ОТЗЫВ

официального оппонента на диссертационную работу Мазурка Дмитрия Валерьевича «Алгоритмы глубокого машинного обучения в системах анализа сетевого трафика», представленную на соискание учёной степени кандидата технических наук по специальности 2.3.1 — Системный анализ, управление и обработка информации, статистика

Актуальность темы исследования

Современный этап развития телекоммуникаций характеризуется быстрым ростом сложности и объема сетевого трафика, что обусловливает необходимость создания эффективных инструментов анализа для обеспечения доступности и производительности сетей. Системы анализа сетевого трафика играют ключевую роль в процессах принятия решений, включая обнаружение сетевых вторжений, мониторинг производительности и обнаружение утечек данных. На замену традиционным методам анализа трафика, которые становятся недостаточно эффективными в условиях растущей сложности данных, приходят нейронные сети, которые обеспечивают потенциально более высокую точность и производительность. При этом возникают существенные трудности в вопросах интерпретируемости решений нейросетевых классификаторов, обеспечения их функциональной устойчивости на зашумленных данных и ослабления чувствительности к состязательным атакам. Кроме того, нейронные сети требуют своевременной адаптации при изменениях распределения данных.

Повышение интерпретируемости позволяет повысить доверие к алгоритмам и снизить ошибки в принятии решений. Робастность критически важна в условиях действия набора непредсказуемых факторов, характерных для реальных информационных сетей.

Таким образом, диссертационная работа Мазурка Дмитрия Валерьевича, в которой сформулирована и решена научная задача повышения эффективности принятия решений в системах анализа сетевого трафика на основе алгоритмов глубокого машинного обучения, является актуальной и своевременной.

В качестве объекта исследования рассматривается процесс поддержки принятия решений в системах анализа сетевого трафика. Предметом исследования являются алгоритмы глубокого машинного обучения, используемые в системах анализа сетевого трафика.

В диссертации сформулированы и решены следующие задачи:

1. Анализ существующих моделей и алгоритмов глубокого машинного обучения, используемых в задачах анализа сетевого трафика;

2. Разработка модели и алгоритмов повышения интерпретируемости нейросетевого классификатора анализатора сетевого трафика;

3. Разработка алгоритма оценки функциональной устойчивости нейросети анализатора сетевого трафика в условиях искажений данных;

4. Экспериментальное исследование разработанных моделей и алгоритмов.

Объём и структура диссертации

Диссертация состоит из введения, трех глав, заключения, списка обозначений и сокращений, списка использованных источников из 123 наименований, 9 приложений и содержит 116 страниц основного текста, иллюстрированного 27 рисунками, содержит 4 таблицы.

В первой главе проводится анализ объекта исследования, включая сферы применения нейросетевых анализаторов в компьютерных сетях, проблемы использования нейросетей; дана интерпретация проблемы обеспечения качества нейросетевых классификаторов.

Во второй главе разработаны модели и алгоритмы повышения интерпретируемости результатов работы нейросетевого классификатора, в том числе: базовый алгоритм оценки интерпретируемости и модифицированный алгоритм интерпретации с использованием больших языковых моделей.

В третьей главе разработан алгоритм оценки функциональной устойчивости нейросети в условиях искажений входных данных; проведено экспериментальное исследование предложенных моделей и алгоритмов.

В заключении подводятся итоги диссертационного исследования, сформулированы выводы и определены направления дальнейших исследований.

Достоверность и обоснованность научных положений, выводов и рекомендаций

Достоверность результатов исследования подтверждается:

1. Постановкой серии корректных экспериментов на моделях, выполненных на экспериментальных установках;

2. Положительным результатом практического использования разработанных инструментальных средств;

3. Апробацией основных положений и выводов исследования в печати и на профильных научных конференциях.

Научные положения диссертации обосновываются с использованием методов системного анализа, унифицированных методов и процедур математической статистики и автоматизированной обработки данных. Для экспериментальной проверки использовались стандартное и разработанное соискателем программное обеспечение. Результаты диссертационного исследования достаточно хорошо согласуются с фундаментальными положениями системного анализа, теории машинного обучения и анализа данных, не противоречат ранее опубликованным работам и подтверждены статистическими тестами и корреляционным анализом.

Научная новизна результатов диссертации

Научная новизна заключается в следующем:

1. Разработан алгоритм оценки интерпретируемости результатов работы нейросети, отличающийся использованием положительных заключений модели и новой метрики точности, что позволяет численно сравнивать методы интерпретации в задачах бинарной классификации редких событий.

2. Разработан алгоритм оценки устойчивости нейросети анализатора сетевого трафика, отличающийся обоснованным использованием аугментации тестовой выборки с помощью вариационного автокодировщика с условием (cVAE), а также учетом степени переобучения, позволяющий определить пригодность классификатора в условиях зашумленности данных.

3. Предложен модифицированный в части представления и анализа данных алгоритм интерпретации решений классификатора, отличающийся

использованием большой языковой модели (LLM), что позволяет выявлять и корректировать ошибки классификации.

Как показано в диссертации, расширенный метод интерпретации позволяет снизить ошибку первого рода и повысить общую точность системы обнаружения сетевых вторжений на основе нейросетевого классификатора в среднем на 20%. Совместное использование LLM и мультиагентного подхода повышает общую точность классификации без привлечения человека на 23%. Предложенная автором диссертации методика оценки робастности позволяет оценить стабильность точности модели в условиях зашумленности входных данных.

