УТВЕРЖДАЮ
Первый проректор
доктор химических наук

А.В. Метелица
«27» [illegible] 2026 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

Федерального государственного автономного образовательного учреждения высшего образования
«Южный федеральный университет» (ЮФУ)

на диссертационную работу
Русанова Михаила Андреевича

«Интеллектуальные методы обнаружения несанкционированных вторжений в операционные системы»,

представленную на соискание ученой степени
кандидата технических наук
по специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

В рамках диссертационной работы решалась задача разработки интеллектуальных методов, моделей и программных средств обнаружения и классификации несанкционированных вторжений в операционные системы семейства Linux по данным системных событий.

В ходе проведения исследований разработан интеллектуальный метод оценки вероятности компрометации аутентификационных данных, основанный на анализе статистических характеристик случайности паролей и применении моделей машинного обучения. Разработан интеллектуальный метод обработки потоковых событий операционных систем семейства Linux, основанный на использовании контекстного представления и моделей трансформеров, для обнаружения вредоносной активности и классификации атак. Разработан метод параллельной потоковой обработки системных событий, основанный на адаптивном формировании вычислительных пакетов, динамическом выравнивании длины входных последовательностей и группировке событий по вычислительной сложности.

Актуальность темы диссертационной работы

В условиях цифровой трансформации возрастает сложность современных информационно-вычислительных систем, характеризующихся распределенной архитектурой, высокой интенсивностью обмена данными и

увеличением объемов потоковой информации. Современные программные комплексы функционируют в гетерогенных вычислительных средах, включающих облачные платформы, распределенные сервисы и ресурсно-ограниченные вычислительные узлы, что накладывает дополнительные ограничения на методы интеллектуальной обработки системных событий.

Развитие распределенных облачных технологий и программной инфраструктуры, обеспечивающей глобально распределенную обработку данных, приводит к росту объемов потоковых данных о работе программных компонентов. Анализ таких потоковых данных в режиме реального времени с высокой точностью представляет собой сложную научно-практическую задачу.

Традиционные подходы, основанные на правилах, сигнатурах и шаблонах, недостаточно адаптивны и не учитывают связи между событиями, поэтому все чаще применяются методы машинного обучения. Используются модели семейства трансформеров, позволяющие учитывать контекстные взаимосвязи между элементами последовательностей системных событий и предназначенных для анализа текстовых данных. Их применение позволяет выявлять аномалии в последовательности системных событий и обеспечивать устойчивость и защищенность системы. Вместе с тем их практическое применение остается ресурсоемким, что делает актуальной оптимизацию потокового вывода, направленную на повышение пропускной способности, сокращение времени обработки и параллельную обработку данных без изменения архитектуры модели.

Значительный научный вклад в рассматриваемую область внесли следующие исследователи: А.В. Федорченко, И.В. Котенко, А.В. Хорошилов, И.Г. Сидоркина, С. В. Михалищев, A. L. Buczak, E. Guven, R. Sommer и V. Paxson, T. Vyšniūnas, D. Čeponis, N. Goranin, A. Čenys, F. Wang, Q. Weng, M. Zhang, Y. Shao, Z. Alomari, A. Makanju, Z. Li, Zhang S., Zhao P., An Z. и др.

Структура и основное содержание диссертационной работы

Диссертация имеет логичную структуру, что дает возможность последовательно и полно исследовать предложенные в работе методы и алгоритмы. Она состоит из введения, 3-х глав, заключения, списка литературы, содержащего 108 наименований. Объем основного текста работы составляет 130 страниц, включая 30 рисунков и 20 таблиц.

Во введении обоснована актуальность темы диссертации, сформулированы цель и задачи работы, выбраны объект и предмет исследования, показаны научная новизна, практическая и теоретическая ценность полученных результатов, приведены основные положения, выносимые на защиту.

В первой главе выполнен анализ существующих методов обнаружения и классификации вредоносной активности по данным системных событий операционных систем семейства Linux, методов выявления потенциально компрометируемых аутентификационных данных, а также подходов к повышению эффективности интеллектуальной обработки потоковых системных событий.

Во второй главе разработана система обнаружения атак на основе системных событий операционных систем семейства Linux, использующей двухступенчатую схему классификации. Разработан интеллектуальный метод оценки вероятности компрометации аутентификационных данных. Разработан метод оптимизации потокового вывода интеллектуальных систем анализа системных событий.

В третьей главе разработан и реализован программный комплекс оценки вероятности компрометации аутентификационных данных, интегрированный в операционные системы семейства Linux посредством подсистемы Pluggable Authentication Modules (PAM). Также в главе разработан и реализован программный комплекс обнаружения и классификации вредоносной активности в системных событиях операционных систем семейства Linux. Для повышения эффективности эксплуатации разработанного программного комплекса реализован метод потоковой обработки системных событий.

