УДК 004.056 DOI: 10.17587/prin.13.68-80

А. М. Вульфин, канд. техн. наук, доц., vulfin.alexey@gmail.com,
Уфимский государственный авиационный технический университет

Обнаружение сетевых атак в гетерогенной промышленной сети на основе технологий машинного обучения

Рассматриваются вопросы совершенствования алгоритмов обнаружения сетевых атак в гетерогенной сети промышленного Интернета вещей на основе технологий машинного обучения для последующей интеграции с подсистемами центра мониторинга и реагирования на инциденты информационной безопасности. Разработана структурная схема системы обнаружения сетевых атак и алгоритм интеллектуального анализа параметров сетевого трафика в задаче обнаружения вредоносной сетевой активности. Проанализированы варианты построения ансамблей классификаторов на основе моделей машинного обучения и гетерогенных нейросетевых моделей. Оценка F1-меры при работе с тестовыми выборками на распространенных общедоступных наборах размеченного сетевого трафика достигает 96 %. Рассмотрена возможность встраивания полученных моделей. Разработан виртуальный полигон для оценки эффективности применения моделей машинного обучения для обнаружения сетевых атак.

Ключевые слова: *сетевые атаки, машинное обучения, интеллектуальный анализ данных, ансамбль классификаторов, гетерогенная промышленная сеть, мониторинг и реагирование на инциденты информационной безопасности*

Введение

На современном этапе цифрой трансформации индустрии актуальными являются вопросы поддержания работоспособности киберфизических систем, т. е. обеспечения устойчивости протекающих в них физических процессов и непрерывности управления технологическими процессами в условиях возможных внутренних и внешних целенаправленных деструктивных воздействий. Наблюдается тенденция [1] к интеграции устройств промышленного (индустриального) Интернета вещей (IIoT) с традиционными системами сбора данных и управления (SCADA) в составе промышленных систем. Глубокое проникновение IIoT в критическую инфраструктуру и производственный сектор также привело к возрастанию вероятности и числа потенциальных кибератак.

По данным отчета Claroty в 2020 г. число уязвимостей, выявленных в компонентах автоматизированных систем управления технологическими процессами (АСУ ТП), выросло почти на 25 % по сравнению с 2019 г. Обнаруженные уязвимости в основном затрагивают секторы промышленного производства, энергетики и водоснабжения. В первом полугодии 2020 г. по сравнению с 2019 г. число уязвимостей в сфере промышленности выросло на 87,3 %, в секторе водоснабжения — на 122 %, в энергетическом секторе — на 58,9 %.

По данным аналитических отчетов Positive Technologies промышленность уже на протяжении двух лет входит в тройку наиболее часто атакуемых отраслей. Число атак на промышленность увеличилось почти в 2 раза по сравнению с 2019 г.: прирост составил 91 %. В IV квартале 2020 г. треть всех инцидентов в промышленной отрасли была связана с кибератаками, в 84 % атак применялось вредоносное программное обеспечение.

Ущерб от кибератак на энергетические и коммунальные отрасли достигает в среднем 13,2 млн долл. США ежегодно, и повышение рисков вынуждает к выработке общих подходов к обеспечению кибербезопасности [2, 3].

Для выявления целевых атак на промышленные системы необходим анализ значительного объема входящего, исходящего и внутреннего сетевого трафика и потока событий информационной безопасности (ИБ) для выявления аномальной активности, анализа вектора атаки и оценки возможного ущерба. Для решения подобных задач применяется комплексный подход — развертывание центра мониторинга и реагирования на инциденты ИБ (*Security Operation Center* — SOC), осуществляющего, в том числе, сбор, хранение и анализ трафика [4] как корпоративного сегмента, так и сегмента промышленной сети. Это позволяет выделять шаблоны проведения атак или использования уязвимостей. Основной целью управления инцидентами ИБ является обеспечение непрерывного мониторинга событий ИБ, своевременное реагирование на инциденты, устранение последствий и формирование шаблонов реагирования для предотвращения возникновения инцидентов в будущем. Следовательно, для промышленного оборудования

и пограничных систем (точек входа в промышленную сеть) необходимо обеспечить анализ трафика для обнаружения сетевых атак с поддержкой анализа промышленных протоколов. Совершенствование средств защиты сетевой инфраструктуры направлено на развитие инструментов интеллектуального мониторинга сетевого трафика и состояния объектов и узлов промышленной сети.

Целью работы, результаты которой представлены в настоящей статье, является совершенствование алгоритмов обнаружения сетевых атак в гетерогенной сети промышленного Интернета вещей на основе технологий машинного обучения для последующей интеграции с подсистемами центра мониторинга и реагирования на инциденты ИБ.

Обнаружение сетевых атак в промышленных сетях на основе методов машинного обучения

Для оперативного анализа и выявления аномалий работы сетевой инфраструктуры, вызванных действиями злоумышленника, применяют технологии интеллектуального анализа и машинного обучения [5], что нашло отражение в ряде публикаций:

- модель обнаружения гибридных аномалий в высоконагруженных сетях связи на основе методов интеллектуального анализа данных (ИАД) [6];
- платформа обнаружения аномалий для выявления кибератак на облачные вычислительные среды [7];
- комплексная система контроля и обеспечения безопасности сбора данных, реализующая мониторинг трафика в реальном времени, обнаружение аномалий, анализ воздействия, стратегии смягчения последствий [8, 9];
- система обнаружения аномалий на основе алгоритмов машинного обучения для устранения угроз кибербезопасности сетей Интернета вещей в умном городе [10];
- подход на основе кластерного анализа сетевого трафика для обнаружения кибератак, вызывающих аномалии в сетях критической информационной инфраструктуры газокомпрессорных станций [11];
- распределенная система обнаружения вторжений для систем диспетчерского управления и сбора данных [12];
- алгоритм обнаружения аномалий и система обнаружения вторжений с фильтрацией ложных срабатываний и возможностью подтверждения атаки [13];
- система обнаружения аномалий для обнаружения утечек конфиденциальной информации в сетевом трафике энергосистем [14];
- методология создания надежных наборов данных для обнаружения аномалий в АСУ ТП [15].

Для создания моделей машинного обучения (ML-моделей) используют общедоступные размеченные по типам атак и режимам работы базы сетевого трафика (NSL-KDD [16], CICIDS2017 [17], UNSW-NB15 [18], BOT-IOT и др.). Для обнаружения новых сетевых атак, реализуемых с помощью постоянно развивающегося инструментария злоумышленников, необходимо периодическое обновление тренировочных наборов с реализацией новых сценариев атак и фиксацией параметров их проведения для дообучения ML-моделей.

Так, например, в работе [19] описан стенд, построенный с применением промышленного оборудования, для исследований алгоритмов машинного обучения в задачах обнаружения сетевых атак. В ходе реализации сложных атак по различным сценариям собран сетевой трафик, соответствующий нормальной работе системы и аномальным состояниям — сетевым атакам. Особенностью этого набора данных является акцент на использование промышленных протоколов, в первую очередь, протокола Modbus в варианте Modbus-over-TCP [20].

Проведя разведку и закрепившись в промышленной сети, злоумышленник может модифицировать управляющие команды или показания датчиков, что может привести к серьезным киберфизическим последствиям. Сетевые атаки на SCADA-системы условно можно разделить на три категории: разведка, внедрение управляющих команд и атаки отказа в обслуживании (DoS/DDoS).

В работе [19] рассмотрены разведывательные сетевые атаки сканирования для выявления возможных уязвимостей, эксплуатация которых позволит злоумышленнику закрепиться в сегменте промышленной сети. Часть атак, при реализации которых существенно возрастает число пересылаемых пакетов, уверенно обнаруживаются стандартными сигнатурными методами. Но большая часть атак с использованием эксплоитов практически не изменяет основные характеристики трафика промышленных протоколов, что делает очень затруднительным подбор сигнатур для их обнаружения. Применение ML-методов позволяет выявить особенности аномального трафика и построить соответствующий детектор.

