DOI: 5https://doi.org/10.26565/2304-6201-2025-65-06

УДК (UDC) 004.93

Мірошник Марина Анатоліївна *докт. техн. наук, професор; професор кафедри комп'ютерних систем та робототехніки, ННІ комп'ютерних наук та штучного інтелекту, Харківський національний університет імені В. Н. Каразіна, майдан Свободи 6, м. Харків, Україна, 61022*
e-mail: m.miroshnyk@karazin.ua ; https://orcid.org/[0000000222312529]

Шматков Сергій Ігорович *докт. техн. наук, професор; професор кафедри комп'ютерних систем та робототехніки, ННІ комп'ютерних наук та штучного інтелекту, Харківський національний університет імені В. Н. Каразіна, майдан Свободи 6, м. Харків, Україна, 61022*
e-mail: s.shmatkov@karazin.ua; https://orcid.org/0000-0002-0298-7174

Стрілець Вікторія Євгенівна *канд. техн. наук, доцент кафедри комп'ютерних систем та робототехніки, ННІ комп'ютерних наук та штучного інтелекту, Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 6, Харків, Україна, 61022*
e-mail: viktoria.strilets@karazin.ua ; https://orcid.org/0000-0002-2475-1496

Зац Олександр Дмитрович *аспірант ННІ комп'ютерних наук та штучного інтелекту, Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 6, Харків, Україна, 61022*
e-mail: zats2021ki51@student.karazin.ua
https://orcid.org/0000-0002-7623-9187

Дослідження комп'ютерних систем для виявлення вторгнень та мережевих аномалій

Стаття присвячена опису моделей систем виявлення вторгнень та мережевих аномалій з квантовим автокодуванням у комп'ютерних системах. У роботі запропоновано інноваційні методи дослідження систем виявлення вторгнень та мережевих аномалій з квантовим автокодуванням у комп'ютерних системах, здатні забезпечувати швидке реагування і високий рівень адаптивності. Представлена модель квантового автокодера (QAE) для систем виявлення вторгнень для виявлення аномалій. QAE – це оптимізаційна модель, отримана на основі автокодерів, які включають методи відсікання, кластеризації та цілочисельного квантування.

Актуальність роботи полягає у можливості дослідження систем виявлення вторгнень та мережевих аномалій з квантовим автокодуванням у інформаційно-комунікаційних системах. Дослідження було спрямоване на **розробку методу виявлення аномальних атак** в мережевому трафіку IoT, оскільки виявлення аномалії вимагає ретельного спостереження за різними мережевими трафіками. Крім того, мережевий трафік кожного IoT-пристрою відрізняється. Тому у цьому дослідженні використовується алгоритм автокодера для виявлення аномалій. Під час навчання моделі використовувався доброякісний мережевий трафік, очікуючи, що будь-який аномальний трафік призведе до помилки реконструкції аномалії (RE).

Методи дослідження. Методи дослідження систем виявлення вторгнень та мережевих аномалій з квантовим автокодуванням у інформаційно-комунікаційних системах є імовірнісне, верифікаційне моделювання, та використання хмарних обчислень, які надають гнучкість, масштабованість та ресурси для побудови ефективних систем виявлення комп'ютерних атак.

Результати. Було згенеровано набір даних для Інтернету речей в режимі реального часу для звичайного і атакуючого трафіку. Модель автокодера працює з нормальним трафіком на етапі навчання. Потім ця ж модель використовується для реконструкції аномального трафіку, припускаючи, що помилка реконструкції (RE) аномалії буде високою, що допомагає ідентифікувати атаки. Крім того, було вивчено продуктивність автокодерів, використовуючи точність, точність, пригадування і оцінку за допомогою великого експериментального дослідження.

Висновки. Результати показують, що існує компроміс між автокодером і моделлю QAE-u8 в контексті точності та параметрів оцінки процесора, таких як пам'ять і центральний процесор. Таким чином, можна підсумувати, що існує компроміс між автокодером і моделлю QAE-u8 в контексті точності та параметрів оцінки процесора, таких як пам'ять і центральний процесор. У майбутніх дослідженнях планується зосередитися на інших вразливостях пристроїв IoT, щоб розробити більш безпечну інфраструктуру IoT.

Наукова новизна даної роботи полягає в розробці підходів і методів виявлення аномальних атак в мережевому трафіку IoT.

Ключові слова: *комп'ютерна система, системи виявлення вторгнень, системи виявлення мережевих аномалій, квантове автокодування.*

Як цитувати: Мірошник М. А., Шматков С. І., Стрілець В. Є., Зац О. Д. Дослідження комп'ютерних систем для виявлення вторгнень та мережевих аномалій. *Вісник Харківського національного університету імені В. Н. Каразіна, серія Математичне моделювання.*

© Мірошник М. А., Шматков С. І., Стрілець В. Є., Зац О. Д., 2025
This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0.

Інформаційні технології. Автоматизовані системи управління. 2025. вип. 65. С.67-82. https://doi.org/10.26565/2304-6201-2025-65-06

How to quote: M. Miroshnyk, S. Shmatkov, V. Strilets, and O. Zats, "Investigation of computer systems to detect intrusions and network anomalies". *Bulletin of V. N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 65, pp. 67-82, 2025. https://doi.org/10.26565/2304-6201-2025-65-06 [in Ukrainian]

1 Вступ

Впровадження технології Інтернету речей (IoT) у різні сфери господарства вимагає постійного підключення до мережі та обміну даними. Мережі та пристрої IoT можуть стати об'єктом кібер атак для перенапрямлення, злочинного користування або викрадення трафіку. Дане дослідження було спрямоване на розробку методу виявлення аномальної поведінки в мережевому трафіку IoT. Виявлення аномалії вимагає ретельного спостереження за різним мережевим трафіком IoT. У роботі розглянуто мережевий трафік IoT, отриманий в реальному часі з чотирьох основних пристроїв: ThingSpeak-LED, MQTT-Temp (MQTT сенсор), Amazon-Alexa (голосовий помічник) та Wipro-Bulb (розумна лампа). Для кожного IoT-пристрою мережевий трафік відрізняється. Для виявлення атак (аномалій) у трафіку запропоновано використати модель автоенкодера, яка має навчатися на даних за трафіком без атак, припускаючи, що будь-який аномальний трафік призведе до значної помилки реконструкції (RE).

Існує кілька типів кібер атак, які розглядають в IoT мережах. Розподілена атака на відмову в обслуговуванні (DDoS) є однією з найбільш критичних загроз для IoT пристроїв. Такі IoT пристрої як веб-камери, пристрої спостереження за дітьми або принтери через їх вразливість і поширеність є основними цілями для запуску DDoS-атаки для формування ботнету. Атаковані IoT пристрої перенаправляють великий обсяг трафіку на сервери, що призводить до їх несправності.

Атака грубої сили на Secure Shell (SSH) – це ще одна відома кібератака, яка використовує метод проб і помилок для перебору всіх можливих комбінацій для зламу пароля. Більшість пристроїв IoT надають віддалений доступ через протокол SSH з паролями за замовчуванням, що робить їх вразливими до атак даного типу. Зловмисники використовують SSH-атаки грубого перебору з відомими обліковими даними, щоб отримати доступ і експлуатувати пристрої IoT. Якщо пристрій зазнав атаки грубого перебору SSH, то це може призвести до DDoS-атак, і ці дві атаки є шляхом для подальшої несанкціонованої експлуатації. У даному дослідженні увага спрямована на виявлення цих двох найбільш значущих атак на IoT пристрої.

Останніми роками IDS-системи для пристроїв IoT інтегрували методи неконтрольованого навчання (unsupervised learning, або навчання без вчителя). У неконтрольованому навчанні виявлення аномалій є задачею, яка використовується для ідентифікації спостережень, що відхиляються від нормальних подій. Потенційна можливість значної шкоди, спричиненої аномальними діями, робить задачу виявлення атак критично важливою в кіберпросторі. Існують дослідження, у яких запропоновано методи неконтрольованого навчання на основі різних наборів даних мережевого трафіку для перевірки певних систем IDS. Однак виокремити конкретні пристрої IoT у більшості наборів даних складно, а отже, і виявити аномалію в інфраструктурі IoT не просто.

2 Постановка задачі

Із зростанням складності комп'ютерних систем та активним розвитком інтернет-технологій кіберзагрози стають все більш витонченими та масштабними. В останні роки багато дослідників зосередилися на неконтрольованому навчанні для виявлення мережевих аномалій у периферійних пристроях з метою виявлення комп'ютерних атак. Розгортання моделі неконтрольованого автокодера вимагає значних обчислювальних витрат на периферійних пристроях з обмеженими ресурсами.

У дослідженні запропоновано використати **модель квантового автокодера** (QAE) для системи виявлення вторгнень – оптимізаційна модель на основі автокодерів, до якої включені методи відсікання, кластеризації та цілочисельного квантування. Квантовий автокодер uint8 і квантовий автокодер float16 – це два варіанти, які створені для розгортання дорогих в обчислювальному плані моделей штучного інтелекту (ШІ) в пристроях Edge.