В заключении подведены итоги и обобщены результаты проведенных исследований. Разработанные интеллектуальные методы позволяют не только расширить класс задач, решаемых с использованием языковых моделей, но и уменьшить время обработки данных без снижения уровня точности.

Основные результаты диссертационной работы

1. Разработан интеллектуальный метод оценки вероятности компрометации аутентификационных данных операционных систем семейства Linux, основанный на вычислении статистических характеристик случайности в сочетании с моделями машинного обучения.

2. Разработан интеллектуальный метод обработки потоковых событий операционных систем семейства Linux для обнаружения вредоносной активности, основанный на применении контекстного представления событий и моделей трансформеров с предварительной нормализацией и семантическим упрощением событий, обеспечивающий сокращение времени обработки в среднем в 5 раз.

3. Разработан метод параллельной потоковой обработки событий операционных систем семейства Linux с использованием адаптивного формирования вычислительных пакетов, динамического выравнивания длины входных последовательностей и группировки событий по вычислительной

сложности, обеспечивающий сокращение времени обработки в среднем в 2 раза.

Достоверность полученных результатов

Достоверность и обоснованность полученных в диссертационной работе теоретических результатов и формулируемых на их основе выводов подтверждается корректным и обоснованным применением классических методов исследования, строгими математическими доказательствами и результатами анализа эффективности реализации разработанных моделей и методов с использованием языка программирования Python. Результаты теоретического анализа согласуются с результатами экспериментов.

Практическая значимость

Практическая значимость результатов диссертационного исследования заключается в следующем:

1. Разработанный метод выявления потенциально компрометируемых аутентификационных данных позволяет уточнить вероятность их компрометации, что обеспечивает возможность его применения в подсистемах контроля защищенности, аудита безопасности и управления доступом.

2. Разработанный интеллектуальный метод анализа событий операционных систем семейства Linux на основе языковых моделей позволяет уменьшить время их обработки в среднем в 5 раз, что обеспечивает возможность его применения при создании программного обеспечения для центров мониторинга информационной безопасности.

3. Разработанный метод параллельной потоковой обработки событий операционных систем семейства Linux позволяет уменьшить время обработки в среднем в 2 раза и повысить пропускную способность интеллектуальных подсистем мониторинга информационной безопасности на 123% без снижения точности классификации, что обеспечивает возможность его применения при создании программного обеспечения для центров мониторинга информационной безопасности.

Замечания

1. Анализ современного состояния области в первой главе носит избирательный характер. В частности, анализ тактик атак (раздел 1.3) не охватывает случаи, когда отдельные этапы модели Cyber Kill Chain могут отсутствовать или объединяться.

2. При оценке методов классификации паролей не учитываются количественные критерии по вычислительным ресурсам, объему памяти и времени обработки.

3. В целом в диссертации не обсуждаются вопросы конкурентоспособности предложенных решений по сравнению с современными малыми языковыми моделями в задачах потоковой обработки событий операционных систем Linux.

4. В диссертации избыточно введены сокращения. Так, например, введено сокращение ОЕЯ, которое больше в тексте ни разу не используется (стр. 14).

Заключение

Указанные замечания не снижают научную и практическую ценность диссертационной работы. Диссертация является законченным научным исследованием, написанным на высоком уровне. Результаты диссертационного исследования представлены в статьях автора, а также докладывались на всероссийских и международных конференциях. Автореферат диссертации корректно и полно отражает содержание работы.

Диссертационная работа Русанова Михаила Андреевича соответствует требованиям пунктов 9-14 Положения о присуждении ученых степеней, утвержденного постановлением Правительства РФ от 24 сентября 2013 года № 842, предъявляемым к кандидатским диссертациям, а её автор заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.5 Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Отзыв подготовлен профессором кафедры прикладной математики и программирования, доктором технических наук (05.13.18. Математическое моделирование, численные методы и комплексы программ) Анатолием Борисовичем Усовым (344090, г. Ростов-на-Дону, ул. Мильчакова, 8А, тел. раб.: +7(863)2975411, эл. почта: abusov@sfedu.ru).

Отзыв обсужден и утвержден на заседании кафедры прикладной математики и программирования Института математики, механики и компьютерных наук им. И.И. Воровича Южного федерального университета от 27 августа 2026 г., протокол №1. Присутствовало на заседании 8 чел.

Результаты голосования: «за» – 8 чел., «против» – нет, «воздержались» – нет.

Заведующий кафедрой прикладной математики и программирования
Института математики, механики и компьютерных наук им. И.И. Воровича
ФГАОУ ВО «Южный федеральный университет», д.ф.-м.н., профессор

Г.А. Угольницкий