МРНТИ 28.25.77 DOI: https://doi.org/10.62687/STJ.8.1.2025.5

СОЗДАНИЕ МОДУЛЯ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ГРАФЕ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

[1]Б.М. Мазакова*, [1]М. Мусайф
[1]Международный университет Астана, Астана, Казахстан
*e-mail: bayan7080@mail.ru

Б.М. Мазакова – магистр экономики, старший преподаватель высшей школы информационных технологий и инженерии, Международный университет Астана, Астана, Казахстан, e-mail: bayan7080@mail.ru, https://./0000-0003-4904-3557

М. Мусайф – магистр естественных наук, старший преподаватель высшей школы информационных технологий и инженерии, Международный университет Астана, Астана, Казахстан, e-mail: mussaif.marzhan@gmail.com, https://./0000-0003-3795-0424

Аннотация. Быстрое развитие искусственного интеллекта кардинально меняет нашу жизнь и делает её удобней. В частности, обнаружение аномалий в сетевом трафике является одной из удобств, которая представляет собой наибольшее влияние на общество. Традиционно обнаружение аномалий осуществлялось помощью статистических данных, но с появлением машинного обучения, в особенности глубокого обучения, точность обнаружения аномалий значительно повысилась, а сфера применения расширилась.

Алгоритмы обнаружения аномалий - это способы используемые для выявления данных, которые сильно отличаются от нормальных данных и их поведения. Алгоритм эффективно и точно выявлять аномалии в больших объемах данных, снижать риски и затраты, а также повышать удовлетворенность клиентов. Целью данного исследования является анализ возможностей нейросетевых моделей для обнаружения аномалий в сетевом трафике, оценка их эффективности в сравнении с классическими методами защиты, а также разработка практических рекомендаций по их интеграции в системы информационной безопасности. Результаты исследования могут быть применены для:

- Улучшения систем обнаружения вторжений (IDS/IPS) за счет внедрения алгоритмов машинного обучения, повышающих точность и скорость выявления угроз.
- Снижения нагрузки на специалистов по безопасности благодаря автоматизации анализа трафика и минимизации ложных срабатываний.
- Повышения устойчивости к новым видам атак, включая неизвестные ранее угрозы, за счет способности нейросетей выявлять аномалии без заранее заданных правил.
- Оптимизации ресурсов защиты за счет адаптивного подхода, позволяющего системам самостоятельно обучаться на новых данных и изменяющихся условиях сети.

Внедрение нейросетевых технологий в системы кибербезопасности способно стать новым стандартом защиты, обеспечивающим надежное противодействие динамичным и изощренным киберугрозам.

Ключевые слова: нейронные сети, градиентный метод, автоэнкодер, кодировщика-декодера, автокодировщики, обнаружения аномалий, сетевой трафик.

НЕЙРОНДЫҚ ЖЕЛІЛЕРГЕ НЕГІЗДЕЛГЕН ЖЕЛІЛІК ГРАФАДАҒЫ АУЫТҚУЛАРДЫ АНЫҚТАУ ҮШІН МОДУЛЬДІ ӘЗІРЛЕУ

[1]Б.М. Мазакова*, **[1]М. Мусайф**
[1]Астана халықаралық университеті, Астана, Қазақстан
*e-mail: bayan7080@mail.ru

Б.М. Мазакова – экономика магистрі, ақпараттық технологиялар және инженерия жоғары мектебінің аға оқытушысы, Астана Халықаралық университеті, Астана, Қазақстан, e-mail: bayan7080@mail.ru, https://./0000-0003-4904-3557

М. Мусайф – жаратылыстану ғылымдарының магистрі, ақпараттық технологиялар және инженерия жоғары мектебінің аға оқытушысы, Астана Халықаралық университеті, Астана, Қазақстан, e-mail: mussaif.marzhan@gmail.com, https://./0000-0003-3795-0424

Андатпа. Жасанды интеллекттің қарқынды дамуы біздің өмірімізді түбегейлі өзгертіп, оны әлдеқайда қолайлы етіп келеді. Атап айтқанда, желілік трафиктегі аномалияларды анықтау – қоғамға ең үлкен әсер ететін маңызды бағыттардың бірі. Дәстүрлі түрде аномалияларды анықтау статистикалық әдістер арқылы жүзеге асырылып келді, алайда машиналық оқытудың, әсіресе терең оқытудың пайда болуымен аномалияларды анықтау дәлдігі айтарлықтай артты және оны қолдану саласы кеңейді.

