Bulletin of L.N. Gumilyov ENU. Mathematics. Computer science. Mechanics series, 2023, Vol. 142, №1, P.21-34
http://bulmathmc.enu.kz, E-mail: vest_math@enu.kz

МРНТИ: **28.23.25, 50.41.23**

Д.Ж.Сатыбалдина, Н.К. Бисенбаева, Е.Н. Сейткулов, А.К. Сексенбаева

Евразийский национальный университет имени им. Л.Н.Гумилева, ул. Сатпаева, 2, 020000, Астана, Казахстан
(E-mail: satybaldina_dzh@enu.kz, n.kobylandievna@gmail.com, yerzhan.seitkulov@gmail.com, sexenbayeva_ak@enu.kz)

Детектирование и классификация сетевых атак с помощью Splunk Machine Learning Toolkit [1]

Аннотация: В современных условиях внедрения цифровых технологий в различные отрасли экономики, цифровизации государственного управления, сфер здравоохранения, образования и науки, роста числа интернет-услуг и используемых мобильных устройств становятся все более актуальными вопросы обеспечения безопасности систем сотовой связи. Становится все труднее обнаруживать многочисленные и сложные угрозы кибербезопасности по мере развития и расширения источников и методов реализации кибератак. Классические подходы обнаружения сетевых атак, которые в значительной степени полагаются на статическое сопоставление, такие как сигнатурный анализ, черные списки или шаблоны регулярных выражений, ограничены в гибкости и являются малоэффективными для раннего выявления аномалий и оперативного реагирования на инциденты информационной безопасности. Для решения данной проблемы предлагается использование алгоритмов машинного обучения, которые могут обеспечить новые подходы и более высокие показатели обнаружения вредоносной активности в сети. В данной работе используется платформа анализа данных Splunk Enterprise с использованием расширения и дополнительный инструментарий машинного обучения Splunk Machine Learning Toolkit для создания, обучения, тестирования и проверки классификатора сетевых атак. Производительность предложенной модели была оценена с использованием четырех алгоритмов машинного обучения, таких как дерево решений (a decision tree), метод опорных векторов (a support vector machine), случайный лес (a random forest) и двойной случайный лес (a double random forest). Экспериментальные результаты показывают, что все использованные алгоритмы машинного обучения могут эффективно использоваться для обнаружения сетевых атак, а метод двойного случайного леса имеет наилучшую точность обнаружения атак типа «отказ в обслуживании».

Ключевые слова: кибербезопасность, машинное обучение, обнаружение вторжений, сетевая безопасность, сети сотовой связи.

DOI: https://doi.org/10.32523/2616-7182/bulmathenu.2023/1.2

2000 Mathematics Subject Classification: 68M15

Введение. Внедрение цифровых технологий в различные отрасли экономики, цифровизация сфер государственного управления, образования и здравоохранения, рост числа интернет- сервисов и мобильных устройств, используемых потребителями, с одной стороны, и наблюдаемый рост числа источников и методов реализации кибератак в последние годы (см. Рисунок 1), с другой стороны, ставят перед операторами мобильной беспроводной связи задачи развития с учетом проблем кибербезопасности. Системы сотовой связи постоянно эволюционируют, улучшая сетевую архитектуру, интерфейсы и

[1]Данная работа выполнена при финансовой поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан (ПЦФ № BR18574045).

Рис. 1. Статистика и классификация инцидентов кибербезопасности в 1-3 кварталах 2022 года в Республике Казахстан (https://cert.gov.kz/press_club/infographics)

протоколы, повышая пропускную способность передачи данных. Но эволюция приводит и к появлению новых уязвимостей, которые могут использоваться для реализации атак как на сеть доступа, так и на базовую сеть, вызывая отказ в обслуживании или возможность выполнения вредоносного функционала.

Все это приводит к необходимости разработки надежных систем обнаружения сетевых атак и механизмов быстрого реагирования на инциденты кибербезопасности [1]. Примером такого подхода являются системы управления информацией и событиями безопасности (Security Information and Event Management, SIEM), которые становятся важной компонентой экосистемы сетевой безопасности наряду с межсетевыми экранами, системами предотвращения вторжений и обнаружения вторжений (Intrusion Prevention System / Intrusion Detection System, IPS/IDS), решениями по статическому и динамическому анализу вредоносных файлов [2].

Ранее нами был спроектирован и внедрен в одной из государственных организаций программный комплекс для Оперативного центра информационной безопасности (ОЦИБ) [3]. В составе программного комплекса реализована SIEM-система для мониторинга и расследования инцидентов информационной безопасности с визуализацией интерактивными аналитическими панелями (дашбоардами), которые формируются на основе сбора и анализа разнородных данных с различных программно-аппаратных средств, реализованных в ОЦИБ.

Среди различных доступных вариантов SIEM решений с открытым исходным кодом и лицензионных продуктов выбран Splunk Enterprise Security (ES), построенный на основе Splunk®Enterprise [4]. Splunk®Enterprise – это ведущая в отрасли платформа операционной аналитики, которая позволяет анализировать машинные данные, что может расширить возможности устранения неполадок, повысить производительность и улучшить состояние безопасности информационно-коммуникационной инфраструктуры компании [5].

В настоящей работе представлены результаты исследований по реализации классификатора сетевых атак на основе алгоритмов машинного обучения с использованием дополнительного инструментария Splunk Machine Learning Toolkit [6], эталонной базы данных UNSW-NB15 [7], интерпретатора языка Python и поисковых команд языка SPL (Splunk Processing Language). Получены оценки точности классификации сетевых атак с использованием четырех алгоритмов машинного обучения (дерево решений, метод опорных векторов, случайный лес и двойной случайный лес). Экспериментальные результаты показали эффективность использования алгоритмов машинного обучения для детектирования нормальной и аномальной сетевых активностей, а также для классификации сетевых атак.

Остальная часть этой статьи структурирована следующим образом. В разделе 2 описаны связанные работы. В разделе 3 представлены методология предлагаемого

подхода для классификации сетевых атак, набор используемых машинных данных, команды языка SPL для реализации использованных алгоритмов машинного обучения, показатели эффективности алгоритмов обнаружения и классификации сетевых атак. В разделе 4 обсуждаются результаты эксперимента. Заключение и будущие исследования представлены в разделе 5.

