

На правах рукописи



Павлычев Алексей Викторович

**МЕТОДИКА ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК
НА ОСНОВЕ АНАЛИЗА СИСТЕМНЫХ СОБЫТИЙ
ОПЕРАЦИОННОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ
АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ**

Специальность 2.3.6 – Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Томск-2026

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники».

Научный руководитель – Шелупанов Александр Александрович, член-корреспондент РАН, доктор технических наук, профессор

Официальные оппоненты: Буйневич Михаил Викторович, доктор технических наук, профессор, профессор кафедры прикладной математики и безопасности информационных технологий ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России», г. Санкт-Петербург

Золотарев Вячеслав Владимирович, кандидат технических наук, заведующий кафедрой безопасности информационных технологий ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», г. Красноярск

Ведущая организация – ФГБОУ ВО «Уфимский университет науки и технологий», г. Уфа

Защита состоится «15» октября 2026 г. в 15 час. 15 мин. на заседании диссертационного совета 24.2.415.04, созданного на базе ТУСУРа, по адресу: 634050, г. Томск, пр. Ленина, 40, ауд. 201.

С диссертацией можно ознакомиться в библиотеке ТУСУР по адресу: 634045, г. Томск, ул. Красноармейская 146, а также на сайте ТУСУР: <https://postgraduate.tusur.ru/urls/dmlzm65m>.

Автореферат разослан «___» _____ 2026 г.

Ученый секретарь
диссертационного совета

Костюченко Евгений Юрьевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Современные геополитические вызовы диктуют новые требования к киберустойчивости цифровых сервисов, предназначенных для полноценного обеспечения интересов личности, общества и государства.

Указом Президента Российской Федерации от 2 июля 2021 г. № 400 утверждена Стратегия национальной безопасности Российской Федерации. Информационная безопасность впервые выделена в качестве одного из стратегических национальных приоритетов, направленных на обеспечение и защиту национальных интересов Российской Федерации. В стратегии целью обеспечения информационной безопасности определено укрепление суверенитета Российской Федерации в информационном пространстве.

В условиях фактической кибервойны наибольшую опасность для цифрового суверенитета России представляют злоумышленники с высоким потенциалом - профессиональные политически мотивированные хакеры из недружественных государств.

Согласно изученным аналитическим отчетам, в 2023-2025 годах наблюдается значительный рост инцидентов информационной безопасности. Сложившаяся политическая обстановка говорит о дальнейшем росте хакерских атак на российскую информационную инфраструктуру с использованием новых видов кибероружия.

Взрывной рост технологий искусственного интеллекта, а также наличие большого количества материалов в открытом доступе делает хакерские атаки все более изощренными, при этом зачастую не требуя от их организаторов глубоких познаний в сфере используемых технологий.

Проблемам выявления компьютерных атак, обнаружения вторжений и применения методов машинного обучения в системах обеспечения информационной безопасности посвящено значительное количество исследований российских и зарубежных ученых.

Существенный вклад в развитие теоретических и практических аспектов защиты информации, обнаружения компьютерных атак и построения систем мониторинга безопасности внесли российские исследователи А.И. Гетьман, М.Н. Горюнов, А.С. Шабуров, Ш.Г. Магомедов, И.В. Котенко, О.И. Шелухин, Д.И. Раковский, С.А. Коноваленко, М.В. Буйневич, К.Е. Израйлов и др.

Вопросы анализа сетевого трафика, обнаружения аномалий, применения машинного обучения в задачах кибербезопасности получили развитие в работах зарубежных исследователей R. Lippmann, S.K. Sahu, N. Moustafa, A. Khraisat, M. Ghurab, T. Mehmood, F. Jemili, S. J. Yang, R.U. Khan, W. L. Al-Yaseen, S. M. Kasongo, A.M. Chandrashekhar, D.M. Farid, C. Smiliotopoulos, G. Kambourakis и др.

Анализ научных публикаций показывает, что большинство существующих подходов ориентировано преимущественно на исследование сетевого трафика и использование готовых наборов данных, которые обладают рядом ограничений, связанных с устареванием сценариев атак,

недостаточным учетом современных угроз и ограниченным использованием системных событий операционной системы.

Недостаточно исследованными остаются вопросы формирования наборов данных на основе системных событий операционной системы, построения формальных моделей компьютерных атак с учетом полного спектра системных событий.

Несмотря на значительное количество научных работ в области обнаружения компьютерных атак, задача разработки методики выявления компьютерных атак на основе анализа системных событий операционной системы с использованием алгоритмов машинного обучения остается **актуальной** и требует дальнейшего исследования.

Целью исследования является создание методики выявления компьютерных атак с включением анализа системных событий операционной системы методами машинного обучения.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Разработка методики выявления компьютерных атак с использованием алгоритмов машинного обучения при обработке системных событий операционной системы;
2. Проведение анализа видов и содержания событий операционной системы с целью построения формальной модели компьютерной атаки;
3. Модернизация алгоритма моделирования компьютерных атак и формирования набора данных из записей системных событий операционной системы;
4. Проведение экспериментального исследования разработанной методики выявления компьютерных атак, подтверждение достоверности и оценка результатов работы методики.

Объектом исследования являются компьютерные системы, подвергшиеся несанкционированному воздействию (компьютерным атакам).

Предметом выступает процесс обнаружения компьютерных атак с использованием методов анализа данных, основанных на записях системных событий операционной системы.

Основные методы исследования, примененные в диссертационной работе – это аналитические методы моделирования, системного анализа, теории защиты информации, методы машинного обучения.

Научная новизна результатов работы и проведенных исследований:

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.

Достоверность и обоснованность предлагаемых научных положений, результатов и выводов работы подкрепляется разносторонним изучением современного состояния предметной области, системным обоснованием предложенных моделей, не противоречащих известным положениям других авторов, проведением эксперимента, подтверждающего результаты теоретических изысканий, апробацией полученных результатов в научных публикациях и докладах на международных и российских научных и научно-практических конференциях, а также практикой внедрения результатов исследования.

Научная значимость работы состоит в развитии теории и методологии обеспечения информационной безопасности в части создания новых способов обнаружения признаков несанкционированного воздействия на информационную систему с использованием современных аналитических инструментов.

Практическая значимость результатов исследования состоит в расширении возможностей выявления признаков компьютерных атак с использованием анализа системных событий операционной системы.

Реализация результатов работы. Работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках гранта № 40469-23-2021-К («Грант ИБ МТУСИ»).

Положения, выносимые на защиту:

1. Применение предложенной методики обнаружения компьютерных атак с включением анализа системных событий операционной системы методами машинного обучения позволяет достичь точность обнаружения 0,9965, что на 8% выше точности сигнатурных методов и более чем на 6% выше точности классификаторов, обученных на сетевом трафике.

Паспорт специальности, пункт 6: методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях;

2. Разработанная формальная модель компьютерных атак, основанная на анализе системных событий операционной системы, обеспечивает универсальность и позволяет описывать признаки атак без использования дополнительных инструментов мониторинга.

Паспорт специальности, пункт 3: методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса;

3. Алгоритм моделирования компьютерных атак и формирования наборов данных из системных событий операционной системы позволяет расширить спектр выявляемых тактик MITRE ATT&CK в 4 раза по сравнению

с существующими подходами, обеспечить полное покрытие угроз, а также повысить достоверность данных за счет валидации выполнения сценариев и передачи метаданных.

Паспорт специальности, пункт 6: методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.