Аномалияларды анықтау алгоритмдері – қалыпты деректерден және олардың мінез-құлқынан айтарлықтай ерекшеленетін деректерді табуға арналған тәсілдер. Мұндай алгоритмдер үлкен көлемді деректерде аномалияларды тиімді әрі дәл анықтауға, тәуекелдер мен шығындарды азайтуға, сондай-ақ пайдаланушылардың қанағаттанушылығын арттыруға мүмкіндік береді.

Жұмыстың мақсаты. Бұл зерттеудің мақсаты – желілік трафиктегі аномалияларды анықтау үшін нейрондық желі модельдерінің мүмкіндіктерін талдау, олардың дәстүрлі қорғаныс әдістерімен салыстырғандағы тиімділігін бағалау және оларды ақпараттық қауіпсіздік жүйелеріне интеграциялау бойынша практикалық ұсыныстар әзірлеу.

Зерттеу нәтижелерін төмендегі бағыттарда қолдануға болады:

- Кірісті анықтау жүйелерін (IDS/IPS) машиналық оқыту алгоритмдері арқылы жетілдіру, бұл қауіптерді анықтаудың дәлдігі мен жылдамдығын арттыруға мүмкіндік береді.
- Трафикті талдауды автоматтандыру және жалған ескертулерді азайту арқылы қауіпсіздік мамандарының жүктемесін төмендету.
- Алдын ала белгіленген ережелерсіз аномалияларды анықтау қабілетінің арқасында жаңа және бұрын белгісіз шабуыл түрлеріне төзімділікті күшейту.
- Желінің өзгермелі жағдайларына бейімделіп, жаңа деректер негізінде өздігінен оқуға мүмкіндік беретін икемді тәсілдер арқылы қорғау ресурстарын оңтайландыру.

Нейрондық желі технологияларын киберқауіпсіздік жүйелеріне енгізу динамикалық және күрделі кибершабуылдарға сенімді қарсы тұруды қамтамасыз ететін жаңа қорғаныс стандарты бола алады.

Түйін сөздер: нейрондық желілер, градиенттік әдіс, автоэнкодер, кодтаушы-декодтаушы, автокодировщиктер, аномалияларды анықтау, желілік трафик.

DEVELOPMENT OF A MODULE FOR ANOMALY DETECTION IN A NETWORK GRAPH BASED ON NEURAL NETWORKS

[1]B.M. Mazakova*, **[1]M. Musaif**
[1]Astana International University, Astana, Kazakhstan
*e-mail: bayan7080@mail.ru

B.M. Mazakova – master of Economics, Senior Lecturer of the School of Information Technology and Engineering, Astana International University, Astana, Kazakhstan, e-mail: bayan7080@mail.ru, https://./0000-0003-4904-3557

M. Musaif – master of Natural Sciences, Senior Lecturer of the School of Information Technology and Engineering, Astana International University, Astana, Kazakhstan, e-mail: mussaif.marzhan@gmail.com, https://./0000-0003-3795-0424

Abstract. The rapid development of artificial intelligence is fundamentally transforming our lives and making them more convenient. In particular, anomaly detection in network traffic is one of the advances that has a significant impact on society. Traditionally, anomaly detection was carried out using statistical methods; however, with the emergence of machine learning–especially deep learning–the accuracy of anomaly detection has greatly improved, and its application scope has expanded.

Anomaly detection algorithms are methods used to identify data that significantly deviates from normal data and its behavior. Such algorithms make it possible to detect anomalies effectively and accurately in large data volumes, reduce risks and costs, and increase user satisfaction.

Purpose of the study. The purpose of this research is to analyze the capabilities of neural network models for detecting anomalies in network traffic, evaluate their effectiveness compared with classical security methods, and develop practical recommendations for integrating them into information security systems.

Practical significance. The results of this study can be applied to:

- Improving intrusion detection systems (IDS/IPS) through the introduction of machine learning algorithms that enhance the accuracy and speed of threat detection.
- Reducing the workload on security specialists by automating traffic analysis and minimizing false positives.
- Increasing resistance to new types of attacks, including previously unknown threats, due to the ability of neural networks to detect anomalies without predefined rules.
- Optimizing security resources through adaptive approaches that allow systems to learn independently from new data and changing network conditions.

The integration of neural network technologies into cybersecurity systems may become a new standard of protection, providing reliable defense against dynamic and sophisticated cyber threats.

Keywords: neural networks, gradient method, autoencoder, encoder–decoder, autoencoders, anomaly detection, network traffic.