Связанные работы. В последние годы растет число исследований, посвященных совершенствованию методов обнаружения сетевых атак, из них ряд исследований по использованию машинного обучения для выявления аномалий в сети.

В обзорной работе [8] описано множество методов обнаружения вторжений для борьбы с угрозами сетевой безопасности, которые можно в целом разделить на системы обнаружения вторжений на основе сигнатур и системы обнаружения вторжений на основе аномалий. Авторы показали, что традиционные подходы на основе сигнатур проверяют сетевые пакеты и пытаются сопоставить их с базой данных хэшей известных атак. Но эти методы не могут идентифицировать атаки нулевого дня, таргетированные атаки, полиморфные варианты вредоносного программного обеспечения (ВПО). Анализ сетевых пакетов, ВПО на основе аномалий оказался более эффективным для детектирования таких сложных кибератак благодаря тому, что распознавание аномальной активности пользователя не зависит от базы данных сигнатур [8].

Методы детектирования кибератак на основе аномалий авторы работы [8] разделяют на три группы: основанные на статистике, основанные на знаниях и основанные на машинном обучении. Эти классы методов вместе с примерами их подклассов представлены на рисунке 2. В рамках первого подхода производится сбор и проверка каждой записи данных в наборе элементов с последующим построением статистической модели нормального поведения пользователя. При втором подходе исследователи идентифицируют нормальные и аномальные спецификации протоколов и экземпляры сетевого трафика. Для реализации последней группы методов создаются шаблоны нормального трафика и аномальных ситуаций и поведения пользователей, на которых проводится обучение, тестирование классификаторов на основе методов машинного обучения шаблонов из наборов обучающих данных.

Авторы обзора более подробно рассмотрели несколько исследований с использованием методов машинного обучения для обнаружения атак нулевого дня и показали, что существующие подходы могут иметь проблемы с генерированием и обновлением информации о новых атаках и дают большое количество ложных срабатываний или низкую точность. Это связано с тем, что большинство существующих методов машинного обучения обучаются на основе наборов данных DARPA/KDD99, собранных в 1999 году, которые не включают более новые действия вредоносных программ. Таким образом, существует потребность в более новых и полных наборах данных, содержащих широкий спектр действий вредоносного ПО.

Далее представлен краткий обзор исследований, в которых авторы использовали тот или иной метод машинного обучения для выявления аномалий в сети или сетевых атак определенного типа. В работе [9] для выявления атак типа «отказ в обслуживании» (Denial of Service, DoS) используется модель, основанная на сборе данных файлов логгирования событий на платформе Spark, и классификация сетевых атак по методу случайного леса (a random forest) с точностью 99,2%. Авторы показали, что модель может использоваться для обработки крупномасштабных потоков DNS-запросов, что полезно для практического использования.

Авторы работы [10] предложили подход для обнаружения DoS-атак на основе инфраструктуры больших данных. Предложенное решение включает в себя модули сбора сетевого трафика в реальном времени и модуль обнаружения. Модуль сбора сетевого трафика собирает и извлекает особенности трафика, используя модель микропакетной обработки. Модуль обнаружения использует алгоритм классификации Spark-ML на основе метода случайного леса для обнаружения DoS-атак на сетевом трафике. Для оценки точности обнаружения алгоритм оценивался и сравнивался на наборах данных NSL-KDD и UNSW-NB15. Экспериментальные результаты показывают, что предложенный алгоритм

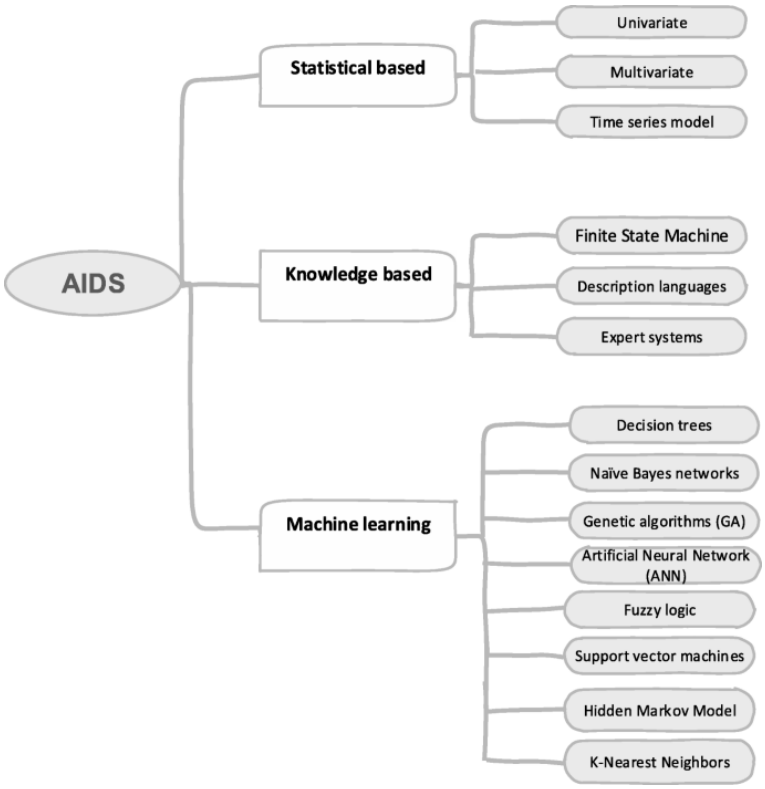

Рис. 2. Классификация систем детектирования кибератак на основе аномалий (Anomaly-based Intrusion Detection Systems, AIDS) [8]

обнаружения достиг уровня точности 99,95% и 98,75%, соответственно, для двух наборов данных.

В работе [11] предложены модели глубокого обучения для обнаружения и снижения риска DDoS-атак, нацеленных на централизованный контроллер в программно-определяемой сети, с использованием рекуррентной нейронной сети с долгой краткосрочной памятью (Long short-term memory, LSTM) и сверточной нейронной сетью (convolutional neural network, CNN). Точность классификации DDoS-атак сверточной нейронной сетью была невысокой, 66%. Модель LSTM дала точность 89,63%, что превосходит показатели результативности 86,85% и 82,61% для классических методов машинного обучения - метода опорных векторов (a support vector machine SVM) и наивного байесовского классификатора (Naive Bayes classifier) соответственно.

