

УДК 004.056.5

doi: 10.15622/rcai.2025.074

## ПРИМЕНЕНИЕ МЕТОДОВ КЛАССИФИКАЦИИ И КЛАСТЕРИЗАЦИИ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Мешков (*meshkov.av@itmo.ru*)

Национальный исследовательский университет ИТМО,  
Санкт-Петербург

В данной статье рассматриваются способы борьбы с растущей сложностью киберугроз путем разработки методов и алгоритмов для расследования инцидентов безопасности в операционных системах Windows и Linux. Используя фреймворк MITRE ATT&CK, предлагаемый подход облегчает сопоставление событий безопасности с соответствующими тактиками, техниками и процедурами атакующих, позволяя проводить структурированную классификацию и кластеризацию. Для оптимизации анализа событий применяются передовые методы предварительной обработки и алгоритмы машинного обучения, что значительно сокращает время обработки и сохраняет точность анализа. Экспериментальные оценки подтверждают эффективность использования фреймворка в повышении возможностей обнаружения и реагирования на инциденты информационной безопасности (ИБ). Будущие направления исследований включают совершенствование производительности алгоритмов и адаптацию фреймворка к возникающим проблемам кибербезопасности.

**Ключевые слова:** инциденты ИБ, MITRE ATT&CK, машинное обучение.

### Введение

Возрастающая сложность киберугроз обуславливает необходимость разработки современных методов расследования инцидентов информационной безопасности. Традиционные подходы к обеспечению защиты информационных систем оказываются недостаточно эффективными в условиях постоянно эволюционирующих тактик злоумышленников, эксплуатирующих уязвимости как в сетевой инфраструктуре, так и в операцион-

ных системах. Это актуализирует потребность в применении передовых технологий, обеспечивающих более высокую точность и оперативность обнаружения и анализа событий информационной безопасности.

В современных условиях особую значимость приобретает применение методов машинного обучения, обеспечивающих интеллектуальную поддержку процессов анализа и интерпретации событий информационной безопасности. Алгоритмы классификации позволяют автоматически отнести каждое событие к определённой категории, соответствующей конкретной технике или стадии атаки, что существенно ускоряет первичную фильтрацию и приоритизацию инцидентов. В то же время кластеризация предоставляет возможность выявления структурных связей между событиями, обнаружения аномалий и ранее неизвестных сценариев атак. Комбинированное применение этих методов позволяет реализовать более гибкий, адаптивный и масштабируемый подход к расследованию инцидентов, особенно в условиях кроссплатформенной среды и ограниченных временных ресурсов на реагирование.

В исследовании рассматриваются методы и алгоритмы, направленные на автоматизацию процессов расследования инцидентов информационной безопасности в информационных системах. Основное внимание уделено снижению времени анализа событий при сохранении глубины и строгости оценки. В качестве концептуальной основы используется фреймворк MITRE ATT&CK, позволяющий соотносить регистрируемые события с конкретными тактиками и техниками атак, что обеспечивает формализованный и воспроизводимый подход к расследованию.

## 1. Методы

На начальном этапе осуществляется систематизированный сбор данных о событиях информационной безопасности, в результате которого формируется выборка, включающая разнородные события, зафиксированные в операционных системах Windows и Linux. Данные агрегируются из нескольких источников, что позволяет обеспечить репрезентативность и разнообразие выборки – от штатной активности до потенциально вредоносного поведения. Целью данного этапа является формирование достоверного и полноценно размеченного набора данных, пригодного для разработки, обучения и тестирования алгоритмов обнаружения атак, при этом обеспечивается охват широкого спектра событий, типичных для различных операционных сред.

Формально такой набор можно описать следующим образом:

$$D = \{E_i | i = 1, \dots, N\}, \quad (1.1)$$

где  $E_i$  – отдельное событие с множеством связанных атрибутов, а  $N$  – общее количество событий в наборе данных.

На следующем этапе производится сопоставление каждого события в  $D$  с соответствующими тактиками и техниками из матрицы MITRE ATT&CK. Это позволяет осуществить формализованную классификацию событий в соответствии с известными ТТР (Tactics, Techniques, and Procedures), обеспечивая содержательную разметку выборки с привязкой к моделям поведения злоумышленников.

Пусть  $T$  – множество всех тактик и техник из MITRE ATT&CK, где каждый элемент  $t \in T$  представляет конкретную технику или тактику. Тогда для каждого события  $E_i$  определяется функция  $f: E_i \rightarrow T \in T$  соответствующая  $E_i$  и паре "тактика-техника"  $t_{ij}$ , что в результате:

$$f(E_i) = t_{ij}, t_{ij} \in T, \quad (1.2)$$

где  $t_{ij}$  – пара "тактика-техника", соответствующая конкретному событию  $E_i$ . Такое отображение позволяет установить семантическую связь между событиями и известными векторами атак, что является основой для последующего обучения классификационных и кластеризационных моделей.