Система обнаружения сетевых атак в гетерогенной сети промышленного Интернета вещей

Структурная схема системы обнаружения сетевых атак в гетерогенной сети промышленного Интернета вещей на основе интеллектуального анализа данных представлена на рис. 1. Коллектор (4) сетевых сессий собирает параметры трафика с агентов, установленных в ключевых точках сетевой инфраструктуры: агрегирующих коммутаторах, пограничном межсетевом экране, с точек доступа в виде дампа трафика канального уровня и в формате сессий (семейство протоколов netFlow). Модули (5) предобработки, выделения признаков и хранения статистики сетевого трафика позволяют фиксировать в долгосрочном хранилище (ICS БД) компактное описание сетевых сессий, что позволяет проводить ретроспективный анализ накопленных данных и оперативное обновление индикаторов компрометации при взаимодействии (6) с внешними платформами киберразведки. Модуль анализа и генерации признаков (8) используется при подготовке размеченных данных для по-

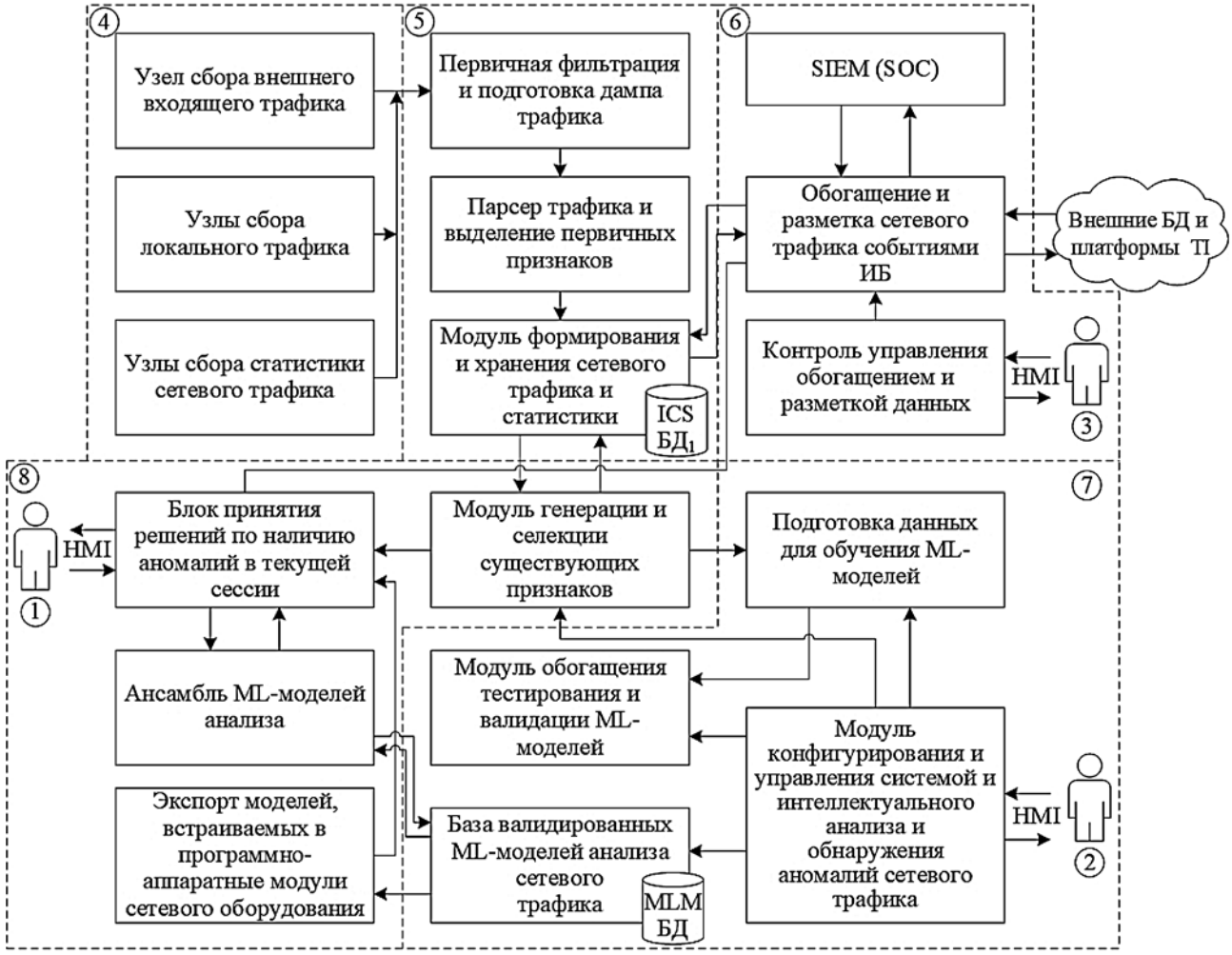

Рис. 1. Структурная схема системы обнаружения сетевых атак на основе интеллектуального анализа данных:
HMI — *Human-machine interface*, человеко-машинный интерфейс; платформа TI — *Threat Intelligence*, платформа управления данными киберразведки

строения и обучения моделей машинного обучения, сохраняемых в БД (MLM БД) для дальнейшего использования при оперативном анализе входящего и внутреннего сетевого трафика.

Модуль обогащения, тестирования и проверки ML-моделей позволяет провести дополнительную разметку сетевого трафика, связав определенные события ИБ с соответствующими сетевыми сессиями.

Оперативное двухстороннее взаимодействие системы в целом с подсистемой управления событиями безопасности и центром мониторинга ИБ и реагирования на инциденты (SIEM (SOC)) позволяет передавать метрики и дополнительную информацию о параметрах текущего состояния сети для последующей агрегации и анализа. Процессом разметки (обогащения) записей сетевых сессий управляет специалист (3) по сетевой безопасности текущего сегмента.

Специалист по интеллектуальному анализу данных (2) управляет работой ансамбля ML-моделей, выполняет задачи по корректировке параметров его работы и своевременного обновления банка моделей.

Итоговый блок принятия решений по обнаружению атак взаимодействует со специалистом (1) по сетевой безопасности и визуализирует результаты анализа ансамбля ML-моделей.

Обобщенный алгоритм интеллектуального анализа параметров сетевого трафика в задаче обнаружения аномалий и вредоносной сетевой активности изображен на рис. 2. Представлены основные этапы сбора и обработки данных для построения и использования ML-моделей.

В целях оценки эффективности предлагаемого решения использовались общедоступные размеченные по типам атак и режимам работы базы данных сетевого трафика (NSL-KDD, CICIDS2017, UNSW-NB15, сети промышленного Интернета вещей — WUSTL-IIOT-2018; беспроводные промышленные сенсорные сети — WSN-DS-2016) и полусинтетические наборы, собранные с использованием полунатурного стенда, моделирующего сегменты корпоративной и промышленной сетей.

Особенностью указанных наборов данных является акцент на использование промышленных протоколов (таких как Modbus). Применение методов машинного обучения и интеллектуального анализа данных позволяет выявить при этом особенности аномального вредоносного трафика атак и внедренных эксплоитов, построить соответствующий детектор.

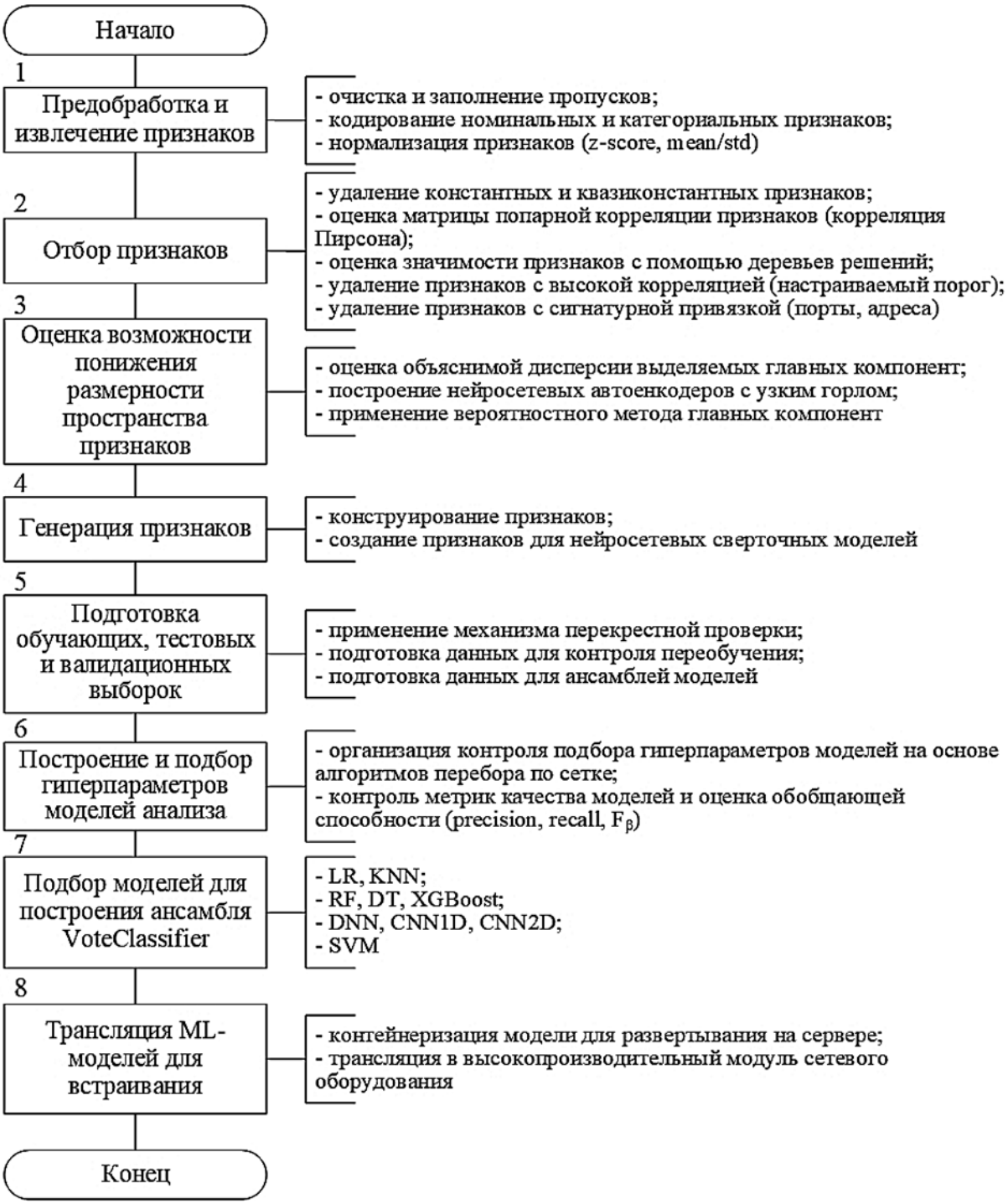

Рис. 2. Обобщенный алгоритм интеллектуального анализа сетевого трафика в задаче обнаружения аномалий и вредоносной сетевой активности

Вычислительные эксперименты

Предлагаемый алгоритм интеллектуального анализа сетевого трафика применялся для анализа наборов данных, представленных в табл. 1.

