УТВЕРЖДАЮ
Ректор ТУСУРа
_____ В.М. Рулевский
«10» апреля 2026 г.

ЗАКЛЮЧЕНИЕ

Федерального государственного автономного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники»

Диссертация «Методика обнаружения компьютерных атак на основе анализа системных событий операционной системы с использованием алгоритмов машинного обучения» выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники» (ТУСУР).

В период подготовки диссертации соискатель Павлычев Алексей Викторович работал в Дальневосточном федеральном университете в должностях директора Центра информационной безопасности и доцента департамента информационной безопасности.

Павлычев А.В. имеет высшее юридическое образование. С 2009 по 2019 год проходил военную службу по контракту. В 2019 году прошел профессиональную переподготовку по программе «Информационная безопасность. Техническая защита информации».

Научный руководитель – Шелупанов Александр Александрович, член-корреспондент РАН, д-р техн. наук, профессор, заведующий кафедрой комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) Федерального государственного автономного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники».

По итогам обсуждения принято следующее заключение:

В представленной диссертационной работе Павлычева А.В. предлагается **решение важной научно-технической задачи** разработки методики выявления компьютерных атак с использованием современных аналитических инструментов, решение которой вносит значительный вклад в развитие кибербезопасности, основанное на передовых технологиях искусственного интеллекта и машинного обучения.

В работе раскрыта **актуальность проблемы** в контексте возрастающих внешних угроз и применением злоумышленниками новых тактик, техник и инструментов, приведен анализ трудов российских и зарубежных исследователей, произведена оценка степени проработанности задачи выявления компьютерных атак посредством анализа системных событий операционной системы с использованием методов машинного обучения.

Разработана авторская методика выявления компьютерных атак с использованием алгоритмов машинного обучения при обработке системных событий операционной системы. Предложена формальная модель компьютерных атак и легитимных действий пользователей, которая позволяет выявлять компьютерные атаки с использованием системных событий операционной системы. Разработан алгоритм моделирования компьютерных атак и формирования набора данных из системных событий операционной системы.

Проведена нотация методики выявления компьютерных атак в соответствии с серией ГОСТ 59709-59712, а также осуществлена ее модификация посредством добавления новых функциональных блоков, связанных с обработкой событий операционной системы методами машинного обучения.

Разработана формальная модель, позволяющая относить любое действие в операционной системе к легитимному событию или компьютерной атаке на основе идентификаторов событий операционной системы.

Предложен алгоритм моделирования компьютерных атак и формирования набора данных, включающий этап валидации полученных результатов. В соответствии с разработанным алгоритмом в ходе эксперимента собран набор данных, содержащий 1 473 559 записей о действиях пользователей и компьютерных атаках с привязкой к событиям операционной системы, что существенно превосходит существующие открытые наборы данных по объему, разнообразию и релевантности к задачам кибербезопасности.

Личный вклад автора состоит в создании методики обнаружения компьютерных атак на основе анализа системных событий операционной системы с использованием алгоритмов машинного обучения, разработке формальной модели компьютерных атак по записям системных событий, а также в создании алгоритма моделирования компьютерных атак и легитимных действий пользователей. Автором создан программный комплекс, обеспечивающий решение задач выявления компьютерных атак посредством анализа журналов системных событий операционной системы. Автору принадлежит ключевая роль в получении основных результатов, составляющих научную основу диссертационной работы и выносимых на защиту.

Работы [76, 85, 97] выполнены автором единолично. В работах, написанных в соавторстве, автором формулировалась цель проводимых исследований, определялись направления разработки методики выявления компьютерных атак [83] и формальной модели [84]. В работах [48, 49] соискателем исследуются вопросы применения методов машинного обучения при выявлении кибератак, в работах [96, 98] разработан алгоритм формирования размеченного набора данных на основе смоделированных компьютерных атак. Апробация и тестирование разработанных методики и программного комплекса выполнены совместно с сотрудниками ДВФУ, входящих в научную группу соискателя.