У роботі розглянуто згенерований мережевий трафік за допомогою пристроїв IoT, що працюють в режимі реального часу, за наявності (атакуючий трафік) та відсутності атак

(нормальний трафік). Модель автокодера працює з нормальним трафіком на етапі навчання. Потім навчена модель використовується для реконструкції аномального трафіку, припускаючи, що помилка реконструкції аномалії (**RE**) буде високою, що допомагає ідентифікувати атаки. Крім того, проведено дослідження ефективності автокодерів QAE-u8 і QAE-f16 з використанням показників точності та оцінки F1 на основі експериментальних досліджень. Таким чином, у роботі розглянуто мережевий трафік IoT в реальному часі для чотирьох пристроїв: ThingSpeak-LED, MQTT-Temp, Amazon-Alexa та Wipro-Bulb.

Пристрої IoT, на відміну від графічних і центральних процесорів загального призначення, підтримують додатки з обмеженими фізичними ресурсами. Розгортання фреймворку IDS з використанням ШІ в цих пристроях накладає обчислювальні обмеження, такі як обмежений обсяг пам'яті, менша кількість ALU, високий процесорний час тощо. За таких умов безпосередня реалізація алгоритмів ШІ, що споживають багато пам'яті, є ненадійною без оптимізації. Вирішенням цієї проблеми є оптимізація алгоритмів ШІ для IoT пристроїв. Нейронні мережі в оптимізації ШІ містять відсіканя мережі та цілочисельне квантування. Процес відсікання мережі включає видалення надлишкових нейронів, які суттєво не впливають на точність моделі. Це допомагає зменшити обсяг пам'яті та призводить до зниження енергоспоживання. Крім того, можна зменшити значення вагових коефіцієнтів та функції активації, перетворивши загальновживане 32-бітне представлення з плаваючою комою до 16-бітної та 8-бітної цілочисельної точності. Цей процес реалізує техніку пост-квантифікації. Операції над цілими числами зменшують накладні витрати порівняно з операціями з плаваючою комою і зменшують час і складність обчислень [1, 2].

3 Огляд літератури

У [1] описано систему виявлення вторгнень з квантованим автокодуванням для виявлення аномалій в пристроях IoT з обмеженими ресурсами з використанням набору даних RT-IoT. Пропонується модель квантованого автокодера для систем виявлення вторгнень з метою виявлення аномалій. Показано, що розроблена модель перевершує всі інші моделі, зменшуючи середнє використання пам'яті, стиснення пам'яті та пікове використання процесора. Запропонована модель більше підходить для розгортання на периферійних пристроях IoT з обмеженими ресурсами.

У роботі [2] розглянуто підходи до класифікації методів виявлення аномалій у системах, спрямованих на ідентифікацію атак. Проведено аналіз та огляд популярних груп методів, використаних для виявлення аномалій. Зазначено, що ці методи мають низький рівень формалізації для створення моделей атак, а також складнощі з оцінкою їхньої обчислювальної складності, коректності та завершеності.

У [3] розроблено модель виявлення вторгнень на основі покращеного трансформатора. В роботі проаналізовано традиційні алгоритми машинного навчання, методи глибокого навчання та розглянуто переваги використання трансформерних моделей. Запропоновано метод виявлення вторгнень у комп'ютерних мережах, який відрізняється від відомих підходів використанням алгоритму глибокого навчання та включає процедури зменшення кореляції вхідних даних та перетворення даних у певний формат, необхідний для роботи моделі.

У [4] показано, що віртуалізація мереж є сучасним підходом до підвищення ефективності функціонування комп’ютерних мереж. Запропоновано інтегрувати віртуалізацію з методами машинного навчання, зокрема шляхом створення моделі оптимізації мережі на основі графових нейронних мереж. Такий підхід дозволяє врахувати складну взаємодію між топологією мережі, маршрутизацією та вхідним трафіком, забезпечуючи точне прогнозування розподілу затримок і втрат. Проведено аналіз існуючих методів оптимізації мереж та розглянуто віртуалізацію як ефективний інструмент для вдосконалення їх роботи.

У роботі [5] розроблено моделі діагностування інтерактивних комп’ютерних мереж на структурно-логічному рівні, а також методи діагностування, що враховують особливості їх функціонування. Запропоновано методи та процедури синтезу одновимірних і двовимірних мереж із розподіленим управлінням конфігурацією. Проведено аналіз існуючих підходів до діагностування таких мереж, що дозволило створити ефективні моделі діагностики. За результатами проведених експериментів було оцінено тестопридатність розглянутих мереж, підтвердивши їхню функціональність і відповідність поставленим вимогам.

У роботі [6] представлено застосування методу пошуку аномалій для виявлення мережевих атак. Дослідження присвячене моделі виявлення мережевих вторгнень у трафіку, сформованому на основі стека протоколів TCP/IP. Проведено аналіз основних об’єктів локальної обчислювальної мережі та визначено ключові параметри для контролю кожного типу об’єктів. У роботі запропоновано методи пошуку аномалій, які базуються як на аналізі за заздалегідь визначеними правилами, так і на використанні ймовірнісних моделей. Розроблена модель системи забезпечує виявлення атак на ключові об’єкти, що піддаються моделюванню.

У роботі [7] запропоновано методи створення тестів для інтерактивних комп'ютерних мереж на структурно-логічному рівні. Для таких мереж розроблені методи синтезу перевіряючих послідовностей з використанням циклічних, відмінних і характеристичних символів в автоматній моделі комірки мережі. Розроблений новий підхід до модифікації автоматної діаграми комірки, яка не має відмінної послідовності. Цей метод включає введення додаткового вхідного символу та використання кодів станів, які формують Гамільтонів цикл у послідовності переходів. Також представлені методи та процедури для синтезу одновимірних і двовимірних мереж з розподіленим управлінням конфігурацією.

У роботі [8] запропоновано застосування систем запобігання та виявлення вторгнень для забезпечення комплексного захисту мережі. На основі порівняльного аналізу цих систем було виявлено їхні недоліки, а також сформульовано вимоги для створення так званої "суперсистеми", здатної ефективно запобігати та виявляти кібератаки і вторгнення.

У роботі [9] розглянуті методи виявлення аномалій на етапі попередньої обробки даних, зокрема методи стандартного відхилення, локального рівня викидів і ізолюючого лісу. Визначена залежність між числом виявлених аномалій і пороговими значеннями для кожного з цих методів. Якість попередньої обробки даних оцінювалась за допомогою класифікаторів, побудованих на основі методів K-найближчих сусідів і беггінгу.

У роботі [10] досліджено методи виявлення аномалій у наборах даних під час управління процесами в державних системах. Основну увагу приділено вибору метрик для оцінювання точності виявлення викидів, а також визначенню ефективних математичних моделей і методів для розв’язання задачі виявлення аномалій у пробних вибірках. Отримані результати включають: огляд метрик, що застосовуються для оцінки ефективності математичних моделей і методів виявлення аномалій, огляд традиційних підходів і методів глибокого навчання для виявлення викидів, аналіз ефективності та якості моделей і методів на основі 12 пробних вибірок.

У роботі [11] проведено аналіз та прогнозування характеристик комп’ютерної мережі, зокрема досліджено трафік з позиції часових рядів. Розглянуто моделі трендів у часових рядах, критерії їх виявлення та методи оцінювання. Для оцінки тренду було обрано основний метод тест Манна-Кендалла, результати якого інтерпретовано за допомогою методу консенсусу. Розв’язано задачу прогнозування трафіку комп’ютерної мережі з урахуванням трендових показників та вирішено задачу збору та попередньої обробки даних про роботу комп’ютерної мережі, включаючи формалізацію, кількісний і якісний аналіз, створено унікальний набір даних шляхом парсингу логів (системних файлів) моніторингу трафіку, який використано для побудови моделей виявлення трендів та прогнозування мережевих характеристик.

У роботі [12] було проведено аналіз характеристик систем виявлення мережевих вторгнень в інформаційні системи та ідентифікації ознак комп'ютерних атак на підприємствах. Розглянуто можливі дії зловмисників та досліджено методи і принципи налаштування оптимальних систем виявлення мережевих вторгнень. Проаналізовано потенціал розробки та застосування комп'ютеризованих систем для виявлення вторгнень у мережу, а також вивчено властивості комп’ютерних атак у сучасних умовах. Розроблено рекомендації для впровадження систем виявлення атак, вторгнень та ознак кібератак. Пропоновані рішення спрямовані на подальшу інтеграцію цих систем у загальну архітектуру захисту інформації будь-якої організації.

У роботі [13] зазначено, що жоден метод захисту від кібератак не може гарантувати повний захист від проникнення зловмисника в комп’ютерну мережу. У випадку злому важливо оперативно виявити порушення, припинити доступ, провести розслідування та усунути вразливості. Для цього застосовуються методи, які допомагають виявляти аномалії та зловживання. Розглянуто використання частотного методу для виявлення аномалій в системі шляхом аналізу ентропії журналу подій. Цей метод дозволяє виявляти аномалії в мережевому трафіку, а також аналізувати журнали подій на хостах для виявлення несанкціонованих дій. Дослідження на основі журналу подій ОС Windows показало, що перевищення порогових значень

кількості різних повідомлень у журналі можна виявити через аналіз ентропії, що допомагає виявляти аномалії в роботі комп'ютерної мережі. Запропонований метод можна інтегрувати в системи виявлення вторгнень, що дозволить швидко інформувати адміністратора безпеки про зловживання та атаки.