Далее рассмотрим специфику реализации алгоритма для каждого из наборов данных.

Предобработка и извлечение признаков. На этапе предобработки удаляются идентичные признаки, заполняются или удаляются признаки, содержащие нечисловые значения NaN и Infinity. Значения категориальных признаков (Flow ID, Source IP, Destination IP и Timestamp) преобразуются в численные значения с помощью соответствующей схемы порядкового или унитарного кодирования (Label Encoder или One-Hot-Encoder).

Далее выполняется нормализация признаков с приведением к нулевому среднему и единичному стандартному отклонению.

Таблица 1

Анализируемые наборы данных сетевого трафика

Набор данных	Число сетей (кластеров)	Длительность сбора данных/число записей	Классы атак	Инструменты извлечения признаков	Число признаков	Детальное описание эксперимента
NSL-KDD [17]	2	5 недель/148 517	4	Bro-IDS	41	[21]
CICIDS2017 [18]	1	5 дней/2 830 540	15	CICFlowMeter	84	[22]
UNSW-NB15 [19]	33	16 дней 15 часов/2 059 419	9	Argus, Bro-IDS и др.	47	[23]
WUSTL-IIOT-2018 [19]	1	25 часов/7 037 983	5	ARGUS	4	[24]
WSN-DS-2016 [25]	5	1 день/374 661	4	LEACH protocol	19	[26]

Поскольку наборы данных не сбалансированы, применяют следующие схемы:

- удаление классов с очень малым числом примеров (например, Heartbleed, Web Attack— Sql Injection, Infiltration, Web Attack — XSS и Bot для набора CICIDS2017);
- аугментация имеющейся выборки на основе алгоритмов увеличения числа примеров миноритарного класса (алгоритмы SMOTE) или удаление примеров мажоритарного класса.

Оценка возможности понижения размерности пространства признаков. Оценка суммарной объяснимой дисперсии данных в зависимости от числа главных компонент для набора данных CICIDS2017 представлена на рис. 3.

Ощутимое влияние на долю объясняемого коэффициента дисперсии оказывают первые 20 главных компонент. Дальнейшая процедура отбора признаков позволит существенно сократить их общее число, поэтому применение процедуры понижения размерности пространства признаков не является необходимым. Для набора данных WSN-DS-2016 лучший результат удалось достичь, применив нейросетевой автоенкодер с четырехслойной архитектурой, осуществляющий нелинейное сжатие пространства признаков. Для набора данных NSL-KDD число выделенных главных компонент варьировалось в пределах 4...24.

Отбор признаков. Ярко выраженные сигнатурные признаки, согласно работе [27], удаляются: Flow ID, Source IP, Source Port, Destination IP, Destination Port, Protocol и Timestamp. Это позволит строить модели ML, которые ориентированы на обнаружение статистических особенностей сетевых сессий, соотнесенных с сетевыми атаками, а не с сигнатурными параметрами, которые могут быть изменены или подделаны злоумышленником, и с которыми хорошо справляются традиционные системы обнаружения сетевых атак.

Далее применяют алгоритмы отбора и оценки значимости признаков. Набор данных разделяют на обучающую и тестовую выборки в соотношении 0,7 и 0,3. На обучающей выборке с помощью алгоритма перекрестной проверки с разбиением на 10 групп строится классификатор на основе дерева решений с последующей оценкой значимости признаков. Пример ранжирования признаков по степени значимости для принятия решения о принадлежности к заданному классу для набора данных CICIDS2017 приведен на рис. 4.

Оценка значимости признаков выполняется также с помощью комитета (k = 250) случайных деревьев решений (RF) с использованием процедуры перекрестной проверки. Гистограмма оценки значимости выделенных с помощью RF признаков представлена на рис. 5.

Для набора данных WUSTL-IIOT-2018 оценка значимости признаков по аналогичному сценарию позволяет выдвинуть гипотезу о возможности оставить один или два наиболее значимых признака для построения классификатора (рис. 6, см. вторую сторону обложки).

Используемые методы отбора признаков позволяют сократить их число в 4—5 раз.

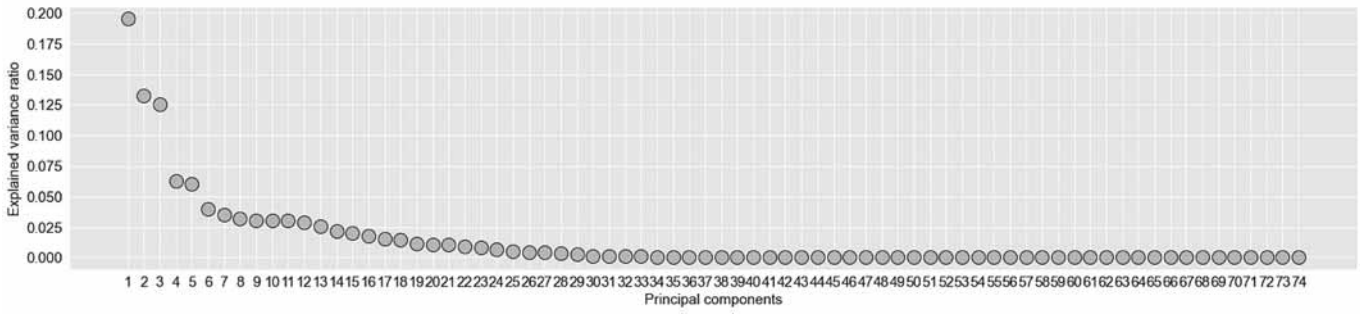

Рис. 3. Зависимость суммарной объяснимой дисперсии (ось ординат) от числа главных компонент (ось абсцисс)

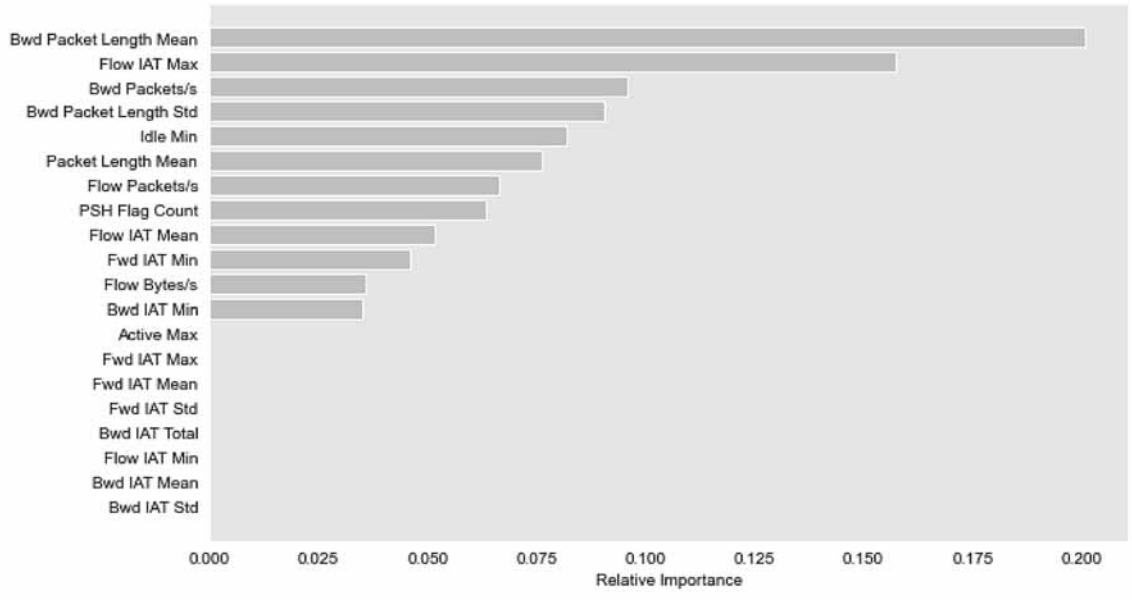

Рис. 4. Гистограмма оценки значимости признаков (ось ординат — признаки), полученная с помощью классификатора на основе дерева решений (ось абсцисс — относительные единицы)

Выполняется поиск и удаление константных и квазиконстантных (с порогом вариабельности (дисперсия) за период анализа (обучающая выборка) 0,005). Далее проводится оценка степени попарной корреляции признаков и удаление признаков с коэффициентом корреляции более установленного порога (например, для набора данных CICIDS2017 порог выбран равным 0,8). Итоговая тепловая карта матрицы попарной корреляции приведена на рис. 7. Полученные результаты согласуются с данными работы [27].