После аннотирования набора данных метками, соответствующими техникам и тактикам MITRE ATT&CK, проводится этап предварительной обработки, направленный на подготовку данных к применению алгоритмов машинного обучения. Предобработка включает нормализацию, фильтрацию и преобразование признаков, что позволяет повысить пригодность данных для задач классификации и кластеризации. Для каждого события  $E_i$  формируется вектор признаков  $x_i$ , который проходит преобразование, обеспечивающее нулевое среднее значение и единичную дисперсию признаков:

$$x'_i = \frac{x_i - \mu}{\sigma}. \quad (1.3)$$

где  $\mu$  – среднее значение, а  $\sigma$  – стандартное отклонение соответствующего вектора признаков. Проведение такой нормализации критически важно для корректного функционирования алгоритмов, чувствительных к масштабам данных, например, опирающихся на евклидовы расстояния.

После завершения предобработки набор данных подвергается анализу с использованием методов машинного обучения для решения задач классификации и кластеризации.

В рамках классификации используется следующее обучение: каждому событию  $E_i$ , представленному вектором признаков  $x_i$ , сопоставляется метка  $y_i$ , отражающая соответствующую технику атаки. Целью классификатора  $h$  является минимизация функции потерь  $L$ , измеряющей отклонение между предсказанным значением  $h(x_i)$  и фактической меткой  $y_i$ :

$$\min_h \sum_{i=1}^N L(h(x_i), y_i). \quad (1.4)$$

В качестве классификаторов могут использоваться алгоритмы, такие как деревья решений, машины опорных векторов (SVM), нейронные сети и другие модели обучения.

Для кластеризации применяются различные методы обучения, например, алгоритм k-средних (k-means) или иерархическая кластеризация. Целью является разбиение множества событий на кластеры  $C_1, C_2, \dots, C_k$  таким образом, чтобы суммарное внутрикластерное расстояние до центров кластеров было минимизировано:

$$\sum_{j=1}^k \sum_{x \in C_j} \|x - \mu_j\|^2, \quad (1.5)$$

где  $\mu_j$  – центр (среднее значение) кластера  $C_j$ . Такое разбиение позволяет выделять группы схожих событий и обнаруживать аномальные кластеры, потенциально указывающие на скрытые угрозы.

Совокупное применение методов классификации и кластеризации формирует основу предлагаемой концепции автоматизированного анализа событий информационной безопасности, обеспечивая как сопоставление с известными шаблонами атак, так и выявление новых векторов угроз в ИТ-инфраструктурах.

## 2. Результаты

Сформированный набор данных включает  $N = 10000$  событий информационной безопасности, собранных из операционных систем Windows и Linux. Он охватывает широкий спектр как нормальной, так и аномальной активности. Каждое событие  $E_i$  было аннотировано соответствующими тактиками и техниками на основе матрицы MITRE ATT&CK, что обеспечило содержательную разметку для последующего анализа. В табл. 1 представлено распределение событий по категориям.

Таблица 1

Категория	Количество событий	Доля, %
Нормальная активность	6000	60
Подозрительная активность	2500	25
Подтверждённые угрозы	1500	15
Итого	10000	100

На этапе предварительной обработки были нормализованы все векторы признаков, что обеспечило единообразие представления данных и корректность их интерпретации алгоритмами. Среднее время предобработки одного события составило 0,01 секунды, что подтверждает масштабируемость решения для больших объёмов данных.

К полученному набору применялись как методы контролируемого обучения (для классификации), так и неконтролируемого обучения (для кластеризации). В табл. 2 приведены сравнительные характеристики эф-

фektivности трёх моделей классификации по метрикам: точность (accuracy), полнота (recall), прецизионность (precision) и среднее время обработки одного события.

Таблица 2

Модель	Точность, %	Прецизионность (Precision), %	Полнота, %	Время обработки (мс)
Дерево решений	92,4	91,2	90,8	12,5
Машина опорных векторов	95,6	94,7	94,2	22,3
Нейронная сеть	97,3	96,8	96,5	35,6

Наилучшие результаты по точности классификации продемонстрировала нейронная сеть, достигшая значения 97,3%, однако при этом характеризующаяся более высоким временем обработки одного события по сравнению с другими моделями.

Для выявления скрытых закономерностей и групп схожих событий в наборе данных была проведена кластеризация без учителя. В качестве основного метода использовался алгоритм k-средних (k-means). Результаты кластерного анализа представлены на рис. 1, где отчётливо прослеживается разделение аномальных событий от рутинной активности, что существенно упрощает идентификацию потенциальных угроз информационной безопасности и способствует более целенаправленному анализу инцидентов.

