Д.А.Добрецова

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

УДК 519.6
DOI: http://dx.doi.org/10.21686/1818-4243-2026-2-4-17

Разработка модели машинного обучения для решения задачи классификации недопустимых событий информационной безопасности

Целью исследования является *разработка и обоснование подхода к выявлению и классификации недопустимых событий информационной безопасности на объектах критической информационной инфраструктуры с использованием методов машинного обучения. Предлагаемый подход направлен на повышение эффективности идентификации недопустимых событий в условиях обработки больших объёмов разнородных данных и ограничений по времени реагирования.*

Актуальность исследования обусловлена ростом количества и сложности кибератак на объекты критической информационной инфраструктуры, а также необходимостью своевременного выявления событий информационной безопасности, способных привести к существенным негативным последствиям для устойчивости функционирования критически важных систем. Ограничения традиционных сигнатурных и экспертных методов, связанные с высокой динамикой событий и наличием шума в данных, требуют применения интеллектуальных методов обработки информации.

Материалы и методы исследования. *В работе использованы методы машинного обучения, статистического анализа и обработки данных событий информационной безопасности. В качестве исходных данных применены журналы событий и сетевой трафик реального объекта критической информационной инфраструктуры энергетического сектора. Разработана методика формирования обучающей выборки, включающая предобработку данных, экспертную разметку, отбор информативных признаков и балансировку классов. Для классификации недопустимых событий использован алгоритм случайного леса.*

Результаты. *Экспериментальные исследования подтвердили эффективность предложенной модели по показателям точности, полноты и F1-меры при минимальном уровне ложноположительных срабатываний. Показана возможность практического применения предложенного подхода для автоматизации процессов мониторинга и выявления недопустимых событий на объектах критической информационной инфраструктуры.*

Ключевые слова: *информационная безопасность, машинное обучение, критическая информационная инфраструктура, классификация событий, недопустимые события, поведенческий анализ, киберугрозы, автоматизация ИБ.*

D. A. Dobretsova

Plekhanov Russian University of Economics, Moscow, Russia

Development of a Machine Learning Model for Solving the Problem of Classifying Unacceptable Information Security Events

The aim of the study *is to develop and substantiate an approach for detecting and classifying unacceptable information security events in critical information infrastructure systems using machine learning methods. The proposed approach is focused on improving the effectiveness of identifying unacceptable events under conditions of large-scale heterogeneous data processing and strict time constraints for response.*

The increasing number and complexity of cyberattacks targeting critical information infrastructure, as well as the need for timely detection of information security events that may lead to significant negative consequences for the stability of critical systems determine the relevance of the study. The limitations of traditional signature-based and expert-driven methods, caused by the high dynamics of security events and data noise, necessitate the use of intelligent data processing techniques.

Materials and methods. *The study employs machine learning methods, statistical analysis, and processing of information security event data. Event logs and network traffic of a real object of critical information infrastructure of the energy sector are used as initial data. A methodology for forming a training sample has been developed, including data preprocessing, expert labeling, informative features' selection, and class balancing. A Random Forest algorithm was used to classify unacceptable events.*

Results. *Experimental results demonstrate the effectiveness of the proposed model in terms of precision, recall, and F1-score with a minimal level of false positives. The findings confirm the practical applicability of the proposed approach for automating monitoring and detection of unacceptable information security events in critical information infrastructure systems.*

Keywords: *information security, machine learning, critical information infrastructure, event classification, unacceptable events, behavioral analysis, cyber threats, information security automation.*

Введение

В последние годы наблюдается существенный рост количества кибератак на критически важные объекты информационной инфраструктуры, что создает риски для устойчивой работы ключевых отраслей, включая энергетику, транспорт и промышленный сектор. Кибератаки были реализованы в 2015 и 2016 годах в отношении энергетической инфраструктуры Украины, где атаки на автоматизированные системы управления технологическими процессами привели к массовым отключениям электроэнергии [1]. В 2021 году кибератака на Colonial Pipeline в США, осуществленная группировкой DarkSide, вызвала перебои в поставках топлива и продемонстрировала уязвимость крупных операторов энергетического сектора перед современными угрозами [2].

Одним из ключевых этапов формирования системы информационной безопасности является комплексный анализ угроз безопасности информации. Согласно методическим рекомендациям ФСТЭК России [3], приоритетной задачей данного процесса выступает выявление потенциальных негативных последствий, возникающих в результате реализации угроз. При этом недопустимые события рассматриваются в качестве факторов, непосредственно приводящих к наступлению указанных последствий [4].

Разделение событий по определённым признакам способствует упрощению их идентификации в сфере информационной безопасности. Задача классификации заключается в распределении событий по категориям с учётом их характеристик, контекста и потенциального уровня угрозы для системы. Основной целью такого подхода является своевременное выявление критически важных инцидентов, требующих оперативного реагирования, а также отделение их от менее значимых событий или обычной активности.

В качестве исходных данных рассматриваются характеристики недопустимых событий, включая их атрибуты, а также признаки, такие как прекурсоры и индикаторы компрометации. В статье [5] представлены примеры прекурсоров недопустимых событий, указывающие на потенциальные угрозы, индикаторов компрометации, свидетельствующие о том, что угроза уже реализуется, и атрибутов событий информационной безопасности.

Научная новизна представленного исследования заключается в разработке прикладной модели машинного обучения, ориентированной на задачи классификации недопустимых событий в системах критической информационной инфраструктуры (КИИ). В отличие от существующих решений, основанных на обобщённых датасетах и универсальных алгоритмах, предложенный подход учитывает специфику отраслевых протоколов, архитектуры промышленных систем и поведенческих шаблонов, характерных для объектов энергетического сектора, а также особенности выявления недопустимых событий информационной безопасности.

В качестве обучающей выборки использован сетевой трафик реального объекта КИИ, что обеспечивает высокую степень достоверности и репрезентативности данных. Обоснована структура события как совокупности атрибутов, индикаторов компрометации и прекурсоров, что позволяет расширить контекст анализа и повысить точность детектирования угроз на ранней стадии их реализации.

