DOI: 10.18137/RNU.V9187.24.01.P.99 УДК 004.855.5

И.С. Поздняк, И.С. Макаров

МОДЕЛИ ОБНАРУЖЕНИЯ АТАК С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация. Рассматриваются некоторые способы обнаружения атак на основе машинного обучения, которые применяются для определения аномалий в готовых наборах трафика. Сделан анализ существующего положения дел в сетевой безопасности. Предложена модель обнаружения атак с использованием методов машинного обучения. Рассмотрены вопросы выбора данных для обучения классификаторов по предварительно сформированным критериям. Проведена предварительная обработка выбранных данных. Приведена классификация атак типа Brute Force и DDoS. Обучение нейронных сетей сводится к минимизации функций потерь путем подбора оптимальных весов нейронов в процессе выполнения того или иного оптимизационного итерационного алгоритма. Сделан вывод об оптимальности модели на основе решающего древа в вопросе классификации на основе логической регрессии.

Ключевые слова: сетевая безопасность, атаки, машинное обучение, DDoS-атака, атака полным перебором Brute Force, Python.

I.S. Pozdnyak, I.S. Makarov

ATTACK DETECTION MODELS USING MACHINE LEARNING METHODS

Abstract. The article discusses some machine learning-based attack detection techniques that are used to identify anomalies in ready-made traffic sets. An analysis of the current situation in network security is provided. The authors propose a model for detecting attacks using machine learning methods and consider the issues of selecting data for training classifiers according to pre-generated criteria. Pre-processing of the selected data has been carried out. The article provides a classification of Brute Force and DDoS attacks. Training neural networks consists of minimizing loss functions by selecting optimal neuron weights during the execution of one or another optimization iterative algorithm. A conclusion is made about the model optimality based on the "decision tree" in the matter of classification based on logical regression.

Keywords: network security, attacks, machine learning, DDoS attack, brute force attack, Python.

Введение

В современном мире в связи с быстрыми темпами развития информационных технологий стремительно увеличивается объем сетевого трафика. Несмотря на то что варианты реализации сетей становятся всё сложнее и сетевым устройствам приходится обрабатывать больше данных, пользователи надеются на высокое качество обслуживания. Наряду с ростом сетевых данных постоянно увеличивается количество нарушений информационной безопасности и угроз сетевой безопасности, появляются новые типы атак, становясь серьезной проблемой по мере развития сети. Разнообразие сетевых сервисов и приложений предоставляет злоумышленникам больше возможностей для компрометации сети, чем когда-либо прежде. Брандмауэры, системы глубокой проверки пакетов (далее – DPI) и системы обнаружения вторжений (далее – IDS) являются типичными инструментами обнаружения аномалий, однако стоимость развертывания этих контрмер велика, кроме того, необходимо учитывать сложность системы.

Безопасность сети можно улучшить, добавив дополнительные устройства безопасности, но это не может обеспечить полную защиту. Необходимо учитывать не только су-

Поздняк Ирина Сергеевна
кандидат технических наук, доцент, доцент кафедры информационной безопасности, Поволжский государственный университет телекоммуникаций и информатики, город Самара. Сфера научных интересов: анализ трафика с целью выявления вторжений, построение систем аутентификации, анализ рисков информационной безопасности. Автор более 110 опубликованных научных работ. SPIN-код: 1462-5700, AuthorID: 665953, ScopusAuthorID: 57207763577.
Электронный адрес: i.pozdnyak@psuti.ru

Макаров Игорь Сергеевич
кандидат технических наук, доцент кафедры программной инженерии, Поволжский государственный университет телекоммуникаций и информатики, город Самара. Сфера научных интересов: анализ трафика с целью выявления аномальных характеристик, построение систем аутентификации, аудит информационной безопасности. Автор более 70 опубликованных научных работ. SPIN-код: 4111-9689, AuthorID: 910136, ScopusAuthorID: 57194032397.
Электронный адрес: i.makarov@psuti.ru

ществующие угрозы, но и будущие. Существующие системы IDS обеспечивают многоуровневую защиту на уровне системы, сети, приложения. Многоуровневая безопасность гарантирует, что последующие уровни остановят злоумышленника, преодолевшего один уровень защиты.