У роботі [14] запропоновано інтелектуальну систему, що виявляє аномалії та ідентифікує пристрої розумних будинків, які використовують колективну комунікацію. Ідея запропонованої системи полягає в об'єднанні розумних будинків в одну комп'ютерну мережу з метою підвищення безпеки як для окремого будинку, так і для всієї мережі в цілому. Однією з переваг цієї системи є зв'язок між кластерами розумних будинків, що дозволяє обмінюватися інформацією про профілі розумних пристроїв в білих списках кожного з кластерів, що додає рівень безпеки на всіх рівнях мережі.

У роботі [15] проведено аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. Для забезпечення захисту як відкритої, так і обмеженої інформації пропонується використовувати комбінацію програмних і апаратних засобів, що забезпечують моніторинг, аналіз і контроль роботи інформаційно-телекомунікаційної системи (ІТС). Серед таких засобів виділяються: міжмережеві екрани, антивірусні програми та системи виявлення та системи виявлення і запобігання вторгнень. У разі захисту існуючих ІТС існує безліч підходів до створення комплексного захисту, який потрібно обирати залежно від розміру ІТС. Для невеликих ІТС достатньо налаштувати міжмережевий екран і антивірусну систему, тоді як для середніх та великих ІТС, наприклад, у випадку хостинг-провайдерів, необхідно застосовувати більш потужні механізми захисту, такі як системи виявлення і запобігання вторгнень.

4 Опис еталонних наборів даних мережевого трафіку

У ШІ критичний аналіз і оцінка системи IDS залежать від типу набору даних, обраного на етапах навчання і тестування. Набір даних DARPA є найпопулярнішим набором даних для мережевих IDS, він містить 41 характеристику в пакетному форматі. Найпоширеніші атаки включають DoS, сканування портів, R2L та U2R. Незважаючи на широке розповсюдження, DARPA страждає від високої надмірності. Набір даних CICIDS містить 80 атрибутів і двонаправлені мережеві траси на основі потоків, він включає трафік ботнетів, DoS, SSH-атак, інфільтрації та веб-атак, які генерували як сервери, так і персональні комп'ютери.

Дослідники з галузі кібербезпеки розробили набір даних UNSW-NB за допомогою інструмента IXIA Perfect Storm. Цей набір даних містить як пакетні, так і часові характеристики. Сімейство атак включає DDoS, DoS, розвідку та крадіжку. Крім того, UNSW запропонувала набір даних BoT-IoT з 72 мільйонів трас, в якому для імітації трафіку IoT використовувався Node-RED, інструмент моделювання проміжного програмного забезпечення. Автори BoT-IoT розробили JavaScript для віртуальних метеостанцій з використанням датчиків IoT, таких як тиск, вологість і температура, і обмінювалися даними через протокол передачі телеметрії в черзі (Message Queuing Telemetry Transport, MQTT). Основні атаки в цьому наборі даних включають DoS і крадіжку інформації. Себастьян Гарсія та Еркіага зібрали набір даних IoT у стратосферній лабораторії університету CTU. Набір даних містить 23 знімки різних мереж, створених на пристроях Raspberry Pi. Набір IoT включав безпечний трафік, зібраний з Amazon Echo, Philips HUE LED Light та розумних дверних замків Somfy Smart. У цьому наборі даних безпечний і шкідливий трафік був захоплений на різних пристроях, що призвело до створення окремих мереж.

У роботі [1] наведено загальнодоступні еталонні набори даних для дослідників. Дослідження показує, що більшість досліджених наборів даних не є частиною інфраструктури IoT. Незважаючи на те, що IoT використовував середовище в реальному часі, сліди атак і доброякісні сліди генерувалися в іншому середовищі. Крім того, в IDS на основі аномалій потрібно повністю аналізувати поведінку всіх пристроїв IoT, щоб виявити нову аномалію в мережі. Тому в даній роботі пропонується розглядати нормальний і атакуючий трафік в одній і тій же мережевій інфраструктурі з пристроями IoT.

5 Огляд методів машинного навчання для виявлення атак

Thudumu представили багаторівневу гібридну IDS для захисту внутрішньотранспортних мереж (IVN) і зовнішніх автомобільних систем від атак. Запропонована модель складається з чотирирівневої мережі. Для виявлення відомих атак були використані деревоподібні моделі ML, такі як дерево рішень (DT), додаткові дерева (ET), випадковий ліс та екстремальний градієнтний

бустинг (XGBoost). Розробка системи виявлення аномалій інтегрувала CL-k-середні, байєсівську оптимізацію з гаусівським процесом (BO-GP) та упереджені класифікатори, в ній зосередилися на виявленні вторгнень у внутрішньотранспортні мережі, використовуючи два загальнодоступних набори даних CICIDS і CAN-intrusion. Дані набори є високо розмірними, тобто мають атрибути, які можуть бути незалежними. У такому випадку можуть поставати проблеми, пов'язані з «прокляттям розмірності».

Eskandari запропонували Passband, інтелектуальний наскрізний дизайн IDS для шлюзів IoT. Цей метод використовує алгоритми Isolation Forest (IF) та Local Outlier Factor (LOF) для виявлення аномалій. Цей метод було протестовано проти сканування портів, SYN-флуду, HTTP- і SSH-атак грубої сили. Метод IF є більш стабільним, ніж LOF, але модель має високу завантаженість процесора. У дослідженні було проведено порівняння класифікатора Ridge, логістичної регресії та ансамблевого методу з точки зору складності та точності реєстрації часу. Виявлено, що продуктивність залежить від характеру набору даних і параметрів, що використовуються під час тестування.

У [1, 3] запропоновано IDS з використанням оптимізації рою частинок (PSO). У роботі застосовано методи вилучення ознак на основі рою частинок для оптимізації алгоритмів машинного навчання (ML). У цій роботі автор застосував PSO до алгоритму дерева рішень (PSO + DT) та алгоритму K-найближчого сусіда (PSO + KNN) для набору даних KDD-CUP99. Алгоритм PSO + KNN показав кращі результати порівняно з іншими алгоритмами. Оскільки набір даних не містить слідів IoT, розгортання на пристроях IoT є недоречним. Також запропоновано модель IDS Stacked Attention Autoencoder (SAAE), в якій шар механізму уваги знаходиться між кодером і прихованим шаром. Цей шар обчислює вектор уваги всіх ознак, щоб визначити внесок кожного атрибуту. Запропонований алгоритм може досягти високої точності у змодельованому середовищі.

Також запропоновано гібридна техніка глибокого навчання для бот-мереж, яка об'єднує автокодер Long Short (LAE) з глибокою двонаправленою довгою короткочасною пам'яттю (BLSTM) для виявлення вторгнень у камерах спостереження. Класифікація атак Mirai та BASHLITE IoT здійснюється шляхом оцінки та тестування мережевого трафіку на різних камерах, включаючи Samsung SNH 1011N, XCS7-1.003-WHT, Simple Home XCS7-1.002WHT та Provision PT-838. Досягнуто кращих показників з точки зору точності. Однак модель зазнала високих втрат при класифікації TCP- і SCAN-атак (Zhang). Для оптимізації алгоритму глибокої нейронної мережі (DNN) розглянуті різні методи стиснення, такі як обрізка, кластеризація і квантування. Для перевірки здатності до стиснення та коректності ResNet18 у цьому дослідженні представлено метод квантування зі збереженням розрідженості та кластерів (PCQAT).

Модель AS-IDS призначена для виявлення атак як на основі сигнатур, так і на основі аномалій, використовуючи набір даних NSL-KDD. Ця модель включає алгоритми Deep Q-Learning, в якому вихідний рівень використовує відношення сигнал/шум (SNR) і пропускну здатність для класифікації (Otoum and Nayak). Існує також модель згорткової нейронної мережі (CNN) для IDS для виявлення викидів. Ця модель використовує набір даних NID та набір даних BoT-IoT для перевірки. Однак модель CNN занадто складна для розгортання з обмеженими ресурсами. Gong застосував модель VecQ для стиснення алгоритмів DNN з використанням наборів даних MNIST, ImageNet, CIFAR, текстів THUCNews та рецензій на фільми IMDB. Параметризація методу оцінки ймовірності, що використовується в процесі квантування, дозволила цій моделі досягти вищої точності. Метод стиснення One-shot pruning quantization (OPQ) для алгоритму DNN вирішує проблему ручного налаштування шляхом використання попередньо навчених вагових параметрів для обчислення розподілу стиснення та спільного використання одного кодового дерева для всіх каналів на кожному рівні замість традиційного квантування по каналах. Однак ці дослідження не враховують обчислювальну складність алгоритмів ШІ на пристроях IoT в режимі реального часу, яка включає в себе споживання пам'яті, навантаження на процесор і час обробки.

У [1] показано різні підходи до оптимізації IDS. Використання алгоритмів ШІ для виявлення атак підвищить продуктивність IDS (Lakhan; Verhelst and Moons). Маючи величезні переваги методів ШІ, розгортання IDS у пристроях IoT є складним завданням. Пристрої IoT мають обмежений обсяг пам'яті, низьку пропускну здатність і малу потужність (Thakkar and Chaudhari; Imteaj). У цій роботі представлено дві моделі QAE, такі як QAE-u8 та QAE-f16, використовуючи комбінацію методів обрізки на основі розрідженості, кластеризації та квантування. Емпіричний аналіз також включає в себе дослідження пристроїв Raspberry Pi.