Авторы работы [12], используя два подхода к машинному обучению (случайный лес и многослойный персептрон) и платформу больших данных (Spark ML), смогли с точностью 99,5% обнаружить атаку типа «отказ в обслуживании» в режиме реального времени за несколько миллисекунд.

Резюмируя краткий обзор разработанных систем, можно сделать предположение, что применение современных методов машинного обучения совместно с технологиями сбора машинных данных в SIEM-системах на платформе операционной аналитики может быть эффективным подходом для разработки систем детектирования аномалий и классификации сетевых атак в целях раннего распознавания и оперативного реагирования на инциденты кибербезопасности.

Исходные данные и методика исследований. В данном разделе представлена методика исследований по проектированию, реализации и тестированию интеллектуальной системы классификации аномального и нормального сетевого трафика на основе применения традиционных алгоритмов машинного обучения и нового метода двойного случайного леса. Для тестирования вышеуказанной методики проведены

экспериментальные исследования по детектированию аномалий для искусственно сгенерированного DNS и наиболее известных категорий кибератак.

Для реализации экспериментов была использована платформа для анализа данных Splunk Enterprise с использованием расширения Machine Learning Toolkit [6]. Данная библиотека содержит более 30 распространенных алгоритмов машинного обучения с открытым исходным кодом на языке Python. Подготовка данных выполнена на сервере Splunk с помощью встроенного языка Search Processing Language (SPL). Для исполнения SPL-скриптов с набором данных используется интепретатор языка Python.

Для проведения эксперимента были выбраны следующие алгоритмы машинного обучения, как наиболее встречающиеся в связанных работах, что позволяет провести в последующем сравнение экспериментальных результатов с результатами других исследователей:

- дерево решений (a decision tree, DT);
- случайный лес (a random forest, RF);
- метод опорных векторов (a support vector machine, SVM).

Данные методы являются классическими, их описание приведено в большом количестве учебников и научных статьях, например, в работах [8, 9, 11].

Также в эксперименте использован метод двойного случайного леса (a double random forest, DRF) как модифицированный метод случайного леса. В работе [13] авторами показано, что точность классификации метода случайного леса может быть улучшена, если использовать ансамбль более разнообразных деревьев, чем деревья с минимальным размером узлов. Для этого был предложен новый метод начальной загрузки обучающей выборки на каждом узле в процессе создания дерева вместо начальной загрузки на корневом узле, как в классическом методе случайного леса. Экспериментальные исследования по распознаванию изображений рукописных цифр от 0 до 9 показывают, что предложенный метод DRF намного превосходит классические ансамблевые методы классификации [13]. Поэтому было интересно попробовать использовать алгоритм DRF с учетом особенностей задач классификации сетевых атак.

В качестве обучающей и тестовой базы данных использована база данных UNSW-NB15, которая была создана в лаборатории Cyber Range ACCS, с использованием генератора аномального сетевого трафика, создаваемого 9-ю видами сетевых атак (см. таблица 1) [14].

Согласно описанию авторов работы [14] для захвата пакетов сетевого трафика объемом 100 ГБ был применен программный инструментарий tcpdump [15], который также использовался для разделения трафика на фрагменты по 1000 МБ. Далее из pcap-файлов с использованием программного обеспечения Argus [16] созданы 4 CSV-файла, содержащих ключевые характеристики как надежные признаки (атрибуты) для классификации нескольких типов атак. Выделено 49 ключевых характеристик (атрибутов для классификации атак), которые разделены на несколько групп: основные (Basic), контентные (Content) и временные (Time).

Таблица 1. Распределение записей по категориям атак в базе данных UNSW-NB15

Типы сетевых атак	**Количество записей**	**Description**
Normal (нормальный трафик)	2 218 761	естественные данные нормального трафика
Fuzzer (трафик, создаваемый программой-фаззером)	24 246	попытка приостановить работу сети путем передачи случайно сгенерированных данных
Analysis (трафик, создаваемый программой-анализатором)	2 677	трафик содержит различные атаки сканирования портов, html-файлов и проникновение спам
Backdoors (бэкдоры)	2 329	техника, при которой механизм безопасности системы скрытно обходится для доступа к компьютеру или его данным
DoS (атаки типа «отказ в обслуживании», в том числе распределенные)	16 353	злонамеренная попытка сделать сервер или сетевой ресурс недоступным для пользователей
Exploits (атаки с использованием эксплойтов)	44 525	злоумышленник знает о проблеме безопасности в операционной системе, использует эти знания, применяя уязвимость
Generic (атака против шифров)	215 481	общий метод работает против всех блочных шифров (с заданным размером блока и ключа), без учета структуры блочного шифра
Reconnaissance (пассивные атаки с целью разведки)	13 987	содержит все попытки проникновения в сеть, которые могут имитировать атаки со сбором информации
Shellcode (двоичный вредоносный код)	1 511	небольшой фрагмент кода, используемый в качестве полезной нагрузки при эксплуатации уязвимости в программном обеспечении
Worms (вредоносный код типа «червь»)	174	вредоносный код, который копирует себя, чтобы распространиться на другие компьютеры

Пример основных характеристик приведен в таблице 2. Записи файла UNSW-NB15_1.csv использованы как обучающая выборка, а файла UNSW-NB15_2.csv – как тестовая.

Схема эксперимента представлена на рисунке 3.

Выборка нужной категории сетевых атак осуществлялась посредством команды Splunk *«search»*:

search attack_cat=Normal OR attack_cat=Dos,

где последний параметр указывает на тип атаки (см. Таблицу 1), в примере использован параметр Dos – атака типа «отказ в обслуживании» (Denial of Service, DoS-атака).

На этапе предобработки преобразуются нечисловые поля (строки или символы) в числовые, используя однократное кодирование, ввиду того, что алгоритмы машинного обучения работают с числовыми данными. Производится нормирование данных, в итоге данные записи сетевого трафика преобразуются в числовую матрицу из вещественных значений атрибутов, которые подаются на алгоритм классификации по одному из 4-х методов машинного обучения.