Разработан и реализован процесс формирования обучающей выборки, включающий очистку, нормализацию, стратификацию по типам событий, экспертную разметку и кодирование категориальных признаков с учётом требований к минимизации информационных утечек в процессе обучения. Верификация качества модели проведена на основе F1-метрики по атакующему классу, что соответствует практическим требованиям эксплуатации в условиях минимально допустимого уровня ложных срабатываний.

Таким образом, отличительной особенностью исследования является ориентированность на отраслевые особенности КИИ, использование полноценных событийных данных с реальных объектов, а также разработка структурированной методики подготовки и оценки обучающих выборок для задач автоматизированной классификации инцидентов информационной безопасности.

Анализ применения модели машинного обучения для решения задачи классификации событий информационной безопасности

Модель машинного обучения (ML-модель) – это математическая конструкция, основанная на алгоритмах анализа данных, которая обучается на исторических данных и использует выявленные закономерности для классификации, прогнозирования и обнаружения аномалий [6]. В контексте информационной безопасности такие модели применяются для автоматизированного выявления угроз, анализа поведения пользователей и систем, а также предсказания потенциальных атак, на основе накопленных данных.

Применение методов машинного обучения в системах кибербезопасности позволяет эффективно выявлять аномалии и инциденты, ускользающие от традиционных сигнатурных средств, включая

скрытные атаки типа APT. Поведенческий анализ пользователей обеспечивает раннее обнаружение внутренних угроз, таких как компрометация учетных данных и эскалация привилегий. ML-модели обеспечивают с обработкой больших объемов событий информационной безопасности, выявляя сложные взаимосвязи между инцидентами и тем самым оптимизируя процесс их корреляции. Использование предиктивной аналитики способствует заблаговременному обнаружению потенциальных атак и позволяет реализовать упреждающее реагирование. Кроме того, автоматизация процессов реагирования с помощью машинного обучения (ML) сокращает время принятия решений и снижает зависимость от человеческого фактора [7–12].

Использование технологий машинного обучения в информационной безопасности позволяет [13–16]:

1. Обнаруживать и предотвращать атаки на ранних стадиях, повышая общую безопасность инфраструктуры на основе анализа сетевого трафика с целью выявления аномалий, которые могут свидетельствовать о потенциальных угрозах.

2. Обнаруживать аномалии и защитить системы от подобных угроз на основе анализа сетевого трафика с целью идентификации вредоносного трафика и защиты от DDoS-атак.

3. Идентифицировать и блокировать потенциально опасные угрозы на основе анализа поведения программ и сетевой активности с целью обнаружения и защиты от вирусов, троянов и другого вредоносного программного обеспечения.

4. Улучшить безопасность промышленных систем на основе анализа уязвимостей в сетях промышленного Интернета вещей.

Модель машинного обучения используется для классификации недопустимых событий информационной безопасности, что позволяет автоматизировать процесс их идентификации и анализа. Классификация представляет собой процесс распределения событий по категориям на основе их атрибутивных характеристик, контекстуальных признаков и степени потенциальной угрозы для информационной системы. Такой подход способствует повышению точности детектирования недопустимых событий информационной безопасности.

Начальным этапом построения модели машинного обучения [17] выступает формирование обучающей выборки на основе специализированных наборов данных, включающих как легитимный трафик, так и различные типы атак; на данном этапе важна не только репрезентативность, но и актуальность включённых признаков. Предварительная обработка данных включает приведение информации к унифицированному формату, устранение пропусков, выбросов и дублирующихся записей, а также нормализацию параметров, обеспечивающую корректную работу алгоритмов. В связи с характерной диспропорцией классов в ИБ-данных производится балансировка выборки методами повторной выборки или синтетической генерации примеров, что позволяет повысить чувствительность модели к редким, но критически важным событиям. После оценки значимости признаков и устранения избыточности выполняется сокращение размерности признакового пространства, направленное на снижение вычислительной нагрузки и предотвращение переобучения. Завершающие этапы включают выбор алгоритма обучения, его калибровку с использованием процедур оптимизации гиперпараметров и последующую валидацию на тестовой выборке, что позволяет оценить устойчивость модели к новым типам атак и определить её пригодность для интеграции в системы мониторинга информационной безопасности, рис. 1.

Таким образом, применение модели машинного обучения для детектирования недопустимых событий требу-

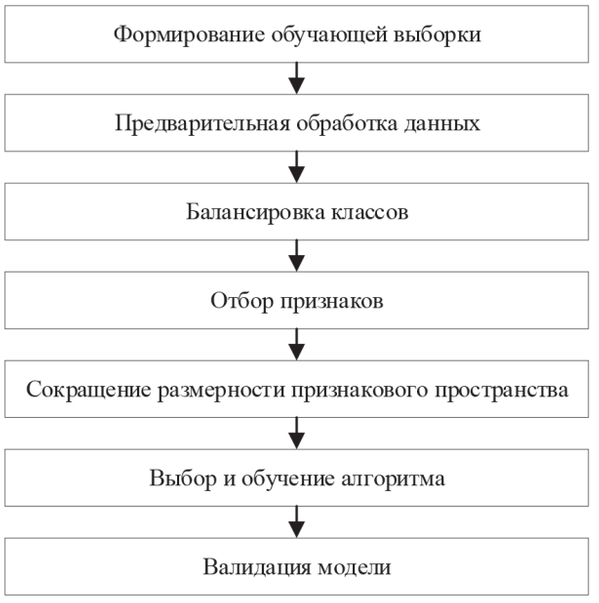

Рис. 1. Этапы построения модели машинного обучения для классификации событий ИБ

Fig. 1. Stages of constructing a machine learning model for classifying information security events

ет формирования обучающей выборки, содержащей релевантные признаки и атрибуты данных. В разработанной модели в обучающую выборку должны быть включены характеристики недопустимых событий, представленные в исследовании [5], что обеспечит корректное обучение модели и её способность эффективно классифицировать и выявлять потенциальные угрозы.

Разработка обучающей выборки для модели машинного обучения

Сформированная обучающая выборка, построенная в соответствии с [17], содержит репрезентативные данные, отражающие характеристики как обычных, так и недопустимых событий, что позволяет модели выявлять закономерности и эффективно распознавать инциденты.

Создание обучающей выборки для модели машинного обучения включает несколько ключевых этапов, каждый из которых направлен на обеспечение качества и релевантности данных для последующего обучения модели, рис. 2.