Достоверность научных положений, результатов и основных выводов работы обеспечивается решением задач по обнаружению компьютерных атак с помощью анализа системных событий операционной системы и алгоритмов машинного обучения. Результаты оценивались на репрезентативной выборке, точность модели составила 0,9965. Проведен детальный анализ ошибочных предсказаний. Для каждой ошибки идентифицирована конкретная сессия, определен вид активности и получена предсказанная моделью вероятность. Проведено прямое сравнительное тестирование разработанного программного средства с существующими инструментами, работающими в той же предметной области. Превышение показателя обнаружения на 7–14% при равных условиях тестирования является статистически значимым и доказывает преимущество подхода на основе машинного обучения в данной задаче.

Выполненные исследования имеют научную новизну и практическую значимость.

Научная новизна полученных в диссертационной работе результатов заключается в следующем.

1. Предложена методика обнаружения компьютерных атак с проведением анализа записей системных событий операционной системы методами машинного обучения, отличающаяся от известных методик, основанных на анализе сигнатур и сетевого трафика;

2. Разработана формальная модель компьютерных атак, основой которой является учет записей системных событий операционной системы. Модель отличается от известных полным охватом всех возможных системных событий;

3. Предложен алгоритм моделирования компьютерных атак и формирования набора данных из системных событий операционной системы, который в отличие от существующих подходов автоматизирует процесс сбора данных и обеспечивает полное покрытие тактик MITRE ATT&CK, а также учитывает валидацию выполнения скриптов и передачу метаданных.

Теоретическая значимость работы заключается в развитии научно-методического аппарата обнаружения компьютерных атак на основе анализа системных событий

операционной системы. Формальная модель компьютерной атаки, описывающая действие злоумышленника через записи событий, позволяет унифицировать процесс обнаружения кибератак без использования дополнительных средств мониторинга. Алгоритм моделирования атак и формирования размеченных наборов данных обеспечивает полное покрытие тактик MITRE ATT&CK и воспроизводимость экспериментов. Указанные результаты вносят вклад в теорию информационной безопасности, расширяя методы выявления угроз на основе поведенческого анализа событий операционной системы.

Практическая значимость работы состоит в формировании прикладного инструментария и экспериментального набора для выявления компьютерных атак в реальных условиях. Сформирован сбалансированный набор данных из 1 473 559 записей о действиях пользователей и компьютерных атаках. На полученном наборе данных обучен классификатор, который достигает точности обнаружения 0,9965, что на 8% выше сигнатурных методов и на 6% выше анализа сетевого трафика. Разработанное программное средство, позволяет анализировать EVTX-файлы и выявлять признаки компьютерных атак. Результаты исследования готовы к использованию в системах мониторинга информационной безопасности.

Практическая значимость результатов диссертационной работы подтверждается их внедрением в деятельность компании-лицензиата ФСТЭК России, корпоративного центра ГосСОПКА ООО «Информационный центр», а также в учебный процесс ДВФУ. Результаты диссертационного исследования также использованы при реализации хоздоговоров, выполнявшихся в ДВФУ.

Полнота изложения материалов диссертационной работы в публикациях

По материалам диссертации Павлычева А.В. опубликовано 11 научных статей, в том числе 8 публикаций в рецензируемых научных изданиях, рекомендуемых для опубликования основных научных результатов диссертаций на соискание ученых степеней кандидата и доктора наук, из них 7 публикаций в рецензируемых журналах из перечня ВАК и 1 публикация в издании, индексируемом Web of Science и/или Scopus, а также получено 1 свидетельство о регистрации программы для ЭВМ. Результаты диссертационной работы в публикациях представлены в полном объеме.

Публикации в журналах, рекомендованных ВАК:

1. **Павлычев А. В.** Выявление сетевых аномалий в системных журналах операционной системы Microsoft Windows с использованием методов машинного обучения / А.В. Павлычев, К.С. Солдатов, В.А. Сказин // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2021. – Т. 24. – №. 4. – С. 27-32.

