УДК 004.056
DOI 10.52575/2687-0932-2025-52-2-465-475
EDN TNAPPX

Обнаружение вторжений в компьютерные сети на основе аномалий с помощью методов машинного обучения

Куценко С.М., Салтанаева Е.А., Ахметов А.М.
Казанский государственный энергетический университет,
Россия, 420066, Республика Татарстан, г. Казань, ул. Красносельская, д. 51
s.koutsenko@mail.ru, elena_maister@mail.ru

Аннотация. Актуальность данной работы основана на необходимости обнаружения вредоносной активности и вторжений в сеть или устройство в рамках мер противодействия и пресечения кибератак и киберпреступлений. Предлагаемое авторами программное обеспечение является системой обнаружения вторжений на сетевом уровне, использующей аномальный подход к интерпретации сетевого трафика и пассивные режимы реагирования и поиска данных. Архитектура предлагаемой сетевой системы обнаружения вторжений содержит в себе модуль прослушивания передаваемых и получаемых пакетов данных и сохранения данных в виде датасета, модуль анализа и реагирования и модуль пользовательского интерфейса. В ходе разработки были подготовлены данные для дальнейшего обучения системы, определены механизмы формирования данных в выбранном обучающем датасете, исходя из изученных механизмов реализован алгоритм по прослушиванию сетевых пакетов и формированию нового тестового датасета. В модуле анализа и реагирования применялись распространенные алгоритмы машинного обучения. Данный модуль также содержит обработчик и дает возможность пользователю выбрать и запустить нужный ему алгоритм машинного обучения. Для оценки качества алгоритмов классификации были смоделированы сетевые атаки на защищаемые компьютерные сети. Тестирование проводилось на сбалансированном датасете, в сети без сетевых атак, а дообученные алгоритмы тестировались в сети без сетевых атак и с сетевыми атаками. Дообученные алгоритмы показали приемлемо высокие результаты точности.

Ключевые слова: компьютерные сети, система обнаружения вторжений, аномалии, машинное обучение

Для цитирования: Куценко С.М., Салтанаева Е.А., Ахметов А.М. 2025. Обнаружение вторжений в компьютерные сети на основе аномалий с помощью методов машинного обучения. *Экономика. Информатика*, 52(2): 465–475. DOI 10.52575/2687-0932-2025-52-2-465-475 EDN TNAPPX

Anomaly-based Intrusion Detection in Computer Networks Using Machine Learning Techniques

Svetlana M. Kutsenko, Elena A. Saltanaeva, Azat M. Akhmetov
Kazan State Power Engineering University,
51 Krasnoselskaya St., Kazan 420066, Republic of Tatarstan, Russia
s.koutsenko@mail.ru, elena_maister@mail.ru

Abstract. The relevance of this paper is based on the need to detect malicious activity and intrusions into a network or device as part of countermeasures and suppression of cyberattacks and cybercrime. The software proposed is a network-level intrusion detection system that uses an anomalous approach to interpret network traffic and passive response and data retrieval modes. The architecture of the proposed network-based intrusion detection system contains a module for listening to transmitted and received data packets and storing the data as a dataset, an analysis and response module, and a user interface module. In the course of development, we

prepared data for further training of the system and determined the mechanisms of data formation in the selected training dataset. Based on the studied mechanisms, we implemented an algorithm for listening to network packets and forming a new test dataset. Common machine learning algorithms were applied in the analysis and response module that contains a handler and allows the user to select and run the desired machine learning algorithm. To evaluate the quality of classification algorithms, network attacks on protected computer networks were simulated. We conducted testing on a balanced dataset, in a network that was free of network attacks, while pre-trained algorithms were tested in a network with and without network attacks. The pre-trained algorithms showed acceptably high accuracy results.

Keywords: computer networks, intrusion detection system, anomalies, machine learning

For citation: Kutsenko S.M., Saltanaeva E.A., Akhmetov A.M. 2025. Anomaly-Based Intrusion Detection in Computer Networks Using Machine Learning Techniques. *Economics. Information technologies*, 52(2): 465–475 (in Russian). DOI 10.52575/2687-0932-2025-52-2-465-475 EDN TNAPPX

Введение

Внедрение информационных технологий способствует не только облегчению быта и автоматизации труда человека, но и всевозможным разрушительным, деструктивным и корыстным целям злоумышленников.

Прослеживается тенденция к увеличению частоты хакерских атак на компьютерные сети, а также сезонность явления, т. е. пропорциональное и закономерное увеличение и уменьшение количества определенных категорий кибератак исходя из временного квартала [Исследование ГК «Солар»: Атаки на российские компании в III квартале 2023 год, 2023, Отчет о DDOS-атаках за третий квартал 2023 года от StormWall, 2023].