Методы машинного обучения. Модели обнаружения аномалий, основанные на машинном обучении, автоматически выявляют закономерности нормального и аномального поведения, обучаясь на больших объемах данных. Эти методы способны обнаруживать отклонения даже в ранее неизвестных данных, что делает их особенно эффективными для выявления сложных взаимосвязей и корреляций. В зависимости от типа доступных данных применяются различные подходы: Контролируемое обучение - модель обучается на размечанных данных, где аномалии заранее определены.

Одним из наиболее перспективных направлений является применение нейросетевых и методов искусственного интеллекта для выявления аномалий и обнаружения вторжений в компьютерных сетях. Исследования показывают, что нейронные сети способны эффективно

обрабатывать большие массивы данных и выявлять скрытые закономерности в сетевом трафике, недоступные традиционным статистическим методам (Адамова, 2023:52; Скрыпников&Денисенко, 2023:40).

Методы машинного обучения широко используются для обнаружения аномалий в сетевых данных. В работах отмечается, что алгоритмы обучения без учителя позволяют выявлять отклонения от нормального поведения сети и обнаруживать потенциальные угрозы на ранних этапах их возникновения (Гурина&Елисеев, 2019:52–62). Дальнейшее развитие получили методы глубокого обучения, обеспечивающие более высокую точность анализа за счет использования многослойных нейронных сетей и способности адаптироваться к изменяющимся характеристикам трафика (Борисов&Будников, 2024:200–202).

Значительное внимание в научных исследованиях уделяется вопросам автоматической идентификации угроз информационной безопасности. Нейросетевые модели позволяют не только классифицировать известные типы атак, но и выявлять ранее неизвестные угрозы, что особенно важно в условиях постоянно эволюционирующих методов кибератак (Ван, 2024:288–291; Юхнов, 2023:26–28). Использование искусственного интеллекта в сфере информационной безопасности способствует повышению адаптивности и устойчивости систем защиты (Володин, 2024:91; Степанов, 2024:314–320).

Методы глубокого обучения. Глубокое обучение позволяет выявлять аномалии за счет сложных нелинейных зависимостей и автоматического извлечения признаков из данных. Этот подход особенно эффективен при работе с высоко размерными данными (например, изображения, временными рядами) и в ситуациях, где ручной подбор признаков затруднен. Основной принцип заключается в обучении модели на нормальных данных, после чего аномалиями считается наблюдения, которые плохо реконструируются или классифицируются. Для разных типов данных применяются специализированные архитектуры:

- Сверточные нейронные сети - для анализа изображений и пространственных данных.
- Рекуррентные нейронные сети - для обработки временных рядов и последовательностей.
- Автоэнкодеры - для выявления аномалий через ошибки реконструкции.

Глубокое обучение демонстрирует высокую точность в задачах, где традиционные методы оказываются неэффективными, например, при анализе многомерных сигналов или обнаруживания редких событий. Однако его ключевые неостатки - высокая вычислительная сложность, необходимость в больших объемах данных и низкая интерпретируемость результатов. Также возможны ложные срабатывания, особенно если аномалии слабо выражены или данные зашумлены.

Методы основанные на расстоянии и плотности. Эти методы выявляют аномалии, анализирую локальную плотность данных.

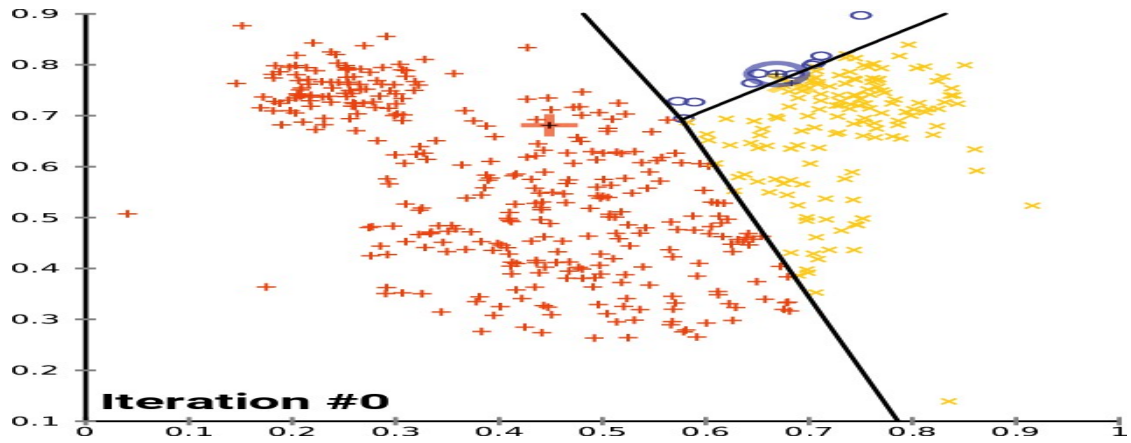

Рисунок 1. Метод к-средних

областях или значительно удаленные от основных кластеров. Наиболее распространенные алгоритмы:

- k-ближайщих соседей - аномалии определяются по большому расстоянию до соседних точек
- Локальный фактор выбросов - оценивает степень изолированности объекта относительно окружения.

