УДК УДК 004.056.5
DOI: http://dx.doi.org/10.21686/1818-4243-2025-1-65-76

Д.А. Евдокимова, А.А. Микрюков

Российский экономический университет им. Г.В. Плеханова, Москва, Россия

Задача детектирования недопустимых событий информационной безопасности в информационной инфраструктуре

Целью исследования *является разработка усовершенствованного подхода к решению задачи детектирования недопустимых событий в области информационной безопасности для повышения точности обнаружения инцидентов и снижения числа ложных срабатываний. Недопустимым событием является событие в результате кибератаки, делающее невозможным достижение стратегических целей организации или приводящее к значительному нарушению ее основной деятельности. В основе предложенного решения задачи детектирования недопустимых событий лежит нейросетевой классификатор, обученный на данных о недопустимых событиях, таких как атрибуты, прекурсоры и индикаторы компрометации недопустимых событий. Данное решение обеспечивает всесторонний анализ событий и снижение вероятности пропуска недопустимых событий, что делает его актуальным для защиты критической информационной инфраструктуры.*

Актуальность данного исследования обусловлена быстрым ростом количества и сложности кибератак, а также необходимостью внедрения автоматизированных методов детектирования угроз, сопровождающимися недопустимыми событиями, которые приводят к негативным последствиям. В условиях увеличивающейся сложности киберугроз и многообразия атак традиционные методы обнаружения становятся недостаточно эффективными, что требует совершенствование существующих технологий для защиты информационных систем.

Новизна разработанных предложений заключается в повышении точности детектирования недопустимых событий за счет использования методов машинного обучения и нейросетевого классификатора, а также сокращении времени реагирования с использованием инструмента сбора, обработки, агрегирования и визуализации Elastic Stack.

Материалы и методы исследования. *Для решения задачи детектирования недопустимых событий использован инструмент Elastic Stack, обеспечивающий сбор, агрегацию и визуализацию данных о событиях. Основным инструментом анализа является нейросетевой классификатор, обученный на наборе атрибутов, прекурсоров и индикаторов компрометации недопустимых событий. Методы исследования включают применение механизмов корреляции событий, анализа аномалий и машинного обучения, которые интегрируются в единую систему.*

Результаты: *предложено решение задачи детектирования недопустимых событий, основанное на применении выявленных атрибутов, прекурсоров и индикаторов компрометации недопустимых событий информационной безопасности.*

Заключение: *выявленные атрибуты, прекурсоры и индикаторы компрометации недопустимых событий обеспечивают решение задачи детектирования недопустимых событий. Применение предложенного решения способствует совершенствованию защиты информационных систем и снижению рисков, связанных с кибератаками, что особенно важно для обеспечения безопасности критической информационной инфраструктуры.*

Ключевые слова: информационная безопасность, детектирование недопустимых событий, машинное обучение, аномальный анализ, сигнатурный анализ, нейросетевой классификатор, атрибуты недопустимых событий.

Darya A. Evdokimova, Andrei A. Mikryukov

Plekhanov Russian University of Economics, Moscow, Russia

The Task of Detecting Unacceptable Information Security Events in the Information Infrastructure

The purpose of the study *is to develop an advanced approach to solving the task of detecting unacceptable events in the field of information security to improve incident detection accuracy and reduce the number of false positives. An unacceptable event is defined as an event resulting from a cyberattack that either makes it impossible to achieve the strategic goals of an organization or significantly disrupts its core activities. The proposed solution for detecting unacceptable events is based on a neural network classifier trained on data related to unacceptable events, including attributes, precursors, and compromise indicators of unacceptable events. This solution provides comprehensive event analysis and reduces the likelihood of missing unacceptable events, making it particularly relevant for protecting critical information infrastructure.*

The relevance of the study is driven by the rapid increase in the number and complexity of cyberattacks and the necessity to implement automated threat detection methods associated with unacceptable events that lead to negative consequences. As cyber threats grow more complex and diverse, traditional detection methods are becoming increasingly ineffective, necessitating improvements in existing technologies to protect information systems.

The novelty of the proposed solutions lies in improving the accuracy of detecting unacceptable events through the use of machine learning methods and a neural network classifier, as well as reducing response time by utilizing the Elastic Stack tool for data collection, processing, aggregation, and visualization.

Materials and methods. *To address the task of detecting unacceptable events, the Elastic Stack tool was employed, enabling the collection, aggregation, and visualization of event data. The primary analytical tool is a neural network classifier trained on a set of attributes, precursors, and compromise indicators of unacceptable events. The research methods include the application of event correlation mechanisms, anomaly analysis, and machine learning, all integrated into a unified system.*

Results. *A solution for detecting unacceptable events was proposed, based on the use of identified attributes, precursors, and compromise indicators of unacceptable information security events.*

Conclusion. *The identified attributes, precursors, and compromise indicators of unacceptable events provide an effective solution for detecting such events. The application of the proposed solution contributes to improving the protection of information systems and reducing risks associated with cyberattacks, which is particularly critical for ensuring the security of critical information infrastructure.*

Keywords: information security, detection of unacceptable events, machine learning, anomaly analysis, signature analysis, neural network classifier, attributes of unacceptable events.

Введение

Современные системы информационной безопасности требуют высокоэффективных решений для предотвращения кибератак, утечек данных и других угроз. Одной из ключевых задач является детектирование недопустимых событий, поскольку их своевременное выявление способствует снижению негативных последствий, которые могут произойти в результате компьютерных инцидентов [1]. В статье [2] негативные последствия рассматриваются как нарушения, которые войдут в реестр недопустимых нарушений кибербезопасности.

Для решения указанной задачи все более актуальными становятся методы машинного обучения и нейросетевые модели, которые позволяют обнаруживать аномалии и недопустимые события в режиме реального времени. Кибератаки и утечки данных требуют оперативного реагирования, однако их обнаружение часто затруднено из-за большого объема данных и разнообразия угроз. В статье рассмотрены вопросы детектирования недопустимых событий на основе использования машинного обучения и нейросетевых моделей для детектирования недопустимых событий, что позволяет обрабатывать данные в режиме реального времени и значительно повышает эффективность информационной безопасности.