На первом этапе сформулирована цель обучения модели. В случае детектирования недопустимых событий информационной безопасности модель должна обеспечивать классификацию событий на допустимые или недопустимые, выявлять аномалии и прогнозировать потенциальные угрозы.

Для формирования обучающей выборки, ориентированной на задачу классификации недопустимых событий информационной безопасности, собраны и систематизированы разнородные данные из сетевых журналов, системных логов, отчётов о киберинцидентах, а также информации о предшествующих атаках и метках событий. При этом обосновано сохранение исходного баланса классов, что обеспечило репрезентативное представление как допустимых, так и недопустимых событий.

На этапе предобработки реализован комплекс процедур очистки данных, включающий удаление дублирующихся и некорректных записей, обработку пропусков с использованием методов заполнения и применение нормализации признаков. Эти меры позволили унифицировать исходные данные и повысить корректность их дальнейшего использования в алгоритмах машинного обучения.

Разметка выборки проведена в полуавтоматическом режиме с учётом отраслевой специфики задачи детектирования недопустимых событий в критической информационной инфраструктуре. В качестве основы использован категориальный признак *Event Type*, на основании которого сформирован бинарный целевой признак *IsAttack*, фиксирующий факт отклонения от допустимого поведения. Предложенный подход обеспечивает включение в процесс разметки отраслевой семантики событий, что позволило повысить интерпретируемость и практическую ценность результатов.

В отличие от универсальных подходов, основанных на обобщённых открытых датасетах, в исследовании использованы данные, полученные непосредственно в производственной среде. Это позволило учитывать контекст функционирования систем и индикаторы компрометации, характерные для промышленных объектов, что обосновывает достоверность и применимость разработанной выборки для решения прикладных задач классификации событий информационной безопасности.

Для оценки качества модели выборка разделяется на:

1. Тренировочную – используется для обучения модели (обычно 70–80% от общего объема данных).

2. Тестовую – применяется для проверки качества классификации модели на ранее не встречавшихся данных.

В случае значительного дисбаланса классов (например, недопустимых событий мень-

Рис. 2. Этапы создания обучающей выборки для модели машинного обучения

Fig. 2. Steps for creating a training set for a machine learning model

ше, чем допустимых) может потребоваться применение методов балансировки:

– Увеличение числа примеров недопустимых событий (Oversampling);

– Уменьшение количества примеров допустимых событий (Undersampling);

– Генерация новых синтетических данных с помощью методов типа SMOTE.

Для компенсации дисбаланса используется система весов для объектов обучающей выборки. Вес W_i зависит от принадлежности примера к классу:

$$W_i = \begin{cases} \frac{1}{2n_1}, & y_i = 1, \\ \frac{1}{2n_0}, & y_i = 0, \end{cases},$$

где n_1 – количество записей класса «Атака», а n_0 – количество записей класса «Норма». Такое нормирование выравнивает вклад каждого класса и снижает влияние дисбаланса на обучение модели.

С учётом необходимости подготовки данных к машинной обработке и обеспечения совместимости с алгоритмами классификации, автором использован метод Label Encoding, применённый к категориальным признакам строкового типа (например, «Location», «Protocol», «User»). Это позволило сохранить семантику атрибутов, не увеличивая размерность выборки, что критически важно при работе с ограниченным количеством событий атакующего класса. Для устранения влияния неоднородности масштабов числовых признаков дополнительно применено масштабирование (MinMax Scaling), обеспечивающее приведение значений к единому диапазону.

Перед обучением модели была проведена валидация качества обучающей выборки, включающая автоматизированную проверку наличия выбросов, анализ распределения классов и перекрёстную проверку корректности присвоенных меток.

Для формирования выборки, адаптированной под задачи классификации недопустимых событий, был использован сетевой трафик объекта критической инфраструктуры энергетического сектора. Такой подход обеспечивает не только отраслевую релевантность, но и отражает реальные поведенческие шаблоны, характерные для защищаемой среды. В отличие от обобщённых тестовых наборов, эта выборка содержит как допустимые операции в SCADA-среде, так и отклонения, сопоставимые с инцидентами информационной безопасности.

Использование реального трафика, полученного с объекта критической информационной инфраструктуры, позволило учесть особенности отраслевых протоколов (включая Modbus, IEC 60870-5-104, DNP3 и др.), типичные шаблоны коммуникаций между элементами автоматизированных систем управления технологическими процессами, а также характерные для отрасли поведенческие паттерны пользователей и сервисов. Используемый подход способствует построению модели, обладающей высокой степенью обобщающей способности и устойчивостью к ложноположительным срабатываниям, что является критически важным условием при эксплуатации в условиях ограниченной допустимости ложных тревог, характерной для критической информационной инфраструктуры.

Процесс предварительной подготовки выборки включал в себя этапы очистки и нормализации данных, аннотирования известных инцидентов и подозрительных аномалий, а также стратификации по различным типам событий, включая как легитимные действия, так и индикации потенциальных угроз. В целях повышения достоверности маркировки и обеспечения корректной классификации использовались экспертные оценки специалистов по информационной безопасности, а также сведения из внутренних журналов инцидентов и баз индикаторов компрометации.

Для построения и обучения модели классификации использовался датасет, содержащий события информационной безопасности, зафиксированные в течение одного операционного дня. Данные были извлечены из журналов корпоративной системы информационной безопасности организации.

Каждая строка датасета соответствует одному событию, зафиксированному в логах. В таблице 1 приведены описания всех атрибутов (признаков), входящих в исходный набор данных [5].

В табл. 2 представлены примеры событий, зафиксированных системой информационной безопасности за один рабочий день в корпоративной сети организации, функционирующей в сфере энергетики. Каждое событие содержит информацию о времени, источнике, типе действия, статусе выполнения, задействованных ресурсах и других критически важных параметрах для анализа инцидентов и аномалий.

Данные были получены из внутренних журналов информационной безопасности организации, включающих сетевые и пользовательские действия. В представленных примерах отражаются различные категории инцидентов. Каждый инцидент сопровождается оценкой уровня важности, длительности и техническим контекстом (протокол, устройство, ресурсы).