Существенными проблемами последних IDS являются:

- недостаточная точность определения угроз;
- динамическое поведение сетевого трафика;
- низкая частота сетевых атак;
- адаптивность к программно-конфигурируемым сетям;
- огромный объем хранимых и передаваемых данных;
- различные устройства доступа к сети.

Большинство существующих IDS представляют собой системы обнаружения на основе сигнатур или аномалий [1]. Системы на основе сигнатур обращаются только к списку известных угроз и их индикаторам компрометации. Они обладают высокой скоростью обработки и точностью определения для известных атак. Тем не менее они не могут идентифицировать атаку нулевого дня и без необходимости выдают предупреждения независимо от результата. Это непрактично для некоторых внутренних атак, кроме того, следует учитывать вид операционной системы, версии и приложений. IDS на основе аномалий могут обнаруживать новое подозрительное поведение, отклоняющееся от нормального. Системы обнаружения вторжений на основе аномалий хорошо справляются с обнаружением атак нулевого дня. Тем не менее повышенная вероятность ложных срабатываний требует дополнительного времени и ресурсов для изучения всех предупреждений о возможных угрозах.

Наряду с этим появляются новые и эффективные методы защиты от сетевых атак, связанные в том числе с методами машинного обучения [2–6].

Машинное обучение

Машинное обучение как аналитический инструмент, основанный на статистике, широко обсуждается и применяется в различных областях. Его способность принимать решения после изучения и анализа данных освобождает людей от обработки огромного их

количества, поэтому машинное обучение обычно используется для исследования сложных сценариев. Кроме того, его реакция на аномальное поведение обычно намного быстрее, чем у людей, что является преимуществом при раннем выявлении. Для известных атак машинное обучение получает опыт из существующих записей, чтобы понять их характеристики, в то время как для неизвестных атак происходит поиск отклонений от внутренних закономерностей данных.

На основе машинного обучения могут создаваться разнообразные модели с различными алгоритмами. Все алгоритмы машинного обучения можно условно разделить на реализующие один из двух основных подходов к решению задачи: *обучение с учителем* и *обучение без учителя* [7]. Ключевое различие между ними состоит в наличии заранее проставленных меток в обучающем наборе данных тренируемой модели.

Как правило, обучение без учителя представляет собой более сложную задачу с менее предсказуемым результатом работы моделей. В большинстве случаев более предпочтительным с точки зрения качества получаемого решения является обучение с учителем, однако последнее требует участия человека в разметке обучающего набора данных, как правило, большого объема. В некоторых случаях это или принципиально невозможно, или требует неадекватно большого времени и человеческого ресурса. В подобной ситуации единственным разумным решением будет прибегнуть к обучению без учителя, оставив за человеком вопросы контроля результата работы алгоритма машинного обучения.

В рамках данной работы перед обучением с учителем будет уделено дополнительное время получению размеченного набора данных, так как трафик можно разметить в полуавтоматическом режиме: автор обучающего набора данных будет заранее знать, является ли трафик вредоносным.

В качестве исходных данных были взяты несколько готовых наборов трафика с атаками [8–11]. Выбор окончательного набора данных для обучения классификаторов производился в соответствии с вторичными критериями, не учитывавшимися в первичном отборе. Эти критерии в своей общности являются более гибкими, и незначительное отклонение по одному или нескольким показателям вполне допустимо.

Рассмотренные варианты сведены в Таблицу 1.