Для сбора и анализа данных о недопустимых событиях, происходящих в различных компонентах информационной инфраструктуры, таких как серверы, сетевые устройства, базы данных, используются SIEM-системы [3]. Для выявления недопустимых событий с учетом их интенсивности в реальном масштабе времени необходимо использовать SIEM-системы нового поколения [4]. Внедрение SIEM-систем нового поколения, которые отличаются высокой масштабируемостью, отказоустойчивостью и способностью к потоковой обработке данных в режиме реального времени, позволяет системам безопасности не только собирать и хранить данные, но и анализировать их для выявления сложных инцидентов. Применение технологий больших данных и потоковой обработки обеспечивает оперативное выявление угроз и реагирование на них.

Время реагирования специалистов по информационной безопасности традиционно связано с завершением или активной фазой кибератаки, когда последствия уже начали проявляться, а негативные последствия уже оказывают влияние на информационную систему. Детектирование недопустимых событий с применением прекурсоров, индикаторов компрометации и атрибутов, позволяет существенно сместить временную шкалу реагирования на более ранние этапы.

Данный подход обеспечивает возможность упреждающего обнаружения потенциальных угроз, что позволяет предотвратить развитие атаки до её реализации. Прекурсоры, как признаки возможных угроз, предоставляют аналитикам возможность выявить ранние сигналы подготовки атаки, а индикаторы компрометации и атрибуты позволяют уточнить характер и контекст угрозы. Таким образом, временной промежуток между обнаружением угрозы и реагированием существенно сокращается, что обеспечивает снижение вероятности нанесения ущерба.

Анализ существующих методов детектирования недопустимых событий информационной безопасности

Детектирование недопустимых событий подразумевает технологический процесс автоматического обнаружения инцидентов или аномалий в информационной системе с помощью программных и аппаратных средств. Этот процесс включает [5]:

1. Использование специальных систем (например, IDS/IPS, SIEM-систем) для мониторинга и анализа сетевого трафика, логов и действий пользователей.

2. Применение алгоритмов (сигнатурных, поведенческих, машинного обучения) для автоматического обнаружения событий, которые нарушают нормальную работу системы или указывают на кибератаки.

Выявление недопустимых событий является важнейшей частью обеспечения безопасности информационных систем, поскольку позволяет своевременно обнаруживать и предотвращать инциденты, которые могут привести к утечке данных, нарушению конфиденциальности или даже к полному отказу системы. К недопустимым событиям относятся аномальное поведение систем, неожиданные изменения конфигураций, несанкционированный доступ к данным и другие подозрительные активности.

В современных условиях количество и сложность кибератак постоянно увеличиваются, что делает критически важным выявление и детектирование недопустимых событий на ранних стадиях. Основной задачей является минимизация времени между обнаружением угрозы и началом реагирования чтобы атакующий не успел реализовать атаку.

Проблемы выявления недопустимых событий в информационной безопасности связаны с техническими, организационными и человеческими факторами. Эти проблемы могут осложнять процесс идентификации угроз и приводить к снижению эффективности систем безопасности. В табл. 1 приведены результаты анализа основных проблем, с которы-

Таблица 1 Table 1

Проблемы выявления недопустимых событий
Problems in detecting unacceptable events

№ п/п	Наименование проблемы выявления недопустимых событий	Причины/описание данной проблемы
1.	Большие объемы данных	Необходимость фильтрации шумов (незначительных или не связанных с безопасностью событий). Сложность выявления действительно критичных событий среди большого числа записей.
2.	Ложноположительные срабатывания	Некорректная настройка систем безопасности. Недостаточная точность алгоритмов машинного обучения или методов аномалий. Ошибки в корреляции событий.
3.	Ложноотрицательные срабатывания	Недостаточная чувствительность механизмов детектирования. Сложные атаки, которые маскируются под нормальные действия. Использование вредоносных инструментов, которые еще не классифицированы системами защиты.
4.	Сложность современных атак	Атаки «нулевого дня» (неизвестные уязвимости). Атакующие, использующие легитимные учетные данные. Целенаправленные атаки (APT), так как традиционные методы обнаружения на основе сигнатур и простого мониторинга могут оказаться неэффективными.
5.	Неадекватные или устаревшие средства мониторинга	Неспособность анализировать сложные сетевые потоки данных. Пропуск более изощренных атак. Ограничение возможностей масштабируемости по мере роста информационной инфраструктуры.
6.	Отсутствие квалифицированных кадров	Задержки в реагировании на инциденты. Ошибки в настройке и управлении системами безопасности.
7.	Инсайдерские угрозы	Отсутствие контроля за внутренними действиями пользователей. Недостаточные меры по выявлению аномалий в поведении сотрудников.
8.	Корреляция событий	Большое количество источников данных (различные устройства, приложения, сети). Неполнота данных, что затрудняет правильную интерпретацию событий. Трудности в создании правильных правил корреляции, которые бы учитывали контекст событий и предсказывали потенциальные угрозы.
9.	Динамическая природа информационной среды	Старые правила и настройки мониторинга могут не быть актуальными для новых конфигураций. Вредоносные действия могут маскироваться под легитимные изменения в сети.
10.	Сложности интеграции различных инструментов безопасности	Недостаточная видимость общей картины безопасности. Дублирование данных и усложнению анализа событий. Отсутствие единой централизованной системы для мониторинга и реагирования на инциденты.

ми сталкиваются специалисты в области информационной безопасности при выявлении недопустимых событий:

Решение вышеуказанных проблем требует применения передовых технологий, таких как машинное обучение, расширение возможностей анализа больших данных, улучшение интеграции систем безопасности и повышение квалификации сотрудников.

Чтобы успешно решить задачу выявления недопустимых событий, необходимо выявить признаки недопустимых событий и их классифицировать. Это позволяет построить эффективные системы мониторинга, анализа и реагирования на угрозы. Признаки недопустимых событий – это индикаторы, которые указывают на возможные угрозы или отклонения в работе системы [6]. Индикаторы могут проявляться в различных формах, включая аномалии в поведении пользователей, системы или сети. Ключевая задача выявления признаков заключается в их идентификации и сборе на ранних этапах возникновения.

Одним из самых сложных этапов при реагировании может являться корректное выявление и оценка потенциальных киберинцидентов, включая заключение о том, действительно ли произошел инцидент, какого он типа, каков его масштаб и опасность [7].