Нейросетевые методы также активно используются при разработке систем обнаружения вторжений. Исследования показывают, что применение совокупностей нейронных сетей и биоинспирированных моделей, включая иммунные нейросетевые системы, позволяет повысить точность обнаружения атак и снизить количество ложных срабатываний (Москвичев, 2019:84–85; Стрижко, 2023:23–33). Сравнительный анализ различных нейросетевых подходов подтверждает, что выбор конкретной модели должен учитывать особенности сетевого трафика и требования к уровню информационной безопасности (Маковейчук, 2024:142–147).

Преимущества таких методов - простота интеграции, гибкость в работе с нелинейными распределениями и кластерами разной плотности. Однако они чувствительны к масштобированию данных и плохо масштабируются на высокоразмерные пространства из-за проклятия размерности. Также их точность снижается, если аномалии расположены близко к нормальным данным или кластеры имеют неравномерную плотность.

Вероятностные методы. Эти подходы на построении вероятностных моделей данных, где аномалии определяются как маловероятные события. К ним относятся:

- Гауссовые смеси - моделируют данные как комбинацию нормальных распределений.
- Байесовские сети - учитывают априорные знания о данных.
- Скрытые марковские модели - применяются для последовательностей.

Вероятностые методы хорошо работают с многомерными данными и позволяют учитывать неопределнность, но требуют значительных вычислительных ресурсов. Их точность зависит от соответствия данных выбранному распределению, а сложные модели могут страдать от переобучения.

Wireshark как инструмент анализа сетевых аномалий. Wireshark - это мощный инструмент для захвата и анализа сетевого трафика, поддерживающий различные ОС. Его ключевые возможности:

- Перехват пакетов в реальном времени с фильтрацией по протоколам, IP-адрессам и другим параметрам.
- Анализ подозрительной активности например, неавторизированных подключений или аномального объёмов трафика
- Отладка сетевых приложений и диагностика проблем производительности.

Wireshark полезен как для специалистов по безопасности, так и для сетевых администраторов, но требует определенного уровня экспертизы для корректной интерпретации данных.

Материалы и методы. Для разработки выявления аномалий в сетевом трафике сначала были выбраны инструменты анализа сетевых аномалий Wireshark, который является бесплатной программой для анализа сетевого трафика.

Wireshark = «сетевой анализатор», который показывает всё, что происходит в сети. А в трудах Я. Т. Маковейчука, Л. А. Мазур и П. П. Танчинца разбираются разные варианты нейросетевых методов для выявления вторжений и аномалий в трафике. Авторы подчёркивают, что нейронные сети лучше справляются с предотвращением утечек информации и атак, чем старые традиционные способы (Маковейчук, 2024; Мазур, 2024; Танчинец, 2024).

Выбран алгоритм нейронной сети для выявления аномалии сетевого трафика

это : Автоэнкодер (AE) – самый распространённый вариант

Прямой проход (кодирование + декодирование):

$$z = f_\theta(x), \quad \widehat{x} = g_\phi(z) \tag{1}$$

Функция потерь (MSE):

$$L_{AE}(x) = \|x - \widehat{x}\|_2^2 = \|x - g_\phi(f_\theta(x))\|_2^2 \tag{2}$$

(можно использовать l_1 или бинарную кросс-энтропию при соответствующих признаках)

Аномалити-скор (reconstruction error):

$$S_{AE}(x) = \|x - \widehat{x}\|_2^2 \tag{3}$$

Правило: если $S_{AE}(x) > \tau$ – помечаем как аномалию (порог τ устанавливают, например, по 95%-перцентилю ошибок на валидации).