Таблица 1

Сравнение наборов данных

Критерий отбора	**Набор данных**			
	CIC-IDS2017	**CSE-CIC-IDS2018**	**HIKARI-2021**	**USB-IDS-1**
Объем	Средний	Большой	Небольшой	Небольшой
Реалистичность	Синтетический, высокая вариация трафика и атак	Синтетический, высокая вариация трафика и атак	Синтетический, низкая вариация трафика и атак	Частично синтетический, низкая вариация трафика и атак
Доверие к авторам	Высокий уровень	Высокий уровень	Высокий уровень	Высокий уровень
Верифицируемость	Сырые данные доступны	Сырые данные доступны	Сырые данные доступны	Сырые данные недоступны
Документация	Достаточная	Достаточная	Достаточная	Достаточная
Трудновоспро-изводимость	Офисная сеть средних размеров	Большая корпоративная сеть	Небольшая локальная сеть	Простейшая архитектура

Источник: здесь и далее таблицы составлены авторами.

Наиболее существенными критериями из представленных являются: реалистичность, объем и трудновоспроизводимость. Верифицируемость, сводящаяся к наличию в свободном доступе «сырых» данных, является несущественным критерием в силу достаточного уровня доверия к авторам всех рассматриваемых наборов. Документация во всех случаях сводится к статье-описанию или публикации, в которых описывается набор данных и методология его получения. Задача описания выделяемых признаков трафика во всех случаях делегируется на документацию используемого для этого программного обеспечения, которая предоставляет минимально достаточную информацию для работы.

Окончательный выбор делаем в пользу CSE-CIC-IDS2018 по причине его большей актуальности, а также из-за объема содержащихся данных. Данный набор разработан канадским Институтом кибербезопасности совместно с Учреждением безопасности связи (Communications Security Establishment) Канады в 2018 году [8].

CSE-CIC-IDS2018 отличается моделированием крупной компьютерной сети, содержащей 420 персональных компьютеров и 30 серверных машин, разделенных на несколько сегментов. Список протоколов и реализованных атак практически идентичен таковому в CIC-IDS2017: трафик в моделируемой системе передавался по протоколам HTTP/HTTPS, SMTP/POP3/IMAP, SSH и FTP; представлены атаки шести разновидностей: BruteForce, DoS, DDoS, Botnet, внедрение и атаки на веб-приложения. Признаки выделялись при помощи CICFlowMeter.

Работа с данными производилась средствами языка программирования Python и его библиотек: Pandas, Scikit-learn, TensorFlow, Matplotlib, Pickle.

Предобработанные данные CSE-CIC-IDS2018 предоставляются в CSV-формате, представляющем собой текстовый документ, содержащий набор строк со значениями колонок, разделенными запятыми или иными разделителями, если это оговорено.

В случае разделенных на разные файлы таблиц важно удостовериться, что они единообразны: имеют одинаковое число столбцов и схожие данные, представленные в них. Это необходимо для унификации при последующей работе с ними.

Для обработки данных и представления их в необходимом и удобном формате следует проделать ряд представленных ниже процедур, которые разделены на этапы.

1. Первичный анализ данных:

• единство формы представления: имеется одинаковое число столбцов, данные, представленные в них, схожие;

• количество пропущенных значений в силу несовершенства предварительной сборки данных;

• приведение признаков объекта к одному из двух типов (числовые и категориальные): изначально некоторые показатели с числовыми признаками таковыми не являются;

• оценка корреляционных характеристик признаков: удаление «сильно коррелирующих» признаков;

• определение малоинформативных признаков: удаление признаков, не несущих в себе полезной информации.

2. Предварительная обработка данных (построение универсального конвейера, преобразующего данные в предпочтительную для машинного обучения форму и исправляющего выявленные проблемы):

• заполнение пропущенных значений: варианты заполнения следует определять в зависимости от природы пропуска;

• обработка малоинформативных признаков: отбрасывание неинформативных признаков набора данных;

• замена названий признаков: замена оригинальных названий признаков на более полные и понятные;

• нормализация признаков: приведение значений признака к узкому диапазону;

• построение конвейера предварительной обработки по результатам всех преобразований этапа предварительной обработки.

На выходе приведенных выше этапов получается тот вид данных, который в дальнейшем будет использоваться для обучения моделей классификаторов.

Для обучения моделей из всех доступных данных будут выделены три выборки: *обучающая*, *валидационная* и *тестовая*.