Апробация работы. Основные и промежуточные результаты исследования докладывались и обсуждались на следующих конференциях:

II Всероссийская научная конференция (с приглашением зарубежных ученых) «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (Ставрополь, 2020);

Межвузовская научно-теоретическая конференция (в рамках Сибирского форума «Информационная безопасность – 2021») (Новосибирск, 2021);

Международная научно-методическая конференция «Интеграция образования, науки, бизнеса и власти» (НМК ТУСУР-2022) (Томск, 2022);

XVIII Всероссийская научно-практическая конференция (в рамках IX Пленума регионального отделения Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» по Сибирскому и Дальневосточному федеральным округам (СибПРОУМО))(Хабаровск, 2022);

II Всероссийская научная школа-семинар «Современные тенденции развития методов и технологий защиты информации» (Москва, 2022);

Международная научно-техническая конференция «Автоматизация» (RusAutoCon-2025) (Сириус, 2025).

Внедрение результатов. Результаты диссертационной работы внедрены в деятельность центра мониторинга ООО «Информационный центр», а также в учебный процесс Дальневосточного федерального университета.

Личный вклад. В диссертационной работе использованы результаты, в которых автору принадлежит определяющая роль. Постановка задачи исследования и верификация результатов в процессе выполнения работы осуществлялась научным руководителем член-корреспондентом РАН, д.т.н., профессором Шелупановым А.А.

Публикации по теме диссертации. По материалам исследования опубликовано 11 работ, в том числе 7 работ в изданиях, рекомендованных ВАК России. Получено 1 свидетельство о регистрации программы для ЭВМ.

Структура и объем работы. Диссертация содержит введение, 4 главы, заключение и список источников из 109 наименований. Объем работы: 157 страниц, в том числе 12 таблиц и 47 рисунков.

Благодарности. Автор выражает благодарность председателю ФУМО ВО ИБ Белову Е.Б. и председателю Сибирского регионального отделения УМО ВО ИБ Шелупанову А.А, за поддержку и мотивацию для занятия

научной деятельностью; научному коллективу Дальневосточного федерального университета и лично Артемьевой И.Л. и Гончаровой С.Н., которые терпеливо обсуждали ход работы и давали ценные советы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, сформулирована цель, определены задачи, научная новизна, практическая и теоретическая значимость полученных результатов, а также положения, выносимые на защиту.

В первой главе проведен обзор различных видов компьютерных атак и методов их обнаружения.

Подробно рассмотрена практика применения методов машинного обучения в области информационной безопасности. Проведен сравнительный анализ указанных методов, а также результаты их работы на датасете NSL-KDD. Результаты приведены в Таблице 1.

Модели машинного обучения, основанные на анализе сетевого трафика, демонстрируют максимальную точность на уровне 0,9279. Приведенные в таблице значения позволяют ввести критерий эффективности для методики обнаружения компьютерных атак с использованием алгоритмов машинного обучения. Предлагаемая методика должна обеспечивать точность $\theta \geq 0,9$.

Таблица 1. Сравнительный анализ методов машинного обучения в задаче обнаружения компьютерных атак

Метод машинного обучения	Преимущества	Недостатки	Примеры применения	Результаты работы алгоритмов на наборе данных NSL-KDD (F1-Score)	Время обучения (сек)
Случайный лес	Высокая точность, устойчивость к переобучению	Требует больше вычислительных ресурсов, чем одиночные деревья	Классификация вредоносного ПО, обнаружение аномалий	0.9279	12.5551
k-ближайших соседей	Простота реализации, не требует обучения	Чувствительность к данным, зависимость от выбора метрики расстояния и параметра k	Классификация сетевого трафика, обнаружение аномалий	0.9231	0.0068
Генетический алгоритм	Глобальный поиск решений, устойчивость к локальным оптимумам	Высокая вычислительная сложность, медленная сходимость	Оптимизация параметров моделей, обнаружение аномалий	0.9135	267.8857

Нейронные сети	Способность моделировать сложные нелинейные зависимости	Требует большого объема данных для обучения, сложность интерпретации	Обнаружение аномалий, классификация вредоносного ПО	0.9000	275.8265
Деревья решений	Простота интерпретации, устойчивость к шуму в данных	Склонность к переобучению, снижение точности на сложных данных с большим количеством признаков	Обнаружение аномалий в сетевом трафике, признаков компьютерных атак	0.8972	0.8664
Индуктивное обучение	Простота интерпретации, применение для задач с четкими правилами	Низкая точность на сложных данных, требует ручного создания правил	Обнаружение аномалий в сетевом трафике, классификация вредоносного ПО	0.8841	0.2138
Метод опорных векторов	Использование для задач классификации с малым объемом данных	Требует большого объема вычислительных ресурсов для больших данных	Обнаружение вторжений, классификация сетевого трафика	0.8194	7.1415
Скрытые Марковские модели	Применяются для анализа временных последовательностей	Требуют большого объема данных для обучения, сложность настройки	Анализ журналов событий, обнаружение аномалий в временных данных	0.7900	8.8711
Автоэнкодеры	Применяются для обнаружения аномалий	Требуют большого объема данных и вычислительных ресурсов	Обнаружение аномалий в сетевом трафике, анализ лог-файлов	0.6975	1055.4080
Кластеризация	Возможность поиска скрытых структур в данных	Требует выбора числа кластеров, чувствительность к начальным условиям	Сегментация сетевого трафика, обнаружение аномалий	0.6973	0.9686
Байесовская сеть	Учет вероятностных зависимостей, интерпретируемость	Требует точного задания априорных вероятностей, сложность для больших данных	Обнаружение аномалий в сетевом трафике, анализ рисков	0.6952	0.0265

В Российской Федерации создана и функционирует государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА). Деятельность данной системы строится на основе национальных стандартов России ГОСТ серии 59709-59712.

На основе данных стандартов в нотации IDEF0 составлена методика выявления компьютерных атак, включающая применение алгоритмов машинного обучения для анализа системных событий операционной системы, что позволяет повысить точность выявления. Исходная и предлагаемая методики представлены на Рисунках 1,2.

