Казахский агротехнический исследовательский университет

им. С. Сейфуллина

УДК 004.056::004.89 На правах рукописи

**РЗАЕВ БАБЫР ТЕМІРБЕКҰЛЫ**

**Идентификация и оценка вредоносного трафика при сетевой передаче данных на основе применения технологии Data Mining**

8D06101 – Аналитика больших данных

Диссертация на соискание степени  
доктора философии (PhD)

Научные консультанты

доктор PhD,

Ж.Т. Бельдеубаева

доктор PhD,

ассоциированный профессор

И.М. Увалиева

Зарубежный научный консультант

доктор технических наук,

профессор

И.С. Лебедев

(Российская Федерация)

Республика Казахстан

Астана, 2024

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| **НОРМАТИВНЫЕ ССЫЛКИ**………………………………………………. | 4 |
| **ОПРЕДЕЛЕНИЯ**…………………………………………………………..…. | 5 |
| **ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**……………………………………... | 7 |
| **ВВЕДЕНИЕ**…………………………………………………………………… | 8 |
| **1 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ ТЕЛЕКОММУНИКАЦИЙ**………….….. | 16 |
| 1.1 Описание исследуемых объектов………………………………………… | 16 |
| 1.2 Угрозы информационной безопасности……………………………..…... | 21 |
| 1.3 Обзор научных исследований………………………………………..…… | 24 |
| 1.4 Обзор систем по обеспечению информационной безопасности………... | 28 |
| 1.5 Обзор состояния информационной безопасности в Республике Казахстан………………………………………………………………………. | 30 |
| 1.6 Обзор проблемы обеспечения информационной безопасности………... | 30 |
| Выводы по разделу 1…………………………………….……………………. | 35 |
| **2 МОДЕЛИ И МЕТОДЫ ИДЕНТИФИКАЦИИ И ОЦЕНКИ ВРЕДОНОСНОГО ТРАФИКА**…………………………………………….. | 36 |
| 2.1 Общая постановка задачи исследования…………………..……………... | 36 |
| 2.2 Модель признакового пространства сетевого трафика…………………. | 37 |
| 2.2.1 Постановка задачи………………………………………………………. | 42 |
| 2.2.2 Количественные характеристики сетевого трафика……………..……. | 43 |
| 2.2.3 Поиск информативных признаков…………………………………....... | 47 |
| 2.3 Метод повышения качественных показателей (полноты и точности) идентификации вредоносного трафика…………………………….………... | 57 |
| 2.3.1 Постановка задачи………………………………………………..……... | 57 |
| 2.3.2 Назначение моделей на сегменты при обработке трафика……….…… | 58 |
| 2.3.3 Сегментирование выборки……………………………………………… | 59 |
| 2.4 Методика идентификации вредоносного трафика………………………. | 64 |
| 2.4.1 Постановка задачи……………………………………………………..... | 64 |
| 2.4.2 Описание методики…………………………………………………..…. | 65 |
| 2.4.3 Описание ансамбля классификаторов…………………………….……. | 68 |
| Выводы по разделу 2………………………………………………………...... | 70 |
| **3 АНАЛИЗ ПРЕДЛОЖЕННЫХ МОДЕЛЕЙ, МЕТОДОВ И АЛГОРИТМОВ К ЗАДАЧЕ ИДЕНТИФИКАЦИИ ВРЕДОНОСНОГО ТРАФИКА**………………………………………………………………..…… | 72 |
| 3.1 Представление данных…………………………………………….……… | 72 |
| 3.2 Анализ модели формирования признакового пространства сетевого трафика………………………………………………………………………… | 74 |
| 3.3 Анализ метода повышения качественных показателей (полноты и точности) идентификации вредоносного трафика……………………….….. | 77 |
| 3.4 Анализ методики идентификации вредоносного трафика…..………….. | 79 |
| 3.5 Анализ применения нейронной сети для классификации сетевого трафика………………………………………………………………………… | 83 |
| Выводы по разделу 3………………………………………………………….. | 90 |
| **4 РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ РЕШЕНИЙ В КОРПОРАТИВНЫХ СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ**……….…….. | 93 |
| 4.1 Адаптирование предлагаемых решений в корпоративных сетях телекоммуникаций……………………………………………….…………… | 93 |
| 4.2 Рекомендации ITU-T. Архитектура безопасности………………..…….. | 96 |
| 4.3 Рекомендации нормативно-правовых актов Республики Казахстан по обеспечению информационной безопасности……………………………..... | 99 |
| Выводы по разделу 4………………………………………………………….. | 101 |
| **ЗАКЛЮЧЕНИЕ**……………………………………………………………… | 102 |
| **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**……………………... | 103 |
| **ПРИЛОЖЕНИЕ А** ‒ Акт оценки результатов на реальных данных………. | 108 |
| **ПРИЛОЖЕНИЕ Б** ‒ Свидетельство на программу для ЭВМ………..……. | 109 |
|  |  |

# **НОРМАТИВНЫЕ ССЫЛКИ**

В настоящей диссертации применяются ссылки на следующие нормативные документы и стандарты:

Закон Республики Казахстан. О науке: принят 18 февраля 2011 года, №407-IV ЗРК.

ГОСО РК 5.04.034-2011. Государственный общеобязательный стандарт образования Республики Казахстан. Послевузовское образование. Докторантура. Основные положения (изменения от 23 августа 2012 г. №1080).

Правила присуждения ученых степеней от 31 марта 2011 года №127.

ГОСТ 7.32-2001. Отчет о научно-исследовательской работе. Структура и правила оформления (изменения от 2006 г.).

ГОСТ 7.1-2003. Библиографическая запись. Библиографическое описание. Общие требования и правила составления.

СТ РК ISO/IEC 15408-3-2017. Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты.