Для написания программы использовался язык программирования Python. Также использовалась среда разработки Pycharm, на рисунке ниже перечислены все библиотеки, которые использовались для разработки.

```
import sys
import os
import pandas as pd
import numpy as np
from datetime import datetime
from sklearn.ensemble import IsolationForest
from sklearn.model_selection import train_test_split
from sklearn.metrics import classification_report, confusion_matrix
import matplotlib.pyplot as plt
from matplotlib.backends.backend_qt5agg import FigureCanvasQTAgg as FigureCanvas
from PyQt5.QtWidgets import (QApplication, QMainWindow, QVBoxLayout, QHBoxLayout, QWidget,
                             QLabel, QPushButton, QComboBox, QSpinBox, QDoubleSpinBox,
                             QTextEdit, QTabWidget, QFileDialog, QMessageBox, QProgressBar)
from PyQt5.QtCore import Qt, QThread, pyqtSignal
import joblib
import seaborn as sns
```

Рисунок 2. Использованные библиотеки sys

Библиотека sys обеспечивает доступ к системным параметрам и функциям интерпретатора Python, позволяя взаимодействовать со средой выполнения. Этот пакет предоставляет инструменты для прямого взаимодействия с интрепретатором языка, кллючая управление аргементам командной строки, настройку путей импорта моделкй обработку системных исключений.

Библиотека os предоставляет инструменты для работы с операционной системой, включая управления файлами, переменными окружения и путями. Поддерживает операции создания/удаления директорий и манипуляции с файловыми путями[18].

Библиотека datetime модуль для обработки временных данных с классами:

- date - работа с датами.
- datetime - дата и время.
- timedelta - временные интервалы

Библиотека pandas мощный инструмент для анализа данных с поддержкой:

- Структур данных Series и DataFrame.
- Чтение различных форматов(CSV, Excel, Json).
- Очистки данных(обработка пропусков, сортировка).
- Интеграция с Matplotlib для визуализации.

Используя все вышеперечисленные методы в данной работе была разработана приложение обнаружения аномалий для удобство использование программы. Таким образом создать свою модель может любой.

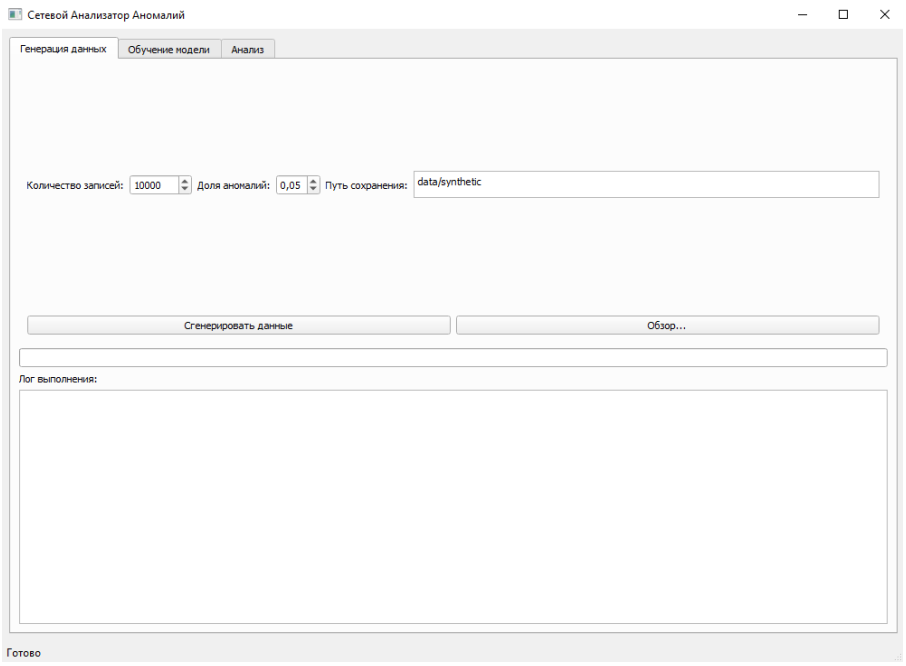

Рисунок 3. Окно генерации данных

Это окно включает в себя функции генерации данных. На этом окне мы можем сгенерировать данные, а также выбрать уже созданные , настроить количество записей и долю аномалий в них (в соответствии с рисунком 3).