На этапе загрузки исходных данных в качестве основы используется файл событий информационной безопасности в формате CSV, содержащий

Таблица 1 / Table 1

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, где 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»

записи о действиях, зафиксированных в информационной системе. Каждая строка в файле представляет собой отдельное событие, включающее совокупность атрибутов, характеризующих параметры действия, его источник, назначение и контекст выполнения.

Для обработки табличных данных применена библиотека pandas, широко используемая в научных и прикладных задачах анализа данных. Считывание содержимого файла и его преобразование в структуру DataFrame осуществляется с помощью функции read_csv(), после чего данные становятся доступны для последующих этапов предобработки и формирования признакового пространства.

Полученная выборка включает около одного миллиона записей, каждая из которых содержит исходные характеристики событий, представленные в таблице 2. Эти данные служат основой для построения обучающей выборки, предназначенной для обучения модели машинного обучения, способной проводить автоматическую классификацию событий на основе поведенческих признаков и отличать нормальную активность от потенциально вредоносных воздействий.

Изначально в загруженном датасете каждое событие имеет категориальный признак Event Type, Бинарный признак IsAttack соответствует «1» в случае атаки и «0» в противном случае, табл. 3.

Рассматривается задача бинарной классификации сетевых событий. Каждое наблюдение описывается вектором

Таблица 2 / Table 2

Пример записей из журнала событий информационной безопасности

Example of entries from the information security event log

Timestamp	Source	Target	Event Type	Event Status	Error Code	Protocol	User	Location	Device Attributes	Preceding Event	Action	Resources	Severity	Duration
01.04.2025 8:15	10.46.183.108	192.168.207.29	Brute Force	Success		DNS	dave	Rostov	IoT	Access	Access	Email	Medium	62.67
01.04.2025 2:35	10.252.37.208	192.168.65.89	Phishing	Failed	ERR04	HTTP	alice	Novosibirsk	Server	Modify	Access	Database	Low	137.46
01.04.2025 9:43	10.77.220.173	192.168.220.73	Intrusion	Failed	ERR01	FTP	charlie	Ekaterinburg	Server	Login	Login	Network Share	Critical	58.65
01.04.2025 11:40	10.164.189.254	192.168.105.173	Normal	Success		HTTPS	bob	Novosibirsk	Mobile	Login	Login	Service	Low	17.06
01.04.2025 12:22	10.8.96.204	192.168.155.192	Normal	Success		DNS	mallory	Kazan	Workstation	Download	Modify	Service	Low	49.19
01.04.2025 5:15	10.188.138.71	192.168.139.222	Insider Threat	Success		HTTPS	dave	Kazan	Workstation	Upload	Login	Service	Medium	103.88
01.04.2025 13:59	10.51.197.174	192.168.225.107	Intrusion	Success		HTTPS	dave	Kazan	Mobile	Modify	Upload	Database	Critical	44.13
01.04.2025 1:18	10.183.86.127	192.168.13.29	Malware	Success		SSH	eve	Kazan	Cloud Instance	Upload	Access	File	High	98.06
01.04.2025 13:14	10.87.28.229	192.168.121.169	Normal	Success		DNS	alice	Rostov	Server	Modify	Modify	Service	Low	27.15

Таблица 3 / Table 3

Создание целевой бинарной метки

Create target binary label

№ п/п	Значение Event Type	Описание значения Event Type	Признак IsAttack
1	Normal	Обычная активность системы	0
2	Intrusion	Попытка несанкционированного доступа	1
3	Malware	Обнаружено вредоносное ПО	1
4	DDoS	Распределённая атака отказа в обслуживании	1
5	Phishing	Попытка фишинга	1
6	Brute Force	Атака методом подбора пароля	1
7	Ransomware	Активность программ-вымогателей	1
8	Insider Threat	Вредоносная активность со стороны внутренних пользователей.	1

признаков $x_i \in \mathbb{R}^p$, а целевая метка y_i принимает значения из множества {0,1}, где 0 соответствует нормальному событию, а 1 – атаке. Таким образом, классификатор определяется как отображение $f: \mathbb{R}^p \to \{0,1\}$. Формирование целевой метки y_i осуществляется на основе категориального признака *Event Type* следующим образом:

$$y_i = \begin{cases} 1, \text{ если } Event\,Type \in A, \\ 0, \text{ иначе,} \end{cases}$$

где A – множество типов событий, относящихся к атакам.

Качество классификатора оценивается через риск, определяемый как математическое ожидание функции потерь:

$$R(f) = \mathbb{E}_{(X,Y)\sim P}\left[l\left(f\left(X\right),Y\right)\right],$$

где l – функция потерь (например, 0-1 loss), а P обозначает неизвестное распределение данных.

На следующем этапе подготовки обучающей выборки решена задача исключения признаков, способных создать эффект утечки информации (data leakage) или негативно повлиять на обобщающую способность алгоритма. Отбор признаков осуществлялся с учётом следующих критериев:

1. Признак должен быть доступен в реальном времени до наступления события, что обеспечивает применимость модели в условиях реального мониторинга;

2. Признак должен обладать предикативной значимостью и потенциальной корреляцией с атакующим или безопасным поведением.

В процессе анализа были исключены следующие категории признаков:

- Целевые признаки, напрямую связанные с меткой класса («Event Type»), использование которых при обучении привело бы к переобучению;
- Описательные текстовые поля, такие как «Event Description», содержащие недоступную в реальном времени информацию и потенциально раскрывающие суть инцидента;
- Признаки с низкой аналитической ценностью, например, «Error Code», которые встречаются нерегулярно и не формируют устойчивых закономерностей;
- Признаки, формально отражающие результат события, а не его предикторы (например, «Timestamp», «Status Code»), поскольку их использование нарушает причинно-следственную структуру модели.

Такой подход к отбору признаков позволил снизить размерность пространства признаков, устранить «шум» в обучающих данных и обеспечить соответствие модели условиям эксплуатации в системах обнаружения атак в режиме реального времени.