6 Дослідження фреймворку QAE IDS для виявлення аномалій у пристроях IoT

У роботі [1,4] основний внесок полягає в тому, що: (a) згенерований набір даних RT-IoT для нормального та атакуючого мережевого трафіку з використанням інфраструктури IoT з розгортанням пристроїв IoT, таких як ThingSpeak-LED, MQTT-Temp (сенсор), Amazon Alexa (голосовий помічник), Wipro bulb (розумна лампа) та Raspberry Pi, в режимі реального часу; (b) запропоновані оптимізовані моделі QAE-u8 та QAE-f16 для IDS для підтримки пристроїв IoT з обмеженими ресурсами з метою зменшення складності ШІ; (c) отримані оцінки запропонованої моделі, які показали, що QAE-u8 досягла кращих результатів, ніж QAE-f16 та модель автокодера за F1-score.

Обчислювальна складність запропонованої моделі вимірювалась з точки зору часу виконання, використання процесора та пам'яті для розгортання в пристроях з обмеженими обчислювальними можливостями. Запропонована модель QAE-u8 значно перевершує QAE-f16 та еталонні моделі автокодерів. Для цього всі три моделі були змодельовані на пристрої Raspberry Pi.

Фреймворк QAE IDS для виявлення аномалій у пристроях IoT з обмеженими ресурсами, як показано на рис. 1, складається з чотирьох етапів, які пропонують: (a) генерацію набору даних, (b) інженерію ознак, (c) фреймворк автокодера, (d) квантування після навчання [1,5].

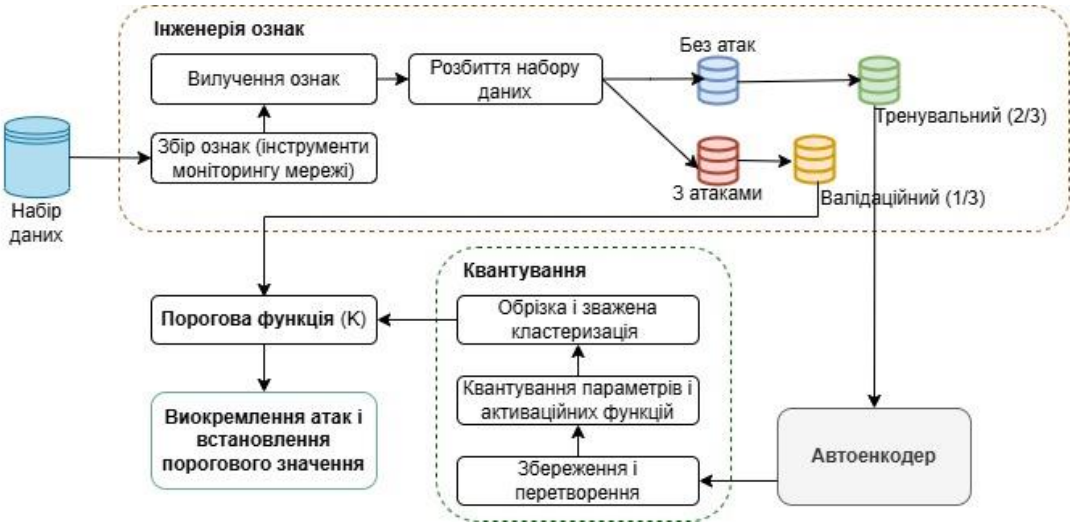


Рис. 1. Система QAE IDS для виявлення аномалій
Fig. 1. QAE IDS anomaly detection system

Створення набору даних є однією з найважливіших задач неконтрольованого навчання. Був запропонований набір даних RT-IoT для навчання та тестування IDS на основі QAE. На рис. 2 показана інфраструктура тестового стенду для генерації набору даних RT-IoT [1,6].

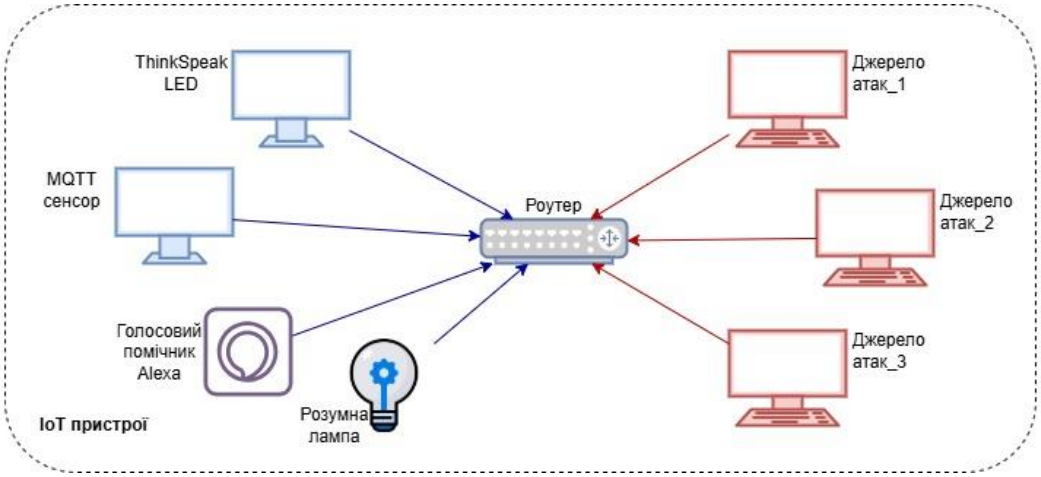


Рис. 2. Інфраструктура набору даних RT-IoT
Fig. 2. RT-IoT data collection infrastructure

Інфраструктура складається з двох частин, а саме: пристроїв-жертв IoT та пристроїв-зловмисників IoT, з'єднаних через маршрутизатор. Мережевий трафік збирається через маршрутизатор за допомогою Wireshark, який є інструментом моніторингу мережевого трафіку з відкритим вихідним кодом і допомагає витягувати траси та конвертувати їх у файл PCAP.

У [1] наведено список пристроїв, операційних систем та відповідних конфігурацій. На цьому наборі даних було створено чотири звичайні профілі та два профілі атаки.

Хмарна платформа *ThingSpeak* – це платформа IoT з відкритим вихідним кодом для візуалізації даних з датчиків та управління виконавчими пристроями. Був створений інтерфейс між платою Intel Galileo Gen 2 та RGB світлодіодним модулем. Згодом за допомогою платформи ThingSpeak здійснюється моніторинг стану світлодіодів. Маршрутизатор записує передачу даних світлодіодного модуля, сполученого з IoT-пристроєм.

Протокол *MQTT* – це протокол публікації/підписки, метою якого є підтримка пристроїв IoT з обмеженими ресурсами для передачі даних з низькою пропускною здатністю. Спочатку встановлюється інтерфейс між пристроєм Raspberry Pi та датчиком температури. Пристрій Raspberry Pi публікує значення температури в MQTT Mosquitto Broker за допомогою бібліотеки Paho MQTT через Інтернет. Використовуючи інструмент Wireshark, можна пасивно відстежити і перехопити внутрішній трафік, в результаті чого збирається набір даних, який містить MQTT-Temp.

Компанія *Wipro* випустила 9-ватну розумну лампу B22 NS9400 як інтегроване рішення для розумного будинку IoT. Мобільні пристрої можуть дистанційно керувати цими лампами за допомогою протоколу WiFi. Набір даних Wipro-Bulb включає повну інформацію про комунікацію *Wipro-Bulb*.

Пристрій *Alexa*, розроблений компанією *Amazon*, підключається до маршрутизатора і перехоплює всю комунікацію на маршрутизаторі. Цей пристрій працює як хмарний голосовий сервіс.

SSH brute-force attack. Механізм автентифікації пристроїв IoT вразливий до атак SSH грубої сили через слабкі паролі. Ця атака не лише підбирає паролі, але й проникає в систему та впроваджує шкідливий код для контролю та атаки на інші підключені пристрої. Допоміжні модулі для входу в SSH, доступні в Metasploit, інструменти з відкритим вихідним кодом, використовуються для генерації трас атаки грубого перебору. Початкова фаза процесу перебору SSH включає в себе сканування портів за допомогою інструменту Network Mapper (Nmap) для виявлення машин з відкритими SSH-портами. Обраний допоміжний модуль 'Scanner SSH' з msfconsole в Metasploit, щоб ініціювати атаку перебором. Msfconsole налаштовується на IP-адресу жертви, ім'я користувача за замовчуванням та файли з паролями для проведення атаки. Після того, як допоміжний модуль успішно зламує облікові дані, встановлюється віддалене з'єднання, що дозволяє отримати доступ до комп'ютера жертви.

Траси *DDoS-атак* були згенеровані за допомогою інструменту Hping3 з декількох IoT-пристроїв Kali Linux. Hping3 – це інструмент з відкритим вихідним кодом, доступний в ОС Kali Linux, який використовується для запуску DDoS-атак на машини-жертви. На початковому етапі створено команду hping3, вказавши IP-адресу та доменне ім'я цільової жертви. hping3 надає функцію сканування 'SYN'. Крім того, була персоналізована конфігурація через встановлення портів джерела, призначення та фрагментацію. Було передано 30 000 TCP SYN-пакетів на пристрій жертви, використовуючи випадкові джерела в процесі атаки. Здатність цих атак щоразу випадково змінювати IP-адреси пристроїв-джерел створює труднощі для адміністраторів у визначенні джерела атак (Jia et al.). Процедура була продовжена на період 120 с, що призвело до генерації значного обсягу пакетів, які перевантажили ресурси комп'ютера-жертви.