Таблица 2. Примеры атрибутов потоков

№ атрибута	**Обозначение**	**Тип данных**	**Описание**
1	srcip	N (номинальный)	IP Адрес источника (Source IP address)
2	sport	I (целое число)	Номер порта источника (Source port number)
3	dstip	N	IP Адрес получателя (Destination IP address)
4	dsport	I	Номер порта получателя (Destination port number)
5	proto	N	Протокол транзакции (Transaction protocol)
29	stime	T (метка времени)	Время начала записи (record start time)
34	synack	F(число с плавающей запятой)	Время между пакетами SYN и SYN_ACK в TCP The time between the SYN and the SYN_ACK packets of the TCP
48	attack_cat	N	Название категории атаки (Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms) см. Таблицу 1
49	Label	B (двоичный)	0 для записи нормального трафика и 1 для записи трафика при сетевой атаке

Форма запроса поиска данных из индексированного дата сета и применения к нему определенного алгоритма машинного обучения приведена в следующем примере:

index=nb15_test|search attack_cat=Normal OR attack_cat=Dos|fields label, ackdat, ct_dst_ltm, ct_dst_sport_ltm, ct_dst_src_ltm, ct_flw_http_mthd, ct_ftp_cmd, ct_src_dport_ltm, ct_src_ltm, ct_srv_dst, ct_srv_src, ct_state_ttl, dbytes, dinpkt, djit, dload, dloss, dmean, dpkts, dtcpb, dttl, dur, dwin, is_ftp_login, is_sm_ips_ports, proto, rate, response_body_len, sbytes, service, sinpkt, sjit, sload, sloss, smean, spkts, state, stcpb, sttl, swin, synack, tcprtt, trans_depth |apply DRF_DOS

Обнаружение аномалий или детектирования определенного вида сетевых атак относится к задачам бинарной классификации, для оценки которой используются следующие: матрица ошибок (a confusion matrix, CM), аккуратность (ac*curacy*), точность (a precision), полнота (a recall) и F-мера [8].

Таблица 3 представляет вид матрицы ошибок для классификатора кибератак, которая может быть использована для оценки производительности алгоритмов машинного обучения. Каждый столбец матрицы представляет экземпляры в прогнозируемом классе, а каждая строка представляет экземпляры в реальном классе.

Таблица 3. Матрица ошибок для задачи классификации атак

Actual Class	Predicted Class	
Class	Normal	Attack
Normal	True negative (TN)	False Positive (FP)
Attack	False Negative (FN)	True positive (TP)

Эффективность алгоритма классификации обычно оцениваются на основе следующих 4-х стандартных показателей, формулы для вычисления которых представлены ниже на основе введеных обозначений в матрице ошибок (см. Таблицу 3).

Показатель *Accuracy* (аккуратность или правильность, точность классификации) определяется как доля правильных результатов по отношению ко всем возможным вариантам предсказания, которая достигается классификатором:

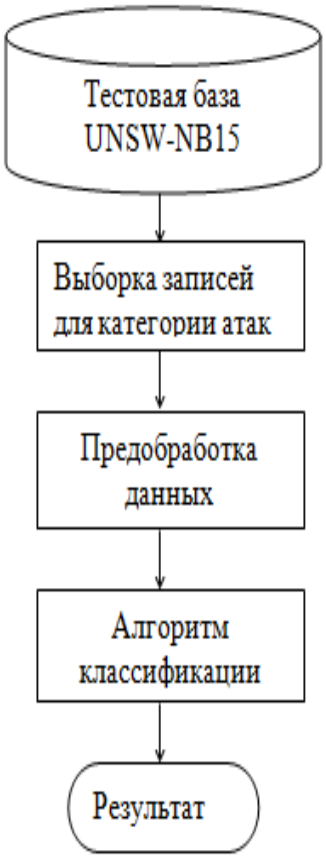

Рис. 3. Схема эксперимента по классификации атак с использованием алгоритмов машинного обучения

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \tag{1}$$

Метрика *Precision* (прецензионность, точность классификации) определяется как доля правильно определенных экземпляров классов сетевых атак, и при этом действительно являющимися трафиками сетевых атак:

$$Precision = \frac{TP}{TP + FP}. \tag{2}$$

Чувствительность (полнота) метода классификации *Recall*, или *True Positive Rate* (TPR), рассчитывается как отношение количества правильно предсказанных атак к общему количеству атак:

$$Recall = \frac{TP}{TP + FN}. \tag{3}$$

Если все сетевые вторжения правильно классифицированы, то показатель TPR равен 1, что крайне редко для реальных систем обнаружения вторжений. Значение TPR чаще стремится к 1.

Также используется способ объединения нескольких критериев в один агрегированный критерий качества $F1$-*score* (*F-мера*) как среднее гармоническое значение точности и чувствительности:

$$F1 - score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{4}$$

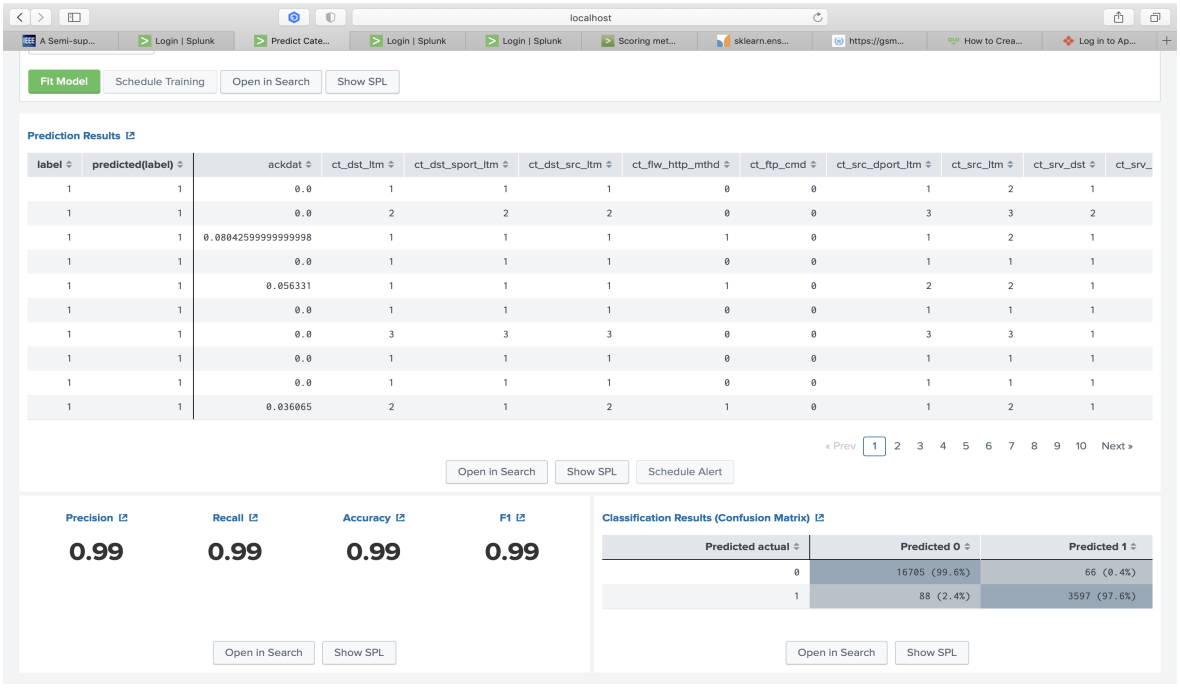

Рис. 4. Результаты классификации трафика для детектирования DoS-атак с помощью алгоритма RF

F-мера достигает максимума при чувствительности и точности, равными единице, и близка к нулю, если один из аргументов близок к нулю.