Для детектирования недопустимых событий информационной безопасности предлагается использовать такие признаки, как прекурсоры и индикаторы компрометации недопустимых событий. Атрибуты, являющиеся характеристиками недопустимых событий, позволяют классифицировать выявленные события.

Прекурсор представляет собой признак, указывающий на возможность возникновения недопустимого события в будущем. Примерами прекурсоров могут быть сканирование портов, обнаружение новой

уязвимости в инфраструктуре организации или активизация угроз со стороны киберггруппировок. Выявление прекурсоров позволяет предпринять превентивные меры, такие как усиление защищённости целевой системы, повышение детализации мониторинга и корректировка политики информационной безопасности. Реагирование на прекурсоры является одним из наиболее эффективных способов предотвращения реализации недопустимых событий.

Индикатор компрометации представляет собой известные данные, указывающие на то, что безопасность объекта мониторинга уже нарушена [8]. Примеры индикаторов включают алерты систем защиты информации (IDS/IPS-системы, SIEM-платформы, антивирусное ПО), зафиксированную вредоносную активность, сбои в работе систем, множественные неуспешные попытки аутентификации или сообщения от ИТ-администраторов.

В компании «Лаборатория Касперского» используется система индикаторов компрометации для обнаружения угроз на основе данных, которые указывают на наличие вредоносной активности или следов кибератак [9]. Использование системы индикаторов позволяет автоматизировать процесс мониторинга и выявления угроз, существенно сокращая время обнаружения инцидентов. Индикаторы компрометации играют важную роль в сокращении времени реагирования (TTR), так как позволяют оперативно идентифицировать активные или потенциальные атаки. Система индикаторов компрометации обеспечивает сбор и обработку данных, что повышает уровень защиты информационных систем организаций и способствует предотвращению развития кибератак на ранних стадиях их жизненного цикла.

В статье [10] автор описывает сценарий реализации недопустимого события в ИТ-инфраструктуре. Проблематика заключается в том, что при недостаточном времени реагирования на инциденты (TTR) специалисты по информационной безопасности не всегда успевают локализовать угрозу, что приводит к успешной реализации атаки и значительным негативным последствиям для информационной инфраструктуры. Важную роль играет соотношение времени атаки (TTA) – времени, необходимого атакующему для достижения своей цели, и времени реагирования. Если TTA меньше TTR, атакующий успевает реализовать свои действия до того, как специалисты начинают реагировать. Это акцентирует внимание на необходимости разработки и внедрения методов, обеспечивающих оперативное обнаружение и реагирование на кибератаки. Использование индикаторов компрометации, атрибутов и прекурсоров недопустимых событий позволяет сместить временной горизонт реагирования на более ранние этапы жизненного цикла атаки, обеспечивая, чтобы TTR был меньше TTA. Такой подход способствует предотвращению реализации угроз на начальных стадиях их развития и минимизации потенциального ущерба, рисунок 1.

Жизненный цикл атаки [11] может быть представлен в виде последовательности этапов, через которые проходит злоумышленник для достижения своих целей в рамках кибератаки, рисунок 2.

На первом этапе проводится разведка, на котором злоумышленники собирают информацию о целевой системе, её

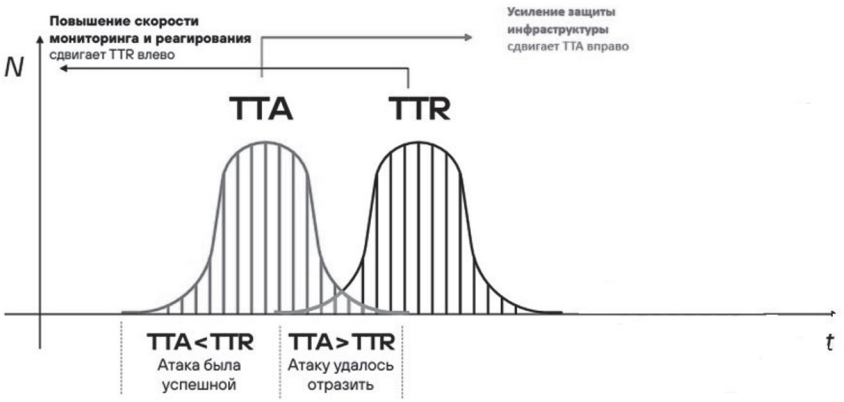

Рис. 1. Анализ времени атаки и времени реагирования, [10]
Fig. 1. Analysis of attack time and response time, [10]

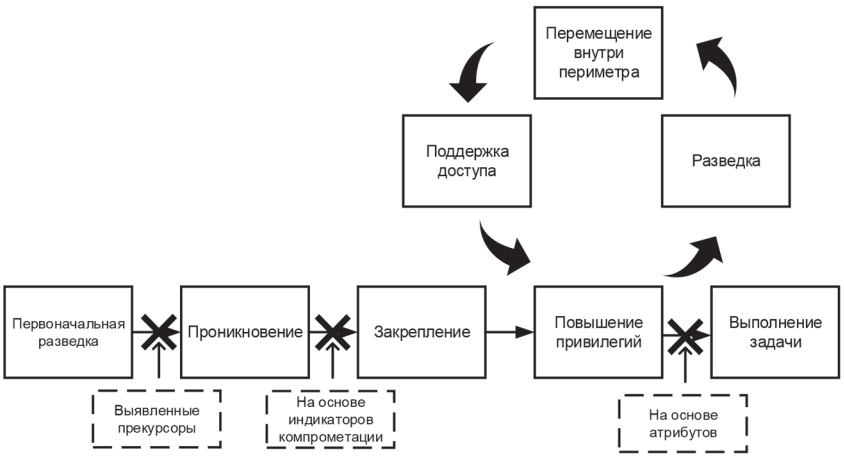

Рис. 2. Этапы реализации компьютерной атаки и ее прерывания
Fig. 2. Stages of computer attack realization and its interruption

