УТВЕРЖДАЮ:

Ректор ФГБОУ ВО ПГУТИ
В.А. Ружников

«23» сентября 2026 г.

ЗАКЛЮЧЕНИЕ
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по диссертационной работе Плавана Алексея Игоревича

Диссертация «Методы обнаружения аномалий в сетевом трафике на основе оптимальной линейной фильтрации» выполнена на кафедре информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Поволжский государственный университет телекоммуникаций и информатики» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

В период подготовки диссертации соискатель Плаван Алексей Игоревич обучался в аспирантуре ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» (2020–2024 гг.), работал в должности инженера кафедры информационной безопасности ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» (2022–2023 гг.), в настоящее время работает в должности инженера-исследователя научно-исследовательской лаборатории «Инфокоммуникационные технологии» ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» (с 2026 г.).

В 2020 г. окончил с отличием ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» по специальности 10.05.02 – Информационная безопасность телекоммуникационных систем.

В 2024 г. окончил очную аспирантуру ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» по направлению подготовки 11.06.01 – Электроника, радиотехника и системы

связи, по специальности 2.2.15 – Системы, сети и устройства телекоммуникаций.

Справка со сведениями о сдаче кандидатских экзаменов по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность по дисциплинам Иностранный язык (английский язык) и История и философия науки выдана в 2026 г. ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики».

Справка со сведениями о сдаче кандидатского экзамена по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность выдана в 2026 г. ФГБОУ ВО «Уфимский университет науки и технологий».

Научный руководитель: Карташевский Вячеслав Григорьевич, д.т.н., профессор кафедры информационной безопасности, заведующий лабораторией «Инфокоммуникационные технологии» ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики».

По итогам обсуждения принято следующее заключение:

1. Диссертационная работа Плавана А.И. является законченной научно-квалификационной работой, соответствующей п. 9 Положения о присуждении ученых степеней, утвержденного Постановлением правительства Российской Федерации №842 от 24.09.2013 г. (с последующими изменениями), в которой содержатся научно обоснованные результаты решения задачи повышения защищенности телекоммуникационных систем за счет повышения эффективности алгоритмов обнаружения аномалий в сетевом трафике на основе его статистических характеристик.

2. Соискателем лично получены все основные результаты, выносимые на защиту:

- алгоритм определения численных индикаторов сетевых атак по статистическим характеристикам трафика, основанный на методе «случайного леса»;

- метод моделирования случайных процессов, представляющих самоподобный Интернет-трафик, основанный на преобразовании распределения Рэлея и применении копулы Фарли-Гумбеля-Моргенштерна;

- методы обнаружения аномалий в сетевом трафике и реализующий их алгоритм, основанные на вычислении минимальной среднеквадратической

ошибки фильтрации и сравнении её с эталонным значением для легитимного трафика;

- механизм формирования признаков для моделей машинного обучения, предназначенных для обнаружения сетевых атак, основанный на вычислении минимальной среднеквадратической ошибки фильтрации для различных представлений трафика.

3. В перечисленных в диссертации работах соискателем лично получены следующие результаты:

- в работе [4] представлен алгоритм определения численных индикаторов сетевых атак по статистическим характеристикам трафика, основанный на методе «случайного леса» и результаты его применения к данным реального сетевого трафика, а также полученные индикаторы для различных атак;

- в работе [5] представлен метод моделирования случайных процессов, представляющих самоподобный Интернет-трафик, основанный на преобразовании распределения Рэлея и применении копулы Фарли-Гумбеля-Моргенштерна;

- в работах [2], [11], [15], [16], [19-21] представлены методы обнаружения аномалий в сетевом трафике, основанные на вычислении минимальной среднеквадратической ошибки фильтрации и сравнении её с эталонным значением для легитимного трафика;

- в работах [3], [22] механизм формирования признаков для моделей машинного обучения, предназначенных для обнаружения сетевых атак, основанный на вычислении минимальной среднеквадратической ошибки фильтрации для различных представлений трафика;

- в работах [1], [6-10], [12-14], [17], [18] представлены результаты моделирования реалистичного сетевого трафика и сетевых атак, а также результаты анализа их статистических характеристик, использовавшиеся в других работах.