В процессе подготовки данных к обучению модели проведён критический анализ информативности и применимости каждого признака. Удаление отдельных полей обосновано их ограниченной предсказательной ценностью, риском утечки информации или несоответствием формату, необходимому для корректной работы алгоритмов машинного обучения. Обоснование исключения конкретных признаков представлено ниже:

- Timestamp — временная метка события не содержит семантической информации, значимой для определения атакующего поведения, и может вносить случайный шум;
- Event Type — категориальный признак, использованный для формирования целевой переменной IsAttack, не может использоваться в обучении во избежание прямой утечки информации;
- Event Description — текстовое описание события, непригодное для использования в большинстве классических алгоритмов без предварительного лингвистического анализа; к тому же, оно часто содержит явные указания на суть инцидента;
- Error Code — характеризуется высокой разреженностью и слабой корреляцией с целевым классом, что ограничивает его полезность в контексте классификации.

Для обеспечения корректной работы модели все входные признаки были приведены к числовому виду, так как большинство алгоритмов машинного обучения (например, решающие деревья, метод опорных векторов) не поддерживают прямую обработку строковых данных. В связи с этим для кодирования категориальных признаков применялся метод Label Encoding, позволяющий преобразовать строковые значения в числовые идентификаторы без увеличения размерности пространства признаков.

Так, например, поле «Location», содержащее значе-

ния «Moscow», «Berlin», «New York», воспринимается моделью как набор символьных строк, не имеющих математической структуры. После кодирования эти значения преобразуются в числовые категории, обеспечивая их включение в процесс построения классификационных правил и снижение риска интерпретационных ошибок.

В данной задаче используется метод Label Encoding — обеспечивает присвоение каждому уникальному значению в столбце уникальный целочисленный идентификатор. Это просто и эффективно для таких моделей, как Random Forest, работающие с категориальными признаками без необходимости бинаризации.

После подготовки и предварительной обработки данных следует этап — разделение датасета на обучающую и тестовую выборки. Это необходимо для объективной оценки качества модели машинного обучения.

Для исключения переобучения модели принято делить данные на две независимые части:

- обучающая выборка (training set) — используется для обучения модели;
- тестовая выборка (test set) — используется исключительно для оценки качества модели, как будто она «предсказывает будущее».

Разделение осуществляется с помощью функции train_test_split из библиотеки sklearn.model_selection.

В задачах с несбалансированными классами (например, когда атак всего 5% событий), при случайном делении может получиться, что в тестовой выборке атак будет слишком мало или вообще не будет. Это исказит метрики точности. Параметр stratify=y гарантирует, что доля классов в train и test будет пропорциональна общей выборке.

Тестирование и апробация на модели машинного обучения с обучающей выборкой

Таблица 4 / Table 4

Матрица ошибок
Error matrix

	Фактический класс: 1 (атака)	Фактический класс: 0 (нормальная активность)
Предсказано: 1 (атака)	True Positive (TP) / 148108	False Positive (FP) / 2
Предсказано: 0 (нормальная активность)	False Negative (FN) / 12425	True Negative (TN) / 86356

На данном этапе проведено непосредственное обучение модели машинного обучения, которая должна научиться классифицировать события информационной безопасности как атаки (IsAttack = 1) или нормальные действия (IsAttack = 0) на основе признаков, подготовленных на предыдущих этапах.

В качестве алгоритма классификации используется алгоритм Случайного леса (Random Forest) — один из самых популярных и эффективных алгоритмов для задач классификации и регрессии. Он хорошо работает с категориальными и числовыми признаками, устойчив к переобучению и не требует масштабирования данных.

Алгоритм случайного леса строит ансамбль B решающих деревьев $\{T_b\}_{b=1}^{B}$. Каждое дерево возвращает оценку вероятности принадлежности объекта к классу «атака»: $p_b(1 \mid x) = \Pr_{T_b}(Y = 1 \mid x)$. Итоговое предсказание ансамбля определяется как усреднение вероятностей по всем деревьям: $\hat{p}_{RF}(1 \mid x) = \frac{1}{B}\sum_{b=1}^{B} p_b(1 \mid x)$. Окончательное решение о классе принимается на основе порога τ: $f(x) = 1\{\hat{p}_{RF}(1 \mid x) \geq \tau\}$, где $\tau \in [0,1]$ – настраиваемый параметр (обычно $\tau = 0{,}5$).

После обучения модели на тренировочной выборке проведена оценка её способности обобщать знания на новых, ранее не встречавшихся данных. Это важнейший этап, поскольку именно он показывает, насколько хорошо модель будет работать в реальных условиях.

В таблице 4 представлены результаты матрицы ошибок.

Обозначение элементов матрицы:

TP – Модель правильно предсказала атаку, и это действительно была атака (148 108);

FP – Модель ошибочно предсказала атаку, но это была нормальная активность (2);

FN – Модель предсказала нормальную активность, но это была атака (12425);

TN – Модель правильно предсказала нормальную активность, и это действительно нормальная активность (86356).

В табл. 5 представлены оценки качества модели на основе метрик классификации.

Анализ метрик классификации показывает, что обученная модель на основе алгоритма случайного леса (Random Forest) продемонстрирова-

Таблица 5 / Table 5

Оценка качества модели
Model quality assessment

Метка класса	precision	recall	f1-score	support
0	0.92	1.00	0.96	148110
1	1.00	0.87	0.93	98781
accuracy			0.95	245891
macro avg	0.96	0.94	0.95	245891
weighted avg	0.95	0.95	0.95	245891

ла высокую эффективность при распознавании как допустимых, так и недопустимых событий информационной безопасности. Результаты представлены в таблице 5.

По классу 0 (нормальные события) зафиксированы значения Precision = 0.92, Recall = 1.00 и F1-score = 0.96, что свидетельствует о корректной идентификации фоновой активности без ложных срабатываний.

Особый интерес представляют результаты по классу 1, отражающему недопустимые события (атаки). Precision = 1.00 означает, что все события, классифицированные моделью как атаки, действительно являются недопустимыми. Значение Recall = 0.87 указывает на способность модели обнаруживать 87% всех инцидентов данного типа, что позволяет минимизировать риск пропуска критически опасных событий. Итоговый показатель F1-score = 0.93 подтверждает высокий уровень сбалансированности между точностью и полнотой классификации именно недопустимых событий.

Общая точность модели (accuracy) составила 0.95, что отражает корректную классификацию 95% всех событий выборки. Дополнительно, значения макро- и взвешенных средних метрик подтверждают устойчивость модели при работе с несбалансированными классами и её практическую пригодность для задач автоматизированного мониторинга.