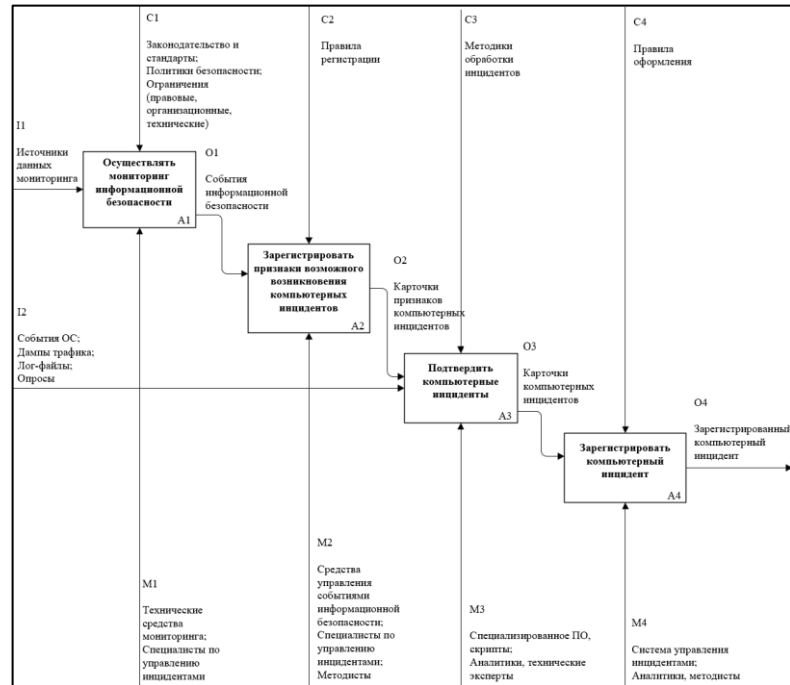


Рис. 1. Методика выявления компьютерных инцидентов в нотации IDEF0

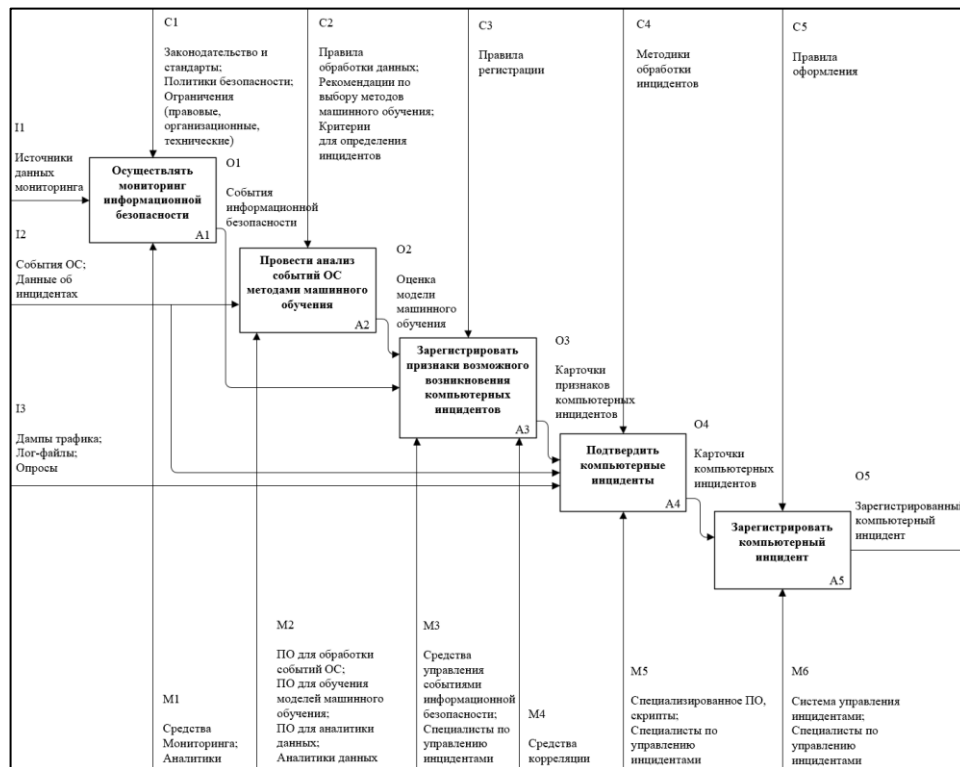


Рис. 2. Предлагаемая методика выявления компьютерных инцидентов

Предлагаемая методика соответствует требованиям стандартов, регламентирующих систему функционирования ГосСОПКА, дополняя и расширяя ее. Методика согласуется с положениями ГОСТ Р 59712-2022 в части применения бессигнатурных методов анализа, основанных на выявлении статистической и иной зависимости между событиями безопасности и формировании профилей функционирования информационных ресурсов. Алгоритм машинного обучения Random Forest, внедренный в методику, реализует данный подход, обеспечивая более эффективное выявление признаков компьютерных атак на основе анализа системных событий операционной системы.

Во второй главе рассмотрена структура системных событий операционной системы Microsoft Windows как самой распространенной в настоящее время. Наибольший интерес для исследователей информационной безопасности представляют следующие журналы операционной системы Windows: Security (Безопасность), System (Система) и Application (Приложение).

На основе проведенного анализа построена формальная модель выявления компьютерных атак и легитимных действий пользователей в операционной системе.

Рассмотрим множество U – множество всех возможных наблюдаемых действий в системе:

$$U = \{A_1, \dots, A_k, L_1, \dots, L_m\}, \quad (1)$$

$$n = k + m, \quad (2)$$

где A – множество действий злоумышленников,

L – множество легитимных действий пользователей,

n – количество всех возможных действий,

k – количество всех возможных действий злоумышленников (компьютерные атаки),

m – количество всех возможных действий легитимных пользователей.

Пусть множество $Sec = \{Sec_1, \dots, Sec_p\}$, множество булевых функций, где p – количество всех возможных событий, отображаемых в журнале Security.

Каждый элемент множества Sec имеет следующий смысл: функция Sec_i имеет значение 1, тогда и только тогда, когда за время выполнения действий происходило i -е событие из множества Sec , множества всех возможных событий журнала Security.

Пусть множество $Sys = \{Sys_1, \dots, Sys_t\}$, множество булевых функций, где t – количество всех возможных событий, отображаемых в журнале System.

Каждый элемент множества Sys имеет следующий смысл: функция Sys_i имеет значение 1, тогда и только тогда, когда за время выполнения действий

происходило i -е событие из множества Sys , множества всех возможных событий журнала System.

Пусть множество $App = \{App_1, \dots, App_s\}$, множество булевых функций, где s – количество всех возможных событий, отображаемых в журнале Application.

Каждый элемент множества App имеет следующий смысл: функция App_i имеет значение 1, тогда и только тогда, когда за время выполнения действий происходило i -е событие из множества App , множества всех возможных событий журнала Application.

Определим любой элемент множества U , множества всех возможных действий как набор следующих векторов.

Каждый элемент U_i из множества U имеет вид:

$$U_i = \left\{ \begin{bmatrix} Sec_{1,i} \\ \dots \\ Sec_{p,i} \end{bmatrix}, \begin{bmatrix} Sys_{1,i} \\ \dots \\ Sys_{t,i} \end{bmatrix}, \begin{bmatrix} App_{1,i} \\ \dots \\ App_{s,i} \end{bmatrix} \right\}, i = \overline{1, n}. \quad (3)$$

Пусть $\varphi(U_i): U_i \rightarrow \{0,1\}$ – функционал, обозначающий выполнение действия U_i и приводящий либо к безопасному состоянию системы (0), либо к небезопасному состоянию (1).

В силу стохастической природы событий и пересечения сигнатур атак с легитимной активностью необходимо дополнительное введение порога классификации θ :

Пусть $P(\varphi(U_i) = 1)$ – это число, рейтинг угрозы от 0 до 1.

Тогда правило классификации примет следующий вид:

Если $P(\varphi(U_i) = 1) \geq \theta$, то действие считается атакой;

Если $P(\varphi(U_i) = 1) < \theta$, то действие считается легитимным.

Определим область вероятностей компьютерной атаки как $V = \{U_i: U_i \in U, P(\varphi(U_i) = 1) \geq \theta\}$.

Исходя из вышеперечисленного существуют множества L (множество всех легитимных действий) и множество A (множество всех компьютерных атак): $L = \{L_1, \dots, L_k\}$ и $A = \{A_1, \dots, A_m\}$.

Элемент $U_i \in U$ является элементом множества A тогда и только тогда, когда $U_i \in V$.

Элемент $U_i \in U$ является элементом множества L тогда и только тогда, когда $U_i \notin V$.