Для понижения размерности пространства признаков CICIDS2017 и визуализации распределения примеров по классам применен метод стохастического вложения соседей с *t*-распределением для понижения размерности пространства признаков и визуализации распределения примеров по классам (рис. 8, см. вторую сторону обложки). Визуализация классов атак и нормальной работы набора данных WUSTL-IIOT-2018, напротив, позволяет сделать однозначный вывод о наличии структуры данных с сокращенным набором признаков и возможности дальнейшего построения классификатора (рис. 9, см. вторую сторону обложки).

Построение классификаторов и ансамблей. Для решения задачи обнаружения сетевых атак на основе формализованного вектора признаков необходимо создание и подбор параметров моделей машинного обучения. Применена процедура оптимизации

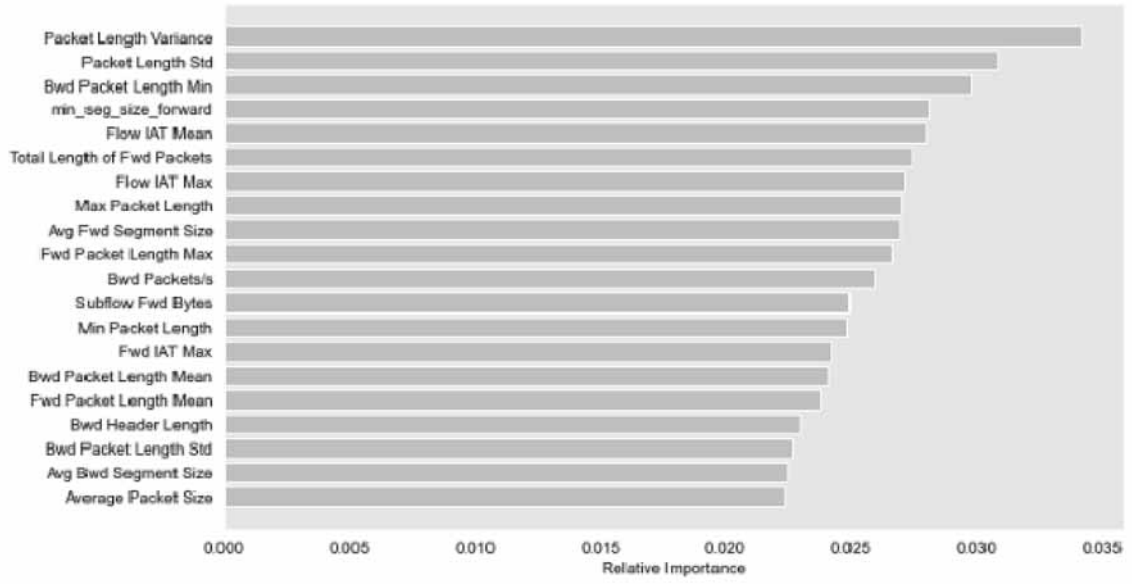

Рис. 5. Гистограмма оценки значимости признаков (ось ординат — признаки), полученная с помощью классификатора на основе комитета деревьев решений (ось абсцисс — относительные единицы)

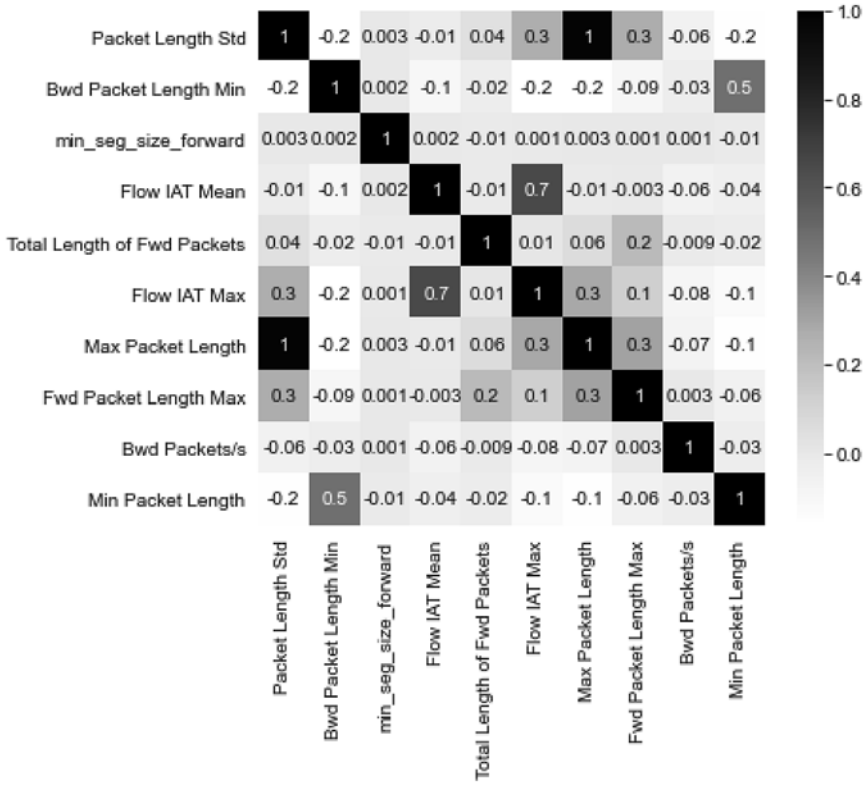

Рис. 7. Матрица попарной корреляции после исключения связанных признаков CICIDS2017 (коэффициент корреляции в диапазоне [−1, 1])

гиперпараметров каждой модели с применением поиска по сетке, перекрестной проверкой с десятью проходами и оценкой качества модели на выделяемой тестовой выборке.

Применяемые классификаторы [28]:

- на основе алгоритма градиентного бустинга для ансамбля деревьев решений (XGBClassifier);
- на основе комитета деревьев решений (*Random Forest*, RF);
- на основе k-ближайших соседей (*K-Nearest Neighbors*, KNN);
- на основе машины опорных векторов (*Support Vector Machines*, SVM);
- на основе логистической регрессии (*Logistic* Regression, LR);
- на основе "мелкой" нейронной сети прямого распространения — многослойный персептрон (shallow MLP);
- на основе сверточных нейронных сетей с одномерным и двумерным входным слоем (CNN1D и CNN2D соответственно);
- на основе глубокой нейронной сети (DNN).

Для классификатора на основе сверточной нейронной сети с двумерным входным слоем признаков CNN2D векторы признаков образцов набора преобразованы в графические примитивы размерностью 5×2 (CICIDS2017) в градациях серого (рис. 10).

На заключительном этапе строится ансамбль классификаторов, включающий в себя комитет деревьев решений (RF), классификатор на основе алгоритма градиентного бустинга на ансамбле деревьев решений (XGBClassifier) и ExtraTreesClassifier. Последний реализует метаоценку, соответствующую набору рандомизированных деревьев решений, или деревьев на различных подвыборках набора данных, использует усреднение для повышения точности прогнозирования и контроля избыточной подгонки отдельных моделей. Параметры комитета: тип голосования — soft (голосование и взвешивание предсказаний моделей для каждого класса); веса моделей распределены как {2, 1, 3}.

После подбора параметров классификаторов и выбора ML-моделей, продемонстрировавших приемлемую обобщающую способность, выполняется итоговая оценка моделей. По сочетанию времени, затрачиваемого на обучение модели, суммарного числа настраиваемых параметров модели, показателей F1-меры и правильности (Acc — Accuracy) итоговой модели на тестовой выборке выбран классификатор на основе комитета деревьев решений (табл. 2).

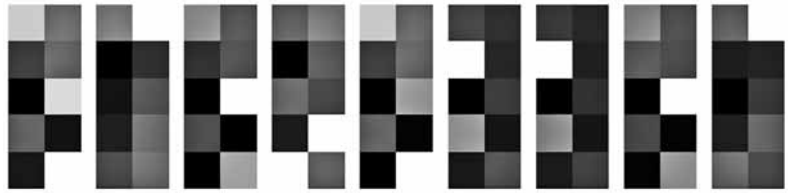

Рис. 10. Двумерное представление признаков примеров набора данных

Таблица 2

Результаты тестирования классификатора

Классификатор	CICIDS2017		NSL-KDD		UNSW-NB15		WUSTL-IIOT-2018		WSN-DS-2016	
	Acc	F1	Acc	F1	Acc	F1	Acc	F1	Acc	F1
RF	0,967	0,910	0,896	0,885	0,897	0,810	0,999	0,919	0,999	0,947

Одни из лучших результатов показывают классификаторы XGBClassifier, случайный лес и нейросетевые модели. В абсолютном значении лучшую эффективность показал VotingClassifier.

