ОТЗЫВ

на автореферат диссертации Мазурка Дмитрия Валерьевича «АЛГОРИТМЫ ГЛУБОКОГО МАШИННОГО ОБУЧЕНИЯ В СИСТЕМАХ АНАЛИЗА СЕТЕВОГО ТРАФИКА», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.1 Системный анализ, управление и обработка информации, статистика (технические науки)

Диссертационное исследование, представленное Мазурком Дмитрием Валерьевичем на тему разработки методов оценки и повышения интерпретируемости нейросетевых классификаторов сетевого трафика, посвящено решению остро актуальной проблемы современной кибербезопасности. В условиях экспоненциального роста объемов данных и усложнения архитектуры вычислительных сетей классические сигнатурные методы анализа становятся неэффективными, а применение моделей глубокого обучения зачастую упирается в проблему «черного ящика». Стремление диссертанта обеспечить синергию высокой точности классификации с прозрачностью принимаемых решений определяет несомненную теоретическую значимость и практическую востребованность работы.

Ключевой научной ценностью исследования является формирование комплексного подхода к верификации доверия к нейросетевым моделям. Автором получены следующие существенные научные результаты:

1. Предложена оригинальная методика количественной оценки интерпретируемости, базирующаяся на анализе истинно положительных срабатываний модели (что позволяет избежать искажений из-за дисбаланса классов) и введении специализированной метрики точности интерпретации. Это дает возможность проводить объективный метрологический сравнительный анализ различных подходов *Explainable AI* (*XAI*) при детекции редких аномалий в трафике.
2. Разработан метод стресс-тестирования робастности классификатора, основанный на синтетической аугментации тестовых выборок с использованием условных вариационных автокодировщиков (*cVAE*). Важным методологическим отличием является учет коэффициента переобучения сети при генерации зашумленных сценариев, что позволяет прогнозировать деградацию качества распознавания в реальных нестационарных средах эксплуатации.
3. Обоснована архитектура гибридной системы поддержки принятия решений, интегрирующей нейросетевой классификатор и большую языковую модель (*LLM*). Отличительной особенностью предложенного алгоритма является использование семантических возможностей *LLM* для лингвистического аудита логов внимания нейросети и автоматической коррекции ложноположительных срабатываний через динамическую реконфигурацию весов признаков.

Результаты исследования получили должное признание: они отражены в 14 публикациях, включая 3 статьи в рецензируемых изданиях из перечня ВАК и одну — в международной базе Scopus/Web of Science. Практическая применимость подтверждена 7 свидетельствами о государственной регистрации программ для ЭВМ, а апробация проведена на профильных международных конференциях.

Вместе с тем, работа вызывает ряд дискуссионных вопросов и содержит аспекты, требующие дополнительного пояснения:

В работе отдельно не рассмотрено влияние порога формирования положительного решения классификатора на состав проверяемых тревог и величину эффекта предложенной

процедуры. Было бы полезно подробнее разграничить применимость алгоритма при различных порогах и результаты, полученные в исследованном режиме.

При экспериментальной оценке опубликованная разметка CSE-CICIDS2018 принимается в качестве эталона. В работе недостаточно подробно обсуждается чувствительность полученных оценок к возможным неточностям эталонных меток.

В работе отмечено снижение времени ответа участников по мере выполнения заданий, однако отдельно не разграничены период освоения интерфейса и последующая работа с ним. Такое разграничение позволило бы точнее интерпретировать среднее время принятия решения.

Указанные замечания носят уточняющий характер, продиктованы высоким уровнем проработки материала, и ни в коей мере не ставят под сомнение научную новизну и целостность проведенного исследования.

Диссертация представляет собой завершенный научно-квалификационный труд, в котором решена важная задача синтеза интерпретируемого искусственного интеллекта для задач мониторинга информационной безопасности. Глубина теоретического анализа, строгость математического аппарата и подтвержденная экспериментальная база полностью соответствуют требованиям п. 9–14 Положения ВАК РФ о присуждении ученых степеней. Считаю, что ее автор, Мазурок Дмитрий Валерьевич, достоин присуждения искомой ученой степени кандидата технических наук по специальности 2.3.1 — «Системный анализ, управление и обработка информации, статистика».

Отзыв составил руководитель учебного центра Регионального аттестационного центра, общество с ограниченной ответственностью «ИнфоЦентр» (РАЦ ООО «ИнфоЦентр»), , к.т.н. Вертилевский Никита Валерьевич

Шифр научной специальности 05.12.13 «Системы, сети и устройства телекоммуникаций»

Я, Вертилевский Никита Валерьевич, даю согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

_____ / Вертилевский Никита Валерьевич / «10» 03 2026г.

Подпись дата

Подпись Вертилевского Н.В. удостоверяю:

Полное наименование организации: Региональный аттестационный центр, общество с ограниченной ответственностью «ИнфоЦентр» (РАЦ ООО «ИнфоЦентр»)

Адрес: 600005, Российская Федерация, г. Владимир, Октябрьский проспект, д. 36

Тел: +7 (4922) 25-00-25, доб. 125, эл. почта: info@icentr.ru