Все формулы для вычисления описанных выше метрик эффективности алгоритма машинного обучения реализованы в библиотеке scikit-learn инструмента Machine Learning Toolkit, так же, как и три используемых алгоритма машинного обучения (дерево решений DT, случайный лес RF, метод опорных векторов SVM). Для реализации классификации с использованием нового метода – двойной случайный лес DRF – на языке Python был разработан дополнительный плагин (программный модуль) SPL-DRF.

При реализации модуля SPL-DRF в целях повышения быстродействия выполняется параллельное построение деревьев и параллельное вычисление прогнозов с помощью параметра n_jobs. Если n_jobs=k, тогда вычисления разделяются на k заданий, которые и выполняются на k ядрах машины. Если n_jobs= -1 тогда используются все ядра, имеющиеся на машине. Таким образом, получено значительное ускорение при построении большого количества деревьев или когда построение одного дерева требует значительного количества времени в больших наборах данных.

Результаты эксперимента.

На рисунках 4-6 представлены скриншоты с результатами тестирования классификатора нормальных и аномальных сетевых трафиков из базы данных UNSW-NB15B и с использованием алгоритмов DT, RF, SVM, соответственно. В примерах представлены данные для атак типа «отказ в обслуживании (Denial of Service, DoS).

Как видно из рисунков 4-6, в нижней левой части представлены вычисленные значения метрик эффективности алгоритмов в классификации. Использование представления с двумя разрядами после запятой не позволяет точно определить, имеется ли различие в значениях разных метрик. В правой нижней части скриншотов представлены матрицы ошибок для каждого алгоритма классификации. Используя эти данные, можно повторно произвести вычисления по формулам (1)-(4) и уточнить значения всех метрик, используемых в машинном обучении.

В таблице 4 сведены все экспериментальные результаты, с представлением 4-х разрядов после запятой, полученные после изменения настроек алгоритмов.

Таблица 4. Сравнение результатов классификации при использовании разных алгоритмов машинного обучения

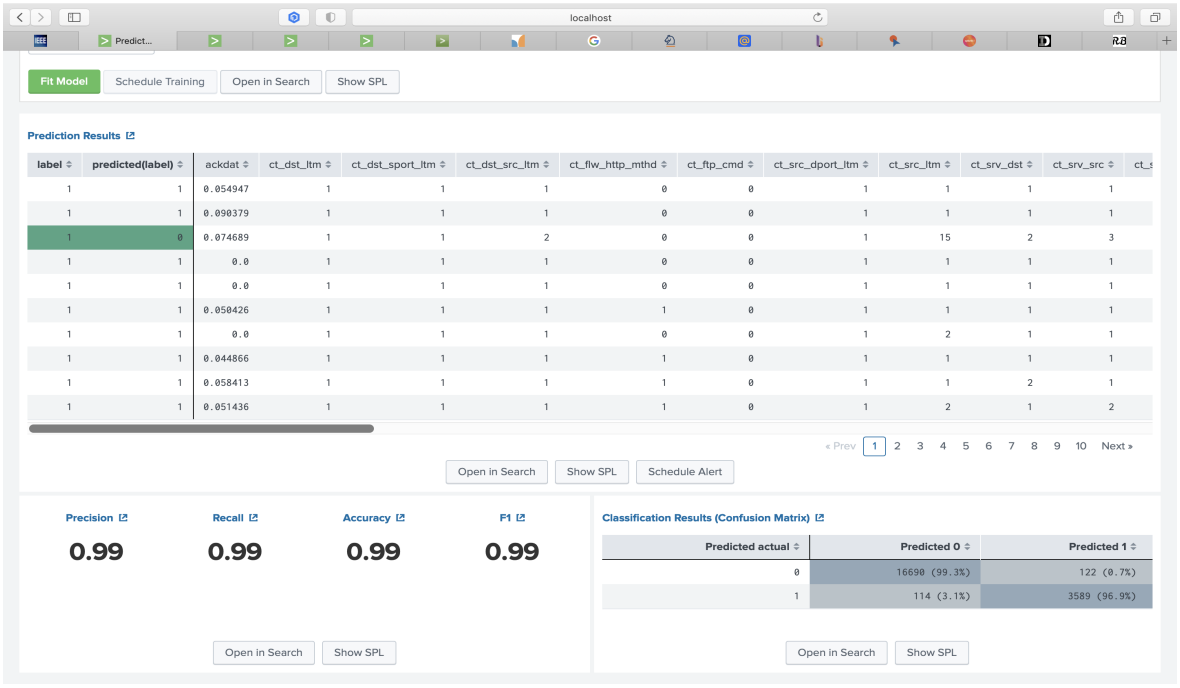

Рис. 5. Результаты классификации трафика для детектирования DoS-атак с помощью алгоритма DT