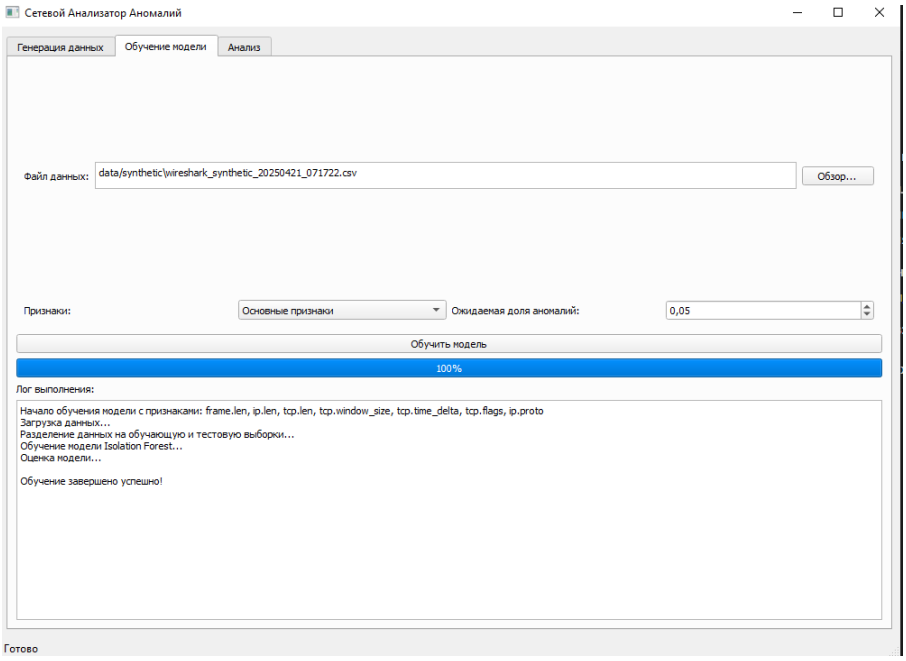

Рисунок 4. Окно обучения модели

В окне обучения модели предусмотрен набор функций, включающий выбор данных для обучения, настройку параметров обучения, а также запуск алгоритма обучения модели (рисунок 4) в соответствии со схемой, представленной на рисунке 3.

Рисунок 5. Окно анализа данных

В окне обучения модели доступны несколько функций. Выбор данных для обучения, настройка обучения и так же возможен запуск алгоритма обучения модели.

Практическая значимость нейросетевых методов заключается также в их использовании для предотвращения утечек информации. В научных публикациях отмечается, что интеллектуальные модели анализа трафика способны выявлять аномальные шаблоны передачи данных, потенциально связанные с несанкционированным доступом и утечками конфиденциальной информации (Танчинец, 2024:41–44). Дополнительные методические подходы к обнаружению аномалий в сетевом трафике представлены в электронных научных ресурсах, что способствует расширению инструментальной базы исследований в данной области (Method for detecting anomalies in network traffic, n.d.).

Использование нейросетевых модулей для обнаружения аномалий позволяет значительно повысить точность мониторинга и выявления угроз делая это своевременно. В отличие от традиционных методов, такие модели имеют возможность выявлять закономерности в данных без явных правил или аннотаций, что делает их особенно подручными для обнаружения аномалий и неизвестных ранее атак.. Это значительно усиливает защиту корпоративных сетей и сложных инфраструктур, где классические методы уступают в надежности. Интеграции нейросетей в системы обнаружения аномалий становится критически важным этапом для совершенствования информационной безопасности. Нейросети не только повышают точность обнаружения угроз, но и обеспечивают масштабируемость защиты в условиях роста данных, делая их незаменимыми элементом современных кибербезопасных архитектур.

Выводы. В рамках проведенного исследования достигнуты следующие результаты:

1. Выбран алгоритм нейронной сети для выявления аномалии сетевого трафика автоэнкодер (AE)

2. На языке программирования Python разработана система мониторинга и прогнозирования аномалии сетевого трафика

3. Весь процесс выполняется в фоновом потоке, что помогает интегрироваться с графическим интерфейсом, не блокируя его.Сначала устанавливаем фиксированное случайное начальное число с помощью np.random.seed (42), чтобы гарантировать воспроизводимость результатов. Затем, если каталог self.save_path еще не существует, он создается с помощью os.makedirs.Далее создается словарь данных, соответствующий каждому

ключевому полю сетевого пакета. Для каждого поля создается значение self.num_samples. Используются различные дистрибутивы.Временные метки Frame.time записываются в формате времени.Размеры пакетов frame.len, ip.len и tcp.len распределены нормально. IP-адреса генерируются случайным образом в виде строк, Протоколы, флаги, методы и другие поля выбираются из заданного набора с заданной вероятностью.dns.count.queries получен из распределения Пуассона.tcp.time_delta исходит из экспоненциального распределения.