Подготовка ML-моделей для встраивания. Обученные ML-модели RF и MLP предлагается использовать в виде встраиваемых программных модулей соответствующего сетевого оборудования. С помощью транслятора с языка Python созданы заголовочные файлы и файлы реализации на языке C с выгрузкой коэффициентов обученных моделей в качестве статических параметров. Дальнейшая компиляция с помощью кросс-компилятора позволила собрать исполняемые модули для платформы ARM семейства специализированных процессоров NXP LX2160A.

Разработка полигона для тестирования предложенных решений

Для тестирования предлагаемых моделей машинного обучения разработана архитектура стенда промышленного объекта, имитирующая основные элементы инфраструктуры (рис. 11), и включающая основные уровни: полевой, сбора данных, управления и т. п.

Мониторинг состояния информационной и сетевой инфраструктуры реализован на основе развернутого решения на базе ELK-стека (Elasticsearch, Beats, Logstash, Kibana) [29].

Процесс мониторинга [29] разбит на пять шагов.

1. Источником событий выступают AuditBeat и WinlogBeat на серверах.

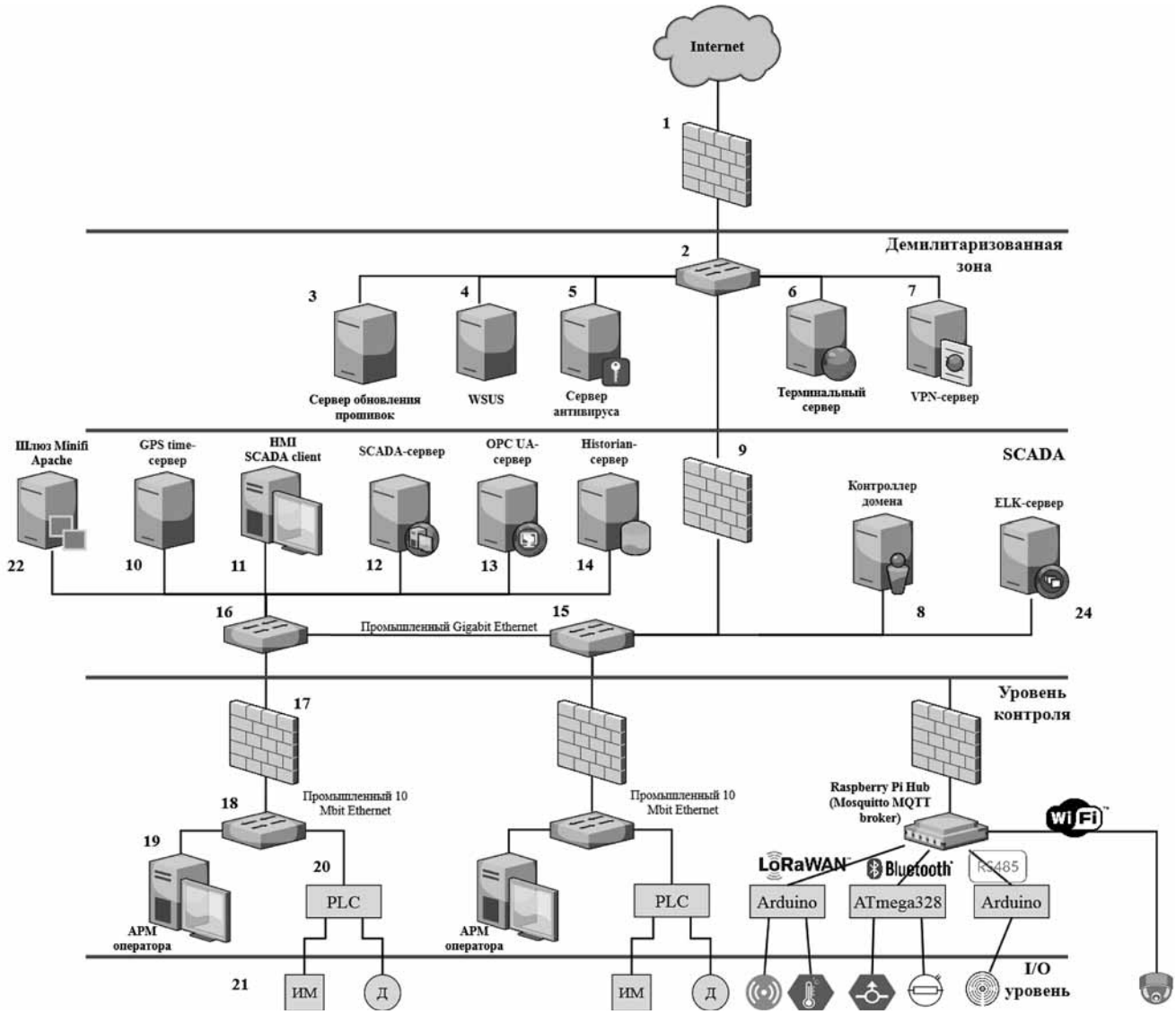

Рис. 11. Архитектура стенда промышленного объекта:
ИМ — исполнительные механизмы; Д — датчики

2. Данные собираются в SIEM-системе Apache NiFi.

3. Хранение происходит в Elasticsearch.

4. Данные обрабатываются и визуализируются с помощью Kibana.

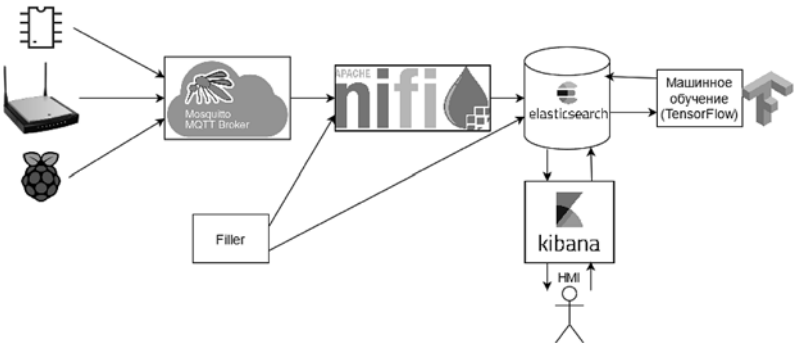

Рис. 12. Упрощенная схема системы сбора и обработки данных о событиях ИБ модельного объекта:
Filler — источник дополнительных данных о событиях ИБ

5. Полученная информация анализируется экспертами.

Упрощенная схема системы сбора и обработки данных о событиях ИБ модельного объекта приведена на рис. 12.

Данные поступают в систему мониторинга, сбора и корреляции событий ИБ в промышленной сети через коллектор данных (реализованный с помощью MQTT-брокера). Связующим звеном является Apache NiFi-сервер, пересылающий полученные данные в Elasticsearch, где к ним может иметь доступ подсистема машинного обучения на базе TensorFlow.

Согласно архитектуре стенда (см. рис. 11 и 12), в системе эмуляции и виртуализации EVE-NG [30] спроектирован и реализован стенд, изображенный на рис. 13.

Краткие описания устройств в составе стенда приведены в табл. 3.