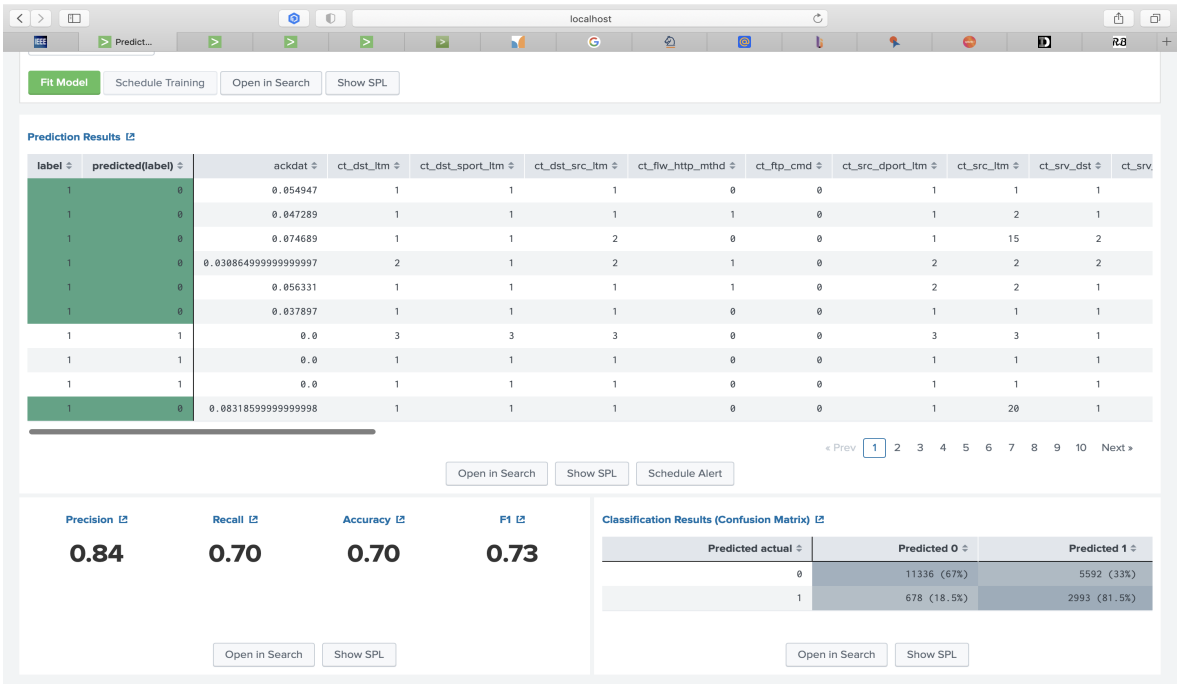

Рис. 6. Результаты классификации трафика для детектирования DoS-атак с помощью алгоритма SVM

Алгоритм машинного обучения	**Accuracy**	**Precision**	**Recall**	**F1-score**
Случайный лес (RF)	0,9925	0,9948	0,9961	0,9954
Дерево решений (DT)	0,9885	0,9932	0,9927	0,9930
Машина опорных векторов (SVM)	0,6985	0,8370	0,6945	0,7329
Двойной случайный лес (DRF)	0,9984	0,9987	0,9993	0,9990

На рисунке 7 представлены оценки точности классификации DoS-атак с использованием разработанного программного модуля SPL-DRF и базы данных UNSW-NB15B.

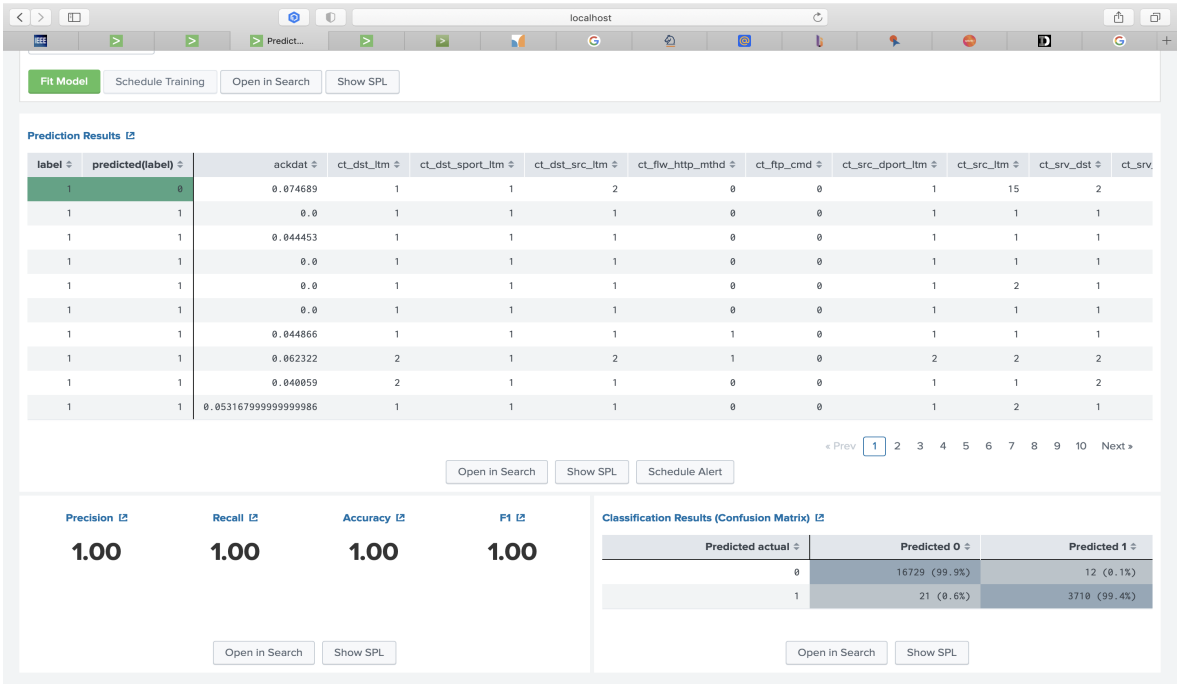

Рис. 7. Результаты классификации трафика для детектирования DoS-атак с помощью алгоритма DRF

Экспериментальные результаты тестирования обученного классификатора на базе данных UNSW-NB15B показывают, что наилучшие результаты по детектированию Dos-атак по точности классификации и параметру ложного срабатывания дает алгоритм «случайный лес» по сравнению с другими использованными классическими методами машинного обучения. Результаты для метода RF также хорошо согласуются с оценками точности классификации Dos-атак 99,2% и 98,75%, полученными авторами работ [9] и [10] соответственно. Полученные оценки точности классификации DoS-атак с использованием реализованного метода двойного случайного леса (a double random forest, DRF) и базы данных UNSW-NB15B показывают улучшение по сравнению с немодифицированным методом случайного леса.