В наборе данных CSE-CIC-IDS2018 представлено несколько разновидностей атак одного типа. Поскольку в данной работе акцент установлен на бинарной классификации, различные вариации однотипных атак объединены в один класс. Таким образом, решается задача оценки принадлежности трафика к типовой атаке, а не к ее конкретной реализации.

Классы в наборе данных CSE-CIC-IDS2018 обладают различной степенью сбалансированности. Для улучшения качества обучения классификаторов в данной работе приводятся данные к идеальной классовой сбалансированности (50 % записей с вредоносным трафиком и 50 % записей с трафиком легитимным). Для достижения такого результата в зависимости от объема данных меньшего из классов будем пользоваться одной из двух стратегий – недосемплированием или пересемплированием [12].

Идея *недосемплирования* заключается в ограничении объема большего класса до объема меньшего класса путем отброса произвольных записей первого. Этот подход применяется при достаточно большом количестве записей, принадлежащих меньшему из классов. В такой ситуации потеря некоторого объема данных не окажет значительного эффекта на модель, в то время как скорость обучения повысится.

Суть *пересемплирования* сводится к дублированию записей меньшего из классов, пока объемы классов не сравняются. В этом случае используются все данные, однако конкретные записи будут обладать большей специфичностью ввиду своего неоднократного вхождения в выборки. Этим приемом будем пользоваться в случае, если объем меньшего из классов оказывается недостаточен.

Классификация атаки типа Brute Force

В наборе данных CSE-CIC-IDS2018 представлено два варианта атаки Brute Force: Brute Force на FTP и Brute Force на SSH. Произведем замену меток классов в таблице, сводя метки классов к двоичной модели. Для этого заменим все метки нормального трафика нулем, а вредоносного – единицей. В результате будем наблюдать значительный дисбаланс классов. Для получения данных с идеально сбалансированными классами необходимо использовать подход недосемплирования. Полученные таким образом данные впоследствии прогоняются через конвейер предварительной обработки и разделяются на обучающую, валидационную и тестовую выборки, которые используются для обучения моделей.

Характеристики полученных выборок сведены в Таблицу 2.

Таблица 2

Характеристики выборок для атаки типа BruteForce

Характеристика	Выборка		
	Обучающая	**Валидационная**	**Тестовая**
Общее число записей	609516	76190	76190
Число записей с меткой вредоносного трафика	304729 (50,0 %)	38268 (50,2 %)	38238 (50,2 %)
Число записей с меткой легального трафика	304787 (50,0 %)	37922 (49,8 %)	37952 (49,8 %)

Далее применим модель логистической регрессии, которая хорошо изучена и реализована многими библиотеками, в частности библиотекой Scikit-learn [13]. В случае использования реализации классификатора, предоставляемого Scikit-learn, остается только подобрать оптимальные гиперпараметры модели и предоставить ей качественные данные для обучения. Рассмотрим такие метрики качества, как *точность*, которая представляет собой долю правильных ответов модели в пределах класса (характеризует число ложных срабатываний детектора атак), и *полнота*, которая представляет собой долю истинно положительных классификаций и характеризует число ошибок 2-го рода. Так как в IDS (системах обнаружения вторжений) гораздо важнее не пропустить атаку, чем не поднимать ложную тревогу, более значимой метрикой в данной работе выступает полнота [14].

Метрика точности рассчитывается как

$$Pres = \frac{TP}{TP + FP}, \tag{1}$$

где TP – число истинно положительных предсказаний (вредоносный трафик, который был классифицирован как вредоносный); FP – число ложноположительных предсказаний (легальный трафик, который был классифицирован как вредоносный, – ошибка 1-го рода).

Метрика полноты рассчитывается по формуле

$$R = \frac{TP}{TP + FN}, \tag{2}$$

где FN – число ложноотрицательных предсказаний (вредоносный трафик, который был классифицирован как легальный, – ошибка 2-го рода).