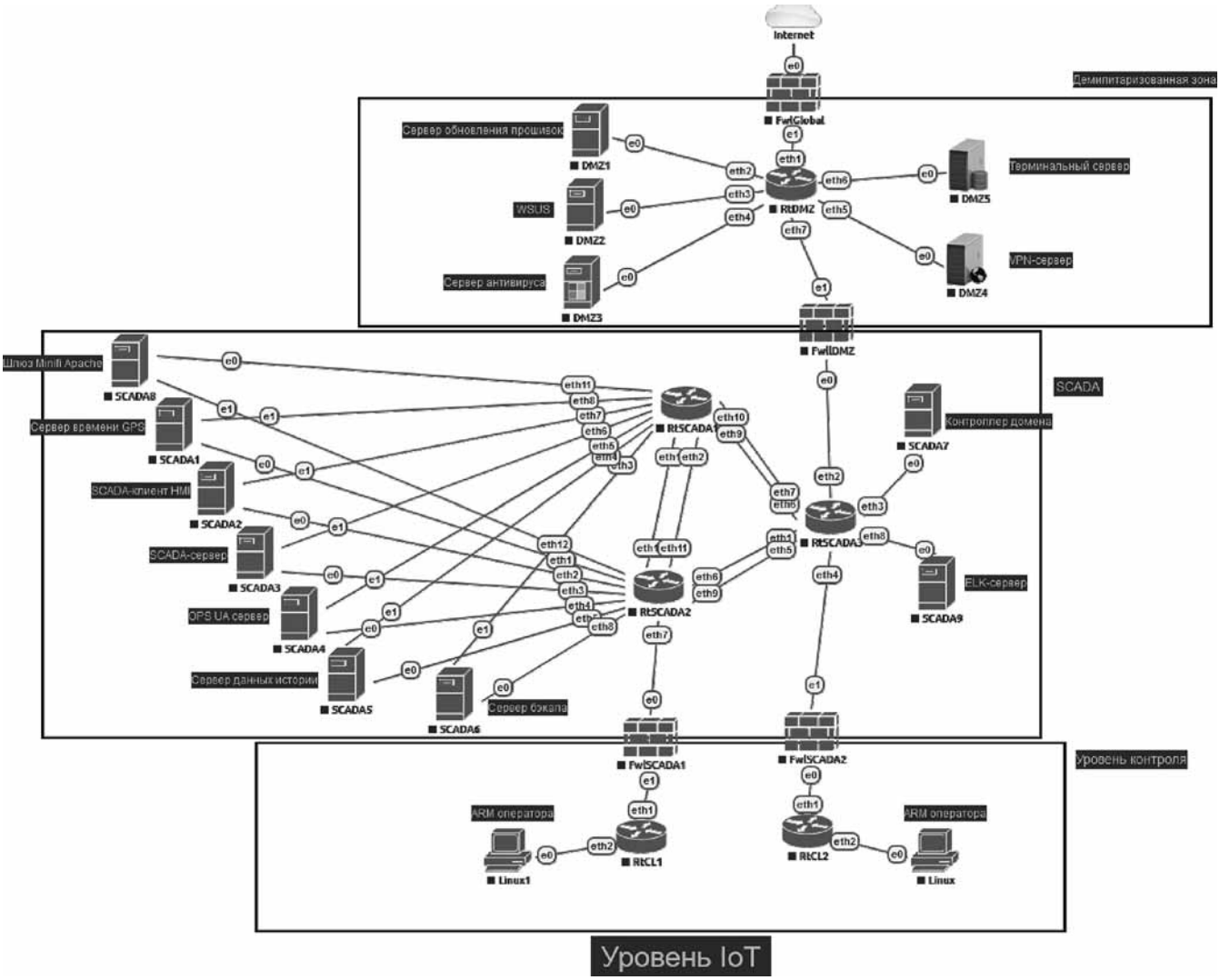

Рис. 13. Архитектура разработанного стенда сегмента промышленной сети:
e0-e1, eth0-eth10 — нумерация сетевых интерфейсов

Таблица 3

Список использованных устройств и их характеристики

№	Зона	Имя устройства	Тип устройства	Название устройства	Используемый образ
1	Демилитаризованная зона	FwlGlobal	Межсетевой экран pfSense	—	Pfsense-CE-2.4.5
2	Демилитаризованная зона	RtDMZ	Маршрутизатор Mikrotik	—	mikrotik-7.0b
3	Демилитаризованная зона	DMZ1	Linux-сервер	Сервер обновления прошивок	linux-Kali-full
4	Демилитаризованная зона	DMZ2	Linux-сервер	WSUS	windows-server-2016
5	Демилитаризованная зона	DMZ3	Linux-сервер	Сервер антивируса	linux-Kali-full
7	Демилитаризованная зона	DMZ4	Linux-сервер	VPN-сервер	linux-Kali-full
6	Демилитаризованная зона	DMZ5	Linux-сервер	Терминальный сервер	linux-Kali-full
9	Демилитаризованная зона	FwlDMZ	Межсетевой экран pfSense	—	pfsense-CE-2.4.5
8	SCADA	SCADA7	Linux-сервер	Контроллер домена	linux-Kali-full
10	SCADA	SCADA1	Linux-сервер	Сервер времени GPS	linux-Kali-full
11	SCADA	SCADA2	Linux-сервер	SCADA-клиент HMI	linux-Kali-full
12	SCADA	SCADA3	Linux-сервер	SCADA-сервер	linux-debian8-openscada
13	SCADA	SCADA4	Linux-сервер	OPS UA-сервер	linux-Kali-full
14	SCADA	SCADA5	Linux-сервер	Сервер данных истории	linux-Kali-full
15	SCADA	RtSCADA1	Маршрутизатор Mikrotik	—	mikrotik-7.0b
16	SCADA	RtSCADA3	Маршрутизатор Mikrotik	—	mikrotik-7.0b
17	SCADA	FwlSCADA1	Межсетевой экран pfSense	—	pfsense-CE-2.4.5
22	SCADA	SCADA8	Linux-сервер	Шлюз Minifi Apache	linux-Debian-10-srv
23	SCADA	RtSCADA2	Маршрутизатор Mikrotik	—	mikrotik-7.0b
24	SCADA	SCADA9	Linux-сервер	ELK-сервер	linux-ELK
25	SCADA	SCADA6	Linux-сервер	Сервер бэкапа	linux-Debian-10-srv
26	SCADA	FwlSCADA2	Межсетевой экран pfSense	—	pfsense-CE-2.4.5
18	Уровень контроля	RtCL1	Маршрутизатор Mikrotik	—	mikrotik-7.0b
19	Уровень контроля	Linux	ПК с ОС Linux	ARM оператора	linux-tinycore-6.4
27	Уровень контроля	RtCL2	Маршрутизатор Mikrotik	—	mikrotik-7.0b
28	Уровень контроля	Linux1	ПК с ОС Linux	ARM оператора	linux-tinycore-6.4

ELK-сервер (24) осуществляет сбор всех типов данных для их последующего использования в системе машинного обучения распознавания аномалий сетевого трафика.

Эксперименты в виртуальном полигоне с разработанными ML-моделями и сценариями реализации сетевых атак подтвердили эффективность предлагаемого решения.

Заключение

Разработана и описана структурная схема системы обнаружения сетевых атак на основе интеллектуального анализа данных.

Разработаны алгоритмы интеллектуального анализа параметров сетевого трафика в задаче обнаружения вредоносной сетевой активности. Приведена общая схема алгоритма. Проанализированы варианты построения ансамблей и комитетов классификаторов на основе традиционных моделей машинного обучения (модели случайного леса, рандомизированные деревья решений и пр.) и гетерогенных нейросетевых моделей (глубокие нейронные сети, сверточные нейронные сети и модели на основе автоенкодеров с долгой краткосрочной памятью). Оценка F1-меры при работе с тестовыми выборками достигает 96 %.

Проанализирована возможность встраивания полученных моделей в качестве модулей сетевого оборудования для повышения оперативности анализа сетевого трафика промышленных систем или использования в составе сетевой системы обнаружения вторжений.

Эффективность полученных решений при оценке качества обнаружения сетевых атак на исходных наборах данных сравнима для протестированных моделей. Наиболее перспективным для применения в специализированных сигнальных процессорах

сетевого оборудования является классификатора на основе комитета случайных деревьев. Данный классификатор обеспечивает хорошее качество обнаружения сетевых атак и не требует значительных вычислительных ресурсов при запуске модели с подобранными в процессе обучения коэффициентами.

Разработан виртуальный полигон для оценки эффективности применения ML-моделей для обнаружения сетевых атак. Дальнейшие исследования направлены на разработку методики испытаний моделей в различных сценариях реализации целенаправленных многошаговых сетевых атак.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-08-00668.