Литература

Адамова, 2023 – Адамова А.А. Анализ безопасности сетевого трафика посредством нейросети // Математическое моделирование и информационные технологии. – 2023. – С. 52. [Rus]

Борисов&Будников, 2024 – Борисов Д.А., Будников К.И. Применение глубокого обучения для анализа сетевого трафика // Математическое и компьютерное моделирование. – 2024. – С. 200–202. [Rus]

Ван, 2024 – Ван Х. Использование нейросетей для автоматической идентификации угроз информационной безопасности // Экономика строительства. – 2024. – С. 288–291. [Rus]

Виноградов, 2024 – Виноградов О.Е. Применение метода изолирующего леса для обнаружения сетевых аномалий в аппаратно-программном комплексе «Безопасный город» // Научно-технический сборник Поволжья. – 2024. – С. 76–78. [Rus]

Володин, 2024 – Володин А.А. Развитие и проблемы использования искусственного интеллекта в области информационной безопасности // Политехнический молодежный журнал. – 2024. – С. 91. [Rus]

Гурина&Елисеев, 2019 – Гурина А.О., Елисеев В.Л. Обнаружение аномалий на основе машинного обучения // Защита информации. – 2019. – С. 52–62. [Rus]

Каменко, 2023 – Каменко Д.А. Автоматизация метода изолирующего леса // Новые направления развития приборостроения. – Минск, 2023. – С. 233. [Rus]

Маковейчук, 2024 –Маковейчук Я.Т. Сравнение подходов к обнаружению вторжений с применением нейросетей для анализа сетевого трафика // Безопасные информационные технологии. – Москва, 2024. – С. 142–147. [Rus]

Мазур, 2024 – Мазур Л.А. Исследование нейросетевых методов обнаружения аномалий сетевого трафика для защиты информации // Школа молодых новаторов. – Курск, 2024. – С. 80–84. [Rus]

Москвичев, 2019 – Москвичев А.Д. Система обнаружения вторжений на основе иммунной системы нейросетевых детекторов // Colloquium Journal. – 2019. – С. 84–85. [Rus]

Скрыпников&Денисенко, 2023 – Скрыпников А.В., Денисенко В.В. Применение нейросетей для анализа сетевого трафика // Материалы LXI отчетной научной конференции. – 2023. – С. 40. [Rus]

Станкевич, 2016 – Станкевич А.А. Разработка дисциплины обслуживания на основе нейросетевого прогноза трафика дифференцированных услуг : автореф. дис. … канд. техн. наук. – 2016. [Rus]

Степанов, 2024 – Степанов Г.В. Использование искусственного интеллекта в сфере информационной безопасности // Интеллектуальный потенциал XXI века. – 2024. – С. 314–320. [Rus]

Стрижко, 2023 – Стрижко М.А. Модуль интеллектуального анализа сетевого трафика в системах обнаружения вторжений на базе совокупности нейронных сетей // Вестник Донецкого национального университета. – 2023. – С. 23–33. [Rus]

Танчинец, 2024 – Танчинец П.П. Нейросетевые подходы к обнаружению аномалий в сетевом трафике для предотвращения утечек информации // Вопросы обеспечения безопасности в киберпространстве. – Махачкала, 2024. – С. 41–44. [Rus]

Шуленина, 2019 – Шуленина А.В. Применение нейросетей для классификации сетевого трафика // Молодой ученый. – 2019. – № 49. – С. 26–28. [Rus]

Юхнов, 2023 – Юхнов В.И. Применение искусственного интеллекта для решения задачи обеспечения безопасности информации, передаваемой в сетях // Труды Северо-Кавказского филиала МТУСИ. – 2023. – С. 26–28. [Rus]

Метод выявления аномалий в сетевом трафике – Метод выявления аномалий в сетевом трафике [Электронный ресурс]. – URL: https : //cyberleninka.ru/article/n/metod – vyyavleniya – anomaliy – v – setevom – trafike. [Rus]

References

Adamova, A. A. (2023). Analiz bezopasnosti setevogo trafika posredstvom neyroseti [Analysis of Network Traffic Security Using Neural Networks].//Matematicheskoe modelirovanie i informatsionnye tekhnologii, p. 52. [In Russ]

Borisov, D. A., & Budnikov, K. I. (2024). Primenenie glubokogo obucheniya dlya analiza setevogo trafika [Application of Deep Learning for Network Traffic Analysis]//Matematicheskoe i komp'yuternoe modelirovanie, pp. 200–202. [In Russ]

Van, H. (2024). Ispol'zovanie neyrosetey dlya avtomaticheskoy identifikatsii ugroz informatsionnoy bezopasnosti [Use of Neural Networks for Automatic Identification of Information Security Threats]. Ekonomika stroitel'stva, pp. 288–291. [In Russ]

