

ОТЗЫВ

официального оппонента
кандидата технических наук, заведующего кафедрой безопасности
информационных технологий
ФГБОУ ВО «Сибирский государственный университет науки и технологий
имени академика М.Ф. Решетнева»
Золотарева Вячеслава Владимировича
на диссертацию
Павлычева Алексея Викторовича на тему
«Методика обнаружения компьютерных атак на основе анализа системных
событий операционной системы с использованием алгоритмов машинного
обучения», представленную на соискание ученой степени кандидата
технических наук по специальности
2.3.6. Методы и системы защиты информации, информационная
безопасность

Актуальность темы. Диссертация А.В. Павлычева посвящена решению актуальной задачи повышения эффективности обнаружения компьютерных атак за счет использования методов машинного обучения для анализа системных событий операционной системы.

В условиях стремительного роста числа кибератак, усложнения их сценариев и активного применения злоумышленниками технологий искусственного интеллекта традиционные сигнатурные методы обнаружения становятся недостаточно эффективными. Особую значимость приобретает разработка методов, позволяющих выявлять аномальную активность на основе поведенческих паттернов, фиксируемых в журналах операционной системы.

Работа Павлычева А.В. выполнена с учетом актуальных задач, поставленных в рамках Стратегии национальной безопасности Российской Федерации, и соответствует приоритетным направлениям развития системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Соответствие содержания основным положениям диссертации.
Диссертация состоит из введения, четырех глав, заключения, списка

литературы из 109 наименований и двух приложений. Общий объем работы – 157 страниц, содержит 47 рисунков и 12 таблиц.

Во введении обоснована актуальность, сформулированы цель и задачи, научная новизна, практическая значимость, положения, выносимые на защиту.

В первой главе проведен обзор видов компьютерных атак и методов их обнаружения, выполнен анализ применения алгоритмов машинного обучения в задачах кибербезопасности, предложена авторская методика выявления атак с использованием системных событий.

Во второй главе исследованы структура и содержание журналов Windows, построена формальная модель компьютерной атаки, рассмотрены перспективы адаптации под отечественные ОС.

В третьей главе разработан алгоритм моделирования атак и формирования датасета, описана реализация исследовательского стенда, представлен и проанализирован полученный набор данных.

В четвертой главе проведена апробация методики: преобразование данных, обучение и сравнение классификаторов, интерпретация результатов, разработано и внедрено программное средство.

В заключении подведены итоги, сформулированы основные результаты и направления дальнейших исследований.

Научная новизна. Научная новизна результатов диссертационной работы заключается в следующем.

Разработана методика обнаружения компьютерных атак, основанная на анализе системных событий операционной системы с применением алгоритмов машинного обучения. В отличие от известных подходов, ориентированных преимущественно на анализ сетевого трафика или сигнатур, предложенная методика использует записи журналов Security, System и Application Windows в качестве основного источника данных, что позволяет выявлять атаки на уровне хоста с высокой точностью;

Построена формальная модель компьютерной атаки, представляющая любое действие в системе в виде вектора признаков, соответствующих факту наступления определенных событий (Event ID) в системных журналах. Модель обеспечивает универсальность и может быть адаптирована для операционных систем семейства Linux, в том числе для российских ОС;

Предложен алгоритм моделирования компьютерных атак и формирования наборов данных из системных событий, обеспечивающий автоматизацию сбора, разметки и валидации данных с привязкой к тактикам и техникам MITRE ATT&CK. Алгоритм позволяет значительно расширить покрытие выявляемых угроз по сравнению с существующими аналогами;

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации.

Обоснованность научных положений, выводов и рекомендаций, сформулированных в диссертационной работе А.В. Павлычева, обеспечивается корректным применением научного аппарата, последовательной логикой исследования и подтверждается результатами экспериментальной апробации.

Автором использован комплекс взаимодополняющих методов: системный анализ при исследовании видов и содержания системных событий операционной системы; методы теории множеств и формального моделирования при построении модели компьютерной атаки; методы машинного обучения при разработке классификаторов. Выбор методов соответствует поставленным задачам и специфике предметной области. Применение нотации IDEF0 для формализации методики выявления компьютерных инцидентов согласуется с требованиями серии ГОСТ Р 59709-59712 и обеспечивает преемственность по отношению к действующим нормативным документам в области управления компьютерными инцидентами.

Обоснованность предложенной методики обнаружения компьютерных атак, включающей анализ системных событий операционной системы

методами машинного обучения, подтверждается результатами сравнительного анализа восьми классификаторов, проведённого на сформированном наборе данных. Достигнутая точность 0,9965 превосходит результаты известных подходов, основанных на анализе сетевого трафика и сигнатурном анализе журналов. Корректность сравнения обеспечивается использованием единого набора данных, общепризнанных метрик и процедуры кросс-валидации. Полученный результат согласуется с данными предшествующих публикаций автора, посвящённых применению алгоритма Random Forest для выявления сложных компьютерных инцидентов.

Обоснованность разработанной формальной модели компьютерных атак, основанной на анализе системных событий операционной системы, подтверждается экспериментально. Автором показано, что каждому виду компьютерной атаки или пользовательского действия соответствует характерный набор значений Event ID из журналов Security, System и Application. Данный факт установлен на основе анализа 1 473 559 записей и визуализирован в работе. Формальная модель обладает свойством универсальности: её структура не зависит от конкретного типа операционной системы, что подтверждено анализом перспектив адаптации под отечественные ОС семейства Linux.