Опубликованные работы полностью отражают основное содержание диссертационной работы. Все основные положения и результаты, выносимые на защиту, отражены в публикациях автора: по главе 1 – [1], [4], [10], по главе 2 – [5], [6-9], [12-14], [17]; по главе 3 – [2], [11], [15], [16], [18], [19-21]; по главе 4 – [3], [22]. Девять работ написаны автором единолично (из них две статьи ВАК), другие совместно с научным руководителем или другими членами научного коллектива.

4. Для достижения поставленной цели решаются следующие научные задачи:

1. Проведен анализ статистических характеристик реального сетевого трафика, таких как автокорреляционная функция и вероятностное распределение интервалов времени между пакетами, размеров пакетов и других параметров, и установить влияние различных видов атак на статистические характеристики трафика.

2. Проведено моделирование реалистичного сетевого трафика, соответствующего нормальной активности пользователей и проведению атаки, изучить свойства объединенного трафика.

3. Разработаны методы обнаружения аномалий в сетевом трафике на основе оптимальной линейной фильтрации.

4. Исследована возможность применения признаков на основе статистических характеристик трафика в методах машинного обучения для повышения точности обнаружения аномалий.

5. Проведена оценка эффективности разработанных методов на смоделированном и реальном трафике по различным метрикам.

5. Актуальность темы исследования обусловлена неуклонным увеличением количества и масштабов сетевых атак, которые могут быть обнаружены за счет анализа изменений статистических характеристик трафика в сети. Эффективность статистических методов, по сравнению с методами машинного обучения, остается высокой при сравнительно низких вычислительных затратах, а также они зачастую предоставляют лучшую интерпретируемость результатов.

6. Степень достоверности результатов проведенных исследований, их новизна и значимость

Обоснованность и достоверность результатов работы обеспечивается корректным и обоснованным применением методов исследования, проведением вычислительных экспериментов на открытых наборах данных, проверкой статистической значимости полученных результатов, а также апробацией результатов исследований на международных и всероссийских конференциях и публикацией результатов в рецензируемых научных изданиях из перечня ВАК и индексируемых в Scopus и Web of Science.

7. Научная новизна работы заключается в следующем:

1. Разработан алгоритм определения численных индикаторов сетевых атак по статистическим характеристикам трафика, *основанный* на методе «случайного леса», *отличающийся* возможностью определения не только важности признаков, но и их пороговых значений, и *позволяющий* оценивать их статистическую значимость.

2. Разработан метод моделирования случайных процессов, представляющих самоподобный Интернет-трафик, *основанный* на

преобразовании распределения Рэлея, *отличающийся* применением копулы Фарли-Гумбеля-Моргенштерна для выражения аналитической связи между АКФ исходного и преобразованного процессов, и *позволяющий* повысить точность воспроизведения заданных статистических характеристик при моделировании легитимного трафика.

3. Разработаны методы обнаружения аномалий в сетевом трафике и реализующий их алгоритм, *основанные* на вычислении минимальной среднеквадратической ошибки фильтрации и сравнении её с эталонным значением для легитимного трафика, *отличающиеся* возможностью учитывать шум наблюдений, и *позволяющие* выявлять сетевые атаки, связанные с изменением статистических характеристик трафика.

4. Предложен механизм формирования признаков для моделей машинного обучения, *основанный* на вычислении минимальной среднеквадратической ошибки фильтрации для различных представлений трафика, *отличающийся* объединением множества отсчетов АКФ в единый скалярный признак ошибки, и *позволяющий* повысить эффективность обнаружения сетевых атак алгоритмами обучения без учителя.

8. Теоретическая значимость исследования заключается в разработке алгоритма определения значимых статистических признаков различных видов сетевых атак, способа моделирования случайных процессов с заданными характеристиками на основе копул, алгоритмов обнаружения аномалий в сетевом трафике на основе минимальной среднеквадратической ошибки оптимального фильтра Колмогорова-Винера, которые позволяют эффективно выявлять аномальные последовательности в трафике. Применение данных результатов может позволить оперативно выявлять потенциальные угрозы и снизить риск инцидентов безопасности.

