

**ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.1.120.01,
созданного на базе
Федерального государственного бюджетного учреждения науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
Министерства науки и высшего образования РФ
по диссертации на соискание ученой степени кандидата наук**

аттестационное дело № _____
решение диссертационного совета от 29 сентября 2026 года № 2026/25

О присуждении Русанову Михаилу Андреевичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Интеллектуальные методы обнаружения несанкционированных вторжений в операционные системы» по специальности 2.3.5 – «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» принята к защите 03 июля 2026 года (протокол № 2026/16) диссертационным советом 24.1.120.01, созданным на базе Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ; адрес: 109004, г. Москва, ул. А. Солженицына, дом 25), создан Приказом Минобрнауки России о советах по защите докторских и кандидатских диссертаций от 2 ноября 2012 г. № 714/нк.

Соискатель Русанов Михаил Андреевич, 04 января 1999 года рождения.

В 2023 году соискатель окончил Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет». В 2026 году окончил аспирантуру аккредитованного образовательного частного учреждения высшего образования «Московский финансово-юридический университет МФЮА».

Работает главным экспертом в Акционерном обществе «Газпромбанк» (ведомственная принадлежность: Центральный банк Российской Федерации).

Диссертация выполнена в аккредитованном образовательном частном учреждении высшего образования «Московский финансово-юридический университет» в институте информационных технологий на кафедре информационных и математических инноваций (ведомственная принадлежность: нет (ОКОГУ 4210014)).

Научный руководитель – кандидат физико-математических наук, доцент Лапина Мария Анатольевна, Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет», факультет математики и компьютерных наук имени профессора Н.И. Червякова, доцент кафедры вычислительной математики и кибернетики.

Официальные оппоненты:

1. Кознов Дмитрий Владимирович, доктор технических наук, доцент, профессор кафедры системного программирования Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет»,
2. Котенко Игорь Витальевич, доктор технических наук, профессор, главный научный сотрудник Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук»

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное автономное образовательное учреждение высшего образования «Южный Федеральный Университет», г. Ростов-на-Дону в своем положительном отзыве, подписанном Угольницким Геннадием Анатольевичем, доктором физико-математических наук, профессором, заведующим кафедрой прикладной математики и программирования института математики, механики и компьютерных наук имени И.И. Воровича, указала, что диссертационная работа содержит новые научные результаты, имеющие существенное значение для науки и практики.

Соискатель имеет 6 опубликованных работ, в том числе по теме диссертации опубликовано 6 работ, из них в рецензируемых научных изданиях опубликовано 5 работ.

Все изложенные в диссертационной работе результаты получены лично автором. Из результатов работ, выполненных коллективно, в диссертацию включены только полученные непосредственно автором. В опубликованных работах автором исследованы методы машинного обучения для обнаружения сетевых атак, проведен сравнительный анализ алгоритмов классификации и определены возможности их применения для выявления вредоносной активности; исследована эффективность методов машинного обучения для решения задачи обнаружения и классификации вредоносной активности в событиях операционных систем семейства Linux, проведен сравнительный анализ моделей и определен алгоритм, обеспечивающий наилучшие показатели качества классификации; разработан и исследован метод идентификации потенциально компрометируемых паролей учетных записей на основе

статистических характеристик символьных последовательностей и моделей машинного обучения; исследованы методы дистилляции и квантизации трансформерных моделей для обнаружения вредоносной активности в условиях ограниченных вычислительных ресурсов; исследованы способы повышения вычислительной эффективности моделей машинного обучения на основе адаптивного формирования вычислительных пакетов, динамического выравнивания длины входных последовательностей и группировки данных по вычислительной сложности.

Наиболее значимые работы по теме диссертации:

1. Rusanov M. Optimization of Machine Learning Algorithms with Distillation and Quantization for Early Detection of Attacks in Resource-Constrained Systems / M. Rusanov, M. Babenko, M. Lapina // Big Data and Cognitive Computing. – 2025. – Т. 9. – №. 12. – С. 303.
2. Rusanov M. Identification of exploited unreliable account passwords in the information infrastructure using machine learning methods / M. Rusanov, M. Babenko, M. Lapina, M. Sajid // Big Data and Cognitive Computing. – 2024. – Т. 8. – №. 11. – С. 159.
3. Rusanov M. A. Detection of SQL injection attacks through the network logs using machine learning methods / M. A. Lapina, N. R. Kapshuk, M. A. Rusanov, E. F. Timofeeva // Труды института системного программирования РАН. – 2025. – Т. 37. – №. 5. – С. 81-92.
4. Rusanov M. A. Research of machine learning methods for detecting network attacks / M. A. Lapina, N. V. Podruchny, M. A. Rusanov, M. G. Babenko // Труды Института системного программирования РАН. – 2025. – Т. 37. – №. 4-2. – С. 147-174.
5. Русанов М.А. Криптографическая система на основе хаотической системы Лоренца / М.А. Русанов, С.В. Данилкин, П.И. Карасев, А.А.Л. Алмали // Приборы и системы. Управление, контроль, диагностика. 2023, – №. 3. – С. 48-53.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и достижениями в данной отрасли науки, наличием публикаций в сфере исследований, соответствующей теме диссертации, и способностью определить научную и практическую ценность диссертации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- разработан интеллектуальный метод оценки вероятности компрометации аутентификационных данных операционных систем семейства Linux на основе статистических характеристик случайности и моделей машинного обучения, позволяющий уточнить вероятности их компрометации;

- разработан интеллектуальный метод анализа событий операционных систем семейства Linux на основе языковых моделей с использованием контекстного представления, предварительной нормализации и семантическим упрощением событий, что позволяет сократить время их обработки в среднем в 5 раз;
- разработан метод параллельной потоковой обработки событий операционных систем семейства Linux на основе адаптивного формирования вычислительных пакетов, динамического выравнивания длины входных последовательностей и группировки событий по вычислительной сложности, позволяющего сократить время обработки в среднем в 2 раза и повысить пропускную способность на 123% без снижения точности классификации.