Обоснованность алгоритма моделирования компьютерных атак и формирования наборов данных из системных событий операционной системы обеспечивается реализацией полного цикла сбора данных на специально разработанном исследовательском стенде. Стенд включает четыре сетевых сегмента, что соответствует типовой архитектуре корпоративной сети. Применение средств автоматизации, YAML-правил и механизмов валидации выполнения скриптов обеспечивает воспроизводимость эксперимента.

Достоверность результатов диссертации. Достоверность полученных результатов обеспечивается:

корректным применением математического аппарата (теория множеств, формальное моделирование, методы машинного обучения);

использованием общепризнанных метрик оценки качества классификации (F-мера, матрица ошибок, кросс-валидация);

проведением вычислительных экспериментов на специально разработанном исследовательском стенде с эмуляцией реальных сценариев атак и легитимной активности;

валидацией модели на независимом наборе данных (EVTX-ATTACK-SAMPLES), подтвердившей высокую обобщающую способность;

сравнением разработанного программного средства с существующими аналогами;

практическим внедрением результатов в деятельность центра ГосСОПКА ООО «Информационный центр» и в учебный процесс ДВФУ.

Ценность результатов диссертационной работы для науки и практики. Разработанные в диссертации методика, формальная модель и алгоритм формирования датасетов могут быть использованы:

при создании систем обнаружения вторжений и мониторинга информационной безопасности, ориентированных на анализ системных журналов;

для автоматизации процесса сбора и разметки данных в задачах машинного обучения в области кибербезопасности;

в качестве основы для адаптации подходов к отечественным операционным системам в рамках импортозамещения.

На базе полученных результатов создано программное средство `evtx_ml_analyzer`, прошедшее апробацию и внедренное в практическую деятельность по расследованию компьютерных инцидентов. Разработанный датасет и подходы могут служить основой для дальнейших исследований в области поведенческого анализа угроз.

Подтверждение опубликования основных результатов диссертации в научной печати.

Основные результаты опубликованы в 11 научных работах, в том числе 7 статьях в рецензируемых журналах, рекомендованных ВАК РФ, получено 1 свидетельство о государственной регистрации программы для ЭВМ. Результаты апробированы на всероссийских и международных конференциях, внедрены в деятельность организации и учебный процесс.

При общей положительной оценке диссертационной работы необходимо отметить следующие замечания:

Отсутствие сравнительного анализа с современными методами глубокого обучения. В работе рассмотрены классические алгоритмы машинного обучения, однако не проведено сравнение с современными нейросетевыми подходами (например, Transformer-архитектурами для анализа последовательностей событий), что могло бы дать дополнительную оценку эффективности.

Ограниченность экспериментальной базы. Основные эксперименты проведены на операционной системе Windows. Хотя в работе сделан вывод о возможности адаптации под Linux, практическая реализация для отечественных ОС не представлена. Расширение эксперимента на российские ОС (Astra Linux, «РЕД ОС» и др.) существенно повысило бы ценность работы.

Недостаточная детализация критериев сбалансированности датасета. В работе указано, что датасет сбалансирован, но не приведено формального обоснования выбора объемов выборок для каждого класса и методов фильтрации сессий. Это затрудняет воспроизводимость эксперимента.

Отсутствие четких рекомендаций по применению разработанного ПО. В тексте приведено описание программного средства, но не сформулированы конкретные сценарии его использования, требования к инфраструктуре, ограничения и возможные режимы работы.

Опечатки и стилистические погрешности. В тексте встречаются отдельные грамматические и технические ошибки, а также различное оформление ссылок и сокращений, что несколько затрудняет чтение работы.

Указанные замечания носят рекомендательный характер и не снижают общей высокой оценки диссертационного исследования.

Заключение по работе. Диссертационная работа Павлычева А.В. является завершенным научно-квалификационным исследованием, в котором решена актуальная задача разработки методики обнаружения компьютерных атак на основе анализа системных событий операционной системы с использованием алгоритмов машинного обучения.

Результаты работы имеют существенное значение для развития теории и практики обеспечения информационной безопасности, обладают научной новизной и практической значимостью.

Диссертация соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» (п. 3, п. 6), а также критериям, установленным Положением о присуждении ученых степеней.

Соискатель, Павлычев Алексей Викторович, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:

кандидат технических наук, заведующего кафедрой безопасности информационных технологий ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева»

«22» сентября 2026 г.



Золотарев Вячеслав Владимирович

Почтовый адрес:

660037, Сибирский федеральный округ, Красноярский край, г. Красноярск, проспект им. Газеты Красноярский рабочий, 31

Телефон: 8(391) 222-76-39. E-mail: zolotarev@sibsau.ru

ПОДПИСЬ
УДОСТОВЕРЯЮ.

ГЛ. СПЕЦИАЛИСТ ПО ПЕРС.

КАДУШКИНА Я.В.



Специальность, по которой защищена диссертация:
05.13.01 Системный анализ, управление и обработка информации

 Золотарев В.В.

Я, Золотарев В.В., даю согласие на включение своих персональных данных в документы, связанные с работой диссертационного совета, и дальнейшую обработку.

 Золотарев В.В.

Золотарев В.В.
Удостоверен
Уполномоченный

Подпись 
удостоверяю.
Гл. специалист по перс. 
Кадушкина Я.В.