Существует стратегическая необходимость как в системах обнаружения вторжений (СОВ) в частности, так и в системе мер противодействия и пресечения кибератак и киберпреступлений в целом. Важными требованиями к таким системам являются высокие аналитические и прогностические способности, низкая частота ложных срабатываний, работа в режиме реального времени, высокая скорость вычислений, оптимальная производительность.

Несмотря на то, что на рынке информационной безопасности уже длительное время присутствуют СОВ с открытым исходном кодом, почти все они имеют недостаток, так как являются сигнатурными, т. е. не способными распознать сетевые атаки, отсутствующие в базе сигнатур [Репозиторий свободной системы обнаружения вторжений Open Source Tripwire, 2024, Репозиторий свободной системы обнаружения вторжений Snort, 2024, Репозиторий свободной системы обнаружения вторжений Zeek, 2024].

По этой причине актуальной является разработка СОВ на сетевом уровне, использующей аномальный подход к интерпретации сетевого трафика и пассивные режимы реагирования и поиска данных.

Объекты и методы исследования

Система обнаружения вторжений (СОВ) – это программный или аппаратный комплекс, предназначенный для обнаружения вредоносной активности и вторжений в сеть или устройство централизованного сбора, регистрации и фильтрации поступающих сигналов и дальнейшего уведомления о случившемся нарушении администратора сети.

Под аномалиями в системах обнаружения вторжений подразумеваются данные, чьи характеристики выбиваются из нормального, шаблонного поведения других данных в устройстве.

Архитектура предлагаемой сетевой СОВ содержит в себе несколько связанных между собой модулей [Мартин, 2022]. Каждый из модулей отвечает за определенный функционал системы.

Модуль «Сетевой анализатор и коллектор» берет на себя роль сенсорной системы СОВ и центра распределения информации. Данный модуль обнаруживает используемые порты и устройства в сети компьютера, прослушивает передаваемые и получаемые пакеты данных, обрабатывает, нормализует и форматирует данные о соединениях и сохраняет данные в виде csv датасета в хранилище данных.

Модуль «Алгоритмы машинного обучения с учителем» является системой анализа и реагирования [Григорьев, 2023]. Для модуля реализуются и обучаются 5 алгоритмов классификации, каждый из которых по выбору пользователя проводит анализ прослушанных сетевых пакетов, выявляя в данных о соединениях точечные аномалии, что позволяет классифицировать соединение как сетевую атаку или безопасное соединение. После классификации данных модуль сохраняет предсказанную информацию в датасет и выводит результат работы через интерфейс.

Модуль «Графический интерфейс приложения» исполняет роль системы вывода СОВ. В модуле реализуются необходимые элементы пользовательского интерфейса, которые позволяют конечному пользователю управлять функционалом программного обеспечения (ПО) и получать уведомления о результатах работы системы.

Для обучения моделей машинного обучения был выбран набор данных CSE-CIC-IDS2018 [A Realistic Cyber Defense Dataset, 2024]. Данный датасет содержит в себе в общей сложности более 450 Гб данных, полученных и дополняемых с 2018 по 2024 год из трафика в сети Института кибербезопасности Университета Нью-Брансуика, Канада. Набор данных состоит из организованных по дням файлов, содержащих записи безопасного и аномального сетевого трафика, а также записи журналов событий для устройств в сети. Поскольку датасет имеет большой размер, было решено, что для изучения и первоначального обучения алгоритмов из множества файлов достаточно рассмотреть 10 файлов. При необходимости количество используемых файлов можно увеличить.

Записи в файлах датасета CSE-CIC-IDS2018 характеризуются набором из 80 атрибутов. Атрибуты были получены при помощи генератора и анализатора сетевого трафика CICFlowmeter-V3.0, разработанного авторами датасета. Например, атрибут Label в выборке является меткой, маркером класса и используется для обучения алгоритма и распознавания класса записи при обучении, и для проверки результата предсказания алгоритма классификации при тестировании.

Данные в датасете – это проанализированные соединения в реальной инфраструктуре сети, использующие протоколы TCP и UDP относительно транспортного уровня; HTTP, HTTPS, FTP и SSH относительно прикладного уровня, а также протоколы электронной почты SMTP, IMAP, POP3. Цифровые данные, передающиеся по сети между устройствами, являются как безопасными соединениями, отмечаемыми меткой «Bening», так и различными сетевыми атаками. Сетевые атаки делятся на группы, которые описаны в табл. 1.

При проектировании модуля «Алгоритмы машинного обучения с учителем» был определен список распространенных методов машинного обучения, которые используются для решения задач классификации [Плас, 2021, Madani, 2023]. Это следующие методы машинного обучения:

– метод k-ближайших соседей;
– метод опорных векторов;
– метод Наивный байесовский классификатор;
– метод «Дерево решений»;
– метод «Случайный лес».

После программирования главного исполняемого файла был создан модуль с сетевым анализатором и коллектором (сниффером). В рамках этого этапа разработки были подготовлены данные для дальнейшего обучения системы; определены механизмы формирования данных в выбранном обучающем датасете; исходя из изученных механизмов реализован алгоритм по прослушиванию сетевых пакетов и формированию нового тестового датасета [Траск, 2022].