Предложенный подход позволяет представить рассматриваемый объект (действие) в виде набора признаков, соответствующих наступлению определенного события, которое фиксируется в журналах Security, System и Application.

Российские ОС на базе Linux, как и Windows, используют комплексные системы журналирования для аудита и диагностики. Основным подсистемам Windows (Security, System, Application) в Linux соответствуют:

Журнал безопасности. Основные события входа и выхода, аутентификации, использования привилегий фиксируются в журналах `secure`, `auth.log`. Аналогично журналу `Security` в Windows, эти данные критичны для расследования инцидентов.

Системный журнал. Общесистемные сообщения, данные от ядра `kern.log`, служб и драйверов записываются в `syslog` или системный журнал `journald`. Это прямой аналог журнала `System` в Windows.

Журналы приложений. Приложения и сервисы могут писать в собственные файлы логов (`/var/log/`) или в централизованную систему `journald`. Это соответствует назначению журнала `Application` в Windows.

Предложенный подход к построению формальной модели позволяет обнаруживать компьютерные атаки без использования дополнительных инструментов мониторинга, что повышает его универсальность и снижает затраты на внедрение.

Модель может быть переиспользована для отечественных операционных систем в рамках политики импортозамещения.

В третьей главе рассмотрены различные подходы к моделированию атак и формированию наборов данных. Сравнительная характеристика приведена в Таблице 2.

Таблица 2. Подходы к моделированию атак и формированию датасетов

Автор, год публикации	Описание атак по MITRE ATT&CK, покрытие тактик	Источник данных	Описание моделирования атак, инструменты	Описание формирования датасета, инструменты	Дополнительная информация
John Dwyer, Traian Marius Truta, 2013	нет	Win Event Logs	частично, ручной метод	частично, SQL-запросы	
Christos Smiliotopoulos et al., 2022, 2023	да, боковое перемещение	Sysmon	частично, ручной метод	да, ETCExptool	
Khaled Rahal, Arbia Riah, Thibault Debatty, 2024	да, закрепление	Win Event Logs, Sysmon	да, для атак Caldera, Atomic Red Team, для пользователей GHOSTS Framework	нет	Автоматизация атак с помощью YAML-правил, Chocolatey для развертывания инфраструктуры, валидация выполнения скриптов
Layla Husselman, 2025	да, повышение привилегий, получение учетных данных, предотвращение обнаружения, боковое перемещение	Win Event Logs	нет, использовались публичные наборы данных	да, Splunk	В работе приведены результаты сигнатурного выявления данных атак, которые составили 0,9165

Настоящая работа	да, повышение привилегий, закрепление, получение учетных данных, предотвращение обнаружения	Win Event Logs	да, для атак Caldera, Atomic Red Team, для пользователей скрипты Python	да, Elastic	Автоматизация атак с помощью YAML-правил, валидация выполнения скриптов, передача метаданных об атаках и пользовательской активности
------------------	---	----------------	---	-------------	--

Можно выделить следующие лучшие практики, применяемые при моделировании:

1. Описание по MITRE ATT&CK. Использование общепринятой таксономии для классификации атак;
2. Виртуализация. Применение виртуальных сред для безопасного моделирования атак;
3. Автоматизация. Разработка скриптов и конфигурационных файлов для автоматизации процесса сбора и разметки данных;
4. Метаданные. Включение дополнительной информации для точной разметки событий;
5. Реалистичность. Стремление к созданию датасетов, отражающих реальные условия;
6. Баланс классов. Учет несбалансированности данных в реальных условиях, а также при обучении моделей;
7. Документация. Детальное описание процесса создания датасета для воспроизводимости.

Проведенный анализ существующих подходов и лучших практик дает возможность сформулировать алгоритм моделирования компьютерных атак и формирования набора данных из записей событий операционной системы. Визуальное представление алгоритма в виде блок-схемы представлено на Рисунке 3.

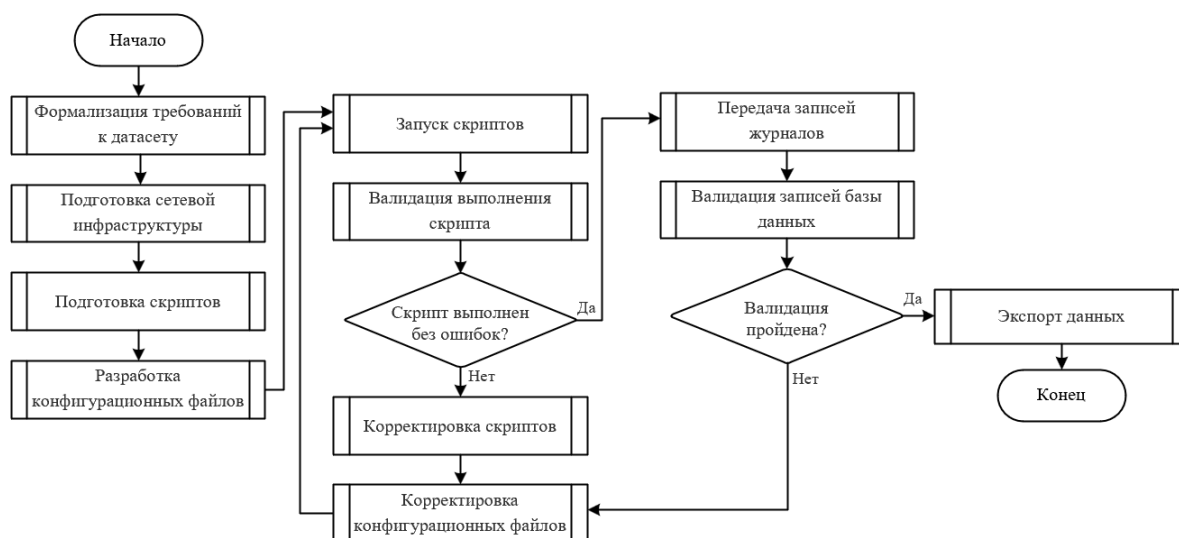


Рис. 3. Алгоритм моделирования атак и формирования набора данных

Данный алгоритм включает в себя следующие шаги:

1. Формализация требований к датасету. На этапе планирования необходимо четко определить целевые показатели: соотношение легитимных и атакующих событий, покрытие тактик и техник согласно MITRE ATT&CK, требуемый объем записей, временные рамки. Данный этап позволяет объективно оценить результат на шагах валидации и собрать качественный датасет.