Метрикой, объединяющей в себе точность и полноту, выступает *F*-мера. Если точность или полнота стремятся к нулю, то *F*-мера тоже стремится к нулю. Рассчитывается *F*-мера по формуле

$$F = \frac{2 \cdot Pres \cdot R}{Pres + R}. \tag{3}$$

Рассчитывая данные метрики, можно сравнить классификаторы.

Модель решающего дерева, как и модель логистической регрессии, реализована в библиотеке Scikit-learn. Обученная модель безошибочно классифицирует данные тестовой выборки.

Нейронные сети являются более сложными моделями с гибкой архитектурой, поэтому их готовой реализации не существует. Библиотека Scikit-learn, предоставляющая реализации классификаторов логистической регрессии и решающего дерева, не предоставляет инструментария для работы с нейронными сетями. Вместо этого можно воспользоваться профильной библиотекой Tensor Flow, которая содержит удобный интерфейс по-

строения, конфигурации и работы с произвольными нейронными сетями, которые будут использованы для получения соответствующего классификатора [15].

Обучение нейронных сетей сводится к минимизации функции потерь путем подбора оптимальных весов нейронов в процессе выполнения того или иного оптимизационного итерационного алгоритма. Базовым и универсальным вариантом функции потерь для задачи двоичной классификации является бинарная перекрестная энтропия, измеряющая расхождение между двумя распределениями:

$$CE = -\log(p) + (1-y)\cdot\log(1-p), \quad (4)$$

где p – прогноз модели; y – истинное значение метки.

Характеристики моделей каждого вида сведены в Таблицу 3.

Таблица 3

Характеристики моделей для атаки типа Brute Force

Модель	Метрика качества				Размер модели
	Аккуратность	**Точность**	**Полнота**	***F*-мера**	
Логистическая регрессия	0,999829	0,999658	1,0	0,999829	7 кб
Решающее дерево	1,0	1,0	1,0	1,0	9 кб
Нейронная сеть	1,0	1,0	1,0	1,0	111 кб

В целом полученные классификаторы показали отличные результаты при минимальных манипуляциях с моделями. Вследствие этого валидационная выборка оказалась невостребованной во всех трех случаях.

На основании данных Таблицы 3 можно утверждать, что оптимальной моделью для выявления атак типа Brute Force является модель на основе решающего дерева. При этом классификатор на основе логистической регрессии показал результат, максимально приближенный к оптимальному. Все ошибки, допущенные моделью, были ошибками 1-го рода, что допустимо в рамках IDS. Данный классификатор также годен к использованию.

Классификатор на основе нейронной сети показал те же результаты, что и классификатор на основе решающего дерева, но его использование в IDS является очевидно избыточным в связи с большим размером модели.

Классификация атаки типа DDoS

В наборе данных CSE-CIC-IDS2018 обрабатывать будем только ту часть записей, в которой содержится вредоносный трафик. Произведем замену меток классов в полученной таблице с данными, выполнив преобразования, аналогичные вышеприведенным для Brute Force. После обработки данных наблюдаем дисбаланс классов. Алгоритм балансировки и его реализация аналогичны приведенным выше за исключением того, что в этот раз доминирующим классом является класс вредоносного трафика.

Пропустим сбалансированные данные через конвейер предобработки, сохраним параметры нормализации и разобьем данные на выборки.

Характеристики полученных выборок сведены в Таблицу 4.

Таблица 4

Характеристики выборок для атаки типа DDoS

Характеристика	Выборка		
	Обучающая	**Валидационная**	**Тестовая**
Общее число записей	1255427	156928	156929
Число записей с меткой вредоносного трафика	628360 (50,1 %)	78919 (50,3 %)	78656 (50,1 %)
Число записей с меткой легального трафика	627067 (49,9 %)	78009 (49,7 %)	78273 (49,9 %)

Рассмотрим классификатор на основе логистической регрессии со стандартными параметрами. Программная реализация модели, процесса её обучения и оценки остается прежней. В результате обучения получена модель со следующими значениями метрик качества по тестовой выборке: аккуратность – 0.993258; точность – 0.986899; полнота – 0.999822; F-мера – 0.993318.