Feature Engineering. Зібрані файли PCAP з Wireshark конвертуються і вивантажуються у вигляді CSV-файлів за допомогою інструменту CICFlowmeter.

У [1] показаний повний набір даних RT-IoT. Було згенеровано двонаправлений потік пов'язаних з часом характеристик, які допомагають розрізняти DDoS-атаки. Щоб запобігти надмірному пристосуванню під час навчання, такі ознаки, як адреса джерела, призначення та FlowID, були вилучені. Крім того, числові значення були закодовані для категорійних ознак, таких як протокол і послуга. Також повний набір даних був нормалізований із середнім значенням нуль і стандартним відхиленням одиниця. Для виявлення аномалій нормальний набір даних був позначений нулем, а набір даних атаки – одиницею. Нарешті, на етапі навчання використовується 70% набору даних, а на етапі тестування (валідації) використовується 30% .

7 Дослідження стиснення моделі та зменшення завантаження процесора

Розглянемо побудову фреймворку автокодера для навчання нормальної поведінки мережевого трафіку пристроїв IoT. Автокодер – це модель неконтрольованого навчання на основі методів реконструкції. Механізм алгоритму автокодера полягає в реконструкції тих самих вхідних даних у вихідні дані. При виявленні аномалій ідея використання автокодера полягає в тому, що аномальний трафік не зможе відновити свій вхідний трафік на виході. Отже, помилка виникає через те, що модель навчається виключно на звичайному (нормальному) мережевому трафіку. Модель автокодера складається з прихованих шарів, що мають кодер φ, який перетворює вихідний набір даних χ в латентний простір F для стиснення, та декодер θ, який відновлює вихідний набір даних з латентного простору. Крім того, в кодері можна зменшити кількість прихованих шарів, що дозволить виділити лише суттєву інформацію та ігнорувати шум. Розглянута модель складається з шести прихованих шарів з трьома рівними кодувальниками та декодувальниками, з функцією активації «relu». Оскільки пристрої IoT мають обмежені ресурси, модель автокодера містить процедуру оптимізації, яка складається з обрізання, кластеризації та квантування.

7.1 Післятренувальне квантування

Для зменшення завантаження процесора і пам'яті, наскільки це можливо, при збереженні точності моделі важливою задачею є оптимізація моделі. Щоб оптимізувати модель вже навченого автокодера був застосований метод пост-тренінгового квантування. Цей метод містить обрізання, кластеризацію та квантування. Квантування після навчання складається з кількох кроків.

Першим кроком для стиснення моделі є обрізання. Обрізка – це вибір найбільш значущих нейронів, не беручи до уваги шари з надлишковими або нульовими ваговими коефіцієнтами.

На другому кроці застосовується метод вагової кластеризації. Тут ваги шарів кластеризуються і згодом змінюються на основі центроїдів кластерів. Цей підхід допомагає ще більше зменшити розмір моделі. На основі аналізу компромісу між точністю та кількістю кластерів було обрано вісім кластерів для вагової кластеризації.

Третій крок квантування передбачає перетворення кластеризованої моделі у формат TFlite з метою покращення продуктивності моделі з точки зору процесорної обробки, розміру моделі та використання пам'яті. На цьому кроці всі ваги і зсув у форматі float32 перетворюються у беззнакові 8-розрядні цілі числа та 16-розрядні числа з плаваючою комою.

На останньому етапі квантована модель була навчена і протестована, перш ніж завантажити її на пристрій IoT для остаточних прогнозів. *Алгоритм 1* показує псевдокод для Q-Autoencoder [1,7,8].

Алгоритм 1. Запропонована модель квантованого автокодера для виявлення аномалій
Вхід: тренувальний набір $x_1, \dots, x_n \in R$, кодер φ and decoder θ
Вихід: знайдений поріг

```
procedure Q-Autoencoder
    Repeat:
          побудова φ: χ→F, θ: F→χ′
                де φ = h(Wχ + b) і θ = g(W′φ + b′)
          обчислення втрати L = ‖χ − χ′‖²
    Until argmin_{φ,θ} ‖χ − (φ·θ)χ‖² => досягнення мінімуму помилки RE
    Обчислення порогу за формулою (2)
    Pruning
    Обчислення w′ = argmin_w ‖χ − χ′‖² + λ Σ_{i=0}^{k} |w_i| => L1 нормалізація
    If ваги набули значення нуль, then обрізати ваги
    Перенавчити модель
    Застосовувати кластеризацію зі збереженням розрідженості
    For кожного шару do
          Сформувати групу вагів у 8 кластерів
          Оновити ваги на основі їх кластерних центроїдів
    end for
    Квантизувати параметри і функції активації до float16 і unit8
end procedure
```

7.2 Аналіз результатів експериментів

Розглянемо результати навчання моделі для вилучення ознак та оцінку продуктивності автокодера та порівнюємо його з іншими оптимізованими автокодерами.

Виділення ознак. Спочатку були навчені чотири різні нормальні набори даних IoT за допомогою автокодера: (a) ThingSpeak-LED, (b) MQTT-Temp, (c) Amazon Alexa, (d) Wipro-Bulb. Далі до навченої моделі був застосований набір даних для реконструкції як нормального, так і аномального трафіку. Були розраховані значення RE, використовуючи формулу (1) для середньої абсолютної помилки і формулу (2) для середньої квадратичної помилки [1,8,9]:

$$MAE_{RE} = \frac{1}{n}\sum_{i=1}^{n}\|\chi - \chi'\|^2, \quad (1)$$

$$MSE_{RE} = \frac{1}{n}\sum_{i=1}^{n}\|\chi - \chi'\|, \quad (2)$$

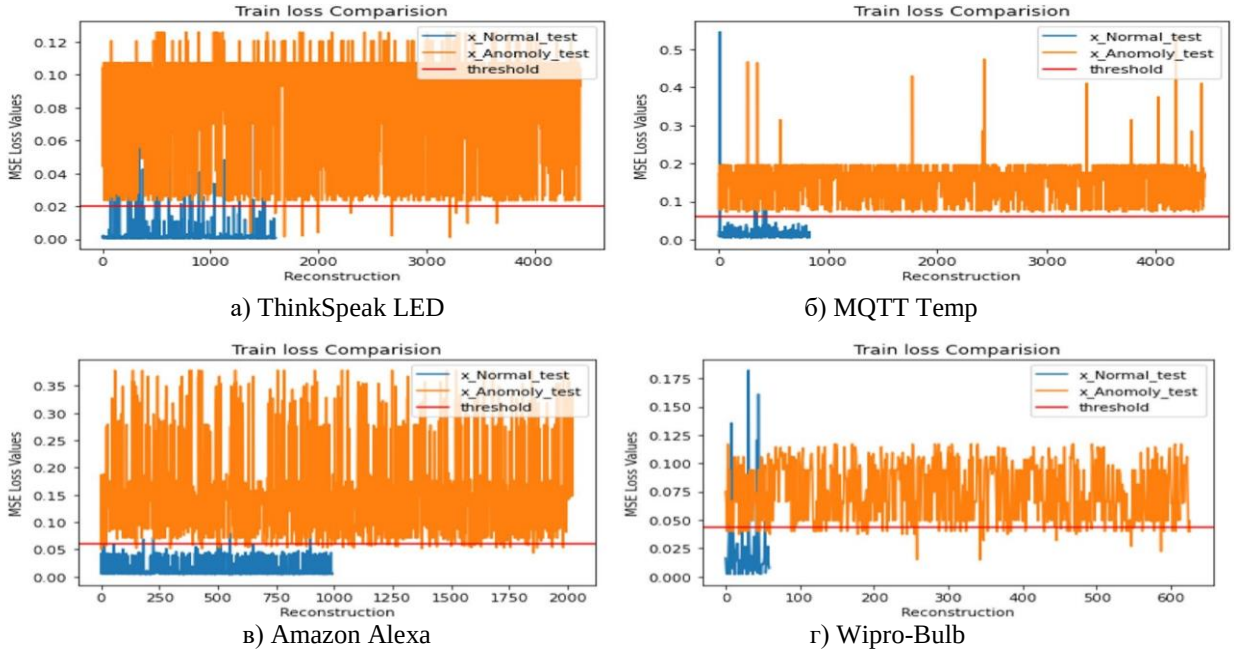
де n – кількість записів у даних. Згідно з моделлю автокодера, якщо модель навчена тільки для нормального трафіку, вона повинна генерувати високе значення RE для аномального трафіку під час прогнозування.

За допомогою похибки реконструкції, можна розрахувати поріг для розрізнення нормального та аномального трафіку за формулою (3):

$$threshold = \mu(RENormal)+\sigma(RENormal), \quad (3)$$

де μ – середнє значення, σ – стандартне відхилення, RENormal – RE нормального трафіку.

На рис. 3 [1,10,11] показано графічне представлення різниці нормального та аномального трафіку за допомогою порогового значення, розрахованого на основі помилки реконструкції після декодування нормального датасету.