Практическая значимость диссертации

Практическая значимость исследования обусловлена разработкой эффективных алгоритмов и программного обеспечения, позволяющих, согласно представленным данным (с. 91, табл. 4) существенно повысить качество работы нейросетевого классификатора по сравнению с типовой реализацией. В частности, переход к использованию конечной модели LLM позволит улучшить показатель робастности (по сравнению с базовыми моделями 1 и 2) на 48,3 %, а показатель робастности улучшить (по сравнению с базовой моделью 3) на 27 %.

Автором диссертации лично и в соавторстве разработаны следующие программные средства: модифицированный алгоритм интерпретации с LLM (свидетельство № 2024682393); программа для оценки повышения интерпретируемости (свидетельство № 2024682916); модуль оценки значимости по результатам эксперимента (свидетельство № 2024682642); модуль оценки актуальности факторов защищенности (свидетельство №2021618487); модуль тестирования скорости и точности (свидетельство №2021618197); модуль аудита на подверженность состязательным атакам (свидетельство №2021619081) и графический интерфейс к нему (свидетельство №2021618155).

Результаты диссертационного исследования внедрены в ООО «ВОЙС КОММЬЮНИКЕЙШН», ООО «ЮКИТЕХ ЛАБ», ООО «НТЦ «СИСТЕМИНВЕСТ», ООО «АйТиАрт» и в учебный процесс Владимирского государственного университета. Полученные при исследовании рекомендации

могут быть реализованы в технических вузах при изучении дисциплин по машинному обучению и анализу сетевого трафика.

Анализ содержания диссертации

Диссертация по содержанию соответствует паспорту специальности 2.3.1. Системный анализ, управление и обработка информации, статистика: в частности, пунктам 2, 3 и 12.

Содержание автореферата полностью соответствует диссертации.

Основные результаты диссертации опубликованы в 14 научных работах, в том числе одна статья опубликована в журнале с индексацией в международных базах Scopus и Web of Science, три статьи опубликованы в рецензируемых изданиях, рекомендуемых ВАК, автором получено 7 свидетельств о государственной регистрации программ для ЭВМ. Результаты апробированы на конференциях: 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), международных научно-практических конференциях: II «Наука, технологии и инновации: стратегии развития в современном мире», II «Исследования и инновации: синергия знаний и практики», IX и VIII «Наука и глобальные вызовы: перспективы развития», II «Европейские научные исследования», «Инновационное развитие современной науки: проблемы, закономерности, перспективы»; VIII Всероссийской научно-практической конференции «Информационные технологии и автоматизация управления».

Замечания по диссертации

1. Формула (26, с. 80 диссертации, R_overfit) весьма приближенно оценивает переобучение. При этом разница в точности на обучающих и тестовых выборках может быть обусловлена не только переобучением, но и разным распределением данных (ковариатным сдвигом). Использование этой эвристики в формуле итоговой робастности (25, с. 80) предполагает необходимость дополнительного анализа факторов, способных вызвать искажение оценки.

2. Все эксперименты проведены на одной архитектуре (DNN) и одном датасете (CSE-CIC-IDS2018). В диссертации не показано, насколько предложенный метод интерпретации будет эффективен применительно к CNN и LSTM.

3. В диссертации не рассматривается сценарий, при котором LLM генерирует уверенное, но ложное объяснение, предлагая оператору (либо автоматической системе) изменить правильный ответ нейросетевого классификатора на неправильный. Не приведены статистика таких случаев и оценка их влияния на итоговую скорректированную точность. Без этого утверждение соискателя о возможности полного исключения человека из цепочки принятия решений (с. 73-74) выглядит неубедительно.

Общий вывод

Указанные замечания не снижают общей положительной оценки диссертации и могут рассматриваться как рекомендации для дальнейших исследований. В целом диссертационная работа представляет собой законченный научный труд теоретического и практического характера с рекомендациями применения, выполненный на высоком научном уровне. Автореферат соответствует содержанию диссертации.

Диссертационная работа полностью соответствует требованиям «Положения о порядке присуждения ученых степеней», предъявляемым к кандидатским диссертациям, а ее автор, Мазурок Дмитрий Валерьевич, заслуживает присвоения ученой степени кандидата технических наук по специальности 2.3.1 – Системный анализ, управление и обработка информации, статистика.

Официальный оппонент
профессор кафедры информационных технологий и систем
ФГАОУ ВО «Российский государственный гуманитарный университет»
доктор технических наук, профессор

Евгений Николаевич Надеждин

Подпись Надеждина Е.Н. **заверяю**
Заместитель директора Департамента кадров
01 СЕН 2026
Н.Н. Толстых

Сведения об оппоненте: Надеждин Евгений Николаевич, гражданин Российской Федерации, доктор технических наук (научная специальность 20.02.14 «Вооружение и военная техника, комплексы и системы военного назначения»), профессор, профессор кафедры информационных технологий и систем Федерального государственного автономного образовательного учреждения высшего образования «Российский государственный гуманитарный университет».

Адрес: 125047, г. Москва, Кировоградская улица, д.25, корпус 2, к. 204.

Телефон: +7 (495) 250-64-36.

E-mail: ism@rggu.ru.