianyi, Yevhen Bondarenko Hardware and software complex for the functioning of a neural network for identification and traffic management in 5G/IMT-2020 networks. The IV International Conference «Emerging Technology Trends on the Smart Industry and the Internet of Things «TTSIIT», Kyiv, Ukraine, January 21-22, 2025, Kyiv, KNUBA. P.44-49. https://drive.google.com/file/d/145aOtud0A7zl4N9RKXiFyt9iMLKYsMt_/view

21. J. Yao, Y. Wang, Q. Li, Mao, "An Efficient Routing Protocol for Quantum Key Distribution Networks", Entropy, 2022, 24, 911.

22. Study on Scenarios and Requirements for Next Generation Access Technologies (3GPP TR 38.913 version 14.2.0 Release 14). https://www.etsi.org/deliver/etsi_tr/138900_138999/138913/14.02.00_60/tr_138913v140200p.pdf