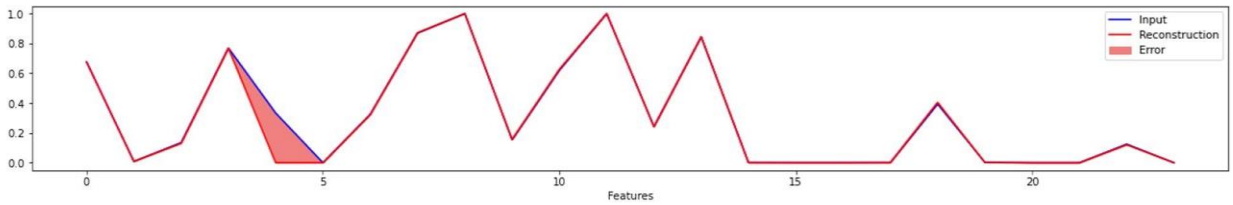
а) ThinkSpeak LED б) MQTT Temp

в) Amazon Alexa г) Wipro-Bulb

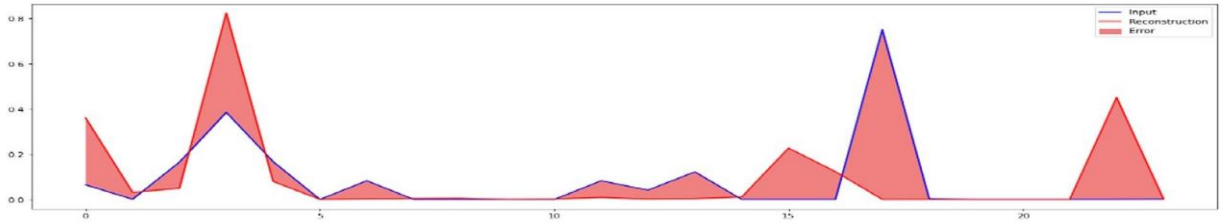
Рис. 3. Вимірювання порогу аномалії для різних нормальних наборів даних
Fig. 3. Measuring the anomaly threshold for different normal data sets

Далі були об'єднані всі сліди нормального мережевого трафіку з різних пристроїв IoT, щоб сформувати остаточний набір даних RT-IoT. Цей остаточний набір даних містить ознаки з високим RE лише для того, щоб зменшити обчислювальну складність. У [1] показано вилучені ознаки з кожного набору даних для виявлення мережевих аномалій.

Проведено навчання на RT-IoT за допомогою автокодера та перераховані RE для нормального та аномального трафіку (рис. 4, 5).



а)



б)

Рис. 4. Похибка реконструкції RT-IoT:а – без атак; б – з атаками
Fig. 4. Reconstruction error RT-IoT: a - without attacks; б – with attacks

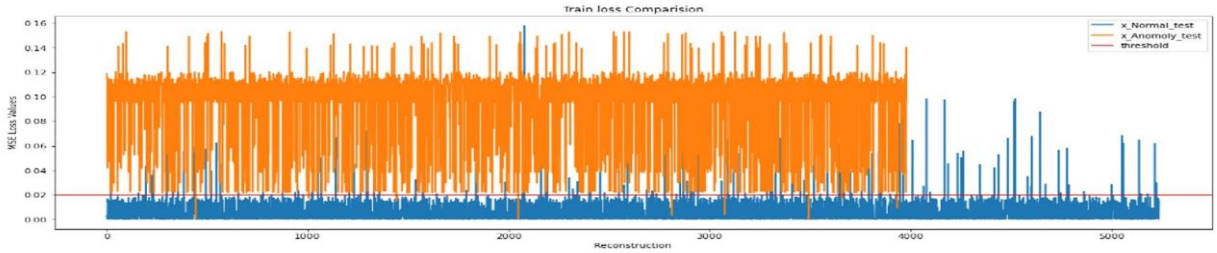


Рис. 5. Поріг RT-IoT
Fig. 5. RT-IoT threshold

Рис. 4a і b ілюструє правильність RE шляхом побудови графіків для всіх вилучених ознак. З рисунку видно, що RE є високим для аномального трафіку у всіх наборах даних порівняно з нормальним трафіком. Нарешті, був розрахований поріг для виявлення аномального трафіку за формулою (3). На рис. 5 показано генерацію помилок у нормальному та аномальному трафіку і також пороговий рівень для розрізнення аномалій [1,12,13].

7.3 Оцінка ефективності моделі

Спочатку був розглянутий лише нормальний трафік, щоб виділити ознаки для виявлення аномалій. Потім всі ознаки були об’єднані у запропонований набір даних RT-IoT2022, щоб оцінити продуктивність. Було досліджено такі метрики оцінки ефективності, як точність (accuracy), презицийність (precision), відгук (recall) і оцінка F1, щоб перевірити запропоновану навчальну модель. Показник точності вимірює частку правильно передбаченого нормального або аномального трафіку. Через рекомендацію не покладатися лише на точність, коли існує дисбаланс у кількості випадків між класами, також розглянуто метрику прецизійності. Precision вимірює частку точно передбачених хибних спрацьовувань. Чутливість, або відгук, моделі на реальну ситуацію, або істинність, показує частку передбачених правильних відповідей серед усіх правильних відповідей. Показник F1 обчислює середнє гармонійне значення точності та пригадування, щоб краще зрозуміти результати в незбалансованому наборі даних.

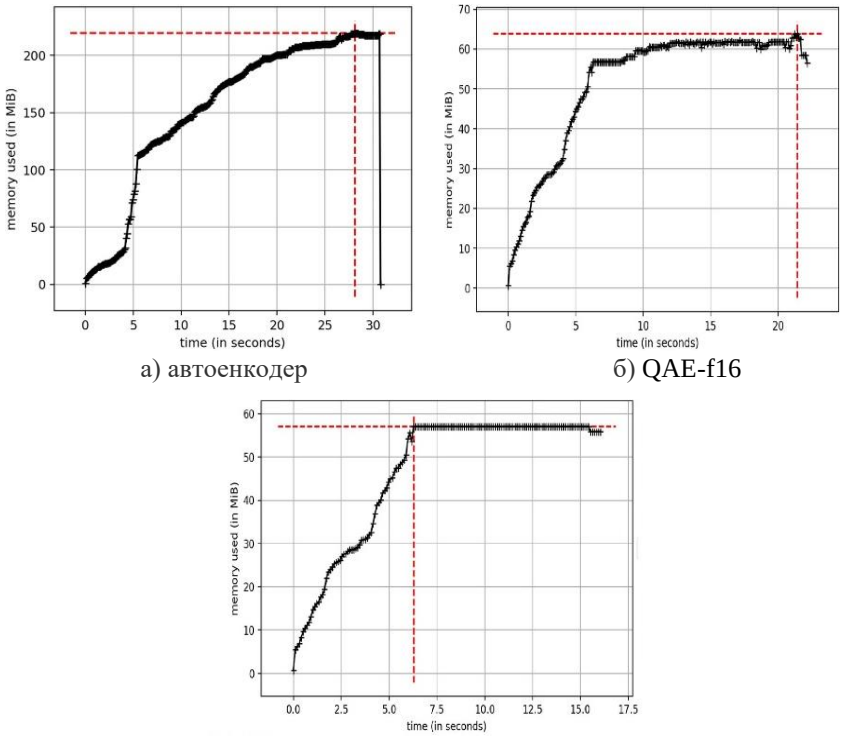
За результати було виявлено, що значення точності для кожного окремого IoT пристрою склало не менше 91,5%, найвище значення досягнуто для MQTT сенсорів. Середнє значення показника F1 склало 98%, що говорить про високу ефективність запропонованої моделі.

8 Результати та обговорення

Побудовані моделі були протестовані на сучасних пристроях Raspberry Pi. Конфігурація пристрою IoT з обмеженими ресурсами – 2 ГБ оперативної пам'яті та чотирьохядерний 64-розрядний процесор ARM Cortex-A53 з тактовою частотою 1,2 ГГц. Інструменти штучного інтелекту, задіяні в даній роботі, – це TensorFlow-1.2 та пакет підтримки tflite. На пристрої

Raspberry Pi були перевірені істинні значення часових витрат, завантаження процесора та пам'яті для автокодерів QAE-f16 та QAE-u8.

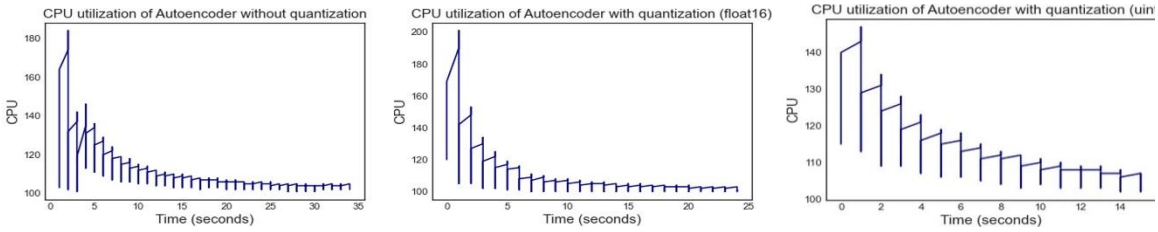
На рис. 6 і 7 показано споживання пам'яті та завантаження процесора на пристроях з обмеженими ресурсами [1,14,15].