2. Подготовка сетевой инфраструктуры. На данном этапе готовится сетевая инфраструктура, на которой будут эмулироваться компьютерные атаки и легитимные действия пользователей. Также в инфраструктуре разворачиваются средства автоматизации и база данных для хранения полученных записей событий операционной системы;

3. Подготовка скриптов. Ведется разработка набора скриптов атак и пользовательских действий. Атаки должны привязываться к матрице MITRE ATT&CK. Эмуляция пользовательских действий необходима для создания реалистичных данных для датасета;

4. Разработка конфигурационных файлов. Для автоматизации процесса формирования датасета и его воспроизводимости создаются конфигурационные YAML-правила – файлы, в которых описываются условия атаки (например, уязвимость, версия ПО), действия (эксплуатация уязвимости, выполнение команд, выполнение кода), параметры (IP-адреса, порты), зависимости (например, необходимость предварительной аутентификации), а также количество итераций запуска скриптов. Инструменты автоматизации (такие как Metasploit Framework) загружают эти правила и выполняют атаки в автоматическом или полуавтоматическом режиме. Для избежания зацикливания в качестве одного из параметров указывается количество итераций выполнения скрипта;

5. Запуск скриптов. Согласно конфигурационному файлу осуществляется запуск скриптов, эмулирующих компьютерные атаки и легитимные действия пользователей;

6. Валидация выполнения скрипта. С помощью специальных индикаторов осуществляется проверка выполнения скрипта;

7. В случае, если валидация не пройдена, производится доработка скриптов, а также конфигурационных файлов, в которых указывается новая последовательность выполнения и количество итераций. Далее осуществляется повторный запуск скриптов;

8. Передача записей событий. На данном этапе осуществляется передача и сохранение информации из системных событий операционной системы. Также передаются метаданные (например, вид атаки или действия пользователя) и уникальный идентификатор сессии;

9. Валидация записей базы данных. На данном этапе проводится проверка полученных записей на предмет достаточности и сбалансированности данных, а также иных критериев, установленных на этапе планирования;

10. В случае, если данных недостаточно, либо фиксируется дисбаланс классов, с помощью редактирования конфигурационного файла указывается недостающее количество необходимых скриптов и проводятся дополнительные итерации их выполнения;

11. Экспорт данных. На финальном этапе алгоритма осуществляется сохранение полученных данных в удобном для дальнейшего использования формате.

В рамках исследования спроектирован и развернут исследовательский стенд, в который входит 4 типовых сетевых сегмента:

1. Сегмент атакующих – включает пару машин на Windows и Linux (Kali), с которых производятся атаки;

2. Сегмент пользователей – набор машин на Linux и Windows, имитирующих рабочие места сотрудников. На них расположены разработанные скрипты, имитирующие легитимные действия пользователей;

3. Серверный сегмент – сегмент, имитирующий серверы атакуемой организации, в него входят такие сервисы как файловый сервер, сервер Active Directory, WEB-сервер и другие;

4. Сегмент обработки данных – тут размещаются серверы-обработчики, в том числе сервер базы данных, в которую передаются записи из системных событий пользовательской машины и метаданные, необходимые для разметки;

На Рисунке 4 приведены основные элементы информационной инфраструктуры для проведения эксперимента.

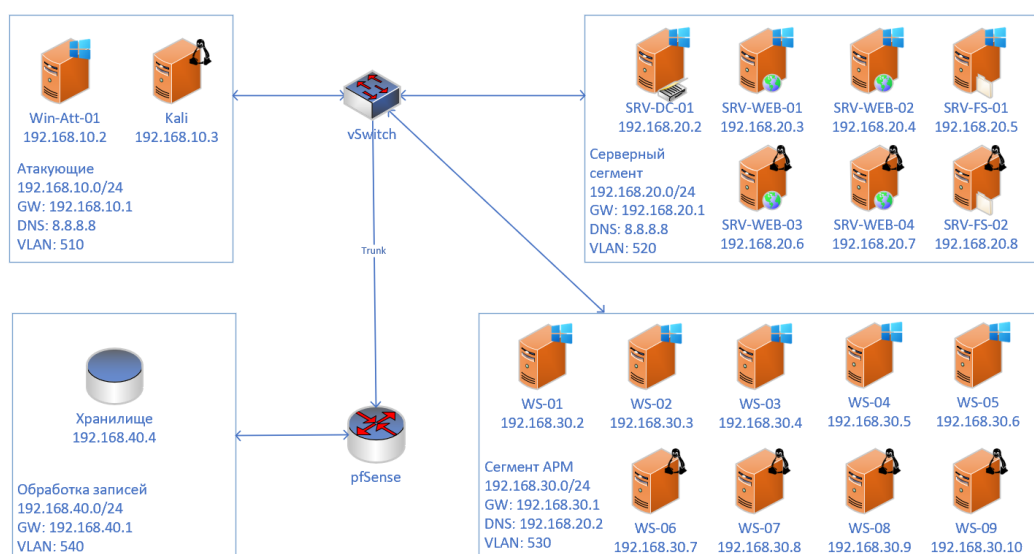


Рис. 4. Основные элементы исследовательского стенда

В качестве программной среды для исследования выбрана следующая конфигурация: гипервизор Oracle VM VirtualBox для эмуляции элементов компьютерной сети; специализированное ПО Winlogbeat для передачи системных журналов; база данных Elastic для хранения информации из системных событий и метаданных.

Действия, воспроизводимые в информационной системе в рамках исследования, включают в себя две группы:

1. Компьютерные атаки;
2. Легитимные действия пользователей.

Для моделирования компьютерных атак разработан ряд атакующих скриптов:

1. Подбор паролей для компрометации учетных записей - атака на SMB-сервис с перебором логинов и паролей (тактика TA0006: Получение учетных данных);
2. Изменение параметров учетных записей для получения повышенных прав или обхода контроля доступа - добавление пользователя в группу администраторов (тактика TA0004: Повышение привилегий);
3. Использование встроенной службы Windows Background Intelligent Transfer Service для скрытой загрузки и выполнения вредоносного кода (тактика TA0003: Закрепление);
4. Запуск вредоносного кода через доверенные системные утилиты - выполнение DLL через rundll32.exe для обхода антивируса (тактика TA0005: Предотвращение обнаружения).

Для моделирования легитимных действий пользователей разработаны скрипты, эмулирующие распространенные сценарии офисной работы:

1. Просмотр веб-страниц и видеоконтента при помощи браузера;
2. Работа с пакетом офисных приложений;
3. Получение и отправка электронной почты;
4. Использование файлового хранилища.

С целью автоматизации запуска компьютерных атак и различных пользовательских сценариев дополнительно разработан управляющий скрипт. Данный программный продукт также предназначен для передачи метаданных, для дальнейшей передачи в базу данных и разметки полученных результатов.

Передаваемые метаданные содержат информацию о виде действия: компьютерная атака (ATTACK), либо легитимные действия (USER_ACTION), а также номер техники из матрицы MITRE ATT&CK и конкретный тип пользовательских действий (WEB, OFFICE, FTP, MAIL).

В результате эксперимента сформирован набор данных, содержащий размеченную информацию о записях системных событий, полученных с виртуальной машины, на которой были реализованы различные компьютерные атаки и сценарии пользовательской работы. Общий вид полученного набора представлен на Рисунке 5. Итоговое количество собранных событий составило 1 473 559.

Описание полей в наборе данных:

1. @timestamp – дата и время регистрации события;
2. winlog.channel – системный журнал Windows, в котором зафиксировано событие. Принимает одно из следующих значений: Security, System, Application;
3. event.code – код события Event ID из набора Windows Event Logs;

- 4. `fields.category` – указывает на вид события и принимает два значения: `ATTACK` – компьютерная атака, `USER_ACTION` – пользовательские действия;
- 5. `fields.session` – уникальный идентификатор сессии, в рамках которого зафиксировано событие;
- 6. `fields.sub_category` – конкретный вид компьютерной атаки или пользовательского действия.

