ОТЗЫВ

официального оппонента 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.

Актуальность темы исследования. Диссертационная работа Русанова Михаила Андреевича посвящена решению актуальной научной задачи разработки интеллектуальных методов, моделей и программных средств обнаружения и классификации несанкционированных вторжений в операционные системы семейства Linux. Актуальность темы обусловлена ростом сложности современных информационно-вычислительных систем, увеличением объема потоковых системных событий, распространением распределенных и облачных инфраструктур, а также необходимостью выявления сложных и многоэтапных атак в условиях ограниченных вычислительных ресурсов. Традиционные сигнатурные и эвристические подходы не всегда обеспечивают достаточную адаптивность при обнаружении модифицированных атак и скрытых сценариев вредоносной активности. В связи с этим использование методов машинного обучения и языковых моделей для анализа системных событий является перспективным направлением исследований. Таким образом, тема диссертационной работы, направленной на разработку интеллектуальных методов обнаружения вредоносной активности и оценки угроз компрометации учетных данных, является актуальной и имеет существенное научное и практическое значение.

Структура и содержание диссертации. Диссертационная работа состоит из введения, трех глав, заключения и списка литературы. Полный объем диссертации составляет 130 страниц, включая 30 рисунков и 20 таблиц. Список литературы содержит 108 наименований.

Во введении обоснована актуальность темы исследования, сформулированы объект, предмет, цель и задачи работы, определены научная новизна, теоретическая и практическая значимость полученных результатов, приведены положения, выносимые на защиту, сведения об апробации и внедрении результатов.

Первая глава. Первая глава «Исследование методов обнаружения несанкционированного вторжения в операционные системы» посвящена анализу существующих решений, подходов к повышению вычислительной эффективности

интеллектуальных систем анализа системных событий, тактик атак и вопросов защищенности учетных записей. В главе рассмотрены сигнатурные, эвристические и интеллектуальные подходы к анализу системных событий, а также методы повышения вычислительной эффективности интеллектуальных систем анализа журналов и потоковых данных. Отдельное внимание уделено анализу тактик атак, представленных в MITRE ATT&CK, вопросам защищенности учетных записей и критериям оценки паролей. Показано, что современные методы машинного обучения и модели семейства трансформеров обеспечивают высокое качество классификации, но требуют оптимизации для практического применения в средах с ограниченными ресурсами.

Вторая глава. Вторая глава «Разработка методов и алгоритмов обнаружения несанкционированного вторжения в операционные системы с использованием технологии машинного обучения» посвящена разработке метода и алгоритма раннего обнаружения атак, метода и алгоритма идентификации эксплуатируемых паролей, а также метода параллельного вывода. В рамках главы предложен метод раннего обнаружения атак на основе предварительной обработки, форматирования, нормализации и контекстного представления системных событий. Рассмотрены задачи бинарной классификации вредоносной активности и многометочной классификации обнаруженных событий по тактикам MITRE ATT&CK. Также разработан метод идентификации потенциально эксплуатируемых паролей, основанный на статистических характеристиках случайности и алгоритмах машинного обучения. Отдельно представлен метод параллельного потокового вывода, направленный на повышение пропускной способности интеллектуальной системы анализа событий.

Третья глава. Третья глава «Разработка программного комплекса системы обнаружения атак» посвящена архитектуре и программной реализации разработанных методов, а также экспериментальной оценке их эффективности. Описана архитектура программного комплекса, включающая модули предварительной обработки и нормализации событий, обучения базовой модели бинарной классификации, дистилляции, квантизации, вычисления метрик качества, классификации тактик MITRE ATT&CK и анализа архитектур моделей трансформеров. Также представлена архитектура программного комплекса обнаружения потенциально эксплуатируемых злоумышленником паролей, включая реализацию вычислительного модуля оценки вероятности компрометации аутентификационных данных. Проведенные эксперименты подтверждают эффективность применения дистилляции знаний, квантизации и пакетной потоковой обработки для уменьшения времени обработки системных событий без существенного снижения качества классификации. Для потоковой обработки

системных событий показано увеличение пропускной способности в 2,23 раза по сравнению с базовой схемой обработки и в 1,4 раза по сравнению с использованием только пакетной обработки.

В заключении сформулированы основные результаты диссертационного исследования и выводы о возможности практического применения разработанных методов и программных средств в интеллектуальных подсистемах мониторинга информационной безопасности.

Автореферат адекватно отражает структуру и содержание диссертации в целом.

Научная новизна диссертационной работы определяется следующими результатами:

1) Разработан интеллектуальный метод оценки вероятности компрометации аутентификационных данных операционных систем семейства Linux, отличающийся от существующих подходов использованием статистических характеристик случайности в сочетании с моделями машинного обучения.

2) Разработан интеллектуальный метод обработки потоковых событий операционных систем семейства Linux для обнаружения вредоносной активности, отличающийся от существующих методов применением контекстного представления событий на основе моделей трансформеров с предварительной нормализацией и семантическим упрощением событий, что позволяет повысить точность классификации атак и уменьшить время работы моделей.