Попробуем подобрать оптимальные гиперпараметры классификатора. В результате получим более качественную модель. Сохраним подогнанную модель средствами библиотеки Pickle. Метрики качества классификатора с базовыми и оптимальными гиперпараметрами сведены в Таблицу 5.

Далее обучим классификатор на основе решающего дерева со стандартными параметрами для атаки типа DDoS. Программная реализация процесса обучения аналогична упомянутой выше. В результате получена модель со следующими значениями метрик качества по тестовой выборке: аккуратность – 0,999981; точность – 0,999987; полнота – 0,999975; *F*-мера – 0,999981.

Произведем подбор гиперпараметров. Полученный в результате перебора классификатор имеет те же значения метрик качества, что и базовый. Делаем вывод, что базовый вариант справлялся с задачей оптимальным образом.

Таблица 5

Значения метрик качества классификаторов на основе логистической регрессии для атаки типа DDoS

Классификатор	Метрика качества			
	Аккуратность	**Точность**	**Полнота**	***F*-мера**
Классификатор с базовыми параметрами	0,993258	0,986899	0,999822	0,993318
Классификатор с оптимальными параметрами	0,993373	0,987109	0,999835	0,993431

Обучим базовую модель классификатора на основе нейронной сети. В результате получим нейронную сеть со следующими значениями метрик качества по тестовой выборке: аккуратность – 0,999471; точность – 0,999364; полнота – 0,999580; *F*-мера – 0,999472.

При этом перебор функций активации, оптимизационных алгоритмов и скорости обучения не дал нужного результата. Принимаем базовую модель за оптимальную.

Характеристики лучших моделей каждого вида для атаки типа DDoS сведены в Таблицу 6.

Таблица 6

Характеристики моделей для атаки типа DDoS

Модель	Метрика качества				Размер модели
	Аккуратность	**Точность**	**Полнота**	***F*-мера**	
Логистическая регрессия	0,993373	0,987109	0,999835	0,993431	7 кб
Решающее дерево	0,999981	0,999987	0,999975	0,999981	15 кб
Нейронная сеть	0,999471	0,999364	0,999580	0,999472	110 кб

В связи с порядком значений метрик качества полученных моделей валидационная выборка оказалась невостребованной во всех трех случаях.

На основании данных Таблицы 6 можно утверждать, что оптимальной моделью для выявления атак типа DDoS является модель на основе решающего дерева. При этом классификатор на основе логистической регрессии показал результат, максимально приближенный к оптимальному. Использование нейронной сети избыточно.

Заключение и выводы

Для закрепления результатов над полученными моделями были проведены дополнительные испытания. Была произведена попытка классификации данных в выборке, содержащей исключительно легальный трафик, с которой модели справились хорошо. При попытке классифицировать атаку, родственную той, к обнаружению которой готовился классификатор (атака DoS для классификаторов DDoS), были получены результаты, превосходящие случайное угадывание, что подтверждает возможность обнаружения неизвестных ранее атак по признакам известных. При попытке классификации неизвестной классификатору атаки (Brute Force для классификаторов DDoS) модели ожидаемо не справились с задачей.

Таким образом, потенциально перспективными способами улучшения результатов в этом могут стать следующие.

1. Альтернативная предварительная обработка данных с упором на решение задачи классификации конкретной атаки.

2. Значительное усложнение архитектуры моделей (особенно перспективны нейронные сети). В случае решающих деревьев хорошей идеей будет применение ансамблевого решения – решающего леса.

3. Более тщательный перебор гиперпараметров моделей, связанный с резким повышением требований к вычислительным мощностям или времени обучения.

В дальнейшем предполагается рассмотреть метрики качества для других видов атак с использованием тех же типов классификаторов: решающее дерево, логистическая регрессия, нейронная сеть; также будут использованы предложенные способы улучшения результатов.

