

## **ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА**

доктора технических наук, профессора

**Буйневича Михаила Викторовича**

на диссертационную работу **Павлычева Алексея Викторовича**, выполненную на тему «Методика обнаружения компьютерных атак на основе анализа системных событий операционной системы с использованием алгоритмов машинного обучения» и представленную на соискание ученой степени кандидата технических наук по специальностям 2.3.6 - «Методы и системы защиты информации, информационная безопасность»

### **Актуальность темы исследования**

Диссертационная работа Павлычева А.В. посвящена решению одной из наиболее острых проблем современной кибербезопасности - своевременному и точному обнаружению компьютерных атак за счет разработки соответствующих высокоэффективных методов, способных противостоять быстро эволюционирующему ландшафту угроз.

Актуальность темы обусловлена совокупностью взаимосвязанных факторов, имеющих как государственно-политическое, так и научно-техническое измерение.

Во-первых, геополитический контекст придает работе Павлычева А.В. особую остроту. В условиях фактической кибервойны, объявленной России недружественными государствами, наблюдается значительный рост как количества, так и сложности кибератак со стороны высокомотивированных и хорошо финансируемых хакерских групп, использующих, в том числе, технологии искусственного интеллекта для обхода средств обнаружения; прогнозируется дальнейшая эскалация угроз. Утверждение Стратегии национальной безопасности Российской Федерации (Указ Президента № 400 от 02.07.2021) и выделение информационной безопасности в качестве одного из 9 стратегических приоритетов подтверждают высокую государственную значимость исследований в данной предметной области.

Во-вторых, научно-методологический пробел, на который указывает диссертант, заключается в том, что подавляющее большинство существующих исследований и готовых решений сосредоточено либо на анализе сетевых пакетов, либо на использовании устаревших и ограниченных наборов данных (KDD'99, NSL-KDD, DARPA), которые не отражают современных тактик и техник атак (в частности, актуальных версий матрицы MITRE ATT&CK). Системные события операционной системы, содержащие богатую поведенческую информацию о процессах, изменениях в реестре, аутентификации и действиях пользователей, остаются недостаточно изученным, а потому и слабо используемым источником для построения моделей машинного обучения. Отсутствие формальных моделей, описывающих компьютерные атаки через призму системных журналов, а также дефицит открытых размеченных датасетов, охватывающих широкий

спектр современных угроз, сдерживают развитие интеллектуальных систем обнаружения нового поколения. Представленная работа направлена на восполнение именно этого пробела, что определяет ее несомненную ценность.

В-третьих, практическая востребованность темы подтверждается созданием и функционированием в Российской Федерации государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), деятельность которой регламентируется национальными стандартами (ГОСТ Р 59709–59712). Эти стандарты прямо допускают применение как сигнатурных, так и бессигнатурных методов, основанных на выявлении статистических зависимостей и формировании профилей функционирования информационных ресурсов. Однако действующие методики и инструментарий центров мониторинга не используют в полной мере потенциал машинного обучения для анализа системных журналов, что делает разрабатываемую диссертантом методику практически необходимой для повышения эффективности работы центров ГосСОПКА и расследования инцидентов.

В-четвертых, импортозамещение и технологический суверенитет также актуализируют тему. Переход на отечественные операционные системы на базе Linux требует пересмотра подходов к мониторингу и обнаружению атак. Предложенная диссертантом формальная модель, адаптируемая под различные ОС, создает теоретическую основу для создания систем защиты, не зависящих от зарубежных проприетарных решений, что соответствует стратегическим задачам развития информационной безопасности в Российской Федерации.

В связи с вышеизложенным, считаю, что тема диссертации, направленная на создание формализованной методики обнаружения компьютерных атак на основе анализа системных событий с использованием алгоритмов машинного обучения, является, безусловно, *актуальной* на современном этапе развития отрасли.

### **Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертационной работе**

Обоснованность научных положений, выводов и рекомендаций, сформулированных в диссертации является следствием корректно выстроенной методологической логики исследования и глубокой проработки теоретической базы.

Последняя опирается на глубокий и критический анализ современного состояния проблемы: диссертантом детально изучены более 100 источников, включая фундаментальные работы российских ученых и зарубежных исследователей, а также актуальные аналитические отчеты за 2023–2025 гг. и официальные нормативные документы. Такой широкий обзор позволил

объективно определить нерешенные задачи и сформулировать цель работы, не противоречащую известным положениям, а органично их дополняющую и развивающую.

Методологический аппарат исследования выбран адекватно поставленным задачам: применены апробированные методы системного анализа, теории защиты информации, математического моделирования (включая аппарат булевых функций для формализации системных событий) и машинного обучения. Выбор алгоритмов (случайный лес, деревья решений, метод опорных векторов и др.) выполнен на основе сравнительного анализа, причем для каждого метода приведены обоснования его применимости к данным конкретного типа (бинарные признаки, разреженность, зашумленность).