уязвимостях и конфигурации. Этот этап закладывает основу для последующих действий атакующего. Прерывание атаки на первом этапе возможно на выявленных прекурсоров, таких как сканирование портов, попытки установления соединения с неизвестных IP-адресов или анализ периметра сети. На втором этапе – проникновении, злоумышленники получают доступ к целевой системе через уязвимости или некорректные настройки безопасности. Прерывание атаки на этом этапе возможно на основе индикаторов, таких как множественные попытки авторизации или аномалии в сетевом трафике. Закрепление является следующим этапом, на котором атакующие устанавливают механизмы для сохранения доступа к системе, например, с помощью вредоносного программного обеспечения или настройки скрытых учётных записей. Далее следует этап повышения привилегий, на котором злоумышленники получают доступ к правам администратора или другим высоким привилегиям, позволяющим управлять целевой системой. Прерывание атаки на этом этапе возможно на основе выявленных индикаторов компрометации и атрибутов, таких как изменения в конфигурации системы или запуск несанкционированных процессов. После этого атакующие переходят к выполнению задачи, которая может включать кражу данных, шифрование файлов, внедрение вредоносного кода или другие деструктивные действия. На этом этапе атака может быть завершена, если её не удалось остановить на предыдущих этапах.

Выявление различных типов признаков недопустимых событий позволяет эффективно выявлять и прерывать кибератаки на разных этапах их жизненного цикла. Прекурсоры, указывающие на потенциальные угрозы, обеспечивают возможность выявления атаки уже после этапа первоначальной разведки, предотвращая её дальнейшее развитие. Индикаторы текущей активности атакующего позволяют идентифицировать угрозу и принять меры после этапа проникновения в систему. Атрибуты, детализирующие действия атакующего, становятся ключевыми для анализа и нейтрализации угрозы после этапа повышения привилегий.

К основным признакам недопустимых событий относятся:

1. Аномальное поведение учетных записей и систем. Например, входы в систему в нехарактерное время, попытки доступа к ресурсам с неизвестных IP-адресов или необычными правами доступа.

2. Изменения конфигураций. Это несанкционированные изменения настроек системы, перезагрузки или сбои без видимых причин.

3. Аномалии в сетевом трафике. Может происходить резкое увеличение объемов трафика, использование нетипичных портов и протоколов, многократные неудачные попытки авторизации.

4. Ошибки и сбои в работе приложений. К ним относятся внезапные сбои, ошибки в работе программного обеспечения, снижение производительности серверов или систем.

5. Прекурсоры недопустимых событий. Признаки, указывающие на возможность

Рис. 3. Классификация признаков недопустимых событий

Fig. 3. Classification of signs of unacceptable events

угрозы в будущем, такие как сканирование портов, обнаружение новой уязвимости, попытки установить соединение с подозрительными IP-адресами или аномальная активность со стороны пользователей.

6. Индикаторы компрометации недопустимых событий. Признаки уже произошедших или происходящих угроз, включая сообщения от систем защиты (IDS/IPS, SIEM), множественные неудачные попытки аутентификации, вредоносную активность или сообщения об аномалиях от администраторов.

После выявления признаков недопустимых событий решается задача их классификации, чтобы оптимизировать процесс детектирования угроз и выработать стратегию реагирования на инциденты. Признаки недопустимых событий могут быть разделены на несколько категорий в зависимости от их характера и критичности.

На рисунке 3 представлена классификация недопустимых событий, основанная на Методике ФСТЭК России [12].

Признаки внешних угроз включают попытки несанкционированного доступа, DDoS-атаки, фишинговые атаки, внедрение вредоносного программного обеспечения. Эти события обычно связаны с действиями злоумышленников, которые пытаются получить доступ к системе извне.

К внутренним угрозам относят действия инсайдеров, которые могут включать умышленные или неумышленные действия сотрудников. К ним относятся несанкционированные изменения в конфигурациях, злоупотребления правами доступа, ошибки пользователей.

Признаками системных сбоев и уязвимостей являются системные сбои, вызванные ошибками в программном обеспечении, несовместимостью оборудования или перегрузками. Эти события часто связаны с техническими проблемами, но могут использоваться злоумышленниками для атак.

К критичным признакам относят события, указывающие на немедленную угрозу информационной безопасности. Например, активные попытки взлома или удаленного доступа к конфиденциальным данным.

Средние по уровню атаки могут указывать на наличие уязвимостей или потенциальные угрозы, но не требуют немедленного вмешательства. Например, множественные неудачные попытки входа или предупреждения антивирусного программного обеспечения.

Признаки осуществления низкоприоритетных атак указывают на незначительные инциденты, такие как ошибки в работе программного обеспечения или незначительные отклонения в работе системы, которые могут быть решены в плановом порядке.

Анализ показал, что существующие методы детектирования недопустимых событий, такие как использование сигнатурных и поведенческих подходов, обладают рядом ограничений, включая неспособность эффективно выявлять сложные или неизвестные угрозы. Основными проблемами являются большое количество ложноположительных и ложноотрицательных срабатываний, низкая адаптивность к новым угрозам, а также недостаточная интеграция данных из различных источников.

В статье предложено использовать усовершенствованный подход, основанный на применении нейросетевого классификатора, который анализирует атрибуты, прекурсоры и индикаторы компрометации недопустимых событий. Этот подход включает использование инструмента Elastic Stack для сбора и предварительной обработки данных, а также машинного обучения для повышения точности классификации. Предложенное решение позволяет сместить временной горизонт реагирования на более ранние этапы жизненного цикла атаки, обеспечивая предотвращение реализации угроз.

Решение задачи детектирования недопустимых событий информационной безопасности

Предложенный подход обеспечивает раннее выявление угроз на основе идентификации недопустимых событий, что позволяет сократить время реагирования:

1. Раннее обнаружение угроз: Применение инструментов мониторинга событий и корреляции данных позволяет выявить аномалии и сигнатуры атак на самых ранних стадиях проникновения в систему. Использование инструмента Elastic Stack для сбора и визуализации событий обеспечивает эффективное объединение данных для их последующего анализа.

2. Анализ и корреляция событий: Нейросетевой классификатор, обученный на атрибутах недопустимых событий, способен выявлять как известные, так и неизвестные угрозы. Это позволяет сократить время на анализ и быстрее переходить к обработке инцидентов.