Таблица 1
Table 1

Группы атак и их описание
Attack groups and their descriptions

Название	Описание
Brute Force Attack	Атака грубой силой, или атака методом перебора. Заключается в вычислении всех возможных комбинаций паролей, ключей, данных или информации.
Heartbleed Attack	Уязвимость чтения за пределами буфера в криптографической библиотеке OpenSSL, позволяющая получать несанкционированный доступ к памяти на сервере или клиенте для чтения и извлечения данных.
Botnet	Атаки, выполняемые со стороны удаленно управляемой и разветвленной сети устройств.
DoS/DDoS Attack	Атака на вычислительную систему с целью вызвать отказ в ее обслуживании.
SQL Injection	Атака, использующая язык запросов SQL для управления и получения информации.
XSS	Атака, заключающаяся во внедрении в веб-страницу вредоносного кода, выполняющего межсайтовые сценарии.
Infiltration Attack	Атака изнутри сети или устройства, для чего используются уязвимости в установленных сторонних приложениях и бэкдоры.

Результатом пофайлового анализа стал выбор двух рабочих файлов – 22-02-2018.csv и 23-02-2018.csv. Их преимущества: все записи являются числовыми, что избавляет от необходимости в кодировании категориальных переменных; файлы содержат наибольшее количество групп сетевых атак: «Brute Force», «XSS», «SQL Injections».

Недостатками являются: атака «XSS» представлена как подвид, разновидность атаки «Brute Force», однако в действительности является отдельным типом атак; присутствуют записи с нетиповыми или бесконечными значениями.

Обнаруженные ошибки были исправлены, и создана объединенная выборка с названием Othrys_IDS_Dataset.

Получившаяся выборка оказалась не сбалансирована, т. е. количество записей нормальных соединений многократно превышает количество записей сетевых атак. Для исправления дисбаланса классов применен метод случайного сэмплирования, а именно случайным образом удалены записи с меткой «Bening», так, чтобы отношение сетевых атак к нормальным удовлетворяло процентному соотношению 30:70.

После отбора признаков выборки данных (с целью удаления незначащих признаков, признаков с избыточными связями и наименьшей важностью) осталось 10 признаков, представленных на рис. 1, которые будут участвовать в разработке и дальнейшем обучении алгоритмов классификации [Kelleher, 2019, Kneusel, 2022].

В результате оптимизации был сформирован новый датасет «train_dataset.csv», содержащий 3093 записей, из которых 2165 соединений с меткой «Bening», 611 с меткой «Brute Force», 230 с меткой «XSS» и 87 с меткой «SQL Injection». Оптимизированный датасет содержит 11 обновленных атрибутов – 10 основных признаков и 1 признак-метку, представленных в табл. 2.

Модуль с алгоритмами машинного обучения исполняет роли подсистем анализа и реагирования в системах обнаружения вторжений [Weber, 2020, Yuxi (Hayden) Liu, 2020]. Реализован обработчик, который дает возможность пользователю выбрать и запустить нужный ему алгоритм машинного обучения.