	@timestamp	winlog.channel	event.code	fields.category	fields.session	fields.sub_category
0	Apr 28, 2025 @ 15:11:40.080	Security	4624	USER_ACTION	20250427221113	OFFICE
1	Apr 28, 2025 @ 15:11:40.080	Security	4672	USER_ACTION	20250427221113	OFFICE
2	Apr 28, 2025 @ 15:11:40.048	System	6	USER_ACTION	20250427221113	OFFICE
3	Apr 28, 2025 @ 15:11:40.036	Security	4624	USER_ACTION	20250427221113	OFFICE
4	Apr 28, 2025 @ 15:11:40.036	Security	4672	USER_ACTION	20250427221113	OFFICE
...	...	...	...	...	...	...
1642041	May 1, 2025 @ 21:41:15.803	Security	4672	ATTACK	20250501214051	SYSTEM_BINARY_PROXY_EXECUTION_(T1218)
1642042	May 1, 2025 @ 21:41:15.799	Application	4625	ATTACK	20250501214051	SYSTEM_BINARY_PROXY_EXECUTION_(T1218)
1642043	May 1, 2025 @ 21:41:15.748	System	24	ATTACK	20250501214051	SYSTEM_BINARY_PROXY_EXECUTION_(T1218)
1642044	May 1, 2025 @ 21:41:15.748	System	1	ATTACK	20250501214051	SYSTEM_BINARY_PROXY_EXECUTION_(T1218)
1642045	May 1, 2025 @ 21:41:15.748	Security	4616	ATTACK	20250501214051	SYSTEM_BINARY_PROXY_EXECUTION_(T1218)

1473559 rows × 6 columns

Рис. 5. Визуальное представление сформированного набора данных

На Рисунке 6 представлено распределение EventID для каждого вида активности в журналах Security, System и Application.

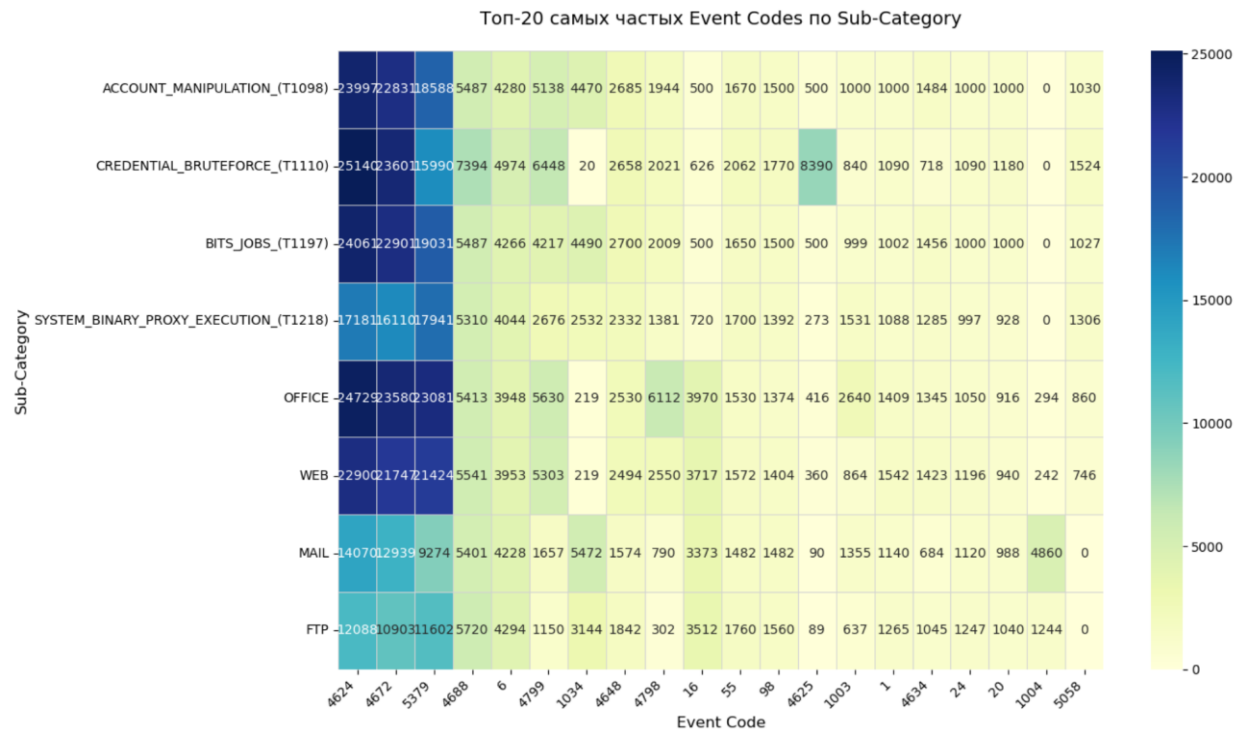


Рис. 6 Распределение EventID по всем категориям

Таким образом, предложенная формальная модель нашла свое подтверждение в ходе эксперимента, демонстрирующего, что каждому виду компьютерной атаки или пользовательского действия соответствует характерный набор значений EventID из системных событий операционной системы Windows.

В четвертой главе проведена апробация разработанной методики выявления признаков проведения компьютерных атак с помощью анализа системных событий операционной системы Windows и алгоритмов машинного обучения.

Произведено преобразование полученных данных о записях системных событий операционной системы в наборы признаков объекта. Каждый признак будет иметь числовое значение, соответствующее количеству зафиксированных Event ID в ходе реализации сценария атаки или пользовательской активности, а также 0 в случае, если запись о наступлении данного события отсутствует.

Набор исследуемых данных формируется следующим образом: в качестве названий столбцов используются уникальные идентификаторы событий, в качестве строк – наборы значений признаков исследуемых объектов, как показано на Рисунке 7.

В качестве целевого признака введен тип действия: легитимная пользовательская активность или компьютерная атака.

	fields.session	0	1	6	12	14	15	16	18	20	...	16384	16394	16962	16977	16983	50036	50103	51046	sub_category_encoded	target
0	20250412144135	1	4	18	2	2	0	2	2	4	...	2	2	2	2	2	2	2	2	5	0
1	20250412144551	0	3	19	2	2	0	2	2	4	...	0	1	2	2	2	2	2	2	4	0
2	20250412145345	1	4	17	2	2	0	2	2	4	...	2	2	2	2	2	2	2	2	5	0
3	20250412145802	0	3	17	2	2	0	2	2	4	...	0	1	2	2	2	2	2	2	4	0
4	20250412150131	2	4	17	2	2	0	2	2	4	...	2	3	2	2	2	2	2	2	5	0
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
9995	20250428232302	1	3	9	1	1	0	1	1	2	...	3	0	1	1	1	0	0	1	5	0
9996	20250519131652	0	1	8	1	1	0	1	1	2	...	0	1	1	0	1	1	0	1	0	1
9997	20250518004124	0	2	0	0	1	0	2	1	0	...	0	1	1	0	3	1	1	1	2	1
9998	20250405154854	0	3	8	2	1	2	2	1	2	...	1	1	1	1	1	0	2	0	3	1
9999	20250331135527	0	1	10	3	0	0	1	1	2	...	2	1	1	1	2	1	1	0	0	1

10000 rows × 123 columns

Рис. 7. Наборы признаков в преобразованном датасете

К полученному датасету в соответствии с алгоритмом последовательно применены методы машинного обучения: деревья решений, К-ближайших соседей, наивный Байесовский классификатор, опорных векторов, случайный лес, линейный дискриминантный анализ, многослойный перцептрон, логистическая регрессия. Дополнительно для оценки качества моделей использовалась кросс-валидация. Результаты обучения классификаторов приведены на Рисунке 8.