3. Сокращение времени реагирования: Автоматизация процессов реагирования на основе машинного обучения обеспечивает оперативное принятие решений. Такой подход исключает длительные задержки на этапе реагирования, что позволяет остановить атаку до её завершения.

4. Локализация и восстановление: Оперативное реагирование позволяет локализовать угрозу и минимизировать последствия инцидента, предотвращая переход атаки в стадию реализации недопустимого события.

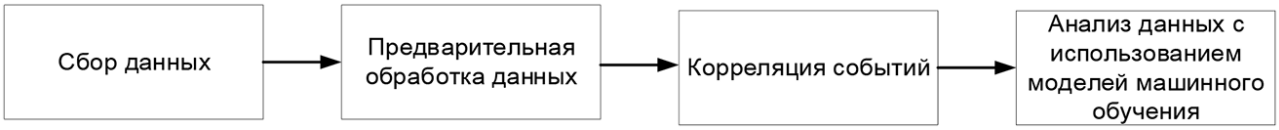

Рис. 4. Процесс детектирования недопустимых событий
Fig. 4. Process of detecting unacceptable events

Процесс детектирования недопустимых событий является многоуровневым и включает в себя сбор, фильтрацию, анализ и реагирование на потенциальные угрозы. Классификация событий на основе признаков упрощает процесс идентификации событий информационной безопасности. Решение задачи классификации событий информационной безопасности сводится к разделению событий на категории на основе их характеристик, контекста и потенциальной угрозы для системы. Основная цель классификации заключается в том, чтобы отличать критичные инциденты, требующие немедленного реагирования, от менее значимых событий или нормальной активности.

На рисунке 4 представлен процесс детектирования недопустимых событий информационной безопасности, который включает следующие этапы.

На этапе сбора данных осуществляется мониторинг сетевого трафика, активности пользователей и систем в реальном времени. Для этого используются специализированные инструменты, обеспечивающие централизованный сбор и передачу информации для дальнейшего анализа.

На этапе предварительной обработки данных проводится нормализация и фильтрация поступающей информации. Это позволяет устранить избыточные или нерелевантные данные, обеспечивая их готовность к дальнейшему анализу.

На этапе корреляции событий выполняется анализ выявленных событий на предмет взаимосвязи, их группировка и сопоставление с известными угрозами. Такой подход позволяет определить потенциальные инциденты и минимизировать вероятность ложных срабатываний.

На этапе анализа данных с использованием моделей машинного обучения обработанные и скоррелированные данные передаются в обученные алгоритмы. Эти модели позволяют выявлять аномалии, индикаторы компрометации и скрытые угрозы, которые могут быть неочевидны при стандартных методах обнаружения. Результаты анализа обеспечивают своевременное выявление недопустимых событий и предотвращение развития инцидентов безопасности.

В статье [13] авторы анализируют различные подходы к обработке событий, начиная с нормализации данных и заканчивая многоуровневой корреляцией и анализом ущерба. Основное внимание уделено созданию схемы корреляции, состоящей из нескольких уровней, на каждом из которых выполняются определенные этапы обработки. Но рассмотренный поход не учитывает задачу идентификации недопустимых событий.

Решение задачи классификации событий информационной безопасности, отличительными свойствами которого являются особенности обработки недопустимых событий в части выявления их корре-

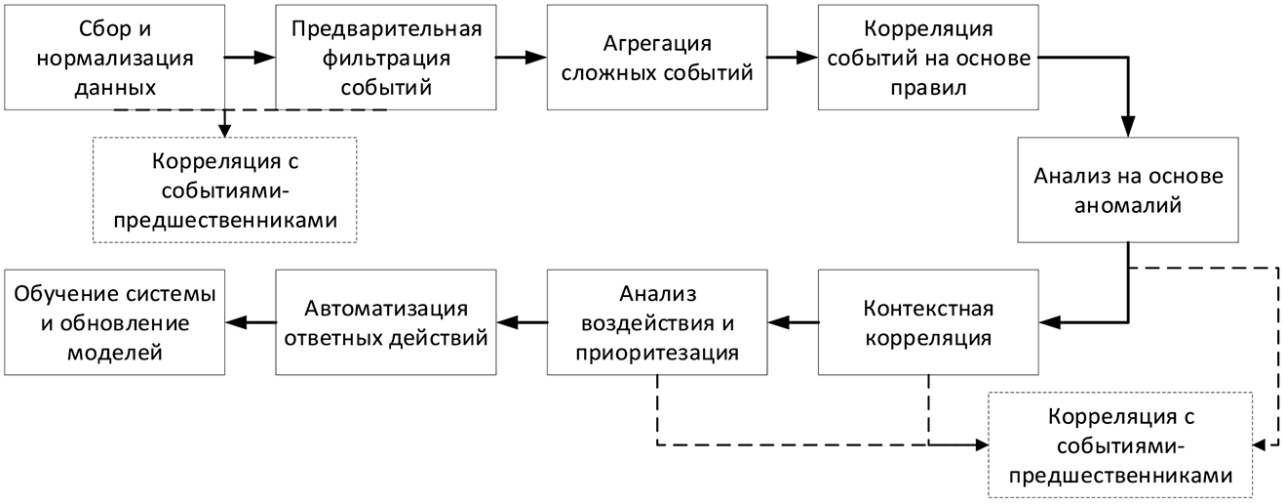

Рис. 5. Последовательность корреляции недопустимых событий
Fig. 5. Correlation sequence of unacceptable events

ляции с другими событиями, а также с событиями-предшественниками (прекурсорами), включает следующие ключевые этапы и процессы, приведенные на рисунке 5.

Решение задачи классификации недопустимых событий информационной безопасности и их взаимосвязи с событиями-предшественниками позволяет не только более точно идентифицировать инциденты, но и выявлять их на ранних стадиях развития. Это способствует упреждающему реагированию и снижению потенциального ущерба для информационных систем. Анализ событий-предшественников дает возможность распознавать закономерности, которые могут свидетельствовать о подготовке атаки, что особенно важно в условиях увеличивающейся сложности и масштабности киберугроз.