а) автоенкодер б) QAE-f16

в) QAE-u8

Рис. 6. Використання пам'яті автокодера, моделі QAE-f16, QAE-u8
Fig. 6. Using the memory of the auto-encoder, models QAE-f16, QAE-u8



а) автоенкодер б) QAE-f16 в) QAE-u8

Рис. 7. Завантаження процесора автокодера, моделей QAE-f16, QAE-u8
Fig. 7. Processor load of the autocoder, models QAE-f16, QAE-u8

У [1] наведено повний аналіз усіх трьох запропонованих моделей. Узагальнення результатів, що стосуються всіх трьох запропонованих моделей.

Результати показують, що модель автокодера QAE-u8 споживає менше пам'яті та процесора. Таким чином, з наведеного вище обговорення можна вивести, що QAE-u8 має перевагу в умовах обмежених ресурсів. На рис. 8 показано графіки чисельних результатів.

Запропонована модель QAE не лише забезпечує переваги у продуктивності, але й підвищує енергоефективність за рахунок зменшення витрат на пам'ять для зберігання даних та підвищення ефективності обчислень. Це суттєво сприяє широкому впровадженню IDS на основі QAE-u8 у сільському господарстві та медичних пристроях IoT, оскільки ці пристрої потребують недорогих в обчислювальному плані технологій штучного інтелекту.

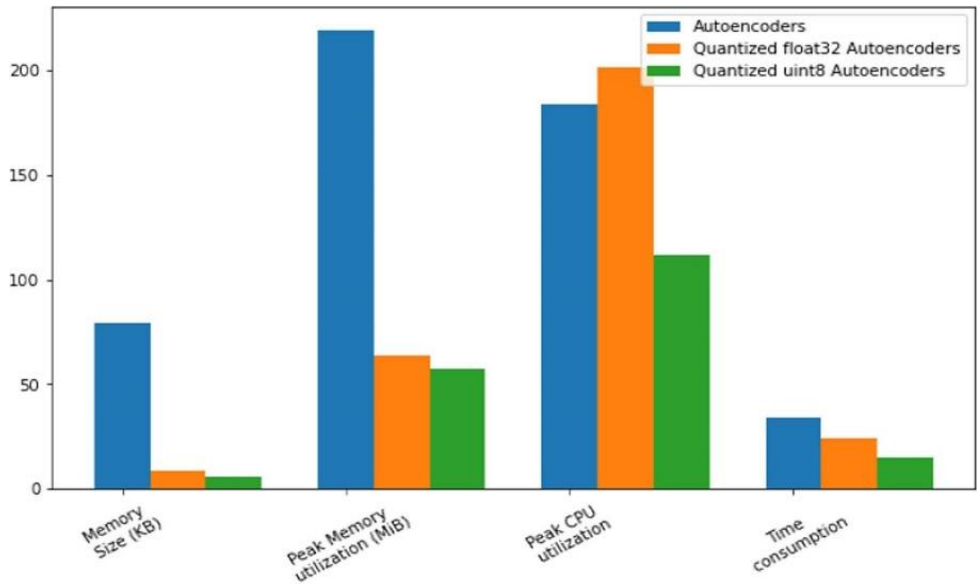


Рис. 8. Використання процесора автокодера, моделей QAE-f16 та QAE-u8
Fig. 8. Use of the autocoder processor, models QAE-f16 and QAE-u8

9 Висновки

У дослідженні розглянуло створення набору даних RT-IoT з використанням середовища IoT, яке виявляє аномалії за допомогою моделі автокодера. Набір даних включає Amazon Alexa, ThingSpeak-LED, MQTT-Temp, WiproBulb, мережевий трафік SSH та DDoS. Модель автокодера розраховує RE та порогові значення для виявлення аномалій в інфраструктурі IoT. Однак, основним недоліком побудови IDS на основі автокодерів в пристроях IoT є те, що вони обмежені в ресурсах, зокрема, в пам'яті, обчислювальній здатності та потужності. Тому в цьому дослідженні було запропоновано дві оптимізовані моделі автокодерів, QAE-u8 та QAEf16, для побудови фреймворку IDS. Оптимізація моделей автокодерів включає в себе методи обрізання, кластеризації та квантування. Проведено фінальне прогнозування моделі на пристрої Raspberry Pi, де спостереження за QAE-u8 показали, що розмір пам'яті стиснувся до 92,23%, а використання пам'яті зменшилося до 70,01%. Пікове завантаження процесора знизилося до 27,94%. Крім того, спостерігається значне зменшення часу, що витрачається на прогнозування, з 35 до 15 секунд. Результати показують, що запропонована модель QAEu8 може перевершити оригінальну модель автокодера в контексті зменшення обсягу пам'яті, процесора та використання пам'яті. Отже, вона підходить для пристроїв IoT з обмеженими ресурсами. Також проаналізована точність, ефективність, запам'ятовування та показник F1 для всіх трьох моделей. Результати показують, що QAE-u8 з MAE досягнув багатообіцяючих показників за метриками оцінювання порівняно з моделлю QAE-f16, але дещо нижчих показників порівняно з базовою моделлю автокодера. Таким чином, можна зробити висновок, що існує компроміс між автокодером і моделлю QAE-u8 в контексті точності та параметрів оцінки процесора, таких як пам'ять і центральний процесор.

СПИСОК ЛІТЕРАТУРИ

1. Sharmila, B.S., Nagapadma, R. Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. *Cybersecurity* , 2023. 6, 41. https://doi.org/10.1186/s42400-023-00178-5
2. Рубан І. В., Мартовицький В. О., Партика С. О. Класифікація методів виявлення аномалій в інформаційних системах. *Системи озброєння і військова техніка*, 2016. №. 3. С. 100-105. https://openarchive.nure.ua/server/api/core/bitstreams/7c434471-942c-40a7-b70c-0cc2655a42fe/content
3. Gavrylenko , S., Poltoratskyi , V., & Nechyporenko , A. Intrusion detection model based on improved transformer (Модель виявлення вторгнень на основі покращеного трансформатора). *Advanced Information Systems*, 2024. 8(1), С. 94–99. https://doi.org/10.20998/2522-9052.2024.1.12 http://ais.khpi.edu.ua/article/view/299010

4. Зац, О., Стрілець, В., Шматков, С., Ющенко, В. Віртуалізація мереж – підхід до оптимізації комп'ютерних мереж. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління»*, 2024. Вип. 61, С. 33-43. https://doi.org/10.26565/2304-6201-2024-61-04
5. Мірошник М., Корольова Я., Деменкова С., Шафранський А. Моделі діагностування інтерактивних комп'ютерних мереж на структурно-логічному рівні. *Вісник Національного технічного університету" ХПІ". Серія: Інформатика і моделювання*. 2024., 1-2 (11-12). – с. 96-104. http://pim.khpi.edu.ua/article/view/308453 https://doi.org/10.20998/2411-0558.2024.01.08
6. Пахомов Ю.В., Корольова Я. Ю., Демченко К. В., Деменкова С.Д. Використання метода пошуку аномалій для виявлення мережевих атак. *Вісник Харківського національного університету імені В.Н.Каразіна, сер. «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління»*. 2023. вип. 59. С.35-48. https://periodicals.karazin.ua/mia/article/view/23836 https://doi.org/10.26565/2304-6201-2023-60-02
7. Лобойченко Д.А. Мірошник М.А. , Шкіль О.С. , Рахліс Д.Ю., Мірошник А.М. Методи побудови тестів для інтерактивних комп'ютерних мереж на структурно-логічному рівні. *Вісник Національного технічного університету "Харківський політехнічний інститут". Збірник наукових праць. Серія: Інформатика та моделювання*. 2023. № 1 – 2 (9 – 10). с. 81-92 (137 с.). DOI: https://doi.org/10.20998/2411-0558.2023.01.07
8. Коробейнікова Т.І., Цар О.О. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. *Національний університет «Львівська політехніка»*, Україна. May 2023, *Грааль науки*. С.317-325. DOI:10.36074/grail-of-science.12.05.2023.050, License, CC BY-SA 4.0
9. Гавриленко С.Ю., Зозуля В.В. Дослідження методів виявлення аномалій на етапі попередньої обробки даних. *Системи управління, навігації та зв'язку,* 2022, випуск 1(67), С. 52-56. doi: 10.26906/SUNZ.2022.1.052
10. Lykhach O., Ugryumov M., Shevchenko D., & Shmatkov S. Anomaly detection methods in sample datasets when managing processes in systems by the state. *Bulletin of V.N. Karazin Kharkiv National University, Series «Mathematical Modeling. Information Technology. Automated Control Systems»*, 2022, 53, 21-40. https://doi.org/10.26565/2304-6201-2022-53-03
11. Стрілець В.Є., Дорошенко М.І. Аналіз і прогнозування характеристик комп'ютерної мережі. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління»*, 2022. Вип. 55. С. 49 – 57. https://doi.org/10.26565/2304-6201-2022-55
12. Лук'яненко Т. Ю., Поночовний П.М., Легомінова С.В. Методика виявлення мережевих вторгнень і ознак комп'ютерних атак на основі емпіричного підходу. *Сучасний захист інформації*. № 2 (2022). С.15-21. https://doi.org/10.31673/2409-7292.2022.021521
13. Панченко М.В., Біглан А.М., Бабенко Т.В., Тимофєєв Д.С. Виявлення аномалій інформаційної безпеки на основі аналізу ентропії інформаційної системи. *Енергетика і автоматика*, 2022. №1. https://doi.org/10.31548/energiya
14. Нічепорук А.О., Нічепорук А.А., Савенко О.С., Казанцев А.Д. Інтелектуальна система виявлення аномалій та ідентифікації пристроїв розумних будинків із застосуванням колективної комунікації. *Хмельницький національний університет. Електротехнічні та комп'ютерні системи*. 2021. № 34 (110).
15. Мєшков В., Віролайнен В. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. *Проблеми безпеки інформації в інформаційно-комунікаційних системах*. 2015. С. 1-4. https://ela.kpi.ua/handle/123456789/17609

REFERENCES

1. Sharmila, B.S., Nagapadma, R. Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. Cybersecurity 6, 41 (2023). https://doi.org/10.1186/s42400-023-00178-5

2. Ruban I. V., Martovytskyi V. O., Partika S. O. Classification of anomaly detection methods in information systems. *Armament systems and military equipment*. 2016. no. 3. pp. 100-105. https://openarchive.nure.ua/server/api/core/bitstreams/7c434471-942c-40a7-b70c-0cc2655a42fe/content [in Ukrainian].