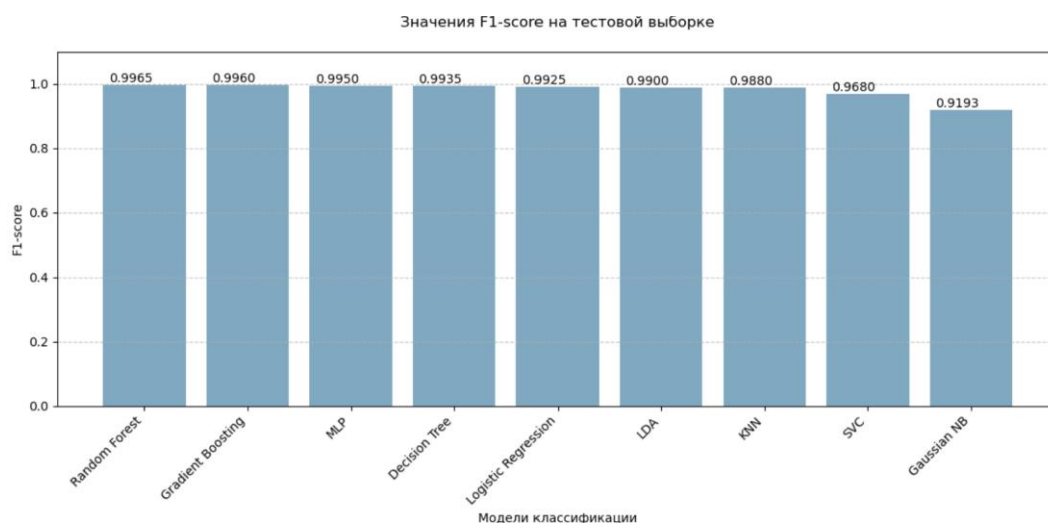


Рис. 8. Результаты обучения классификаторов

Как видно из представленных графиков, лучшие результаты из рассмотренных алгоритмов на заданном наборе данных показал алгоритм классификации «случайный лес» (Random Forest).

Для оценки результатов работы разработанной модели составим и проанализируем матрицу ошибок, приведенную на Рисунке 9.

Всего рассматривалось 2000 объектов. Как видно из указанной матрицы, классификатор верно отнес к классу 1 (компьютерные атаки) 1026 объектов, к классу 0 (легитимные действия пользователей) 968 объектов. Классификатор ошибочно отнес к классу компьютерных атак 4 легитимных действия пользователей, а также 2 кибератаки классифицировал как легитимное действие.

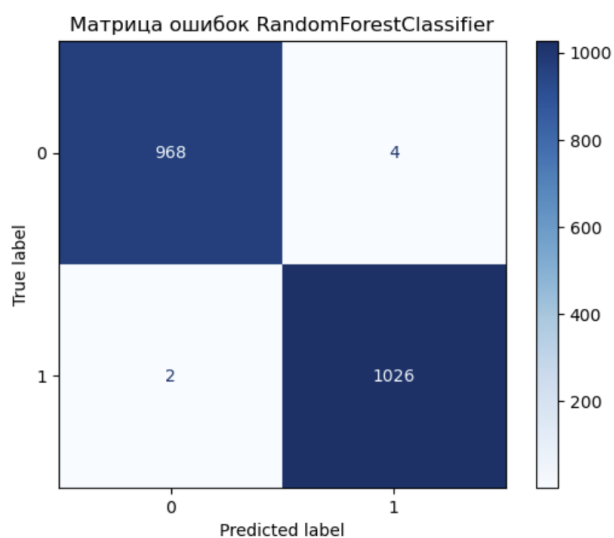


Рис. 9. Матрица ошибок для разработанной модели

Для оценки работы классификатора проведено детальное изучение ошибочных предсказаний. Ложноотрицательные предсказания с вероятностью 40% и 29% относятся к технике T1218, в рамках которой эксплуатируются легитимные исполняемые файлы, что затрудняет выявление такого рода компьютерных атак.

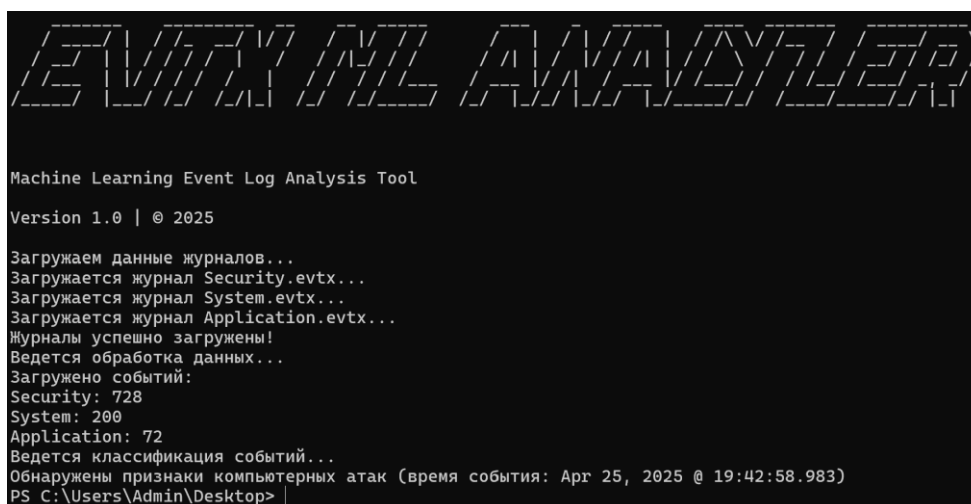
Ложноположительные предсказания касаются двух видов пользовательской активности – офисная работа (вероятность 56%) и работа с веб-приложениями (вероятности 67%, 98% и 77%). Ошибки классификатора связаны с загрузкой файлов и запуском новых процессов в ходе работы в Интернет-браузере.

Итог работы классификатора составил 0,9965, что является высоким результатом, который можно использовать в практической деятельности по выявлению признаков компьютерных атак.

Классификаторы, обученные на сетевом трафике, приведенные в Таблице 1, демонстрируют максимальный результат 0,9279. **Улучшение составляет более 6 %.**

Сигнатурное выявление компьютерных атак по системным журналам дает результат 0,9165. **Улучшение составляет 8 %.**

На базе обученной модели машинного обучения разработано консольное приложение `evtx_ml_analyzer.py`, которое позволяет анализировать файлы системных событий операционной системы Windows, а также выводит информацию о наличии признаков компьютерных атак. Общий вид интерфейса приложения приведен на Рисунке 10.



```

Machine Learning Event Log Analysis Tool
Version 1.0 | © 2025

Загружаем данные журналов...
Загружается журнал Security.evtx...
Загружается журнал System.evtx...
Загружается журнал Application.evtx...
Журналы успешно загружены!
Ведется обработка данных...
Загружено событий:
Security: 728
System: 200
Application: 72
Ведется классификация событий...
Обнаружены признаки компьютерных атак (время события: Apr 25, 2025 @ 19:42:58.983)
PS C:\Users\Admin\Desktop>

```

Рис. 10. Интерфейс программы `evtx_ml_analyzer.py`

Предложенная методика и программный продукт прошли оценку специалистами центра ГосСОПКА на базе ООО «Информационный центр» и внедрены при расследовании компьютерных инцидентов. Получена справка о внедрении.

Проведен сравнительный анализ разработанного приложения с имеющимися аналогами - инструментами `Python_Evtx_Analyzer`, `evtx_detector`.

Работа указанных программ проверена с помощью репозитория журналов операционной системы EVTX-ATTACK-SAMPLES, а также иные наборы журналов, находящиеся в открытом доступе.