Заключение и будущие исследования. В работе представлены результаты исследований по применению современных методов машинного обучения совместно с технологиями сбора машинных данных на платформе операционной аналитики Splunk Enterprise Security. Показано, что предложенный нами подход для разработки систем детектирования аномалий и классификации сетевых атак является эффективным для задач раннего распознавания и оперативного реагирования на инциденты кибербезопасности.

Получены оценки производительности (в метриках задач классификации и распознавания) модели детектирования аномалий с использованием классических алгоритмов машинного обучения (дерево решений, метод опорных векторов, случайный лес). Экспериментальные результаты показывают, что все использованные алгоритмы машинного обучения могут эффективно использоваться для детектирования нормальной и аномальной сетевых активностей, а также для классификации сетевых атак.

Научная новизна работы связана с развитием метода двойного случайного леса. Разработан новый алгоритм построения деревьев решений с использованием всех данных обучающей выборки на каждом промежуточном узле, включая корневой узел. Это позволяет строить более разветвленные ансамбли, чем в методе случайного леса, который строит отдельные деревья, используя начальную загрузку данных только на корневой узел, при этом на вход подается только часть информации, представляющей собой случайную выборку из обучающей базы. Расширены функциональные возможности инструмента Splunk Machine Learning Toolkit, дополнительного программного модуля (плагина) на

языке Python для реализации двойного случайного леса. Для обеспечения быстродействия обработки ансамблей деревьев большого размера использованы возможности языка SPL для параллельного построения деревьев и параллельного вычисления прогнозов. Экспериментальные результаты по детектированию аномалий и классификации сетевых атак показали, что модифицированный метод случайного леса имеет наилучшую точность обнаружения атак типа «отказ в обслуживании по сравнению с использованными классическими алгоритмами машинного обучения.

В будущих работах планируется провести эксперименты с обученной моделью классификации сетевых атак на основе реальных данных анализа сетевого трафика, собираемого со всех устройств в программном комплексе для ОЦИБ. Также будут проведены исследования по детектированию аномалий в сотовом сетевом трафике на основе реальной статистики сотового интернет-провайдера.

Список литературы

1 Zhijun W. et al. Low-rate DoS attacks, detection, defense, and challenges: a survey //IEEE Access. -2020. -T. 8. -P. 43920-43943.

2 Hristov M. et al. Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT //2021 IEEE 20th International Symposium on Network Computing and Applications (NCA). -IEEE, 2021. -P. 1-5.

3 Абдиев Б.С., Сатыбалдина Д.Ж., Бисенбаева Н.К. Программный комплекс для оперативного центра информационной безопасности // Свидетельство о государственной регистрации прав на программу для ЭВМ, №10063 от 21.05.2020 г.

4 Платформа Splunk Security для расширенной аналитики данных и автоматизированного расследования и реагирования на инциденты информационной безопасности. -URL: *https* : *//www.splunk.com/en*$_u$*s/products/cyber* − *security.html*(*Accessed* : 2022 − 10 − 03)

5 Mehta D. An Overview of Splunk//Splunk Certified Study Guide. -2021. -P. 3-26.

6 Инструментарий машинного обучения от Splunk. -URL: *https* : *//www.splunk.com/en*$_u$*s/products/machine*− *learning.html*(*Accessed* : 2022 − 10 − 03)

7 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.

8 Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecur. 2019. -Vol.2. - №. 1. - P. 1-22.

9 Liguo Chen, Yuedong Zhang, Qi Zhao, Guanggang Geng, ZhiWei Yan, Detection of DNS DDoS Attacks with Random Forest Algorithm on Spark // Procedia Computer Science. -2018. -Volume 134.- P. 310-315.

10 Gao Y. et al. A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network //IEEE Access. -2019. -T. 7. -P. 154560-154571.

11 Gadze J. D. et al. An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers //Technologies. -2021. -T. 9. -№. 1. -P. 14.

12 Awan M. J. et al. Real-time DDoS attack detection system using big data approach //Sustainability. -2021. -T. 13. -№. 19. -P. 10743.

13 Han, S., Kim, H. & Lee, YS. Double random forest// Mach Learn. -2020. -P. 1569-1586. *https* : *//doi.org*/10.1007/*s*10994 − 020 − 05889 − 1

14 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.

15 Анализатор пакетов и библиотека C/C++ для захвата сетевого трафика. -URL: *http* : *//www.tcpdump.org/*(*Accessed* : 2022 − 10 − 03)

16 Технология сетевого аудита Argus. -URL: *http* : *//qosient.com/argus/index.shtml*(*Accessed* : 2022 − 10 − 03)

Д.Ж. Сатыбалдина, Н.К. Бисенбаева, Е.Н. Сейткулов, А.К. Сексенбаева

Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Сәтпаев көш., 2, Астана, 010008, Қазақстан

Splunk Machine Learning Toolkit көмегімен желілік шабуылдарды анықтау және жіктеу

Аннотация: Қазіргі кезде экономиканың әртүрлі салаларында цифрлық технологиялардың енгізілуі, мемлекеттік басқарудың, денсаулық сақтаудың, білім берудің және ғылымның цифрлануы, интернет қызметтері мен пайдаланылатын мобильді құрылғылар санының өсуі, ұялы байланыстың қауіпсіздігін қамтамасыз ету мәселелерінің өзектілігінің арта түсуіне алып келді. Кибершабуылдардың көздері мен әдістері дамып, кеңейген сайын киберқауіпсіздіктің көптеген және күрделі қатерлерін анықтау қиындай түсуде. Сигнатуралық талдау, қара тізімдер немесе тұрақты өрнек үлгілері сияқты статикалық сәйкестікке көп негізделген желілік шабуылдарды анықтаудың классикалық тәсілдері икемділігімен шектеледі және аномалияны ерте анықтау және ақпараттық қауіпсіздік

инциденттеріне жылдам әрекет ету үшін тиімсіз. Бұл мәселелерді шешу үшін желідегі зиянды әрекетті анықтаудың жаңа тәсілдері мен жоғары қарқынын қамтамасыз ете алатын машиналық оқыту алгоритмдерін пайдалану ұсынылады. Бұл жұмыста кеңейтуді қолданатын тиімді Splunk Enterprise деректерді талдау платформасы және қосымша Splunk Machine Learning Toolkit желілік шабуыл классификаторын құру, оқыту, сынау және тексеру үшін пайдаланылады.