Список литературы

1. **Moore B.** Gartner's top 10 IoT tech trends // IT Brief. URL: https://itbrief.com.au/story/gartner-s-top-10-iot-tech-trends
2. **Актуальные киберугрозы**: IV квартал 2020 года. Отчет Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q4/
3. **Ландшафт угроз** для систем промышленной автоматизации. 2019 год // Kaspersky ICS CERT. URL: https://ics-cert.kaspersky.ru/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-2019-report-at-a-glance/
4. **Cecil A.** A Summary of Network Traffic Monitoring and Analysis Techniques. URL: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html
5. **Гайфулина Д. А., Котенко И. В.** Применение методов глубокого обучения в задачах кибербезопасности. Часть 1 // Вопросы кибербезопасности. 2020. № 3. С. 76—86.
6. **Monshizadeh M., Khatri V., Atli B., Kantola R.** Performance evaluation of a combined anomaly detection platform // IEEE Access. 2019. Vol. 7. P. 100964—100978.
7. **Moustafa N., Creech G., Sitnikova E., Keshk M.** Collaborative anomaly detection framework for handling big data of cloud computing // 2017 military communications and information systems conference (MilCIS). IEEE, 2017. P. 1—6.
8. **Ten C. W., Manimaran G., Liu C. C.** Cybersecurity for critical infrastructures: Attack and defense modeling // IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans. 2010. Vol. 40, No. 4. P. 853—865.
9. **Ten C. W., Hong J., Liu C. C.** Anomaly detection for cybersecurity of the substations // IEEE Transactions on Smart Grid. 2011. Vol. 2, No 4. P. 865—873.
10. **Alrashdi I., Alqazzaz A., Al Oufi E.** et al. Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning // 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2019. P. 305—310.
11. **Kiss I., Genge B., Haller P., Sebestyen G.** Data clustering-based anomaly detection in industrial control systems // 2014 IEEE 10th International Conference on Intelligent Computer Communication and Processing (ICCP). IEEE, 2014. P. 275—281.
12. **Cruz T., Rosa L., Proença J.** et al. A cybersecurity detection framework for supervisory control and data acquisition systems // IEEE Transactions on Industrial Informatics. 2016. Vol. 12, No. 6. P. 2236—2246.
13. **Tartakovsky A. G., Polunchenko A. S., Sokolov G.** Efficient computer network anomaly detection by changepoint detection methods // IEEE Journal of Selected Topics in Signal Processing. 2012. Vol. 7, No 1. P. 4—11.
14. **Keshk M., Sitnikova E., Moustafa N.** et al. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems // IEEE Transactions on Sustainable Computing. 2019. Vol. 6. № 1. P. 66—79.
15. **Gómez Á. L. P., Fernández-Maimó L., Huertas A.** et al. On the generation of anomaly detection datasets in industrial control systems // IEEE Access. 2019. Vol. 7. P. 177460—177473.
16. **Tavallaee M., Bagheri E., Lu W., Ghorbani A.** A detailed analysis of the KDD CUP 99 data set // 2009 IEEE symposium on computational intelligence for security and defense applications. IEEE, 2009. P. 1—6.
17. **Sharafaldin I., Lashkari A. H., Ghorbani A. A.** Toward generating a new intrusion detection dataset and intrusion traffic characterization // ICISSp. 2018. Vol. 1. P. 108—116.
18. **Moustafa N., Slay J.** UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) // 2015 military communications and information systems conference (MilCIS). IEEE, 2015. P. 1—6.
19. **Teixeira M., Salman T., Zolanvari M., Jain R.** SCADA system testbed for cybersecurity research using machine learning approach // Future Internet. 2018. Vol. 10, No. 8. P. 76.
20. **Miciolino E., Bernieri G., Pascucci F., Setola R.** Communications network analysis in a SCADA system testbed under cyber-attacks // 2015 23rd Telecommunications Forum Telfor (TELFOR). IEEE, 2015. P. 341—344.
21. **Sapozhnikova M. U., Nikonov A. V., Vulfin A. M.** Intrusion detection system based on data mining technics for industrial networks // 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). IEEE, 2018. P. 1—5.
22. **Vulfin A., Vasilyev V., Gvozdev V.** et al Network traffic analysis based on machine learning methods // Journal of Physics: Conference Series. IOP Publishing, 2021. Vol. 2001, No 1. P. 012017.
23. **Gurin M., Vulfin A., Vasilyev V., Nikonov A.** Intrusion detection system on the basis of data mining algorithms in the industrial network // CEUR Workshop Proceedings. 2019. P. 553—565.
24. **Vulfin A., Vasilyev V., Kuharev S.** Algorithms for detecting network attacks in an enterprise industrial network based on data mining algorithms // Journal of Physics: Conference Series. IOP Publishing, 2021. Vol. 2001, No. 1. P. 012004.
25. **Almomani I., Al-Kasasbeh B., Al-Akhras M.** WSN-DS: A dataset for intrusion detection systems in wireless sensor networks // Journal of Sensors. 2016. Vol. 2016. P. 4731953:1-4731953:16.
26. **Васильев В. И., Вульфин А. М., Картак В. М.** и др. Система обнаружения атак в беспроводных сенсорных сетях промышленного Интернета вещей // Труды ИСА РАН. 2019. Т. 69, № 4. С. 70—78.
27. **Горюнов М. Н., Мацкевич А. Г., Рыболовлев Д. А.** Синтез модели машинного обучения для обнаружения компьютерных атак на основе набора данных CICIDS2017 // Труды ИСП РАН. 2020. Т. 32, № 5. С. 81—93.
28. **Kotsiantis S. B.** Supervised machine learning: A review of classification techniques // Informatica. 2007. Vol. 31, No. 3. URL: https://www.researchgate.net/publication/265544297_Supervised_Machine_Learning_A_Review_of_Classification_Techniques
29. **Вульфин А. М.** Система управления данными кибер разведки // Моделирование, оптимизация и информационные технологии. 2021. Т. 9 (1). URL: https://moitvivt.ru/ru/journal/pdf?id=925 DOI: 10.26102/2310-6018/2021.32.1.020.
30. **Tobarra L., Robles-Gómez A., Pastor V.** et al. A Cybersecurity Experience with Cloud Virtual-Remote Laboratories // Multidisciplinary Digital Publishing Institute Proceedings. 2019. Vol. 31, No. 1. P. 3.

Detection of Network Attacks in a Heterogeneous Industrial Network Based on Machine Learning

A. M. Vulfin, vulfin.alexey@gmail.com, Ufa State Aviation Technical University

Corresponding author:

Vulfin Aleksey M., Associate Professor, Ufa State Aviation Technical University
E-mail: vulfin.alexey@gmail.com

Received on January 25, 2021
Accepted on December 15, 2021

The paper discusses the issues of improving algorithms for detecting network attacks in a heterogeneous industrial Internet of Things network based on machine learning technologies for subsequent integration with the subsystems of the center for monitoring and responding to information security incidents. A structural diagram of a network attack detection system and an algorithm for intelligent analysis of network traffic parameters in the task of detecting malicious network activity have been developed. Variants of constructing ensembles of classifiers based on machine learning models and heterogeneous neural network models are analyzed. The F1-measure score when working with test samples reaches 96 %. The possibility of embedding the obtained models as modules of network equipment to increase the efficiency of the analysis of network traffic of industrial systems or use as part of a network intrusion detection system is considered. The efficiency of the obtained solutions in assessing the quality of network attack detection on the original datasets is comparable for the tested models. The most promising for use in specialized signal processors of network equipment is a classifier based on a committee of random trees, since it provides good quality detection of network attacks and does not require significant computing resources when launching a model with coefficients selected during training. Monitoring the state of information and network infrastructure is implemented on the basis of a deployed solution based on the ELK stack. A virtual testing ground has been developed to assess the effectiveness of ML-models for detecting network attacks. Further research is aimed at developing a methodology for testing models in various scenarios for the implementation of targeted multi-step network attacks.

Keywords: *network attacks, machine learning, data mining, ensemble of classifiers, heterogeneous industrial network, monitoring and response to information security incidents*

For citation:

Vulfin A. M. Detection of Network Attacks in a Heterogeneous Industrial Network Based on Machine Learning, *Programmnaya Ingeneria,* 2022, vol. 13, no. 2, pp. 68—80.

DOI: 10.17587/prin.13.68-80

References

1. **Moore B.** Gartner's top 10 IoT tech trends, *IT Brief*, available at: https://itbrief.com.au/story/gartner-s-top-10-iot-tech-trends

2. **Topical Cyber Threats:** Q4 2020. Positive Technologies report, available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q4/

3. **Threat landscape** for industrial automation systems. 2019 year, *Kaspersky ICS CERT,* available at: https://ics-cert.kaspersky.ru/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-2019-report-at-a-glance/

4. **Cecil A.** A Summary of Network Traffic Monitoring and Analysis Techniques, available at: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html.

5. **Gaifulina D. A., Kotenko I. V.** Application of deep learning methods in cybersecurity tasks, *Voprosy kiberbezopasnosti*, 2020, no. 3, pp. 76—86 (in Russian).

6. **Monshizadeh M., Khatri V., Atli B., Kantola R.** Performance evaluation of a combined anomaly detection platform, *IEEE Access*, 2019, vol. 7, pp. 100964—100978.

7. **Moustafa N., Creech G., Sitnikova E., Keshk M.** Collaborative anomaly detection framework for handling big data of cloud computing, *2017 military communications and information systems conference (MilCIS),* IEEE, 2017, pp. 1—6.

8. **Ten C. W., Manimaran G., Liu C. C.** Cybersecurity for critical infrastructures: Attack and defense modeling, *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 2010, vol. 40, no. 4, pp. 853—865.

9. **Ten C. W., Hong J., Liu C. C.** Anomaly detection for cybersecurity of the substations, *IEEE Transactions on Smart Grid*, 2011, vol. 2, no. 4, pp. 865—873.

10. **Alrashdi I., Alqazzaz A., Al Oufi E.** et al. Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning, *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC),* IEEE, 2019, pp. 305—310.

11. **Kiss I., Genge B., Haller P., Sebestyen G.** Data clustering-based anomaly detection in industrial control systems, *2014 IEEE 10th International Conference on Intelligent Computer Communication and Processing (ICCP),* IEEE, 2014, pp. 275—281.

12. **Cruz T., Rosa L., Proença, J.** et al. A cybersecurity detection framework for supervisory control and data acquisition systems, *IEEE Transactions on Industrial Informatics*, 2016, vol. 12, no. 6, pp. 2236—2246.

13. **Tartakovsky A. G., Polunchenko A. S., Sokolov G.** Efficient computer network anomaly detection by changepoint detection methods, *IEEE Journal of Selected Topics in Signal Processing*, 2012, vol. 7, no. 1, pp. 4—11.