Логическая структура диссертации также свидетельствует о высокой степени обоснованности выводов: каждое последующее положение вытекает из предыдущего – от анализа угроз и методов (Глава 1) к формализации модели (Глава 2), затем к алгоритмизации сбора данных (Глава 3) и завершается экспериментальной апробацией (Глава 4). Такая структура исследования обеспечивает внутреннее единство работы и позволяет проследить цепочку рассуждений автора от постановки научной задачи до конечных рекомендаций.

### **Достоверность и новизна полученных результатов**

**Научная новизна** работы определяется новизной полученных в ней основных результатов, которые не были ранее получены другими исследователями в таком представлении, а именно:

- разработана **оригинальная методика** обнаружения компьютерных атак, которая, *в отличие* от традиционных сигнатурных подходов и методов анализа сетевого трафика, базируется на поведенческом анализе системных событий операционной системы с использованием машинного обучения, что обеспечивает повышение точности на 6–8 %.

- построена **формальная модель** компьютерной атаки, основанная на полном множестве событий из журналов Security, System и Application, представленных в виде булевых векторов. Модель *отличается* универсальностью и позволяет описывать атаки без привлечения дополнительных средств мониторинга, а также адаптируется к отечественным ОС на базе Linux.

- предложен **алгоритм моделирования атак и формирования датасета**, который *впервые* автоматизирует сбор и разметку данных, обеспечивает валидацию выполнения сценариев и в 4 раза расширяет покрытие тактик MITRE ATT&CK *по сравнению с известными аналогами*, что существенно повышает качество обучающих выборок.

**Достоверность методики** подтверждается ее соответствием требованиям государственных стандартов (ГОСТ Р 59709–59712), практической применимостью (прошла апробацию и внедрена в центр мониторинга ООО «Информационный центр») и использованием общепризнанного инструментария функционального моделирования IDEF0 (что обеспечивает ее внутреннюю непротиворечивость и корректность на уровне построения процедур)

**Достоверность модели** обеспечивается непротиворечивостью и полнотой ее формализма и подтверждается экспериментально верификацией на реальных данных – каждой категории активности (четыре техники MITRE ATT&CK и четыре типа пользовательских действий) соответствует уникальный и различимый набор EventID. Это служит прямым доказательством того, что предложенная модель адекватно отражает реальную связь между действиями злоумышленников и фиксируемыми системными событиями. Также в работе обосновывается возможность адаптации модели для отечественных ОС на ядре Linux, что свидетельствует о ее концептуальной гибкости и подтверждает ее платформенную инвариантность.

**Достоверность алгоритма** подтверждается тем, что он детально описан, включает формализованные этапы и использует общедоступные инструменты; это обеспечивает полную воспроизводимость эксперимента любым исследователем, что является фундаментальным критерием достоверности в научной методологии. Также алгоритм включает валидацию выполнения скриптов (с помощью индикаторов) и записей базы данных (на достаточность и сбалансированность); это исключает пропуски ошибок на этапе сбора данных и гарантирует, что каждый сценарий действительно был реализован и корректно зафиксирован. В результате работы алгоритма собран датасет из более чем 1,47 млн записей с равномерным распределением по классам (52,5% атак и 47,5% пользовательских действий) и субкатегориям; подобная сбалансированность и объем данных объективно свидетельствуют о корректности работы алгоритма.

### **Замечания по диссертационной работе**

Несмотря на общее положительное впечатление, работа содержит ряд недостатков, которые необходимо отметить:

1) На стр. 6 диссертации и стр. 4 автореферата указано, что: «Объектом исследования являются компьютерные системы, подвергшиеся несанкционированному воздействию (компьютерным атакам)». Это некорректно, поскольку «несанкционированное воздействие» – более широкое понятие, включающее физическое уничтожение носителей, радиоэлектронное воздействие, ошибки персонала и т.д., тогда как «компьютерная атака» ограничена программными и программно-

аппаратными средствами. Приравнивание этих понятий через скобки нарушает терминологию, принятую в российских нормативных документах и документах Регуляторов.

2) Автор сравнивает свое приложение с двумя инструментами, использующими сигнатурный подход, но не сравнивает с другими методами машинного обучения на журналах (например, с работами, использующими глубокое обучение или графовые модели). Также сравнение точности с классификаторами на сетевом трафике (0,9279) не совсем корректно, поскольку те обучались на другом датасете (NSL-KDD) и на других признаках. Следовало бы провести сравнение на едином наборе данных или хотя бы указать это ограничение.

3) В работе не приведены оценки времени обучения и работы классификатора в реальных условиях, не указаны требования к ресурсам (ОЗУ, CPU). Для практического применения это важно, особенно при обработке больших журналов.