Литература

1. *Шелухин О.И., Сакалема Д.Ж., Филинова А.С.* Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие для вузов. М. : Горячая линия – Телеком, 2022. 220 с. ISBN 978-5-9912-0323-4.

2. *Kostas K.* Anomaly Detection in Networks Using Machine Learning. Master thesis. School of Computer Science and Electronic Engineering, University of Essex, 2018. 70 p. URL: https://www.

researchgate.net/profile/Kahraman-Kostas/publication/328512658_Anomaly_Detection_in_Networks_Using_Machine_Learning/links/5bd1d1bf458515343d58eddc/Anomaly-Detection-in-Networks-Using-Machine-Learning.pdf (дата обращения: 18.12.2023).
3. *Бабичева М.В., Третьяков И.А.* Применение методов машинного обучения для автоматизированного обнаружения сетевых вторжений // Вестник Дагестанского государственного технического университета. Технические науки. 2023. Т. 50. № 1. С. 53–61. EDN MGBAGF. DOI : 10.21822/2073-6185-2023-50-1-53-61
4. *Шабуров А.С., Никитин А.С.* Модель обнаружения компьютерных атак на объекты критической информационной инфраструктуры // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2019. № 29. С. 104–117. EDN ZBKJTN.
5. *Saranya T., Sridevi S., Deisy C., Chung T. D., Khan M.K.A.A.* Performance analysis of machine learning algorithms in intrusion detection system: A review // Procedia Computer Science. 2020. Vol. 171. Pp. 1251–1260. DOI: 10.1016/j.procs.2020.04.133
6. *Gibert D., Mateu C., Planes J.* The rise of machine learning for detection and classification of malware: Research developments, trends and challenges // Journal of Network and Computer Applications. 2020. Vol. 153. Article ID 102526. DOI: 10.1016/j.jnca.2019.102526
7. *Флах П.* Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных / Пер. А.А. Сланкина. М. : ДМКПресс, 2015. 400 с. ISBN 978-5-97060-273-7.
8. CSE-CIC-IDS2018 on AWS // University of New Brunswick. Canadian Institute for Cybersecurity. URL: http://www.unb.ca/cic/datasets/ids-2018.html (дата обращения: 18.12.2023).
9. Intrusion Detection Evaluation Dataset (CIC-IDS2017) // University of New Brunswick. Canadian Institute for Cybersecurity. URL: https://www.unb.ca/cic/datasets/ids-2017.html (дата обращения: 18.12.2023).
10. *Ferriyan A., Husni Thamrin A., Takeda K., Murai J.* Generating Network Intrusion Detection Dataset Based on Real and Encrypted Synthetic Attack Traffic // Applied Sciences. 2021. Vol 11. No. 17. Article ID 7868. DOI: 10.3390/app11177868
11. *Catillo M., Del Vacchio A., Ocone L., Pecchia A., Villano U.* USB-IDS-1: A Public Multilayer Dataset of Labeled Network Flows for IDS Evaluation // 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). Taipei, Taiwan, 21–24 June 2021. DOI: 10.1109/DSN-W52860.2021.00012
12. *Дьяконов А.* Дисбаланс классов // Анализ малых данных. КвазиНаучный блог Александра Дьяконова. 2021. 27 мая. URL: https://alexanderdyakonov.wordpress.com/2021/05/27/imbalance (дата обращения: 18.12.2023).
13. Scikit-learn 1.3.2 documentation // Scikit-learn: machine learning in Python. URL: https://scikit-learn.org/stable (дата обращения: 18.12.2023).
14. *Харрисон М.* Машинное обучение: карманный справочник. Краткое руководство по методам структурированного машинного обучения на Python / Пер. В.А. Коваленко. СПб. : Диалектика, 2020. 320 с. ISBN 978-5-907203-17-4.
15. API Documentation // TensorFlow. URL: https://www.tensorflow.org/api_docs (дата обращения: 18.12.2023).