3) Разработан метод параллельной потоковой обработки событий операционных систем семейства Linux, отличающийся использованием адаптивного формирования вычислительных пакетов, динамического выравнивания длины входных последовательностей и группировки событий по вычислительной сложности, что обеспечивает уменьшение времени обработки и повышение пропускной способности интеллектуальных моделей анализа системных событий без изменения архитектуры модели и снижения точности обнаружения и классификации.

Теоретическая значимость диссертационной работы связана с развитием методов интеллектуального анализа системных событий и аутентификационных данных операционных систем семейства Linux. Предложенный метод выявления потенциально компрометируемых аутентификационных данных уточняет оценку вероятности их компрометации за счет анализа косвенных признаков. Метод анализа системных событий на основе языковых моделей расширяет представления о применимости таких моделей к обнаружению сложных и модифицированных атак. Отдельное значение имеет метод параллельной потоковой обработки событий, в котором используются адаптивное формирование

вычислительных пакетов, динамическое выравнивание длины входных последовательностей и группировка событий по вычислительной сложности.

Практическая значимость результатов исследования заключается в возможности использования разработанных методов и программных средств в подсистемах мониторинга информационной безопасности, аудита защищенности, управления доступом и контроля качества аутентификационных данных. Метод выявления потенциально компрометируемых аутентификационных данных может применяться в подсистемах контроля защищенности, аудита безопасности и управления доступом. Применение метода анализа событий операционных систем семейства Linux на основе языковых моделей позволяет уменьшить время их обработки в среднем в 5 раз, что важно для программного обеспечения центров мониторинга информационной безопасности. Применение метода параллельной потоковой обработки событий позволяет уменьшить время обработки в среднем в 2 раза и повысить пропускную способность интеллектуальных подсистем мониторинга информационной безопасности на 123% без снижения точности классификации. Программный комплекс оценки вероятности компрометации аутентификационных данных интегрирован в операционные системы семейства Linux посредством подсистемы Pluggable Authentication Modules (PAM).

Достоверность и обоснованность научных результатов диссертационной работы обеспечиваются корректным применением методов машинного обучения, обработки естественного языка, теории вероятностей, математической статистики, анализа данных и математического моделирования.

Полученные результаты подтверждаются сравнительным анализом моделей, экспериментальной оценкой качества классификации, расчетом метрик точности, полноты, F1-меры, ROC-AUC и PR-AUC, а также анализом времени обработки и пропускной способности программных средств. Реализация разработанных моделей и методов выполнена с использованием языка программирования Python.

Апробация. Основные результаты диссертационной работы были представлены на научных конференциях и опубликованы в печатных работах по теме исследования. По теме диссертации опубликовано 6 печатных работ, в том числе в изданиях, рекомендованных ВАК, Web of Science и Scopus, а также получено 2 свидетельства о государственной регистрации программ для ЭВМ.

Результаты работы докладывались на всероссийских и международных конференциях.

Результаты работы внедрены в подсистемы мониторинга событий информационной безопасности в АО «Газпромбанк» (акт о внедрении 302-3/12/26 от 05.05.2026).

Замечания. Диссертационная работа производит благоприятное впечатление. Вместе с тем к работе можно высказать следующие замечания, которые не снижают ее научной и практической значимости:

1) В работе было бы уместно конкретизировать границы применимости предложенных методов с учетом атак с минимальной наблюдаемой активностью и неполными журналами событий.

2) В работе следовало указать, какие элементы рассмотренного подхода требуют адаптации для применения в трансформерных моделях.

3) Большинство эмпирических подтверждений эффективности предложенных методов обнаружения атак представлено на наборе Linux-APT-Dataset-2024. При этом не исследована переносимость метода на атаки нулевого дня.

4) В работе следовало продемонстрировать преимущество разработанных подходов потоковой обработки событий операционной системы Linux относительно классических сингулярных методов и методов обнаружения аномалий.

5) В диссертации введено большое количество аббревиатур, при этом не все аббревиатуры расшифрованы в тексте. Кроме того, присутствуют кальки англоязычных слов, вроде Simple и Strong.

Указанные замечания носят уточняющий и рекомендательный характер, не снижают научной и практической значимости диссертационного исследования и не влияют на общую положительную оценку полученных автором результатов.

Заключение. Диссертационная работа Русанова Михаила Андреевича выполнена на актуальную тему, обладает внутренним единством, содержит новые научные результаты и имеет практическую значимость.

Содержание диссертации соответствует поставленной цели и задачам исследования. Полученные результаты представляют собой решение актуальной научной задачи разработки интеллектуальных методов обнаружения и классификации несанкционированных вторжений в операционные системы семейства Linux, отражены в опубликованных работах автора, прошли апробацию на научных конференциях и подтверждены практическим внедрением. Автореферат соответствует основному содержанию диссертации. Высказанные замечания носят уточняющий и рекомендательный характер и не снижают общей положительной оценки выполненного исследования.

Считаю, что 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.

Официальный оппонент
доктор технических наук, профессор,
заслуженный деятель науки Российской
Федерации, главный научный сотрудник
Федерального государственного бюджетного
учреждения науки «Санкт-Петербургский
Федеральный исследовательский центр
Российской академии наук» Котенко Игорь Витальевич

Согласен на обработку персональных
данных Котенко Игорь Витальевич

Контактные данные организации: Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», e-mail: info@spcras.ru, +7(812)5083311.

«19» августа 2026 г.