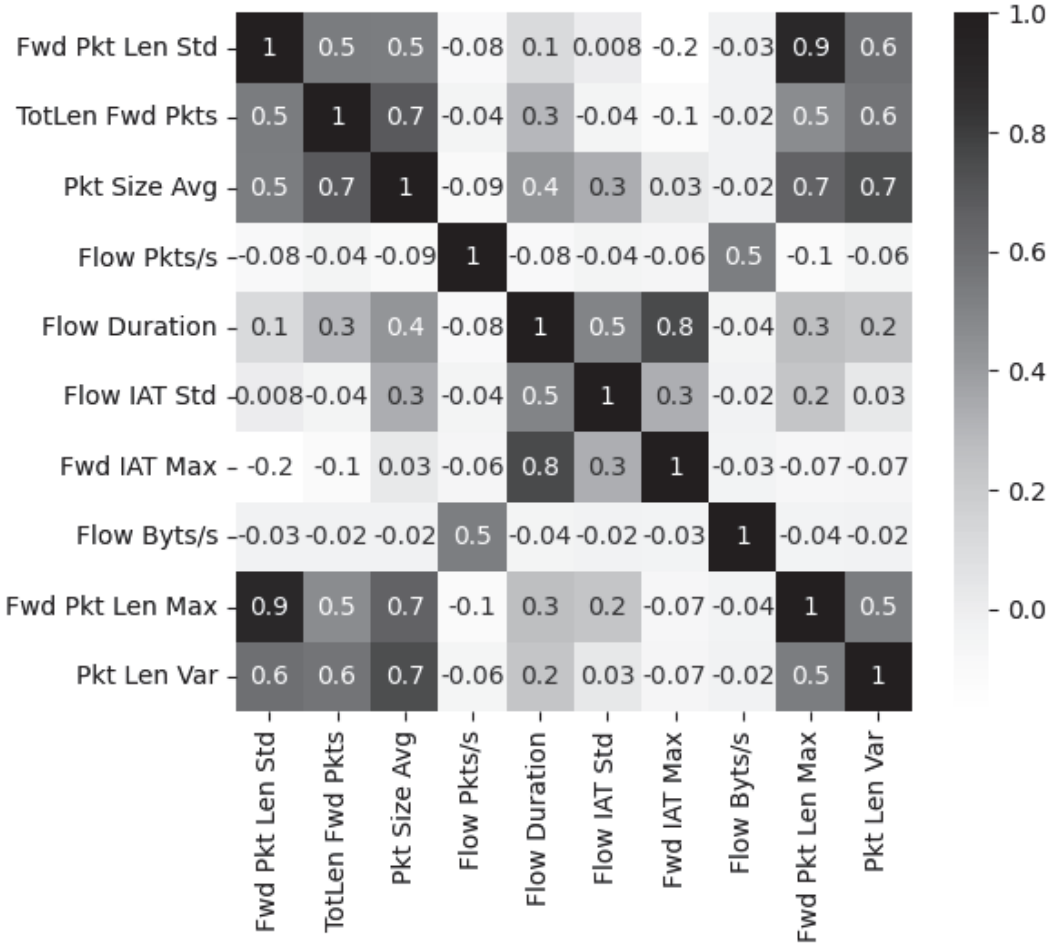

Рис. 1. Корреляционная матрица оставшихся признаков
Fig. 1. Correlation matrix of the remaining features

Таблица 2
Table 2

Обновленные атрибуты и их описание
Updated attributes and their description

№	Название атрибута	Описание
1	Fwd Pkt Len Std	Стандартное отклонение в размерах принимаемого пакета
2	TotLen Fwd Pkts	Общий размер принимаемых пакетов
3	Pkt Size Avg	Средний размер пакета
4	Flow Pkts/s	Скорость передачи данных в пакетах в секунду
5	Flow Duration	Длительность соединения
6	Flow IAT Std	Стандартное отклонение времени между двумя соединениями
7	Fwd IAT Max	Максимальное время между двумя принимаемыми соединениями
8	Flow Byts/s	Скорость передачи данных в байтах в секунду
9	Fwd Pkt Len Max	Максимальный размер принимаемого пакета
10	Pkt Len Var	Минимальное время между поступлениями пакета
11	Label	Метка с названием протокола и типом сценария атаки на сеть

Создаваемые модели обучения первоначально обучаются на оптимизированном и сбалансированном ранее тренировочном датасете «train_dataset.csv». Для каждой модели перед обучением проводится нормализация тренировочных данных, настраиваются значения параметров алгоритма.

Значения параметров для алгоритмов подбирались вручную опытным путем до тех пор, пока во время тестирования алгоритмов показания метрик качества предсказаний не показали наилучший результат.

После обучения алгоритму передается датасет с перехваченными пакетами, для которого модель выдает предсказания. Полученные предсказания записываются в конечный результирующий датасет, отмечая для каждого соединения его тип. Результаты работы алгоритма выводятся в таблицу в окне приложения во вкладках «Monitoring» или «Analytics» главного окна приложения. Пример работы подсистемы показан на рис. 2.