Теоретическая значимость исследования обоснована тем, что:

- разработанный метод выявления потенциально компрометируемых аутентификационных данных позволяет уточнить оценки вероятности их компрометации за счет интеллектуального анализа косвенных признаков;
- разработанный интеллектуальный метод анализа событий операционных систем семейства Linux на основе языковых моделей вносит вклад в развитие теоретических основ для обнаружения вредоносной активности и расширяет представление о их применимости для анализа сложных и модифицированных атак;
- разработанный метод параллельной потоковой обработки событий операционных систем семейства Linux позволяет уменьшить время их обработки за счет адаптивного формирования вычислительных пакетов, динамического выравнивания длины входных последовательностей и группировки событий по вычислительной сложности;
- продемонстрирована возможность реализации системы анализа трассовой информации на основе языковых моделей в средствах защиты информации (СЗИ) операционных систем, которая выполняет интеллектуальную обработку данных с приемлемой точностью и приемлемыми накладными расходами.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

- 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;

- 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;
- 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;
- результаты, полученные в рамках данной работы, были внедрены в подсистемы мониторинга событий информационной безопасности в АО «Газпромбанк» (акт о внедрении 302-3/12/26 от 05.05.2026).

Оценка достоверности результатов исследования выявила:

- результаты экспериментальных исследований согласуются с результатами проведенного теоретического анализа и подтверждают эффективность разработанных методов;
- теоретические результаты и сформулированные на их основе выводы получены с использованием конкретных и обоснованных методов исследования и подтверждены результатами экспериментальной проверки;
- использованы современные методы математического моделирования, машинного обучения, обработки естественного языка, анализа данных, теории вероятностей и математической статистики, а оценка эффективности разработанных моделей и методов выполнена на основе их программируемой реализации с использованием языка Python.

Личный вклад соискателя состоит в разработке интеллектуального метода оценки вероятности компрометации аутентификационных данных на основе анализа статистических характеристик случайности и применения моделей машинного обучения; разработке интеллектуального метода обработки потоковых системных событий операционных систем семейства Linux на основе контекстного представления событий и трансформерных моделей; разработке способов повышения вычислительной эффективности потоковой обработки за счет адаптивного формирования вычислительных пакетов и динамического выравнивания входных последовательностей; разработке программных комплексов обнаружения и классификации вредоносной активности в системных событиях и приложениях на базе нейронной сети; непосредственном участии в постановке и решении исследовательских задач,

проведении экспериментальных исследований, обработке и интерпретации полученных результатов, их апробации и подготовке научных публикаций.

В ходе защиты диссертации были высказаны следующие критические замечания:

- Требуется пояснения оценка необходимой длины входной последовательности. В табл. 2.2 на с. 56 после предварительной обработки приведен 99-й перцентиль длины 428,3 токена, тогда как далее, на с. 88–89, утверждается, что длины 128 токенов достаточно для покрытия более 99% данных. Возможно, здесь используются разные способы подсчета длины, однако из текста это не следует. Поскольку ограничение окна непосредственно влияет и на качество, и на производительность, данный момент необходимо объяснить.
- Одна из основных гипотез работы – небольшие ресурсы для анализа системных событий – требует более тщательного обоснования.
- 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.
- В работе следовало продемонстрировать преимущество разработанных подходов потоковой обработки событий операционной системы Linux относительно классических сингулярных методов и методов обнаружения аномалий.
- 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.
- При оценке методов классификации паролей не учитываются количественные критерии по вычислительным ресурсам, объему памяти и времени обработки.
- 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.
- Диссертант недостаточно изучил и проанализировал отечественный опыт разработки СЗИ операционных систем и не обосновал необходимость использованию технологий ИИ в столь критичной по производительности компоненте программно-аппаратных систем как операционные системы.

Соискатель Русанов Михаил Андреевич согласился с замечаниями, ответил на задаваемые ему в ходе заседания вопросы.

На заседании 29 сентября 2026 г. диссертационный совет принял следующее решение: присудить Русанову М.А. ученую степень кандидата технических наук за решение научной задачи, имеющей значение для развития методов выполнения интеллектуального анализа трассовой информации в СЗИ операционных систем.

При проведении тайного голосования диссертационный совет в количестве 11 человек, из них 8 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 15 человек, входящих в состав совета, проголосовали: за – 10, против – 1.

Заместитель председателя диссертационного совета,
доктор физико-математических наук

Белеванцев А. А.

И.о. ученого секретаря диссертационного совета,
доктор физико-математических наук

Бурдонов И.Б.

29 сентября 2026 г.