2. **Павлычев А.В.** Использование алгоритма машинного обучения Random Forest для выявления сложных компьютерных инцидентов / А.В. Павлычев, М.И. Стародубов, А.Д. Галимов // Вопросы кибербезопасности. – 2022. – Т.51. – № 5. – С. 74-81.

3. **Павлычев А.В.** Модель функционирования вредоносного программного обеспечения на основе анализа системных журналов операционной системы Microsoft Windows / А.В. Павлычев, М.И. Стародубов, А.Д. Галимов // Прикаспийский журнал: управление и высокие технологии. – 2022. – Т.66. – № 4. – С. 24-31.

4. **Павлычев А.В.** Выявление фишинговых интернет-доменов с помощью алгоритмов машинного обучения в режиме потоковой обработки данных / А.В. Павлычев, К.В. Кузьминец // Вопросы кибербезопасности. – 2025. – Т.66. – № 2. – С. 141-153.

5. **Павлычев А.В.** Формирование размеченного набора данных на основе смоделированных компьютерных атак / А.В. Павлычев А.В., К.В. Кузьминец, Д.Е. Бреус, А.А. Шелупанов // Безопасность информационных технологий. – 2025. – Т. 32. – № 4. – С. 1–18.

6. **Павлычев А. В.** Нотация и модификация методики выявления компьютерных инцидентов в соответствии с серией ГОСТ 59709-59712 / А.В. Павлычев // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2025. – Т. 28. – №. 3. – С. 73-81.

7. **Павлычев А.В.** Формальная модель компьютерных атак, основанная на записях системных событий операционной системы / А.В. Павлычев // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2026. – № 1. – С. 159–169.

Публикации, включенные в библиографические базы Web of Science, Scopus:

8. **Pavlychev A.** Automated Collection And Marking Of Operating System Log Entries In The Task Of Detecting Computer Attacks / A. Pavlychev, K. Kuzminetc, D. Breus, A. Shelupanov // Advances in Automation VII. RusAutoCon 2025. Lecture Notes in Electrical Engineering. – 2025. – Vol. 1521. – P. 266–276.

Свидетельства о регистрации программ ЭВМ и баз данных:

9. Свидетельство о государственной регистрации программы для ЭВМ № 2026618641. Российская Федерация. Программа для моделирования компьютерных атак и формирования наборов данных из системных событий операционной системы / **Павлычев А.В.** Заявка № 2026617650. Дата поступления 18.03.2026. Зарегистрировано в реестре программ для ЭВМ 26.03.2026.

Специальность, которой соответствует диссертация

Диссертационная работа Павлычева А.В. на тему «Методика обнаружения компьютерных атак на основе анализа системных событий операционной системы с использованием алгоритмов машинного обучения» соответствует требованиям «Положения о порядке присуждения ученых степеней», предъявляемым ВАК к диссертационным работам на соискание ученой степени кандидата наук, является законченным самостоятельным научным исследованием, имеющим научную ценность.

Содержание диссертации соответствует паспорту специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность, а именно п. 3, п. 6:

- п. 3: Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса;
- п. 6: Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях;

Диссертация «Методика обнаружения компьютерных атак на основе анализа системных событий операционной системы с использованием алгоритмов машинного обучения» Павлычева Алексея Викторовича соответствует требованиям п.9-14 Положения о присуждении ученых степеней и рекомендуется к защите на соискание учёной степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Заключение принято на заседании научно-технического семинара «Интеллектуальные системы моделирования, проектирования и управления» кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) Федерального государственного автономного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники».

Присутствовало на заседании 24 чел. Результаты голосования: «за» - 24 чел., «против» - 0 чел., «воздержалось» - 0 чел., протокол № 432 от 28.02.2026 г.

Заместитель председателя семинара,
канд. техн. наук, доцент, декан
факультета безопасности _____ Е.М. Давыдова

Ученый секретарь семинара, канд. техн.
наук, и.о. зав. кафедрой БИС _____ Е.Ю. Костюченко