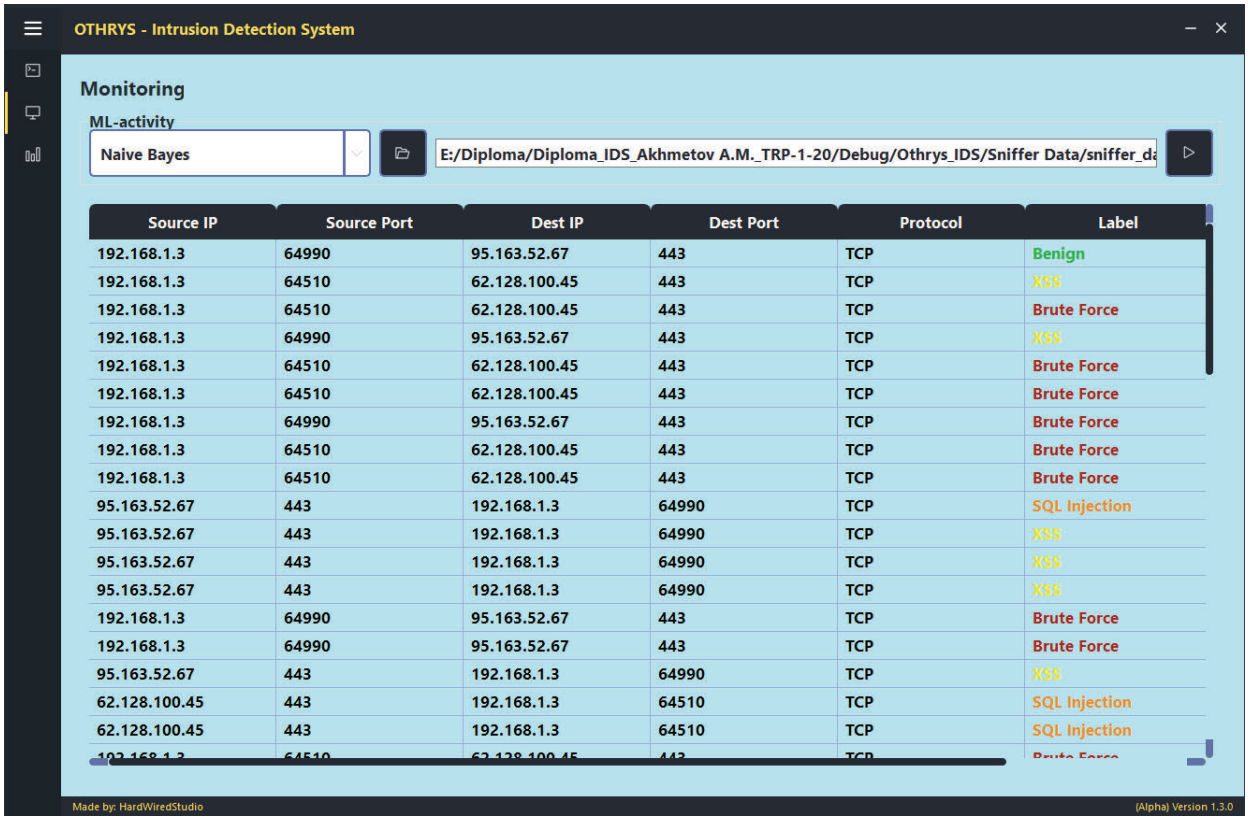

Рис. 2. Пример работы подсистемы «Алгоритмы машинного обучения с учителем»
Fig. 2. Example of work of the subsystem «Machine Learning Algorithms with Teacher»

Результаты и их обсуждение

Тестирование ПО проходило на сбалансированном датасете «train_dataset.csv», для чего он был разделен на тренировочную и тестовую выборки в пропорции 70:30. Качество предсказаний моделей машинного обучения сравнивалось с использованием метрик достоверности, точности, полноты и F1-меры. Результаты проведенной оценки представлены в табл. 3.

По результатам тестирования в сбалансированной выборке самым точным алгоритмом является Случайный лес, а самым неточным – Наивный байесовский классификатор.

Следующее тестирование проводилось в реальной сети. Сначала точность работы алгоритмов оценивали в сети с безопасными сетевыми пакетами, не подвергающейся сетевым атакам. Для безопасной сети было сгенерировано и перехвачено 450 сетевых соединений, которые затем были классифицированы алгоритмами. В таблице 4 показаны метрики качеств для каждого алгоритма.

Таблица 3
Table 3

Результаты оценки качества алгоритмов классификации на сбалансированном датасете
Quality assessment results of classification algorithms on a balanced dataset

Модель	Достоверность	Точность	Полнота	F1-мера
k-ближайших соседей	0,8797672915319	0,8416466226920	0,6479039124479	0,7029592500368
Опорных векторов	0,7537168713639	0,3456178820329	0,3467912881434	0,33906282396848
Наивный байесовский классификатор	0,32967032967032	0,41469417172823	0,5015803202123	0,30791107482902
Дерево решений	0,8998060762766	0,7794999784045	0,7402398242807	0,7579549373090
Случайный лес	0,9082094376212	0,7965777783540	0,7674366527353	0,7808580963596

Таблица 4
Table 4

Результаты предсказаний алгоритмов в сети без сетевых атак
Prediction results of algorithms in a network without network attacks

Модель	Достоверность	Точность	Полнота	F1-мера
k-ближайших соседей	0,83	1	0,83	0,91
Опорных векторов	0,3	1	0,30	0,46
Наивный байесовский классификатор	–	0,1	0,04	0,07
Дерево решений	1	1	1	1
Случайный лес	1	1	1	1

Самыми точными алгоритмами оказались Случайный лес и Дерево решений, в то время как остальные алгоритмы обнаружили в сети с нормальным поведением большое количество сетевых атак. Качество и точность предсказаний 3 из 5 реализованных алгоритмов классификации являются низкими. Такое низкое качество работы алгоритмов связано с проблемой трансферного обучения. Алгоритмы, обученные на одних данных для решения одной задачи, при использовании для решения схожей, но не идентичной задачи (с отличными условиями, характерами переменных и признаков, или тестируемые на других данных), выдают некачественный результат.