4) Датасет собран в изолированной виртуальной среде с ограниченным набором пользовательских сценариев. Хотя диссертант старался сделать его сбалансированным, в реальных корпоративных сетях трафик и поведение пользователей гораздо разнообразнее. Отсутствует анализ устойчивости модели к изменению профиля пользователей, к дрейфу данных. Это может ограничить применимость в динамичных средах.

5) В обзоре литературы (глава 1) приведены устаревшие датасеты (DARPA, KDD'99) и не рассмотрены современные работы, использующие журналы Windows и методы глубокого обучения (например, работы с применением LSTM, трансформеров). Хотя это не снижает новизны собственной работы, но показывает неполноту анализа.

6) Автореферат выполнен с отклонением от ГОСТ Р 7.0.11—2011 «ДИССЕРТАЦИЯ И АВТОРЕФЕРАТ ДИССЕРТАЦИИ. Структура и правила оформления». В частности структурный элемент «ЗАКЛЮЧЕНИЕ» в оппонируемой работе назван «ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ» (в котором смешаны результаты работы и перспективы исследования в предметной области), а структурный элемент «СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ» назван «СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ РАБОТЫ», который к тому не оформлен в нотации Приложения Б «Примеры библиографических записей документов в списке литературы».

Приведенные выше замечания не снижают ценность диссертационной работы и не ставят под сомнение полученные в ней основные научные результаты. Их целесообразно рассматривать как некоторые из направлений дальнейшей работы диссертанта в данной предметной области.

## **Заключение о соответствии диссертации критериям, установленным**

### **Положением о присуждении ученых степеней**

В соответствии с п. 9 Положения в диссертации Павлычева А.В. содержится решение научной задачи создания методики выявления компьютерных атак на основе анализа системных событий операционной системы с использованием алгоритмов машинного обучения, имеющей значение для развития отрасли информационной и кибербезопасности.

В соответствии с п. 10 Положения диссертация Павлычева А.В. обладает внутренним единством (см. раздел отзыва «Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертационной работе», последний абзац), содержит новые научные результаты и положения, выдвигаемые для публичной защиты (см. раздел отзыва «Достоверность и новизна полученных результатов», каждый из которых опубликован без соавторов (см. №№ 6, 7 и 12 в Списке публикаций из автореферата), что свидетельствует о *личном* вкладе автора диссертации в науку.

Также в диссертации приводятся сведения о практическом использовании полученных автором научных результатов в деятельности центра мониторинга ООО «Информационный центр», а также в учебном процессе Дальневосточного федерального университета, что подтверждается актами о внедрении.

В соответствии с п. 11 Положения основные научные результаты диссертации опубликованы в рецензируемых научных изданиях (см. №№ 1-7, 11, 12 по Списку публикаций из автореферата).

В соответствии с п. 12 Положения журналы, где автором опубликованы основные научные результаты диссертации, а именно: 1) Безопасность информационных технологий, 2) Вопросы кибербезопасности, 3) Доклады Томского государственного университета систем управления и радиоэлектроники, 4) Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России» и 5) Прикаспийский журнал: управление и высокие технологии, – включены в Перечень рецензируемых научных изданий (по состоянию на 14.08.2026) за №№ п/п 312, 967, 1161, 1894 и 2258 соответственно.

В соответствии с п. 12(1) Положения авторское свидетельство о государственной регистрации программы для ЭВМ № 2026618641 (№ 12 в Списке публикаций из автореферата), приравнивается к публикациям в рецензируемых изданиях.

В соответствии с п. 14 Положения на все использованные в работе источники и материалы в тексте диссертации имеются ссылки. Оригинальность работы составляет около 90 %.

## Вывод

Диссертация на тему «Методика обнаружения компьютерных атак на основе анализа системных событий операционной системы с использованием алгоритмов машинного обучения» полностью соответствует требованиям п. 9-14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 г. № 842, а ее автор, Павлычев Алексей Викторович, заслуживает присуждения ученой степени **кандидата технических наук** по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Я, Буйневич Михаил Викторович, даю свое согласие на включение своих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

### Официальный оппонент:

доктор технических наук, профессор, профессор кафедры прикладной математики и безопасности информационных технологий федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский университет Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева»

« 10 » сентября 2026 г.

 Буйневич Михаил Викторович

### Информация о диссертации:

Докторская диссертация защищена по специальности 05.13.01 – Системный анализ, управление и обработка информации (2009 г).

### Контактная информация:

ФГБОУ ВО «Санкт-Петербургский университет Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева».

196105, Российская Федерация, г. Санкт-Петербург, Московский проспект, д. 149

Тел: +7 (812) 645-20-15

Email: bmv1958@yandex.ru