9. Практическая значимость исследования заключается в возможности применения полученных результатов для разработки перспективных средств защиты информации и мониторинга сетевого трафика. Внедрение разработанных алгоритмов в существующие корпоративные системы безопасности позволяет повысить число выявленных аномалий, обеспечив своевременное обнаружение и предупреждение атак и снижение количества инцидентов информационной безопасности.

Результаты диссертационной работы были использованы в ООО «Идентификация» при проведении работ по проектированию и разработке перспективных средств защиты информации для своевременного обнаружения и предупреждения компьютерных атак и других угроз в сфере информационной безопасности.

Предложенные технические решения позволили повысить число выявленных аномалий, что привело к снижению вероятности успешной реализации атаки на 22% на тестовых стендах и сократило среднее время обнаружения инцидента на 12 минут. Применение разработанных в диссертации методов и алгоритмов позволяет повысить защищенность информационных систем и обеспечить оперативное выявление атак.

Результаты диссертационной работы Плавана А.И. также внедрены в учебный процесс на кафедре Информационной безопасности ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» и используются при проведении лабораторных и практических занятий по дисциплинам направления подготовки специалистов 10.05.02 «Информационная безопасность телекоммуникационных систем», научно-исследовательских работ, связанных с обнаружением сетевых атак и моделированием сетевого трафика.

10. Личный вклад автора

Основные результаты диссертационной работы, представляющие научную новизну, а также анализ с соответствующими выводами, выполнены автором самостоятельно. Некоторые из этих результатов подготовлены к публикации в сотрудничестве с соавторами, при этом определяющий вклад вносил автор данной работы.

11. Обоснование выбранной специальности и отрасли науки диссертации

Результаты диссертационной работы соответствуют следующим пунктам паспорта научной специальности:

п. 5 – Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет;

п. 6 – Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях;

п. 15 – Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Отрасль науки – технические науки, поскольку приведенные результаты исследований дают существенный технический эффект, а именно повышение эффективности обнаружения сетевых аномалий при внедрении в системы мониторинга трафика.

12. Полнота изложения материалов диссертации в публикациях

По теме диссертационного исследования всего опубликовано 22 работы, отражающих основные полученные результаты, из них: 5 статей в ведущих научных журналах из Перечня рецензируемых научных изданий ВАК при Министерстве науки и высшего образования РФ, 1 научная работа в изданиях, индексируемых ведущими международными реферативными базами Web of Science и Scopus, 6 тезисов международных и 9 всероссийских научных и научно-технических конференций. Во время выполнения научного исследования разработаны 3 программы для ЭВМ и получены свидетельства о государственной регистрации: №2022614836, №2023664160, №2024611818.

Общий объем публикаций – 6,375 п.л., авторский вклад – 4,5625 п.л.

Статьи в рецензируемых научных изданиях из перечня ВАК

1. *Плаван А.И.* Выявление DoS-атак с помощью анализа статистических характеристик трафика / И.С. Поздняк, А.И. Плаван // Инфокоммуникационные технологии. – 2021. – Т. 19. – № 1. – С. 73-80
2. *Плаван А.И.* Среднеквадратическая ошибка фильтрации как критерий обнаружения аномалий сетевого трафика / А.И. Плаван, В.Г. Карташевский // Вестник Российского нового университета. Серия: Сложные системы модели, анализ и управление. – 2023. – № 1. – С. 94-101
3. *Плаван А.И.* Метод выявления аномалий в сетевом трафике на основе фильтра Колмогорова-Винера / А.И. Плаван // Вестник УрФО. Безопасность в информационной сфере. – 2024. – № 1 (51). – С. 53-59
4. *Плаван А.И.* Алгоритм определения численных индикаторов аномалий трафика на основе модели случайного леса / А.И. Плаван // Инфокоммуникационные технологии. – 2026. – Т. 24. – № 1 (93). – С. 26-32
5. *Плаван А.И.* Применение копулы для моделирования случайных процессов с распределением Вейбулла и заданной автокорреляционной функцией / А.И. Плаван, В.Г. Карташевский // Известия Института инженерной физики. Серия: Информатика, вычислительная техника и управление. – 2026. – № 3 (81). – С. 47-52