Основными отличительными характеристиками предложенного подхода являются комплексный анализ контекста, глубокая корреляция событий, а также многошаговое моделирование угроз с применением методов машинного обучения. Такой подход позволяет учитывать не только статические сигнатуры атак, но и динамически изменяющиеся угрозы, включая сложные многоэтапные сценарии. Использование алгоритмов машинного обучения способствует выявлению неизвестных ранее атак, а интеграция с системами событийного мониторинга позволяет в реальном времени обрабатывать большие объемы данных и оперативно принимать меры по защите. Таким образом, предложенная методология является более гибкой, адаптивной и ориентированной на современные методы анализа данных, что делает ее эффективным инструментом для повышения уровня информационной безопасности.

Реализацию предложенного подхода к классификации и выявлению недопустимых событий обеспечивает инструмент, позволяющий обрабатывать большие объемы данных, проводить глубокий анализ контекста и обеспечивать прогнозирование на основе выявленных паттернов. Одним из таких инструментов является Elastic Stack [14], который интегрирует возможности анализа и визуализации с методами машинного обучения, обеспечивая практическое применение предложенного подхода. Он объединяет функционал сбора, анализа, корреляции и визуализации данных, а также использует технологии машинного обучения для обнаружения аномалий. Это позволяет своевременно выявлять потенциальные угрозы и принимать меры реагирования, что значительно повышает уровень защиты современных информационных систем.

На рисунке 6 представлена структурная схема предложенного блока «Идентификация недопустимых событий безопасности».

Представленный на рисунке 6 блок «Модель классификации» реализуется посредством нейросетевого классификатора, который решает задачу детектирования недопустимого события. Данный блок выполняет автоматизированный анализ событий, поступающих в систему, с целью оценки их критичности и определения принадлежности к категории негативных событий информационной безопасности. Классификатор обрабатывает атрибуты событий, включая время, источник, цель, тип события, уровень критичности и другие метаданные. На основе этих данных он устанавливает взаимосвязь между событиями и определяет те из них, которые могут представлять угрозу.

В статье обоснована целесообразность интеграции дополнительного блока для идентификации недопустимых событий информационной безопасности в перспективную SIEM-систему, предложенную в работе [4].

Данный блок обеспечивает расширение функциональной возможности системы путем автоматизированного анализа атрибутов событий, поступающих из различных источников, таких как сетевые журналы, данные приложений и системные логи. Данные об атрибутах поступают в систему Elastic Stack, которая выполняет сбор, обработку и анализ данных. Elastic Stack предоставляет возможность использовать мощные инструменты для анализа событий и построения их корреляций. Обработанные данные передаются в модель классификации, которая с учетом признаков событий проводит их классификацию, с целью определения недопустимого события, что обеспечивает возможность их своевременного обнаружения и принятия мер по реагированию.

Интеграция данного блока в архитектуру SIEM-системы

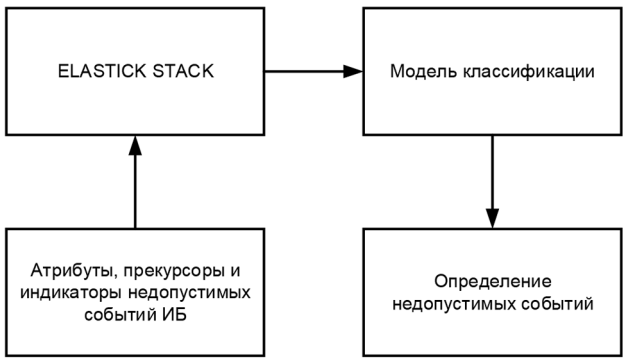

Рис. 6. Блок «Идентификация недопустимых событий ИБ»
Fig. 6. Block “Identification of unacceptable IS events”

позволяет использовать мощные возможности сбора, агрегации и анализа данных для решения задач предиктивного обнаружения сложных атак, включая многоступенчатые и неизвестные угрозы.

Исходными данными являются признаки недопустимых событий: прекурсоры и индикаторы компрометации, а также характеристики недопустимых событий, а именно атрибуты недопустимых событий. На основе материалов работы [6] ниже представлены примеры прекурсоров недопустимых событий, указывающие на потенциальные угрозы:

1. Сканирование портов;
2. Обнаружение новой уязвимости;
3. Установление соединения с неавторизованными IP-адресами;
4. Исследование сети;
5. Аномальные запросы к ресурсам;
6. Изменения в конфигурации системы;
7. Попытки анализа периметра сети злоумышленника.

Ниже представлены примеры индикаторов компрометации, свидетельствующие о том, что угроза уже реализуется, [6].

1. Сообщения от средств защиты информации;
2. Обнаружение вредоносной активности;
3. Множественные неудачные попытки аутентификации;
4. Сбои в работе систем;
5. Изменения в логах;

Таблица 2 / Table 2

Атрибуты недопустимых событий
Attributes of unacceptable events

№ п/п	Наименование атрибута недопустимых событий	Описание атрибута недопустимых событий	Пример
1	Время события (Timestamp)	Указывает точное время, когда событие произошло	2024-10-01 12:30:45 (UTC)
2	Источник события (Source)	Указывает, откуда произошло событие, будь то конкретное устройство, сервер, приложение или сеть	IP-адрес (192.168.1.10), имя хоста (server01), конкретное приложение (Apache Server)
3	Цель события (Target)	Указывает, на что было направлено действие или атака	IP-адрес целевого устройства (192.168.1.20), ресурс (файл, база данных), учетная запись (admin)
4	Тип события (Event Type)	Указывает на характер события — это может быть попытка доступа, сканирование порта, модификация данных и т.д.	Успешная аутентификация, несанкционированный доступ, сканирование портов, изменение файлов
5	Статус события (Event Status)	Указывает результат или статус события	Успешно, Неуспешно, Ошибка
6	Код ошибки или результата (Error Code)	Указывает специфический код, который возвращает система в результате выполнения команды или действия	403 (доступ запрещен), 500 (ошибка сервера), 0xC000006A (неправильный пароль при аутентификации)
7	Протокол (Protocol)	Указывает, какой сетевой или прикладной протокол был использован для события	TCP, HTTP, HTTPS, FTP, SSH
8	Пользователь (User)	Указывает на пользователя, который вызвал событие, или чья учетная запись была затронута	admin, user123, anonymous
9	Местоположение (Location)	Указывает физическое или сетевое местоположение, с которого было инициировано событие	IP-адрес (8.8.8.8), страна (Россия), географическое местоположение (широта, долгота)
10	Характеристики устройства (Device Attributes)	Указывает информацию о клиентском устройстве, с которого произошло событие	Операционная система (Windows 10, Linux), тип устройства (мобильный телефон, ноутбук), версия программного обеспечения (Apache 2.4.46)
11	Событие-предшественник (Preceding Event)	Указывает на события, которые могли предшествовать текущему инциденту	Сканирование порта перед попыткой взлома, неудачная аутентификация перед успешной.
12	Действие (Action)	Описывает конкретное действие, выполненное в ходе события	Создание файла, изменение прав доступа, запуск программы, перезагрузка системы
13	Задействованные ресурсы (Resources)	Указывает на ресурсы, к которым был произведен доступ или которые были изменены в ходе события	Файл (C:\data\file.txt), база данных (employees), системный процесс
14	Уровень важности (Severity)	Указывает уровень критичности события для системы безопасности	Низкий, Средний, Высокий
15	Длительность события (Duration)	Указывает на продолжительность события или инцидента	5 секунд, 2 минуты, 3 часа
16	Описание события (Event Description)	Подробное текстовое описание события, содержащее дополнительную информацию о том, что произошло	«Попытка доступа к защищённой базе данных с использованием несанкционированного IP-адреса»