References

1. Shelukhin O.I., Sakalema D.Zh., Filinova A.S. (2022) *Obnaruzhenie vtorzhenii v komp'yuternye seti (setevye anomalii)* [Detection of intrusions into computer networks (network anomalies] : Textbook for

university students. Moscow : Goryachaya liniya – Telekom Publ. 220 p. ISBN 978-5-9912-0323-4. (In Russian).
2. Kostas K. (2018) *Anomaly Detection in Networks Using Machine Learning.* Master thesis. School of Computer Science and Electronic Engineering, University of Essex. 70 p. URL: https://www.researchgate.net/profile/Kahraman-Kostas/publication/328512658_Anomaly_Detection_in_Networks_Using_Machine_Learning/links/5bd1d1bf458515343d58eddc/Anomaly-Detection-in-Networks-Using-Machine-Learning.pdf (accessed 18.12.2023).
3. Babicheva M.V., Tret'yakov I.A. (2023) Application of machine learning methods for automated detection of network intrusions. *Herald of Dagestan State Technical University. Technical Sciences*. Vol. 50. No. 1. Pp. 53–61. DOI : 10.21822/2073-6185-2023-50-1-53-61 (In Russian).
4. Shaburov A.S., Nikitin A.S. (2019) Model for detecting computer attacks on critical information infrastructure objects. *Bulletin of Perm National Research Polytechnic University. Electrical engineering, information technology, control systems*. Vol. 29. Pp. 104–117. (In Russian).
5. Saranya T., Sridevi S., Deisy C., Chung T. D., Khan M. K. A. A. (2020) Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*. Vol. 171. Pp. 1251–1260. DOI: 10.1016/j.procs.2020.04.133
6. Gibert D., Mateu C., Planes J. (2020) The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. *Journal of Network and Computer Applications*. Vol. 153. Article ID 102526. DOI: 10.1016/j.jnca.2019.102526
7. Flach P. (2012) *Machine Learning: The Art and Science of Algorithms that Make Sense of Data.* Cambridge university press. 416 p. ISBN: 9781139575416 (Russian edition: transl. by A.A. Slankin, Moscow : DMK Press. 400 p.).
8. CSE-CIC-IDS2018 on AWS (2018). *University of New Brunswick. Canadian Institute for Cybersecurity*. URL: http://www.unb.ca/cic/datasets/ids-2018.html (accessed 18.12.2023).
9. Intrusion Detection Evaluation Dataset (CIC-IDS2017) (2017). *University of New Brunswick. Canadian Institute for Cybersecurity*. URL: https://www.unb.ca/cic/datasets/ids-2017.html (accessed 18.12.2023).
10. Ferriyan A., Husni Thamrin A., Takeda K., Murai J. (2021) Generating Network Intrusion Detection Dataset Based on Real and Encrypted Synthetic Attack Traffic. *Applied Sciences*. Vol 11. No. 17. Article ID 7868. DOI: 10.3390/app11177868
11. Catillo M., Del Vacchio A., Ocone L., Pecchia A., Villano U. 2021) USB-IDS-1: A Public Multilayer Dataset of Labeled Network Flows for IDS Evaluation. In: *51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. Taipei, Taiwan, 21–24 June 2021. DOI: 10.1109/DSN-W52860.2021.00012
12. D'yakonov A. (2021) Class Imbalance. *Small data analysis. Quasi-Scientific blog of Alexander Dyakonov*. URL: https://alexanderdyakonov.wordpress.com/2021/05/27/imbalance (accessed 18.12.2023). (In Russian).
13. Scikit-learn 1.3.2 documentation (2023). *Scikit-learn: Machine learning in Python.* URL: https://scikit-learn.org/stable (accessed 18.12.2023).
14. Harrison M. (2019) *Machine Learning. Pocket Reference. Working with Structured Data in Python.* O'Reilly Media, Inc. 320 p. (Russian edition: transl. by V.A. Kovalenko. St. Petersburg : Dialektika Publ. 2020. 320 p.).
15. API Documentation (2023) *TensorFlow.* URL: https://www.tensorflow.org/api_docs (accessed 18.12.2023).