Публикации в трудах, индексируемых Scopus и Web of Science

6. *Plavan A.I.* Statistical analysis of aggregated network traffic model from multiple on/off sources / A.I. Plavan, V.G. Kartashevsky, I.S. Pozdnyak // Proc. SPIE 12564, 2nd International Conference on Computer Applications for Management and Sustainable Development of Production and Industry (CMSD-II-2022) / ред. A. Gibadullin, S. Sadullozoda. – Dushanbe, Tajikistan: SPIE, 21–23 декабря 2022 г. – Т. 12564. – С. 118-124

Работы в сборниках трудов и материалах конференций

7. *Плаван А.И.* Исследование трафика на наличие атак / И.С. Поздняк, В.Г. Карташевский, А.И. Плаван // Проблемы техники и технологий телекоммуникаций ПТиТТ-2020: Материалы XXII Международной научно-технической конференции. – Самара: ПГУТИ, 17–20 ноября 2020 г. – С. 206-207

8. *Плаван А.И.* Моделирование и анализ DDoS-атаки / В.Г. Карташевский, И.С. Поздняк, А.И. Плаван // Материалы XXVIII Российской научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов университета с приглашением ведущих ученых и специалистов родственных вузов и организаций. – Самара: ПГУТИ, 5–8 апреля 2021 г. – С. 63-64

9. *Плаван А.И.* Выявление аномалий в сетевом трафике по критерию среднеквадратической ошибки фильтрации линейного преобразования / А.И. Плаван, И.С. Поздняк // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: материалы VII Всероссийской научно-технической конференции. – Таганрог: Южный федеральный университет, 5–11 апреля 2021 г. – С. 70-74

10. *Плаван А.И.* Сравнительный анализ статистических характеристик DDoS-атак и нормального трафика / А.И. Плаван, В.Г. Карташевский, И.С. Поздняк // Актуальные проблемы науки и техники: Материалы I Международной научно-технической конференции. – Сарапул: Издательство УИР ИжГТУ имени М. Т. Калашникова, 20–22 мая 2021 г. – С. 551-555

11. *Плаван А.И.* Исследование статистических характеристик вредоносного трафика / В.Г. Карташевский, А.И. Плаван, И.С. Поздняк // Проблемы техники и технологий телекоммуникаций ПТиТТ-2021: Материалы XXIII Международной научно-технической конференции. – Самара: ПГУТИ, 23–26 ноября 2021 г. – С. 165-166

12. *Плаван А.И.* Статистический анализ агрегированной модели сетевого трафика / В.Г. Карташевский, А.И. Плаван, И.С. Поздняк // Материалы XXIX Российской научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов университета с приглашением ведущих ученых и специалистов родственных вузов и организаций. – Самара: ПГУТИ, 22–25 марта 2022 г. – С. 58-59

13. *Плаван А.И.* Исследование влияния скорости on/off источника на характеристики моделируемого интернет-трафика / А.И. Плаван // Доклады 77-й всероссийской конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» посвящённой дню радио

(РЭУС-2022). – М.: РНТОРЭС имени А.С. Попова, 8–10 июня 2022 г. – С. 102-105

14. *Плаван А.И.* Обнаружение аномалий сетевого трафика на основе фильтрации линейного преобразования трафика по критерию минимума среднеквадратической ошибки / А.И. Плаван // Сборник трудов II Всероссийской научной школы-семинара «Современные тенденции развития методов и технологий защиты информации». Москва, МТУСИ. – М.: ООО «Брис-М», 18–21 октября 2022 г. – С. 189-198

15. *Плаван А.И.* Моделирование самоподобного трафика с использованием модели Poisson-Pareto-Burst-Process в симуляторе ns-3 / А.И. Плаван // Материалы XXVII Международной научно-технической конференции «Современные средства связи». – Минск, Республика Беларусь: Белорусская государственная академия связи, 27–28 октября 2022 г. – Т. 1. – С. 197-199

16. *Плаван А.И.* Определение ошибки фильтрации трафика с целью обнаружения атаки / А.И. Плаван, В.Г. Карташевский, И.С. Поздняк // Материалы XXIV Международной научно-технической конференции и материалы XX Международной научно-технической конференции (ПТиТТ-2022). В 2-х томах. – Уфа: УУНиТ, 23–25 ноября 2022 г. – Т. 1. – С. 217-219