14. **Keshk M., Sitnikova E., Moustafa N.** et al. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems, *IEEE Transactions on Sustainable Computing*, 2019, vol. 6, no. 1, pp. 66—79.

15. **Gómez Á. L. P., Fernández-Maimó L., Huertas A.** et al. On the generation of anomaly detection datasets in industrial control systems, *IEEE Access*, 2019, vol. 7, pp. 177460—177473.

16. **Tavallaee M.,Bagheri E., Lu W., Ghorbani A.** A detailed analysis of the KDD CUP 99 data set, *2009 IEEE symposium on computational intelligence for security and defense applications,* IEEE, 2009, pp. 1—6.

17. **Sharafaldin I., Lashkari A. H., Ghorbani A. A.** Toward generating a new intrusion detection dataset and intrusion traffic characterization, *ICISSp*, 2018, vol. 1, pp. 108—116.

18. **Moustafa N., Slay J.** UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set), *2015 military communications and information systems conference (MilCIS),* IEEE, 2015, pp. 1—6.

19. **Teixeira M., Salman T., Zolanvari M., Jain R.** SCADA system testbed for cybersecurity research using machine learning approach, *Future Internet*, 2018, vol. 10, no. 8, pp. 76.

20. **Miciolino E., Bernieri G., Pascucci F., Setola R.** Communications network analysis in a SCADA system testbed under cyber-attacks, *2015 23rd Telecommunications Forum Telfor (TELFOR),* IEEE, 2015, pp. 341—344.

21. **Sapozhnikova M. U., Nikonov A. V., Vulfin A. M.** Intrusion detection system based on data mining technics for industrial networks, *2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM),* IEEE, 2018, pp. 1—5.

22. **Vulfin A., Vasilyev V., Gvozdev V.** et al. Network traffic analysis based on machine learning methods, *Journal of Physics: Conference Series. IOP Publishing*, 2021, vol. 2001, no. 1, pp. 012017.

23. **Gurin M., Vulfin A., Vasilyev V., Nikonov A.** Intrusion detection system on the basis of data mining algorithms in the industrial network, *CEUR Workshop Proceedings*, 2019, pp. 553—565.

24. **Vulfin A., Vasilyev V., Kuharev S.** Algorithms for detecting network attacks in an enterprise industrial network based on data mining algorithms, *Journal of Physics: Conference Series. IOP Publishing*, 2021, vol. 2001, no. 1, pp. 012004.

25. **Almomani I., Al-Kasasbeh B., Al-Akhras M.** WSN-DS: A dataset for intrusion detection systems in wireless sensor networks, *Journal of Sensors*, 2016, vol. 2016, pp. 4731953:1—4731953:16.

26. **Vasilyev V. I., Vulfin A. M., Kartak V. M.** et al. System of attacks detection in wireless sensor networks of Industrial Internet of Things, *Trudy ISA RAN*, 2019, vol. 69, no. 4, pp. 70—78 (in Russian).

27. **Goryunov M. N., Matskevich A. G., Rybolovlev D. A.** Synthesis of a Machine Learning Model for Detecting Computer Attacks Based on the CICIDS2017 Dataset, *Trudy ISP RAN*, 2020, vol. 32, no. 5, pp. 81—93 (in Russian).

28. **Kotsiantis S. B.** Supervised machine learning: A review of classification techniques, *Informatica,* 2007, vol. 31, no. 3, available at: https://www.researchgate.net/publication/265544297_Supervised_Machine_Learning_A_Review_of_Classification_Techniques

29. **Vulfin A. M.** Cyber threat intelligence data management system, *Modeling, optimization and information technology.* 2021, vol. 9 (1), available at: https://moitvivt.ru/ru/journal/pdf?id=925, DOI: 10.26102/2310-6018/2021.32.1.020 (in Russian).

30. **Tobarra L., Robles-Gómez A., Pastor V.** et al. A Cybersecurity Experience with Cloud Virtual-Remote Laboratories, *Multidisciplinary Digital Publishing Institute Proceedings*, 2019, vol. 31, no. 1, pp. 3.

ИНФОРМАЦИЯ

Рисунки к статье **А. М. Вульфина**
«ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК В ГЕТЕРОГЕННОЙ ПРОМЫШЛЕННОЙ СЕТИ НА ОСНОВЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ»

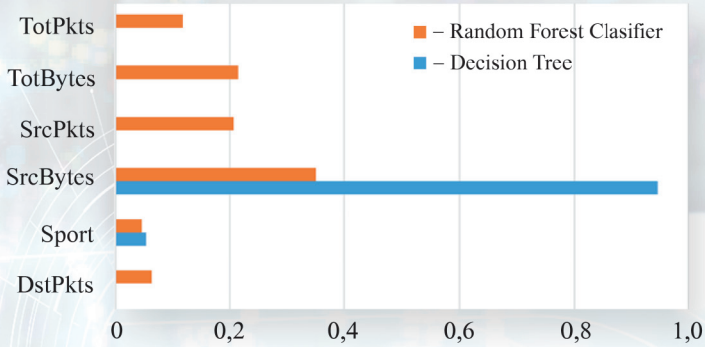

Рис. 6. Оценка значимости признаков с помощью классификатора на основе дерева решений и классификатора на основе комитета случайных деревьев

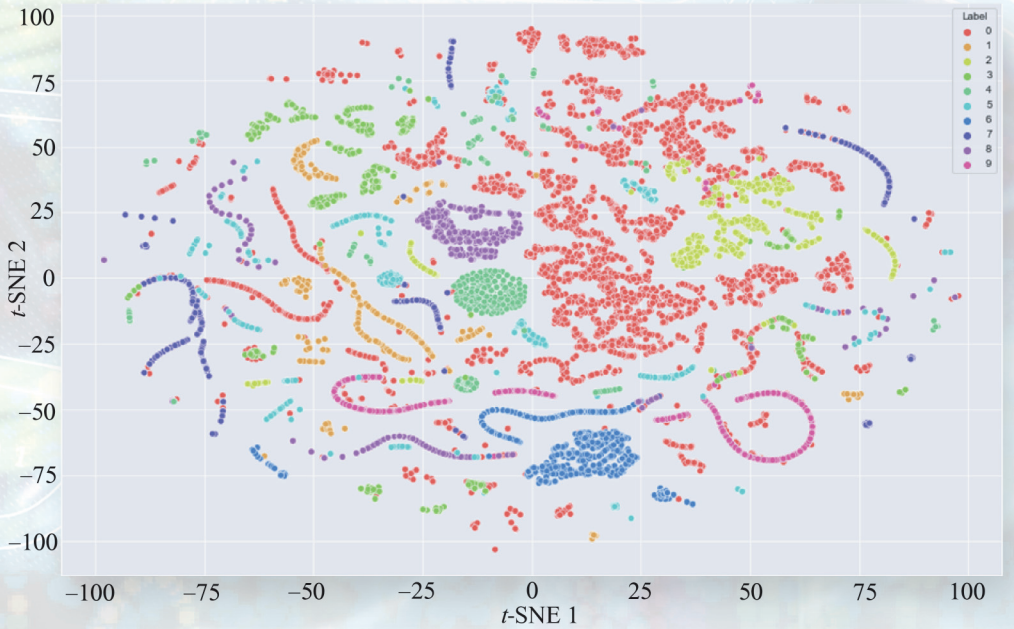

Рис. 8. Визуализация распределения примеров по классам *t*-распределением (по осям – компоненты *t*-SNE-разложения в диапазоне [–100, 100], 0–9 – метки классов)

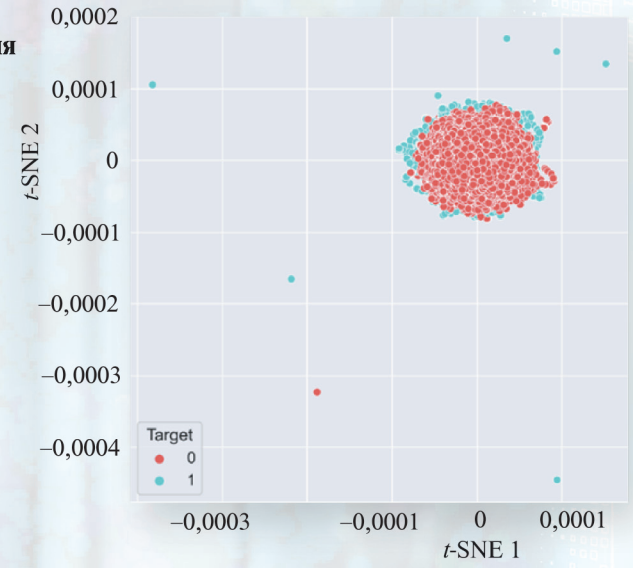

Рис. 9. Визуализация пространства признаков с помощью стохастического вложения соседей с *t*-распределением: 0 – «нормальная работа», 1 – «атака» (по осям – компоненты *t*-SNE-разложения в диапазоне [-100, 100])