Таким образом, модель не только демонстрирует общее высокое качество работы, но и обеспечивает достоверную идентификацию недопустимых событий, что соответствует ключевой цели исследования.

Полученные результаты демонстрируют, что модель является эффективным инструментом для автоматического обнаружения атак в потоке событий безопасности. При этом есть потенциал для дальнейшего повышения полноты выявления атакующих действий с помощью дополнительных методов оптимизации и постобработки.

Разработанная автором методика подготовки и оценки обучающей выборки включает структурированный набор этапов, направленных на формирование качественной и репрезентативной выборки для построения модели машинного обучения на объектах критической информационной инфраструктуры, рис. 3.

В рамках предложенной методики построения обучающей выборки для классификации недопустимых событий информационной безопасности реализуется ряд последовательных этапов, каждый из которых имеет прикладную направленность на обеспечение достоверности, устойчивости и воспроизводимости модели в условиях критической информационной инфраструктуры.

На первом этапе формулируется задача бинарной классификации, направленная на автоматическое разграничение событий на допустимые и недопустимые, в зависимости от их потенциальной угрозы для функционирования системы.

На втором этапе осуществляется сбор исходных данных из различных реальных источников — сетевых журналов, системных логов, телеметрии с объектов КИИ, функционирующих в энергетической отрасли, что позволяет обеспечить отраслевую релевантность выборки.

Формирование меток классов реализуется путём генерации бинарного целевого признака «IsAttack» на основании категориального параметра «Event Type», где события, относящиеся к атакующим действиям, маркируются как положительный класс.

На этапе предобработки выполняется очистка данных от дубликатов и пропусков, нормализация значений, а

Рис. 3. Методика подготовки и оценки обучающей выборки

Fig. 3. Methodology for preparing and evaluating the training sample

также исключение признаков, потенциально способных привести к утечке информации или переобучению модели, включая «Event Type», «Event Description» и «Timestamp».

Кодирование категориальных признаков осуществляется с использованием метода «LabelEncoder», применяемого ко всем строковым атрибутам, включая такие параметры, как «Location», «Protocol», «User» и др., с целью преобразования их в числовой формат, пригодный для машинной обработки.

С целью уменьшения размерности и устранения избыточной информации в признаковом пространстве был проведён корреляционный анализ. Для числовых признаков использовался коэффициент Пирсона, а для категориальных — метрика Cramér's V.

Признаки, демонстрирующие высокую корреляцию ($|r| > 0.85$), были проанализированы на предмет мультиколлинеарности, и дублирующие переменные удалялись. Кроме того, с использованием алгоритма Random Forest была рассчитана важность признаков (feature importance), по результатам которой исключались слабопредсказательные характеристики. Такой подход позволил минимизировать переобучение и повысить устойчивость модели к шумам в исходных данных.

Важность признака *j* определяется как среднее уменьшение критерия качества (например, индекса Джини) [18] по всем деревьям ансамбля:

$$I_j = \frac{1}{B}\sum_{b=1}^{B}\Delta \mathrm{Im}\, p_{b,j},$$

где $\Delta \mathrm{Im} p_{b,j}$ – суммарное уменьшение критерия при использовании признака *j* в дереве T_b.

Балансировка классов реализуется посредством методов повторной выборки (oversampling, undersampling), а также с возможным применением синтетической генерации данных (например, алгоритма SMOTE) для устранения диспропорции между редкими атаками и фоновыми событиями.

На этапе стратификации выборка делится на обучающую и тестовую части с сохранением исходного соотношения классов, что позволяет избежать искажений, связанных с дисбалансом, и обеспечивает репрезентативность тестирования.

Оценка обучающей выборки включает в себя анализ распределения классов, выявление выбросов и контроль достаточности представления различных типов атакующих сценариев.

Заключительный этап верификации модели направлен на оценку её качества по целевым метрикам – «Precision», «Recall» и «F1-score» для атакующего класса, что позволяет объективно оценить способность модели к детектированию критически значимых инцидентов при ограничении ложноположительных срабатываний.

Сравнительный анализ предложенной модели с альтернативными подходами

Для обоснования эффективности предложенного подхода была проведена серия сравнительных экспериментов с использованием четырёх распространённых моделей машинного обучения: логистической регрессии (LR), метода опорных векторов (SVM), градиентного бустинга над решающими деревьями (XGBoost) и случайного леса (Random Forest). Все модели обучались на идентичной выборке, сформированной на основе событий реального объекта критической информационной инфраструктуры, что обеспечило корректность сравнения при сохранении отраслевого контекста.

Логистическая регрессия (LR). Линейный классификатор, оценивающий вероятность принадлежности объекта к классу. Отличается простотой и интерпретируемостью, но плохо выявляет нелинейные зависимости, характерные для атакующих сценариев.

Метод опорных векторов (SVM). Строит разделяющую гиперплоскость и может использовать ядровые функции. Обеспечивает высокую точность на сбалансированных данных, однако чувствителен к параметрам и слабо масштабируется при больших объёмах событий.

Градиентный бустинг (XGBoost). Ансамблевый метод, формирующий модель из последовательности деревьев. Отличается высокой точностью и способностью работать с несбалансированными данными, но требует тщательной настройки и чувствителен к выбросам.

Случайный лес (Random Forest). Ансамбль деревьев решений, объединяющий их предсказания. Устойчив к переобучению, эффективно работает с шумными данными и дисбалансом классов, обеспечивая надёжную классификацию недопустимых событий в критической инфраструктуре.

Для оценки эффективности классификатора используются элементы матрицы ошибок:

TP – количество верно определённых атак (True Positive),

FP – количество ложных срабатываний (False Positive),

FN – количество пропущенных атак (False Negative),

TN – количество верно определённых нормальных событий (True Negative).

На их основе рассчитываются следующие показатели:

Точность (Precision):

$$Precision = \frac{TP}{TP + FP}.$$

Полнота (Recall):

$$Recall = \frac{TP}{TP + FN}.$$

F1-мера:

$$F1 = 2 * \frac{Precision * Recall}{Precision + Recall}.$$

Общая точность (Accuaracy):

$$Accuaracy = \frac{TP + TN}{TP + TN + FP + FN}.$$

Основными метриками оценки качества служили точность (precision), полнота (recall), F1-мера и общая точность классификации (accuracy), табл. 6.