6. Успешные несанкционированные действия к учетным записям;

7. Аномальная сетевая активность;

8. Сообщения от администраторов об аномальном поведении.

На основе [15–17] построена таблица атрибутов недопустимых событий информационной безопасности, табл. 2.

В табл. 2 представлены основные параметры, используемые для классификации и анализа событий, а также их характеристики, включая источник возникновения, временные метки, методы реализации и потенциальные последствия для системы. Особое внимание уделяется взаимосвязи между событиями-предшественниками и реализацией атаки, что позволяет более точно определять возможные угрозы и прогнозировать их развитие. Представленные данные используются для автоматизированного детектирования инцидентов, что снижает вероятность ложных срабатываний и повышает эффективность реагирования на угрозы.

Эти данные проходят этапы структуризации, фильтрации и визуализации с использованием инструмента Elastic Stack. На следующем этапе решается задача классификации с использованием обученной нейронной сети, реализованной в рамках модели классификации, которая обрабатывает данные для определения принадлежности событий к категории недопустимых. Эти элементы являются ключевыми для раннего выявления угроз и автоматизированного детектирования инцидентов безопасности.

Интеграция прекурсоров, индикаторов компрометации и атрибутов недопустимых событий в процесс мониторинга и анализа позволяет не только минимизировать последствия атак, но и предотвращать их, обеспечивая более высокий уровень защищённости информационных систем.

Заключение

В ходе исследования рассмотрены актуальные вопросы, связанные с детектированием недопустимых событий информационной безопасности, и выявлены основные недостатки существующих методов, включая высокую вероятность ложноположительных и ложноотрицательных срабатываний, низкую адаптивность к новым угрозам и сложность интеграции данных из различных источников. Анализ показал, что традиционные подходы, основанные на сигнатурном и поведенческом анализе, не в полной мере обеспечивают детектирование недопустимых событий.

Предложенное в статье решение задачи детектирования недопустимых событий основано на использовании атрибутов, прекурсоров и индикаторов компрометации в сочетании с методами машинного обучения и инструментами потоковой обработки данных, такими как Elastic Stack. Выявленные атрибуты недопустимых событий (например, источник атаки, тип уязвимости, вектор атаки, время возникновения и цель) являются ключевыми элементами, которые позволяют проводить эффективную классификацию, анализ и корреляцию инцидентов информационной безопасности. Методы машинного обучения и инструменты потоковой обработки данных, такие как Elastic Stack, в сочетании с анализом атрибутов, прекурсоров и индикаторов компрометации обеспечивают выявление закономерности, отслеживания тенденций и прогнозирования потенциальных угроз.

Детектирование недопустимых событий с применением индикаторов компрометации, атрибутов и прекурсоров смещает временной горизонт реагирования на угрозы на более ранние этапы, обеспечивая снижение вероятности нанесения ущерба.

Разработанные предложения по решению задачи детектирования недопустимых событий обеспечивают внедрение эффективных решений в области информационной безопасности, особенно в условиях постоянно меняющегося ландшафта киберугроз.

Литература

1. Евдокимова Д.А., Микрюков А.А. Актуальные задачи выявления недопустимых событий на объектах критической информационной инфраструктуры // Открытое образование. 2024. Т. 28. № 4. С. 33–42.

2. Что такое реестр недопустимых событий в информационной безопасности [Электрон. ресурс] // Новости LianMedia.ru. Режим доступа: https://lianmedia.ru/ (дата обращения: 20.12.2024).

3. Котенко И.В., Саенко И.Б., Юсупов Р.М. Новое поколение систем мониторинга и управления инцидентами безопасности // Труды СПИИРАН. 2017. Т. 6. №1. С. 45–59.

4. Котенко И.В., Кулешов А.А., Ушаков И.А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // СПИИРАН. 2021. Т. 65. № 2. С. 5–27.

5. Жаксыбай С.М. Управление событиями информационной безопасности с помощью SIEM-системы. // Intellectual Technologies on Transport. 2023. № S1. Special Issue. MMIS-2023. С. 66–69.

6. Токарев М.Н. SIEM-система как инструмент обеспечения информационной безопасно-

сти в организации // Актуальные исследования. 2024. № 2 (184). Ч.I. С. 51–53.

7. Как работают системы обнаружения и предотвращения вторжений (IDS и IPS). [Электрон. ресурс] // Habr.com. Режим доступа: https://habr.com/ru/articles/710378/ (Дата обращения: 23.12.2024).

8. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения. М.: Стандартинформ, 2022.

9. Индикаторы компрометации в Kaspersky Endpoint Security для Windows 12.0. [Электрон. ресурс] // Support.kaspersky.com. Режим доступа: https://support.kaspersky.com/KESWin/12.0/ru-RU/213408.htm (дата обращения: 13.01.2025).

10. Батюк А. Использование ИИ в средствах обнаружения компьютерных атак и реагирования на инциденты ИБ [Электрон. ресурс] // Positive Technologies. Режим доступа: https://www.ptsecurity.com/ (Дата обращения: 20.12.2024).