Ұсынылған модельдің өнімділігі шешімдер ағашы (a decision tree), тірек векторлары әдістері (a support vector machine), кездейсоқ орман (a random forest) және қос кездейсоқ орман (a double random forest) сияқты төрт машиналық оқыту алгоритмдері арқылы бағаланды. Эксперименттік нәтижелер барлық қолданылатын машиналық оқыту алгоритмдерін желілік шабуылдарды анықтау үшін тиімді пайдалануға болатындығын және қос кездейсоқ орман әдісі таратылған "қызмет көрсетуден бас тарту" шабуылдарын анықтауда ең жақсы дәлдікке ие екенін көрсетеді.

Түйін сөздер: киберқауіпсіздік, машиналық оқыту, басып кіруді анықтау, желі қауіпсіздігі, ұялы байланыс желілер

D.Zh. Satybaldina, N.K. Bisenbaeva, Ye.N. Seitkulov, A.K. Seksenbaeva

L.N. Gumilyov Eurasian National University, Satpayev str., 2, 010008, Astana, Kazakhstan

Detecting and classifying network attacks with Splunk Machine Learning Toolkit

Abstract: In modern conditions of digital technologies implementation in various sectors of the economy, the digitalization of public administration, healthcare, education, and science, the growth in the number of Internet services and mobile devices the issues of ensuring the security of cellular communication systems are becoming increasingly relevant. It is becoming increasingly difficult to detect multiple and complex cyber security threats as the sources and methods of cyber-attacks evolve and expand. Classic network attack detection approaches that rely heavily on static matching, such as signature analysis, blacklisting, or regular expression patterns, are limited in flexibility and are ineffective for early anomaly detection and rapid response to information security incidents. To solve this problem, the use of machine learning (ML) algorithms is proposed. ML methods can provide new approaches and higher rates of detection of malicious activity on the network. In this work, the Splunk Enterprise data analysis platform and the Splunk Machine Learning Toolkit for creating, training, testing, and validating a network attack classifier are used. The performance of the proposed model was evaluated by applying four machine learning algorithms such as a decision tree, a support vector machine, a random forest, and a double random forest. Experimental results show that all used ML algorithms can be effectively used to detect network attacks, and the double random forest method has the best accuracy in detecting distributed denial-of-service attacks.

Keywords: Cyber security, intrusion detection, machine learning, network security, cellular communication networks.

References

1 Zhijun W. et al. Low-rate DoS attacks, detection, defense, and challenges: a survey, IEEE Access. 2020. Vol. 8. P. 43920-43943.

2 Hristov M. et al. Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT, 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA). IEEE, 2021. P. 1-5.

3 Abdiev B.S., Satybaldina D.Zh., Bisenbaeva N.K. Programmnyj kompleks dlya operativnogo czentra informacziionnoj bezopasnosti, Svidetelstvo o gosudarstvennoj registraczii prav na programmu dlya EVM, N10063 ot 21.05.2020 g.

4 Splunk Security platform for advanced data analytics and automated investigations and response. Available at: $https://www.splunk.com/en_us/products/cyber-security.html(Accessed: 2022-10-03)$

5 Mehta D. An Overview of Splunk, Splunk Certified Study Guide. 2021. P. 3-26.

6 Machine Learning Toolkit from Splunk. Available at: $https://www.splunk.com/en_us/products/machine-learning.html(Accessed: 2022-10-03)$

7 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.

8 Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges, Cybersecurity. 2019. Vol. 2, №1. P.1-22.

9 Liguo Chen, Yuedong Zhang, Qi Zhao, Guanggang Geng, ZhiWei Yan, Detection of DNS DDoS Attacks with Random Forest Algorithm on Spark, Procedia Computer Science. 2018. Vol. 134. P. 310-315.

10 Gao Y. et al. A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network, IEEE Access. 2019. Vol. 7. P. 154560-154571.

11 Gadze J. D. et al. An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers, Technologies. 2021. Vol. 9. №1. P. 14.

12 Awan M. J. et al. Real-time DDoS attack detection system using big data approach, Sustainability. 2021. Vol. 13. №19. P. 10743.

13 Han, S., Kim, H. and Lee, YS. Double random forest, Mach Learn. 2020. P.1569-1586. Available at: $https://doi.org/10.1007/s10994-020-05889-1$

14 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.

15 A packet analyzer and a C/C++ library for network traffic capture. http://www.tcpdump.org/ (Accessed:2022-10-03)
16 A network audit technology Argus. Available at: *http : //qosient.com/argus/index.shtml* (Accessed:2022-10-03)

Сведения об авторах:

Сатыбалдина Д.Ж. – ***автор для корреспонденции,*** к.ф.-м.н., доцент, профессор кафедры информационной безопасности, директор НИИ информационной безопасности и криптологии, Евразийский национальный университет имени им. Л.Н.Гумилева, Сатпаева 2, Астана, 010008, Казахстан.

Бисенбаева Н.К. – докторант специальности «8D06104 - Вычислительная техника и программное обеспечение», Евразийский национальный университет имени им. Л.Н.Гумилева, Сатпаева 2, Астана, 010008, Казахстан.

Сейткулов Е.Н. – к.ф.-м.н., профессор кафедры информационной безопасности, Евразийский национальный университет имени им. Л.Н.Гумилева, Сатпаева 2, Астана, 010008, Казахстан.

Сексенбаева А.К. – к.ф.-м.н., доцент, доцент кафедры информационной безопасности, Евразийский национальный университет имени им. Л.Н.Гумилева, Сатпаева 2, Астана, 010008, Казахстан.

Satybaldina Dina Zhagyparovna – ***corresponding author,*** Candidate of Physical and Mathematical Sciences, Associate Professor, Professor of the Information Security Department, Director of the Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University, Satpayeva str., 2, Astana, 010008, Kazakhstan.

Bisenbayeva Nazerke Kobylandievna – Ph.D. student in Computer Science and Software engineering, L.N. Gumilyov Eurasian National University, Satpayeva str., 2, Astana, 010008, Kazakhstan.

Seitkulov Yerzhan Nurakhanovich – Candidate of Physical and Mathematical Sciences, Professor of the Information Security Department, L.N. Gumilyov Eurasian National University, Satpayeva str., 2, Astana, 010008, Kazakhstan.

Seksenbayeva Aisha Kurmanbekovna – Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Information Security Department, L.N. Gumilyov Eurasian National University, Satpayeva str., 2, Astana, 010008, Kazakhstan.

Поступила в редакцию 01.08.2022