3. Gavrylenko , S., Poltoratskyi , V., & Nechyporenko , A. Intrusion detection model based on improved transformer. *Advanced Information Systems*, 2024, 8(1), P. 94–99. https://doi.org/10.20998/2522-9052.2024.1.12 http://ais.khpi.edu.ua/article/view/299010

4. Zats, O., Strilets, V., Shmatkov, S., Yushchenko, V. Virtualization of networks – an approach to optimization of computer networks. *Bulletin of V.N. Karazin Kharkiv National University, series 'Mathematical modelling. Information technologies. Automated control systems'*, 2024. Issue 61, pp. 33-43. https://doi.org/10.26565/2304-6201-2024-61-04 [in Ukrainian]

5. Miroshnyk M., Koroliova Ya., Demenkova S., Shafransky A. Models of diagnosing interactive computer networks at the structural and logical level. Series: Informatics and modelling. *Bulletin of the National Technical University 'KhPI'. Series: Informatics and modelling*. 2024., 1-2 (11-12). P. 96-104. [in Ukrainian]

http://pim.khpi.edu.ua/article/view/308453 https://doi.org/10.20998/2411-0558.2024.01.08

6. Pakhomov Yu.V., Koroliova Ya.Yu., Demchenko K.V., Demenkova S.D. Using the method of anomaly search for detecting network attacks. *V. N. Karazin Kharkiv National University Bulletin, series 'Mathematical modelling. Information technologies. Automated control systems'*. 2023. issue. 59. P.35-48. [in Ukrainian] https://doi.org/10.26565/2304-6201-2023-60-02

7. Miroshnyk M. A., Shkil O.S., Rakhlis D.Yu., Miroshnyk A.M., Loboichenko D.A. Methods of building tests for interactive computer networks at the structural and logical level. *Bulletin of the National Technical University 'Kharkiv Polytechnic Institute'. Collection of scientific papers. Series: Informatics and modelling*. 2023. № 1 – 2 (9 – 10). P. 81-92 (137c.). https://doi.org/10.20998/2411-0558.2023.01.07 [in Ukrainian].

8. Korobeynikova T.I., Tsar O.O. Analysis of modern open intrusion detection and prevention systems. *Lviv Polytechnic National University*, Ukraine. May 2023, *the grail of science*. pp. 317-325. https://doi.org/10.36074/grail-of-science.12.05.2023.050, License, CC BY-SA 4.0 [in Ukrainian]

9. Gavrylenko S., Zozulia V. nvestigation of methods for detecting anomalies at the stage of data pre-processing. *Control, Navigation and Communication Systems*. 2022, Issue 1(67), P. 52-56. [in Ukrainian]. https://doi.org/10.26906/SUNZ.2022.1.052

10. Lykhach O., Ugryumov M., Shevchenko D., & Shmatkov S. Anomaly detection methods in sample datasets when managing processes in systems by the state. *Bulletin of V.N. Karazin Kharkiv National University, Series «Mathematical Modeling. Information Technology. Automated Control Systems»*, 2022, 53, 21-40. https://doi.org/10.26565/2304-6201-2022-53-03 [in Ukrainian].

11. Strilets V.Ye., Doroshenko M.I. Analysis and forecasting of computer network characteristics/ *Bulletin of V. N. Karazin Kharkiv National University. Series 'Mathematical modelling. Information technologies. Automated control systems'*, 2022. Issue 55. P. 49 – 57. https://doi.org/10.26565/2304-6201-2022-55 [in Ukrainian].

12. Lukyanenko T. Yu., Ponochevny P. M., Legominova S. V. Methodology for detecting network intrusions and signs of computer attacks based on an empirical approach. *Modern protection of information*. 2022. No. 2. P. 15-21.DOI: 10.31673/2409-7292.2022.021521 [in Ukrainian].

13. Panchenko M.V., Bigdan A. M., Babenko T. V., Timofeev D. S. Identification of information security anomalies based on information system entropy analysis. *Energy and automation*, No. 1, 2022. DOI 10.31548/energiya [in Ukrainian].

14. Nicheporuk A.O., Nicheporuk A.A., Savenko O.S., Kazantsev A.D. An intelligent system for detecting anomalies and identifying devices of smart buildings using collective communication. Khmelnytskyi National University // ISSN 2221-3805. *Electrical and computer systems*. 2021. No. 34 (110) Information systems and technologies Users/Administrator/Downloads/3196-Article Text-2350-1-10-20210904.pdf [in Ukrainian].

15. Meshkov V., Virolainen V. Analysis of modern systems for detecting and preventing intrusions in information and telecommunication systems. *Problems of information security in information and communication systems*. 2015. P. 1-4. https://ela.kpi.ua/handle/123456789/17609 [in Ukrainian].

Miroshnyk Maryna *Doctor of Technical Sciences, Professor,*
Professor of Computer systems and robotics department,
Institute of Computer Science and Artificial Intelligence,
V. N. Karazin Kharkiv National University, Svobody Sq., 6, Kharkiv, Ukraine, 61022

Shmatkov Sergiy *Doctor of Technical Sciences, Professor,*
Professor of Computer systems and robotics department,
Institute of Computer Science and Artificial Intelligence,
V. N. Karazin Kharkiv National University, Svobody Sq., 6, Kharkiv, Ukraine, 61022

Strilets Viktoriia *Candidate of Technical Sciences, associate professor of Computer systems and robotics department, Institute of Computer Science and Artificial Intelligence,*
V. N. Karazin Kharkiv National University, Svobody Sq., 6, Kharkiv, Ukraine, 61022

Zats Oleksandr *postgraduate student of Institute of Computer Science and Artificial Intelligence,*
V. N. Karazin Kharkiv National University, Svobody Sq., 6, Kharkiv, Ukraine, 61022

Investigation of computer systems to detect intrusions and network anomalies

The article describes models of intrusion and network anomaly detection systems with quantum autocoding in computer systems. The paper proposes innovative methods for researching intrusion and network anomaly detection systems with quantum autocoding in computer systems that can provide fast response and a high level of adaptability. The paper proposes a quantum QAE (Quantised Autoencoder) model is used in intrusion detection systems to identify anomalies. This model is an optimization approach based on autoencoders, which integrates techniques such as cut-off, clustering, and integer quantisation.

Relevance. The significance of this work lies in the ability to investigate intrusion and network anomaly detection systems utilizing quantum autoencoding in information and communication systems. The study focuses on creating a method for detecting anomalous attacks in IoT network traffic, as identifying anomalies requires detailed monitoring of various network activities. Moreover, the network traffic of each IoT device is distinct. Consequently, the study applies an autoencoder algorithm for anomaly detection, using benign network traffic for model training, with the assumption that any anomalous traffic would lead to an anomaly reconstruction (AR) error.

Research methods. methods for studying intrusion detection systems and network anomalies with quantum autocoding in information and communication systems are probabilistic, verification modelling, and the use of cloud computing, which provide flexibility, scalability and resources for building effective computer attack detection systems.

The results. A real-time IoT dataset was created for both normal and attack traffic. During the training phase, the autoencoder model is trained on normal traffic. The same model is then used to reconstruct anomalous traffic, with the expectation that the reconstruction error (RE) for anomalies will be significant, aiding in the detection of attacks. Additionally, the performance of the autoencoder model was evaluated using metrics such as precision, accuracy, recall, and through a comprehensive experimental study.

Conclusions. The results show that there is a trade-off between the autoencoder and the QAE-u8 model in terms of accuracy and processor evaluation parameters such as memory and CPU. Thus, we conclude that there is a trade-off between the autoencoder and the QAE-u8 model in terms of accuracy and processor evaluation parameters such as memory and CPU. In future research, we will focus on other IoT device vulnerabilities to develop a more secure IoT infrastructure.

The scientific novelty of this work is the development of strategies and techniques for identifying anomalous attacks in IoT network traffic.

Keywords: *computer system, intrusion detection systems, network anomaly detection systems, quantum autocoding*.

Надійшла у першій редакції 04.02.2025, в останній - 06.03.2025.
The first version has been received on 04.03.2025, the final version – on 06.03.2025.