17. *Плаван А.И.* Обнаружение аномалий сетевого трафика на основе рассмотрения автокорреляционной функции в скользящем окне / А.И. Плаван // Сборник материалов XIII межведомственной научной конференции «Актуальные направления развития систем обеспечения безопасности объектов государственной охраны и охраняемых объектов, специальной связи для нужд органов государственной власти и специального информационного обеспечения государственных органов». – Орёл: Академия ФСО России, 10 февраля 2023 г. – С. 2

18. *Плаван А.И.* Среднеквадратическая ошибка фильтрации в качестве метрики расстояния для корреляционных матриц / А.И. Плаван // Актуальные проблемы радиоэлектроники и телекоммуникаций: материалы Всероссийской научно-технической конференции. – Самара: ООО «Артель», 25–28 апреля 2023 г. – С. 169-172

19. *Плаван А.И.* Исследование корреляционных свойств сетевого трафика при воздействии DoS-атаки / А.И. Плаван // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием. – Уфа: РИЦ УУНиТ, 19–20 мая 2023 г. – С. 105-108

20. *Плаван А.И.* Сравнительный анализ метрик для определения схожести корреляционных свойств трафика / А.И. Плаван, В.Г. Карташевский // Сборник докладов и тезисов XIII Всероссийской научно-практической конференции «Проблемы передачи информации в инфокоммуникационных системах». – Волгоград: Волгоградский государственный университет, 26 мая 2023 г. – С. 27-30

21. *Плаван А.И.* Использование среднеквадратической ошибки фильтрации для обнаружения кратковременных аномалий сетевого трафика / А.И. Плаван, В.Г. Карташевский // Проблемы техники и технологий телекоммуникаций ПТиТТ-2023: Материалы XXV Международной научно-технической конференции. – Казань: КНИТУ-КАИ, 22–24 ноября 2023 г. – Т. 1. – С. 502-504

22. *Плаван А.И.* Исследование метода обнаружения аномалий в сетевом трафике на основе оптимального фильтра Колмогорова-Винера / А.И. Плаван // Актуальные проблемы радиоэлектроники и телекоммуникаций: материалы Всероссийской конференции. – Самара: ООО «Артель», 23–26 апреля 2024 г. – С. 228-231

Свидетельства о государственной регистрации программ для ЭВМ

23. Свидетельство о государственной регистрации программы для ЭВМ №2022614836. Программный комплекс «PcapStat» : №2022613421 : заявл. 09.03.2022 : опубл. 28.03.2022, Бюл. № 4 / А.И. Плаван. – 1 с.

24. Свидетельство о государственной регистрации программы для ЭВМ №2023664160. PcapConvert : №2023663148 : заявл. 21.06.2023 : опубл. 03.07.2023, Бюл. № 7 / А.И. Плаван. – 1 с.

Свидетельство о государственной регистрации программы для ЭВМ №2024611818. PcapReplay : №2024611026 : заявл. 24.01.2024 : опубл. 24.01.2024, Бюл. № 2 / А.И. Плаван. – 1 с.

Результаты диссертации изложены в указанных работах достаточно полно и подробно.

Диссертация Плавана Алексея Игоревича соответствует п. 14 Положения о присуждении ученых степеней:

- отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации;
- соискатель ссылается на авторов и источники заимствования.

Диссертация «Методы обнаружения аномалий в сетевом трафике на основе оптимальной линейной фильтрации» Плавана Алексея Игоревича рекомендуется к защите на соискание ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Заключение принято на расширенном заседании кафедры информационной безопасности ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики».

Присутствовало на заседании 14 чел., в том числе 6 докторов наук и 4 кандидата наук.

Результаты голосования: «за» - 14 чел., «против» – 0 чел., «воздержались» – 0 чел., протокол № 2 от 23 сентября 2026 г.

Заведующий кафедрой
информационной безопасности,
д.т.н., доцент Шакурский Максим Викторович

Федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет телекоммуникаций и информатики»
Отдел документационного обеспечения

Собственноручную (ые) подпись (и)
Шакурский М.В
заверяю: начальник ОДО ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» И.В. Плеханова
23.09 2026