Сравнительный анализ данных обучающего датасета и данных из реальной тестируемой сети показал, что присутствуют отличия в характерах используемых данных. Для датасета CSE-CIC-IDS2018 замечена низкая скорость передачи данных и долгий межпакетный интервал, в то время как тестируемая сеть обладает высокой скоростью передачи данных и коротким межпакетным интервалом. Также разными сетями используется разное сетевое оборудование с отличными друг от друга настройками сети и устройств.

Для решения возникшей проблемы была проведена отладка с дообучением моделей машинного обучения. В новый тренировочный датасет были добавлены 1400 записей нормальных сетевых соединений из реальной защищаемой сети с меткой «Bening», прослушанные при помощи реализованного модуля сетевого анализатора.

После нормальных сетевых пакетов в защищаемой сети были смоделированы сетевые атаки 3 классов: «Brute Force», «XSS», «SQL Injections». Генерация сетевых атак происходила при помощи программного обеспечения OWASP ZAP (Zed Attack Proxy) (рис. 3). Нападение моделируемых сетевых атак происходило на веб-страницу авторизации пользователя, для чего использовалось веб-приложение, развернутое на сервере внутри защищаемой сети.

Для генерации сетевых атак использовались словари сетевых атак, взятые из открытых источников [Репозиторий с данными об уязвимостях Cross Site Scripting, 2024; Репозиторий с данными по информационной безопасности SecList, 2024]. Также самостоятельно выполнялись Brute Force атаки с попытками перебора паролей к странице авторизации и отправки межсайтовых скриптов. Атаки проводились в активном и пассивном режиме работы, словари с атаками загружались в режиме фаззинга, также использовалась функция Break для попыток перехвата и изменения запросов и ответов. Моделируемые атаки анализировались с помощью инструментов ZAP, а также перехватывались с помощью реализованного модуля сниффера. Проводился анализ записей об атаках и вручную маркировались данные для дальнейшего обучения. В новый обучающий датасет было добавлено по 200 сетевых атак каждого класса.

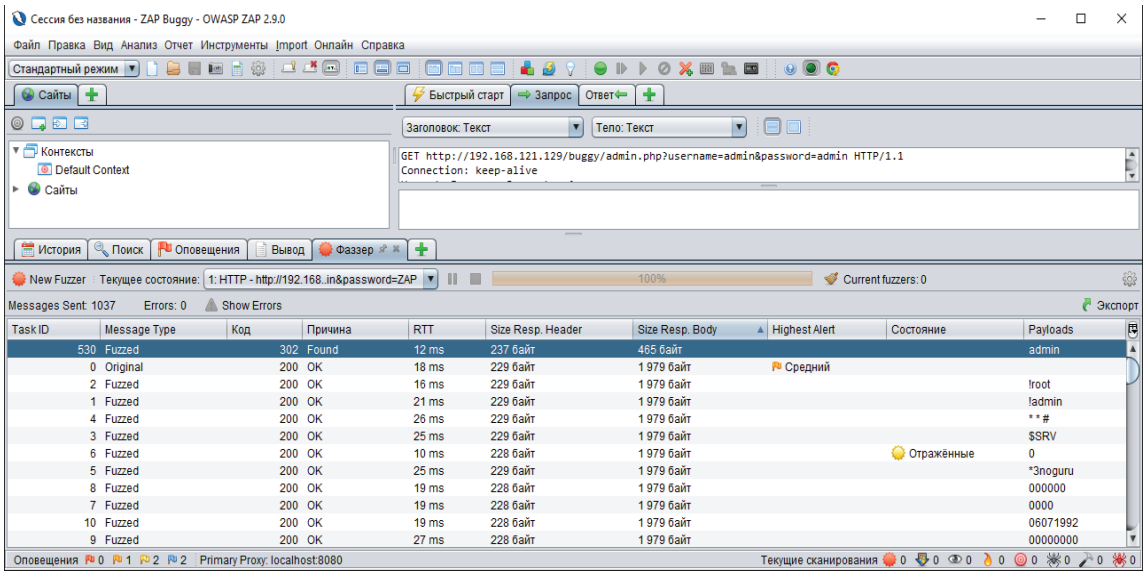

Рис. 3. Пример моделирования сетевой атаки с помощью OWASP ZAP
Fig. 3. Example of modelling a network attack using OWASP ZAP

После дообучения проведено повторное тестирование. Тестирование на безопасной сети показало высокую точность 4 из 5 алгоритмов машинного обучения. В табл. 5 показаны результаты оценки с использованием метрик качества.

Таблица 5
Table 5

Результаты тестирования дообученных алгоритмов в сети без сетевых атак
Results of testing the pre-trained algorithms in a network without network attacks

Модель	Достоверность	Точность	Полнота	F1-мера
k-ближайших соседей	1	1	1	1
Опорных векторов	1	1	1	1
Наивный байесовский классификатор	0,76	0,76	1	0,8649
Дерево решений	1	1	1	1
Случайный лес	1	1	1	1

Для тестирования алгоритмов в сети, подвергшейся известными атакам, было прослушано 200 нормальных соединений и снова смоделировано по 100 сетевых атак каждого класса с помощью инструментов OWASP ZAP. Тестирование показало высокую точность алгоритмов Случайный лес и Дерево решений, самым неточным оказался алгоритм Наивный байесовский классификатор. В табл. 6 показаны результаты оценки с использованием метрик качества.