Как видно из таблицы, модель на основе случайного леса показала наилучшие результаты по всем основным метрикам. Особенно важно, что при полном отсутствии ложноположительных срабатываний (precision = 1.00), модель сохраняет высокий уровень полноты (recall = 0.87), что критично при эксплуатации в

Таблица 6 / Table 6

Сравнительный анализ
Comparative analysis

Модель	Precision (class 1)	Recall (class 1)	F1-score (class 1)	Accuracy
Logistic Regression	0.84	0.72	0.77	0.88
SVM	0.87	0.75	0.80	0.90
XGBoost	0.92	0.85	0.88	0.94
Random Forest	1.00	0.87	0.93	0.95

условиях КИИ. Другие модели демонстрируют либо высокую точность с недостаточной полнотой (например, SVM), либо сбалансированные, но менее выраженные результаты (логистическая регрессия).

Таким образом, предложенный подход демонстрирует превосходство как в части общей точности, так и в способности корректно идентифицировать атаки при минимизации ложных тревог, что особенно значимо при защите объектов, где избыточная реакция может нарушить технологический процесс.

Заключение

В отличие от универсальных решений, применяемых в системах информационной безопасности общего назначения, модель, предлагаемая в данной работе, ориентирована на специфику критической информационной инфраструктуры (КИИ). Недопустимые события в КИИ, как правило, имеют предиктивный контекст и формируются в результате определённой последовательности действий (прекурсоров), что позволяет выстраивать поведенческие цепочки. В структуре событий, использованных в модели, особое внимание уделяется таким признакам, как событие-предшественник (Preceding Event), действие (Action), уровень важности (Severity), характеристики устройства (Device Attributes) и задействованные ресурсы (Resources), поскольку именно они отражают смысловую нагрузку инцидента в промышленной среде. Использование признаков, характерных для протоколов Modbus, IEC-104, DNP3 и иных отраслевых стандартов, позволяет модели учитывать особенности технологических процессов и связи между элементами системы управления.

В ходе проведённого исследования была разработана и экспериментально апробирована модель машинного обучения, предназначенная для классификации недопустимых событий в системах критической информационной инфраструктуры. Основное отличие предложенного подхода заключается в ориентации на отраслевую специфику: модель обучается на реальных событиях, зафиксированных в корпоративной среде энергетического предприятия, с учётом специфики промышленных протоколов и поведенческих паттернов.

Разработанная методика построения обучающей выборки включает семантическое обоснование значимости признаков, стратификацию событий и исключение признаков, способных привести к переобучению или утечке информации. Сравнительный анализ с альтернативными моделями показал превосходство алгоритма случайного леса по метрикам полноты и F1-меры при сохранении нулевого уровня ложноположительных срабатываний.

Предложенный подход обеспечивает высокую точность автоматического выявления атакующих действий при минимизации ложных тревог, что критически важно для условий эксплуатации КИИ. В перспективе планируется расширение выборки, включение методов глубокого обучения и адаптация модели для потоковой обработки событий в режиме реального времени.

Литература

1. Lee R. M., Assante M. J., Conway T. Analysis of the Cyber Attack on the Ukrainian Power Grid [Электрон. ресурс]. SANS Industrial Control Systems, 2016. Режим доступа: https://icscsi.org/library/Documents/Cyber_Events/E-ISAC%20-%20Analysis%20of%20the%20Cyber%20Attack%20on%20the%20Ukrainian%20Power%20Grid.pdf.

2. Cybersecurity and Infrastructure Security Agency (CISA). DarkSide Ransomware: Best Practices for Preventing Business Disruption [Электрон. ресурс]. CISA Reports, 2021. Режим доступа: https://www.cisa.gov/sites/default/files/publications/AA21-131A_Darkside_Ransomware.pdf.

3. Методика оценки угроз безопасности ФСТЭК России [Электрон. ресурс]. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g.

4. Евдокимова Д.А., Микрюков А.А. Актуальные задачи выявления недопустимых событий на объектах критической информационной инфраструктуры // Открытое образование. 2024. Т. 28. № 4. DOI: 10.21686/1818-4243-2024-4-33-42.

5. Евдокимова Д.А., Микрюков А.А. Задача детектирования недопустимых событий информационной безопасности в информационной инфраструктуре // Открытое образование. 2025. Т. 29. № 1. DOI: 10.21686/1818-4243-2025-1-65-76.

6. ML-модель [Электрон. ресурс]. Режим доступа: https://www.decosystems.ru/ml-model/.

7. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94 [Электрон. ресурс]. Gaithersburg: National Institute of Standards and Technology, 2007. 127 с. Режим доступа: https://icscsi.org/library/Documents/Standards/NIST%20-%20800-94%20-%20Guide%20to%20Intrusion%20Detection%20and%20Prevention%20 Systems.pdf.

8. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection [Электрон. ресурс] // IEEE Symposium on Security and Privacy. 2010. С. 305–316. Режим доступа: https://ai.nsu.ru/attachments/download/2429.

9. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey [Электрон. ресурс] // ACM Computing Surveys. 2009. Т. 41. № 3. С. 1–58. Режим доступа: https://vs.inf.ethz.ch/edu/HS2011/CPS/papers/chandola09_anomaly-detection-survey.pdf.

10. Siddiqui M. A., Wang M., Lee J. Detecting Internet Worms Using Data Mining Techniques [Электрон. ресурс] // Journal of Network and Computer Applications. 2008. Т. 31. № 4. С. 300–313. Режим доступа: https://www.researchgate.net/publication/228630212_Detecting_Internet_Worms_Using_Data_Mining_Techniques.

11. Zuech R., Khoshgoftaar T. M., Wald R. Intrusion detection and Big Heterogeneous Data: A Survey [Электрон. ресурс] // Journal of Big Data. 2015. Т. 2. № 1. С. 1–41. Режим доступа: https://www.researchgate.net/publication/276397551_Intrusion_detection_and_Big_Heterogeneous_Data_a_Survey.

12. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection [Электрон. ресурс] // IEEE Communications Surveys & Tutorials. 2016. Т. 18. № 2. С. 1153–1176. Режим доступа: https://www2.cs.uh.edu/~acl/cs6397/Presentation/2016-IEEE-A%20survey%20of%20DM%20and%20ML%20methods%20for%20cyber%20security%20ID.pdf.

13. Positive Technologies. Машинное обучение в информационной безопасности [Электрон. ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/our-technologies/ml-tekhnologii/.

14. Использование машинного обучения для борьбы с DDoS атаками [Электрон. ресурс]. Режим доступа: https://habr.com/ru/articles/785942/.

15. Ангапов В.Д., Бобров А.В., Тимонин В.А., Вишняков А.С. Использование технологий машинного обучения в защите информационных систем // Наука, техника и образование. 2023. № 4(92). С. 20–26. DOI: 10.24411/2312-8267-2023-10401.

16. Machine Learning Based Network Vulnerability Analysis of Industrial Internet of Things [Электрон. ресурс]. Режим доступа: https://arxiv.org/abs/1911.05771.

17. Как самому разработать систему обнаружения компьютерных атак на основе машинного обучения [Электрон. ресурс]. Режим доступа: https://habr.com/ru/articles/538296/.

18. Breiman L. Random Forests [Электрон. ресурс] // Machine Learning. 2001. Т. 45. № 1. С. 5–32. Режим доступа: https://link.springer.com/article/10.1023/A:1010933404324.

References

1. Lee R. M., Assante M. J., Conway T. Analysis of the Cyber Attack on the Ukrainian Power Grid [Internet]. SANS Industrial Control Systems; 2016. Available from: https://icscsi.org/library/Documents/Cyber_Events/E-ISAC%20-%20Analysis%20of%20the%20Cyber%20Attack%20on%20the%20Ukrainian%20Power%20Grid.pdf.

2. Cybersecurity and Infrastructure Security Agency (CISA). DarkSide Ransomware: Best Practices for Preventing Business Disruption [Internet]. CISA Reports; 2021. Available from: https://www.cisa.gov/sites/default/files/publications/AA21-131A_Darkside_Ransomware.pdf.

3. Metodika otsenki ugroz bezopasnosti FSTEK Rossii = Methodology for assessing security threats of the Federal Service for Technical and Export Control of Russia [Internet]. Available from: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g. (In Russ.)

4. Yevdokimova D.A., Mikryukov A.A. Actual tasks of identifying unacceptable events at critical information infrastructure facilities. Otkrytoye obrazovaniye = Open Education. 2024; 28: 4. DOI: 10.21686/1818-4243-2024-4-33-42. (In Russ.)

5. Yevdokimova D.A., Mikryukov A.A. The problem of detecting unacceptable information security events in the information infrastructure. Otkrytoye obrazovaniye = Open Education. 2025; 29: 1. DOI: 10.21686/1818-4243-2025-1-65-76. (In Russ.)

6. ML-model' = ML model [Internet]. Available from: https://www.decosystems.ru/ml-model/. (In Russ.)

7. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94 [Internet]. Gaithersburg: National Institute of Standards and Technology; 2007. 127 p. Available from: https://icscsi.org/library/Documents/Standards/NIST%20-%20800-94%20-%20Guide%20to%20Intrusion%20Detection%20and%20Prevention%20 Systems.pdf.

8. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection [Internet]. IEEE Symposium on Security and Privacy. 2010: 305–316. Available from: https://ai.nsu.ru/attachments/download/2429.

9. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey [Internet]. ACM Computing Surveys. 2009; 41; 3: 1–58. Available from: https://vs.inf.ethz.ch/edu/HS2011/CPS/papers/chandola09_anomaly-detection-survey.pdf.

10. Siddiqui M. A., Wang M., Lee J. Detecting Internet Worms Using Data Mining Techniques [Internet]. Journal of Network and Computer Applications. 2008; 31; 4: 300–313. Available from: https://www.researchgate.net/publication/228630212_Detecting_Internet_Worms_Using_Data_Mining_Techniques.

11. Zuech R., Khoshgoftaar T. M., Wald R. Intrusion detection and Big Heterogeneous Data: A Survey [Internet]. Journal of Big Data. 2015; 2; 1: 1–41. Available from: https://www.researchgate.net/publication/276397551_Intrusion_detection_and_Big_Heterogeneous_Data_a_Survey.

12. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection [Internet]. IEEE Communications Surveys & Tutorials. 2016; 18; 2: 1153–1176. Available from: https://www2.cs.uh.edu/~acl/cs6397/Presentation/2016-IEEE-A%20survey%20of%20DM%20and%20ML%20methods%20for%20cyber%20security%20ID.pdf.

13. Positive Technologies. Mashinnoye obucheniye v informatsionnoy bezopasnosti = Machine Learning in Information Security [Internet]. Available from: https://www.ptsecurity.com/ru-ru/our-technologies/ml-tekhnologii/.

14. Ispol'zovaniye mashinnogo obucheniya dlya bor'by s DDoS atakami = Using Machine Learning to Combat DDoS Attacks [Internet]. Available from: https://habr.com/ru/articles/785942/. (In Russ.)

15. Angapov V.D., Bobrov A.V., Timonin V.A., Vishnyakov A.S. Using Machine Learning Technologies to Protect Information Systems. Nauka, tekhnika i obrazovaniye = Science, Technology, and Education. 2023; 4(92): 20-26. DOI: 10.24411/2312-8267-2023-10401. (In Russ.)

16. Machine Learning Based Network Vulnerability Analysis of Industrial Internet of Things [Internet]. Available from: https://arxiv.org/abs/1911.05771.

17. Kak samomu razrabotat' sistemu obnaruzheniya komp'yuternykh atak na osnove mashinnogo obucheniya = How to develop a computer attack detection system based on machine learning [Internet]. Available from: https://habr.com/ru/articles/538296/. (In Russ.)

18. Breiman L. Random Forests [Internet]. Machine Learning. 2001; 45; 1: 5–32. Available from: https://link.springer.com/article/10.1023/A:1010933404324.

Сведения об авторе

Д.А. Добрецова
Российский экономический университет им. Г.В. Плеханова, Москва, Россия

Information about the author

D.A. Dobretsova
Plekhanov Russian University of Economics, Moscow, Russia