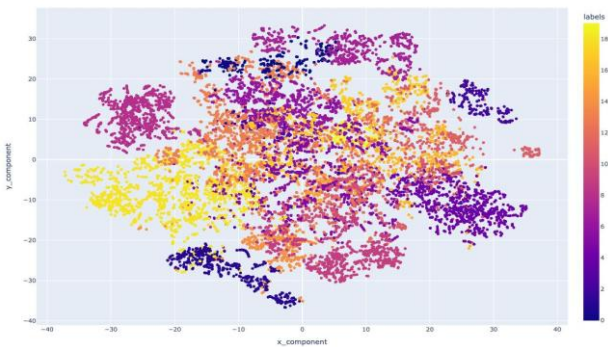


Рис. 1. Результаты кластеризации событий информационной безопасности с использованием алгоритма K-Means

Предложенные в работе методы обеспечили существенное повышение эффективности обработки событий информационной безопасности. Применение алгоритмов машинного обучения, особенно нейросетевых моде-

лей, позволило достичь высокой точности классификации и надёжного выявления атакующих действий. В свою очередь, методы кластеризации продемонстрировали способность эффективно группировать схожие события, что способствует идентификации потенциальных шаблонов атак и аномального поведения.

В совокупности полученные результаты подтверждают результативность предложенного фреймворка в задаче оптимизации процессов расследования инцидентов в информационных системах.

## **Заключение**

Предложенные методы и алгоритмы значительно повысили эффективность обработки событий информационной безопасности. За счёт применения технологий машинного обучения среднее время анализа одного события было снижено приблизительно на 60 % по сравнению с традиционными методами ручного анализа. Этот прирост производительности обусловлен автоматизированной классификацией и кластеризацией, которые существенно упрощают идентификацию критических инцидентов и снижают когнитивную нагрузку на аналитиков.

Дополнительный вклад в точность и стабильность результатов вносит этап предварительной обработки, включающий нормализацию и извлечение признаков. Это обеспечило согласованность и надёжность входных данных, что позволило алгоритмам машинного обучения функционировать с высокой точностью. Структурированный подход к формированию выборки также способствовал беспрепятственной интеграции событий, поступающих из различных источников – как из систем Windows, так и Linux – продемонстрировав гибкость и адаптивность фреймворка в условиях гетерогенной ИТ-среды.

Интеграция алгоритмов классификации и кластеризации в единый аналитический контур позволила значительно оптимизировать процесс расследования инцидентов. Модели классификации обеспечили точное определение типа события, что, в свою очередь, способствовало оперативной приоритизации инцидентов с высоким уровнем риска. Так, нейросетевая модель достигла точности 97,3 %, продемонстрировав высокую надёжность при анализе сложных атакующих сценариев.

Кластеризационные алгоритмы дополнили классификационный анализ, обеспечив выявление скрытых закономерностей и аномальных паттернов поведения в больших объёмах данных. Полученные аналитические сведения способствовали идентификации потенциальных векторов атак, снижая вероятность пропуска критичных угроз. Совместное использование методов контролируемого и неконтролируемого обучения расширило аналитические возможности системы, одновременно повысив её общую эффективность за счёт сокращения объёмов дублирующего анализа и более целенаправленного реагирования.

Разработанный фреймворк продемонстрировал высокую результативность в обнаружении продвинутых киберугроз, включая сложные техники и тактики, формализованные в MITRE ATT&CK. Сопоставление событий с конкретными элементами этой матрицы позволило получить детализированное представление о потенциальных траекториях атаки, что повысило точность и полноту детектирования.

Оценочные метрики, такие как точность, прецизионность и полнота, подтвердили способность решений эффективно различать легитимную и вредоносную активность. В частности, алгоритм машин опорных векторов (SVM) продемонстрировал уровень полноты 94,2 %, что указывает на высокую чувствительность к настоящим позитивным срабатываниям. Алгоритмы кластеризации выявили аномальные кластеры, коррелирующие с известными векторами атак, тем самым подтвердив способность модели выявлять новые и возникающие угрозы.

В целом, предложенные методы и алгоритмы не только повысили скорость и точность обработки событий, но и усилили аналитические и диагностические возможности систем реагирования на инциденты. Полученные результаты позволяют рассматривать данный фреймворк как масштабируемое, адаптируемое и перспективное решение для противодействия растущей сложности киберугроз в условиях современной ИТ-инфраструктуры.

### Список литературы

- [**Stouffer, 2011**] Stouffer K., Falco J., Scarfone K. Guide to Industrial Control Systems (ICS) Security // NIST Special Publication. – 2011. – 800-82. – P. 800-882.
- [**Soares, 2023**] Soares L. The evolution of cyber threats and its future landscape. – 2023.
- [**Shrestha, 2019**] Shrestha A., Mahmood A. Review of Deep Learning Algorithms and Architectures // IEEE Access. – 2019. – P. 1-1. – doi: 10.1109/ACCESS.2019.2912200.
- [**Scarfone, 2007**] Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS) // NIST Special Publication. – 2007. – 800-94.
- [**Abdelwahab, 2024**] Abdelwahab I., Hefny H., Darwish N. Enhancing cybersecurity defenses: a multicriteria decision-making approach to MITRE ATT&CK mitigation strategy // arXiv. 2024. – doi: 10.48550/arXiv.2407.19222.