Таблица 6
Table 6

Результаты тестирования дообученных алгоритмов в сети с сетевыми атаками
Results of testing the pre-trained algorithms in a network with network attacks

Модель	Достоверность	Точность	Полнота	F1-мера
k-ближайших соседей	0,816	0,769	0,846	0,805
Опорных векторов	0,806	0,776	0,803	0,789
Наивный байесовский классификатор	0,613	0,421	0,888	0,571
Дерево решений	0,883	0,818	0,951	0,880
Случайный лес	0,902	0,836	0,973	0,899

Заключение

Таким образом, разработка системы, прослушивающей компьютерную сеть, позволяющей обнаружить среди сетевых соединений аномалии и классифицировать их как сетевые атаки, используя для этого методы машинного обучения, является актуальной в рамках системы мер противодействия и пресечения кибератак и киберпреступлений в целом.

Реализованный функционал ПО обладает следующими возможностями:

– обнаружение используемого сетевого оборудования;

– прослушивание сетевых соединений;

– обработка сетевых пакетов и вычисление пространства признаков;

– формирование датасета из обработанных сетевых соединений;

– анализ прослушиваемых сетевых пакетов и предсказание класса соединения с помощью алгоритмов классификации;

– хранение результатов предсказаний и построение аналитических графиков и таблиц.

Важными требованиями к таким системам являются высокие аналитические и прогностические способности, низкая частота ложных срабатываний, работа в режиме реального времени, высокая скорость вычислений, оптимальная производительность.

Для тестирования качества и оценки точности реализованной системы с помощью инструментов программного обеспечения OWASP ZAP были смоделированы сетевые атаки на защищаемые компьютерные сети. Получен высокий результат точности и качества алгоритмов.

Список литературы

Григорьев А. 2023. Машинное обучение. Портфолио реальных проектов. Спб: Питер, 496 с.

Исследование ГК «Солар»: Атаки на российские компании в III квартале 2023 года [Электронный ресурс]. URL: https://rt-solar.ru/analytics/reports/3889/ (дата обращения: 12.12.2024).

Мартин Р. 2022. Чистая архитектура. Искусство разработки программного обеспечения. Санкт-Петербург: Питер, 352 с.

Отчет о DDOS-атаках за третий квартал 2023 года от StormWall [Электронный ресурс]. URL: https://stormwall.pro/otchet-o-ddos-atakah-2023-tretij-kvartal (дата обращения: 12.12.2024).

Плас Дж. 2021. Python для сложных задач: наука о данных и машинное обучение. СПб: Питер, 576 с.

Репозиторий с данными об уязвимостях Cross Site Scripting (XSS) Vulnerability Payload List [Электронный ресурс]. URL: https://github.com/payloadbox/xss-payload-list (дата обращения: 12.12.2024).
Репозиторий с данными по информационной безопасности SecList [Электронный ресурс]. URL: https://github.com/danielmiessler/SecLists (дата обращения: 12.12.2024).
Репозиторий свободной системы обнаружения вторжений Open Source Tripwire [Электронный ресурс]. URL: https://github.com/Tripwire/tripwire-open-source (дата обращения: 12.12.2024).
Репозиторий свободной системы обнаружения вторжений Snort [Электронный ресурс]. URL: https://github.com/snort3/snort3 (дата обращения: 12.12.2024).
Репозиторий свободной системы обнаружения вторжений Zeek [Электронный ресурс]. URL: https://github.com/zeek/zeek (дата обращения: 12.12.2024).
Траск Э. 2022. Грокаем глубокое обучение. Спб: Питер, 352 с.
A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018) [Электронный ресурс]. URL: https://registry.opendata.aws/cse-cic-ids2018/ (дата обращения: 12.12.2024).
Kelleher J.D. 2019. Deep Learning. The Massachusetts Institute of Technology, 296 p.
Kneusel R.T. 2022. Math for Deep Learning. A practitioner`s guide to mastering neural networks. – San Francisco: No Starch Press, 344 p.
Madani A. 2023. Debugging Machine Learning Models with Python. Develop high-performance, low bias, and explainable machine learning and deep learning models. Birmingham: Packt Publishing Ltd., 344 p.
Weber H. 2020. Big Data and Artificial Intelligence. Complete Guide to Data Science, AI, Big Data and Machine Learning. Independently Published: Hans Weber, 160 p.
Yuxi (Hayden) Liu. 2020. Python Machine Learning By Example. Third Edition. Build intelligent systems using Python, Tensor Flow 2, PyTorch, and scikit-learn. Birmingham: Packt Publishing Ltd., 526 p.