Vinogradov, O. E. (2024). Primenenie metoda izoliruyushchego lesa dlya obnaruzheniya setevykh anomaliy v apparatno-programmnom komplekse «Bezopasnyy gorod» [Application of the Isolation Forest Method for Detecting Network Anomalies in the ``Safe City'' Hardware-Software Complex] // Nauchno-tekhnicheskiy sbornik Povolzh'ya, pp. 76–78. [In Russ]

Volodin, A. A. (2024). Razvitie i problemy ispol'zovaniya iskusstvennogo intellekta v oblasti informatsionnoy bezopasnosti [Development and Challenges of Using Artificial Intelligence in Information Security].// Politekhnicheskiy molodezhnyy zhurnal, p. 91. [In Russ]

Gurina, A. O., & Eliseev, V. L. (2019). Obnaruzhenie anomaliy na osnove mashinnogo obucheniya
[Anomaly Detection Based on Machine Learning]// Zashchita informatsii, pp. 52–62. [In Russ]

Kamenko, D. A. (2023). Avtomatizatsiya metoda izoliruyushchego lesa [Automation of the Isolation Forest Method]// In Novye napravleniya razvitiya priborostroeniya. Minsk, p. 233. [In Russ]

Makoveichuk, Ya. T. (2024). Sravnenie podkhodov k obnaruzheniyu vtorzheniy s primeneniem neyrosetey dlya analiza setevogo trafika [Comparison of Intrusion Detection Approaches Using Neural Networks for Network Traffic Analysis]// Bezopasnye informatsionnye tekhnologii. Moscow, pp. 142–147. [In Russ]

Mazur, L. A. (2024). Issledovanie neyrosetevykh metodov obnaruzheniya anomaliy setevogo trafika dlya zashchity informatsii [Study of Neural Network Methods for Detecting Network Traffic Anomalies for Information Protection]// Shkola molodykh novatorov. Kursk, pp. 80–84. [In Russ]

Moskvichev, A. D. (2019). Sistema obnaruzheniya vtorzheniy na osnove immunnoy sistemy neyrosetevykh detektorov [Intrusion Detection System Based on an Immune System of Neural Network Detectors].//Colloquium Journal, pp. 84–85. [In Russ]

Skrypnikov, A. V., & Denisenko, V. V. (2023). Primenenie neyrosetey dlya analiza setevogo trafika
[Application of Neural Networks for Network Traffic Analysis].//In Materialy LXI otchetnoy nauchnoy konferentsii, p. 40. [In Russ]

Stankevich, A. A. (2016). Razrabotka distsipliny obsluzhivaniya na osnove neyrosetevogo prognoza trafika differentsirovannykh uslug [Development of a Service Discipline Based on Neural Network Forecasting of Differentiated Services Traffic].// PhD dissertation abstract. [In Russ]

Stepanov, G. V. (2024). Ispol'zovanie iskusstvennogo intellekta v sfere informatsionnoy bezopasnosti [Use of Artificial Intelligence in the Field of Information Security]// Intellektual'nyy potentsial XXI veka, pp. 314–320. [In Russ]
Strizhko, M. A. (2023). Modul' intellektual'nogo analiza setevogo trafika v sistemakh obnaruzheniya vtorzheniy na baze sovokupnosti neyronnykh setey [Intelligent Network Traffic Analysis Module in Intrusion Detection Systems Based on a Set of Neural Networks].//Vestnik Donetskogo natsional'nogo universiteta, pp. 23–33. [In Russ]
Tanchinets, P. P. (2024). Neyrosetevye podkhody k obnaruzheniyu anomaliy v setevom trafike dlya predotvrashcheniya utechek informatsii [Neural Network Approaches to Detecting Anomalies in Network Traffic to Prevent Information Leakage]. Voprosy obespecheniya bezopasnosti v kiberprostranstve. Makhachkala, pp. 41–44. [In Russ]
Shulenina, A. V. (2019). Primenenie neyrosetey dlya klassifikatsii setevogo trafika [Application of Neural Networks for Network Traffic Classification].// Molodoy uchenyy, 49, pp. 26–28. [In Russ]
Yukhnov, V. I. (2023). Primenenie iskusstvennogo intellekta dlya resheniya zadachi obespecheniya bezopasnosti informatsii, peredavaemoy v setyakh [Application of Artificial Intelligence to Solving the Problem of Information Security in Networks].// Trudy Severo-Kavkazskogo filiala MTUSI, pp. 26–28. [In Russ]
Method for detecting anomalies in network traffic. (n.d.). Available at: https : //cyberleninka.ru/article/n/metod – vyyavleniya – anomaliy – v – setevom – trafike