Всего проверено 100 различных журналов. Сравнительная характеристика представленных приложений, а также результаты их работы по выявлению атак в Таблице 4.

Таблица 4. Сравнительный анализ приложений

Название	Интерфейс	Метод обнаружения атак	Детализация	Пакетная загрузка	Неизвестные атаки	Количество выявленных атак (из 100)
evtx_ml_analyzer	CLI	машинное обучение	Низкая	Да	Да	96
Python_Evtx_Analyzer	CLI	сигнатурный	Высокая	Да	Нет	82
evtx_detector	CLI	сигнатурный	Средняя	Нет	Нет	89

Достоверность результатов, полученных в ходе исследования и разработки модели машинного обучения для выявления компьютерных атак, подтверждается комплексным подходом к валидации, включающим следующие аспекты:

1. Статистическая значимость и высокая точность модели.

Результаты оценивались на репрезентативной выборке, содержащей 2000 объектов. Матрица ошибок демонстрирует высокие показатели качества классификации;

2. Интерпретируемость и обоснованность ошибок модели.

Проведен детальный анализ ошибочных предсказаний. Для каждой ошибки идентифицирована конкретная сессия, определен вид активности и получена предсказанная моделью вероятность.

3. Объективность валидации на независимых данных.

Для сравнительного анализа разработанного приложения evtx_ml_analyzer использовался публичный набор данных EVTX-ATTACK-SAMPLES, содержащий журналы с известными атаками, а также дополнительные журналы из открытых источников. Тестирование проводилось на 100 независимых файлах журналов, что обеспечивает объективность оценки.

4. Практическое внедрение и экспертиза.

Разработанный на базе модели программный продукт прошел апробацию и внедрен в практическую деятельность специалистами центра ГосСОПКА ООО «Информационный центр». Факт внедрения подтвержден официальной справкой.

5. Сравнение с прямыми аналогами.

Проведено прямое сравнительное тестирование с существующими инструментами (Python_Evtx_Analyzer, evtx_detector), работающими в той же предметной области (анализ EVTX-журналов). Превышение показателя обнаружения на 7–14% при равных условиях тестирования является статистически значимым и доказывает преимущество подхода на основе машинного обучения в данной задаче.

В заключении приведены итоги выполненного исследования, рекомендации, перспективы дальнейшей разработки темы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В результате выполненного исследования в области разработки способа интеллектуального способа выявления компьютерных атак по журналам операционной системы достигнута поставленная цель. Получены следующие основные результаты:

1. Разработана методика выявления компьютерных атак с использованием алгоритмов машинного обучения при обработке системных событий операционной системы, основанная на требованиях стандартов Российской Федерации ГОСТ серии 59709-59712.

2. Разработана формальная модель компьютерных атак и легитимных действий пользователей, которая позволяет выявлять компьютерные атаки с использованием системных событий операционной системы. Предложенная модель может быть переиспользована для отечественных операционных систем в рамках политики импортозамещения.

3. Разработан алгоритм моделирования компьютерных атак и формирования набора данных из системных событий операционной системы, в результате применения которого в 4 раза расширен перечень выявляемых тактик согласно матрице MITRE ATT&CK по сравнению с известными работами. Согласно разработанному алгоритму собран размеченный набор данных из записей системных событий операционной системы.

4. Проведена апробация разработанной методики выявления признаков компьютерных атак и оценка эффективности полученных моделей. В результате работы получен классификатор, который позволяет с точностью 0,9965 выявлять признаки компьютерных атак по записям системных журналов операционной системы. Данный результат более чем на 6 % превосходит точность работы классификаторов, обученных на сетевом трафике, а также на 8% выше результатов сигнатурного анализа.

5. Разработано консольное программное средство `evtx_ml_analyzer.py`, которое позволяет анализировать файлы системных событий операционной системы, а также выводит информацию о наличии признаков компьютерных атак. Проведен сравнительный анализ приложения с известными аналогами. Приложение продемонстрировало максимальный результат, успешно выявив 96 из 100 компьютерных атак.

6. Предложенная методика и программный продукт прошли апробацию специалистами центра ГосСОПКА на базе ООО «Информационный центр» и используются при расследовании компьютерных инцидентов. Получена справка о внедрении.

7. Разработанные в рамках исследования подходы к анализу данных внедрены в учебный процесс департамента информационной безопасности ИМКТ ДВФУ в рамках курса «Интеллектуальные информационные системы», позволяет студентам ознакомиться с различными методами машинного обучения для решения задач в области кибербезопасности. Получена справка о внедрении.

Дальнейшие исследования по теме диссертации направлены на разработку многоклассового классификатора, способного определить конкретный вид атаки или пользовательского действия, а также проведение дополнительных экспериментов по применению предложенной методики к отечественным операционным системам в рамках политики импортозамещения.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ РАБОТЫ

Статьи в ведущих рецензируемых журналах, рекомендованных Высшей аттестационной комиссией (ВАК) для публикации результатов кандидатских и докторских диссертационных работ:

1. Павлычев А. В., Солдатов К. С., Сказин В. А. Выявление сетевых аномалий в системных журналах операционной системы Microsoft Windows с использованием методов машинного обучения // Доклады Томского государственного университета систем управления и радиоэлектроники. 2021. Т. 24. №. 4. С. 27-32.
2. Павлычев А.В., Стародубов М.И., Галимов А.Д. Использование алгоритма машинного обучения Random Forest для выявления сложных компьютерных инцидентов // Вопросы кибербезопасности. 2022. Т.51. № 5. С. 74-81.
3. Павлычев А.В., Стародубов М.И., Галимов А.Д. Модель функционирования вредоносного программного обеспечения на основе анализа системных журналов операционной системы Microsoft Windows // Прикаспийский журнал: управление и высокие технологии. 2022. Т.66. № 4. С. 24-31.
4. Павлычев А.В., Кузьминец К.В. Выявление фишинговых интернет-доменов с помощью алгоритмов машинного обучения в режиме потоковой обработки данных // Вопросы кибербезопасности. 2025. Т.66. № 2. С. 141-153.
5. Павлычев А.В., Кузьминец К.В., Бреус Д.Е., Шелупанов А.А. Формирование размеченного набора данных на основе смоделированных компьютерных атак // 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 // 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 // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2026. № 1. С. 159–169.

В других изданиях, сборниках трудов и тезисов конференций:

8. Павлычев А. В., Сказин В. А. Выявление сетевых аномалий в файлах журналов методами машинного обучения // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации. 2020. С. 175-179.

9. Pavlychev A. V., Skazin V. A., Zotov S. S. Detection of network anomalies in log files using machine learning methods // IOP Conference Series: Materials Science and Engineering. IOP Publishing. 2021. Vol. 1069. No. 1. P. 012021.

10. Павлычев А.В., Стародубов М.И. Анализ системных журналов в задаче выявления вредоносного программного обеспечения // Материалы XVIII Всероссийской научно-практической конференции (в рамках IX Пленума регионального отделения Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» по Сибирскому и Дальневосточному федеральным округам (СибРОУМО)). 2022. С. 176-183.

11. A.V. Pavlychev at al. Automated Collection And Marking Of Operating System Log Entries In The Task Of Detecting Computer Attacks // Advances in Automation VII. RusAutoCon 2025. Lecture Notes in Electrical Engineering. 2025. Vol. 1521. P. 266–276.

Свидетельства о государственной регистрации программы для ЭВМ и баз данных:

12. 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.