References

Grigor'ev A. 2023. Mashinnoe obuchenie. Portfolio real'nyh proektov [Machine Learning. Portfolio of real projects]. Spb: Piter, 496 p.
Issledovanie GK «Solar»: Ataki na rossijskie kompanii v III kvartale 2023 goda [Solar Group Research: Attacks on Russian companies in Q3 2023] [Elektronnyj resurs]. URL: https://rt-solar.ru/analytics/reports/3889/ (data obrashcheniya: 12.12.2024).
Martin R. 2022. Chistaya arhitektura. Iskusstvo razrabotki programmnogo obespecheniya [Pure Architecture. The art of software development]. Sankt-Peterburg: Piter, 352 p.
Otchet o DDOS-atakah za tretij kvartal 2023 goda ot StormWall [DDOS attacks report for the third quarter of 2023 from StormWall] [Elektronnyj resurs]. URL: https://stormwall.pro/otchet-o-ddos-atakah-2023-tretij-kvartal (data obrashcheniya: 12.12.2024).
Plas Dzh. 2021. Python dlya slozhnyh zadach: nauka o dannyh i mashinnoe obuchenie [Python for complex problems: data science and machine learning]. SPb: Piter, 576 p.
Repozitorij s dannymi ob uyazvimostyah Cross Site Scripting (XSS) Vulnerability Payload List [Elektronnyj resurs]. URL: https://github.com/payloadbox/xss-payload-list (data obrashcheniya: 12.12.2024).
Repozitorij s dannymi po informacionnoj bezopasnosti SecList [Elektronnyj resurs]. URL: https://github.com/danielmiessler/SecLists (data obrashcheniya: 12.12.2024).
Repozitorij svobodnoj sistemy obnaruzheniya vtorzhenij Open Source Tripwire [Elektronnyj resurs]. URL: https://github.com/Tripwire/tripwire-open-source (data obrashcheniya: 12.12.2024).
Repozitorij svobodnoj sistemy obnaruzheniya vtorzhenij Snort [Elektronnyj resurs]. URL: https://github.com/snort3/snort3 (data obrashcheniya: 12.12.2024).
Repozitorij svobodnoj sistemy obnaruzheniya vtorzhenij Zeek [Elektronnyj resurs]. URL: https://github.com/zeek/zeek (data obrashcheniya: 12.12.2024).
Trask E. 2022. Grokaem glubokoe obuchenie [Grokai deep learning]. Spb: Piter, 352 p.
A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018) [Elektronnyj resurs]. URL: https://registry.opendata.aws/cse-cic-ids2018/ (data obrashcheniya: 12.12.2024).
Kelleher J.D. 2019. Deep Learning. The Massachusetts Institute of Technology, 296 p.
Kneusel R.T. 2022. Math for Deep Learning. A practitioner`s guide to mastering neural networks. – San Francisco: No Starch Press, 344 p.

Madani A. 2023. Debugging Machine Learning Models with Python. Develop high-performance, low bias, and explainable machine learning and deep learning models. Birmingham: Packt Publishing Ltd., 344 p.
Weber H. 2020. Big Data and Artificial Intelligence. Complete Guide to Data Science, AI, Big Data and Machine Learning. Independently Published: Hans Weber, 160 p.
Yuxi (Hayden) Liu. 2020. Python Machine Learning By Example. Third Edition. Build intelligent systems using Python, Tensor Flow 2, PyTorch, and scikit-learn. Birmingham: Packt Publishing Ltd., 526 p.

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.
Conflict of interest: no potential conflict of interest related to this article was reported.

Поступила в редакцию 03.03.2025
Поступила после рецензирования 29.05.2025
Принята к публикации 04.06.2025

Received March 3, 2025
Revised May 29, 2025
Accepted June 04, 2025

ИНФОРМАЦИЯ ОБ АВТОРАХ

Куценко Светлана Мунавировна, кандидат педагогических наук, доцент, доцент кафедры Информационные технологии и интеллектуальные системы, Казанский государственный энергетический университет, Казань, Россия

Салтанаева Елена Андреевна, кандидат технических наук, доцент кафедры Информационные технологии и интеллектуальные системы, Казанский государственный энергетический университет, г. Казань, Россия

Ахметов Азат Маратович, бакалавр, Казанский государственный энергетический университет, Казань, Россия

INFORMATION ABOUT THE AUTHORS

Svetlana M. Kutsenko, Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Information Technologies and Intelligent Systems, Kazan State Power Engineering University, Kazan, Russia

Elena A. Saltanaeva, Candidate of Technical Sciences, Associate Professor of the Department of Information Technologies and Intelligent Systems, Kazan State Power Engineering University, Kazan, Russia

Azat M. Akhmetov, Bachelor student, Kazan State Power Engineering University, Kazan, Russia