11. Жизненный цикл атак: этапы, методы, и защита. [Электрон. ресурс] // Positive Technologies. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/ (Дата обращения: 20.12.2024).

12. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.

13. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1. // Труды СПИИРАН. 2016. №4(47). С. 5–27.

14. Elastic Stack [Электрон. ресурс] // Elastic.co. Режим доступа: https://www.elastic.co/ (Дата обращения: 02.10.2024).

15. Positive Technologies. MaxPatrol O2 — автопилот для результативной кибербезопасности. 2023. [Электрон. ресурс] // Positive Technologies. Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/products/o2/maxpatrol-o2-pb.pdf (Дата обращения: 02.10.2024).

16. ГОСТ ISO/IEC 27001-2013. Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования (ISO/IEC 27001:2013, IDT). М.: Стандартинформ, 2014.

17. ГОСТ ISO/IEC 27002-2013. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью (ISO/IEC 27002:2013, IDT). М.: Стандартинформ, 2014.

References

1. Evdokimova D.A., Mikryukov A.A. Actual tasks of identifying unacceptable events at critical information infrastructure facilities. Otkrytoye obrazovaniye = Open education. 2024; 28; 4: 33-42. (In Russ.)

2. Chto takoye reyestr nedopustimykh sobytiy v informatsionnoy bezopasnosti = What is the register of unacceptable events in information security [Internet]. LianMedia.ru News. Available from: https://lianmedia.ru/ (Cited: 20.12.2024). (In Russ.)

3. Kotenko I.V., Saenko I.B., Yusupov R.M. New generation of security incident monitoring and management systems. Trudy SPIIRAN = Proceedings of SPIIRAS. 2017; 6; 1: 45-59. (In Russ.)

4. Kotenko I.V., Kuleshov A.A., Ushakov I.A. System for collecting, storing and processing information and security events based on Elastic Stack. SPIIRAN = SPIIRAS. 2021; 65; 2: 5-27. (In Russ.)

5. Zhaksybay S.M. Information security event management using a SIEM system. Intellectual Technologies on Transport. 2023; S1. Special Issue. MMIS-2023: 66-69.

6. Tokarev M.N. SIEM system as a tool for ensuring information security in an organization. Aktual'nyye issledovaniya = Current research. 2024; 2 (184). Part I: 51-53. (In Russ.)

7. Kak rabotayut sistemy obnaruzheniya i predotvrashcheniya vtorzheniy (IDS i IPS) = How intrusion detection and prevention systems (IDS and IPS) work. [Internet]. Habr.com. Available from: https://habr.com/ru/articles/710378/ (Cited: 23.12.2024). (In Russ.)

8. GOST R 59547-2021. Zashchita informatsii. Monitoring informatsionnoy bezopasnosti. Obshchiye polozheniya = Information protection. Information security monitoring. General provisions. Moscow: Standartinform; 2022. (In Russ.)

9. Indikatory komprometatsii v Kaspersky Endpoint Security dlya Windows 12.0. = Indicators of compromise in Kaspersky Endpoint Security for Windows 12.0.. Support.kaspersky.com. Available from: https://support.kaspersky.com/KESWin/12.0/ru-RU/213408.htm (Cited: 13.01.2025). (In Russ.)

10. Batyuk A. Using AI in detecting computer attacks and responding to information security incidents [Internet]. Positive Technologies. Available from: https://www.ptsecurity.com/ (Cited: 20.12.2024). (In Russ.)

11. Zhiznennyy tsikl atak: etapy, metody, i zashchita = Life cycle of attacks: stages, methods, and protection. [Internet]. Positive Technologies. Available from: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/ (Cited: 20.12.2024). (In Russ.)

12. Metodika opredeleniya aktual'nykh ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh, utverzhdena zamestitelem direktora FSTEK Rossii =

Methodology for determining current threats to the security of personal data when processing them in personal data information systems, approved by the Deputy Director of the FSTEC of Russia on February 14; 2008. (In Russ.)

13. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. Analysis of methods for correlating security events in SIEM systems. Part 1. Trudy SPIIRAN = Proceedings of SPIIRAS. 2016; 4 (47): 5-27. (In Russ.)

14. Elastic Stack [Internet]. Elastic.co. Available from: https://www.elastic.co/ (Cited: 02.10.2024).

15. Positive Technologies. MaxPatrol O2 — avtopilot dlya rezul'tativnoy kiberbezopasnosti = Positive Technologies. MaxPatrol O2 — an autopilot for effective cybersecurity. 2023. [Internet]. Positive Technologies. Available from: https://www.ptsecurity.com/upload/corporate/ru-ru/products/o2/maxpatrol-o2-pb.pdf (Cited: 02.10.2024). (In Russ.)

16. GOST ISO/IEC 27001-2013. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy upravleniya informatsionnoy bezopasnost'yu. Trebovaniya = Information technology. Security methods and tools. Information security management systems. Requirements (ISO/IEC 27001:2013, IDT). Moscow: Standartinform; 2014. (In Russ.)

17. GOST ISO/IEC 27002-2013. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Prakticheskiye pravila upravleniya informatsionnoy bezopasnost'yu = Information technology. Security methods and tools. Practical rules for information security management (ISO/IEC 27002:2013, IDT). Moscow: Standartinform; 2014. (In Russ.)

Сведения об авторах

Евдокимова Дарья Александровна
аспирант кафедры прикладной информатики и информационной безопасности
Российский экономический университет им. Г.В. Плеханова, Москва, Россия
Эл. почта: Evdokimova.DA@rea.ru

Микрюков Андрей Александрович
к.т.н., доцент кафедры прикладной информатики и информационной безопасности
Российский экономический университет им. Г.В. Плеханова,
Москва, Россия
Эл. почта: mikrukov.aa@rea.ru

Information about the authors

Evdokimova Darya Alexandrovna
Postgraduate student of the Department of Applied Informatics and Information Security
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: Evdokimova.DA@rea.ru

Mikryukov Andrey Aleksandrovich
Candidate of Technical Sciences, Associate Professor of the Department of Applied Informatics and Information Security
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: mikrukov.aa@rea.ru