ГОСТ Р 7.0.5–2008. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления.

ГОСТ 7.0.11–2011. Диссертация и автореферат диссертации. Структура и правила оформления.

# **ОПРЕДЕЛЕНИЯ**

В настоящей диссертации применяют следующие термины с соответствующими определениями:

**Бэггинг** – мета-алгоритм ансамбля машинного обучения, предназначенный для повышения стабильности и точности алгоритмов машинного обучения, используемых в статистической классификации и регрессии.

**Вредоносное программное обеспечение** – любая программа или файл, разработанный киберпреступниками (часто называемыми хакерами) для кражи данных и повреждения или уничтожения компьютеров и компьютерных систем.

**Вредоносный трафик** – это угроза в виде ссылки, файла или соединения, которые создаются или принимаются по сети и создают инцидент, который может повлиять на безопасность организации.

**База данных –** организованный набор структурированной информации или данных, обычно хранящихся в электронном виде в компьютерной системе.

**Глобальная сеть –** телекоммуникационная сеть, охватывающая большую географическую территорию.

**Информационная безопасность –** практика защиты информации путем снижения информационных рисков.

**Информационная система** – система, необходимая для обработки, передачи и хранения информации, включая финансовые, человеческие, технические и иные ресурсы для распространения информации.

**Киберпреступность** – преступная деятельность, проводимая через локальные сети или сеть Интернет, посредством вычислительных систем.

**Коммутатор** – сетевое оборудование второго уровня модели OSI, которое предназначено для приема/передачи данных от сетевого устройства источника к сетевому устройству назначения.

**Коммутация пакетов** – это метод группировки данных в пакеты, которые передаются по цифровой сети.

**Компьютерный вирус** – вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, и распространять свои копии по разнообразным каналам связи.

**Корпоративная сеть** **телекоммуникаций** – сложная система взаимосвязанных устройств и каналов связи, которые обеспечивают обмен информацией внутри организации

**Кортеж** – упорядоченный набор фиксированной длины.

**Локальная сеть** – компьютерная сеть, которая соединяет компьютеры на ограниченной территории, например, в жилом доме, школе, лаборатории, университетском кампусе или офисном здании.

**Критерий Кайзера** – правило, состоящее в том, чтобы отбросить все компоненты с собственными значениями ниже 1,0 – это собственное значение, равное информации, содержащейся в среднем отдельном элементе.

**Маршрутизатор –** сетевое устройство, которое пересылает пакеты данных между компьютерными сетями.

**Межсетевой экран –** устройство сетевой безопасности, которое отслеживает и фильтрует входящий и исходящий сетевой трафик на основе ранее установленных политик безопасности организации.

**Мониторинг** – система наблюдения и контроля за критичными бизнес-процессами компании, направленная на своевременное выявление проблем и поиска решений.

**Операционная система** – программа, которая управляет ресурсами компьютера, в частности распределением этих ресурсов среди других программ.

**Программно-определяемые сети –** подход к управлению сетью, который обеспечивает динамическую, программно эффективную конфигурацию сети для повышения производительности и мониторинга сети, что больше похоже на облачные вычисления, чем на традиционное управление сетью.

**Риск безопасности** – мера неблагоприятных последствий, которые могут возникнуть в результате использования уязвимости в системе безопасности.

**Сетевой трафик** – объем данных, перемещающихся по сети в определенный момент времени.

**Сетевые аномалии** – внезапные и кратковременные отклонения от нормальной работы сети.

**Сигнатура атаки** – характеристические особенности компьютерного вируса.

**Угроза безопасности** – потенциальное нарушение безопасности.

**Удалённая сетевая атака** – информационное разрушающее воздействие на распределённую вычислительную систему, осуществляемое программно по каналам связи.

**Уязвимость** – параметр, характеризующий возможность нанесения описываемой системе повреждений любой природы теми или иными внешними средствами или факторами.

**Data mining –** процесс сортировки больших наборов данных для выявления закономерностей и взаимосвязей, которые могут помочь решить бизнес-проблемы посредством анализа данных.

**Data set** – термин, используемый для файловой системы мейнфреймов от IBM; коллекция из логических записей, хранящихся в виде кортежа.

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

|  |  |
| --- | --- |
| ВПО | – вредоносное программное обеспечение |
| ИБ | – информационная безопасность |
| ИИ | – искусственный интеллект |
| ИКТ | – информационно-коммуникационные технологии |
| ИТКС | – информационно-телекоммуникационные системы |
| МГК | – Метод Главных Компонент |
| МО | – машинное обучение |
| ОС | – операционная система |
| ПО | – программное обеспечение |
| РК | – Республика Казахстан |
| РС | – рабочая станция |
| ATM | – Asynchronous Transfer Mode |
| CRC | – Cyclic Redundancy Check |
| DLP | – Data Loss Prevention |
| DNS | – Domain Name System |
| DoS | – Denial-of-Service |
| DPI | – Deep Packet Inspection |
| FIRST | – Forum of Incident Response and Security Teams |
| FTP | – File Transfer Protocol |
| HTTP | – HyperText Transfer Protocol |
| HTTPS | – HyperText Transfer Protocol Secure |
| IoT | – Internet of Things |
| IT | – Information Technologies |
| ITU-T | – International Telecommunication Union - Telecommunication sector |
| MAC | – Media Access Control |
| MLP | – Multilayer Perceptron |
| MTU | – Maximum Transmission Unit |
| P2P | – Peer-to-peer |
| PCA | – Principal Components Analysis |
| PPS | – Packets Per Second |
| QoS | – Quality of Service |
| SOC | – Security Operations Center |
| STP | – Spanning Tree Protocol |
| TI | – Trusted Introducer for Security and Incident Response Teams |
| TCP/IP | – Transmission Control Protocol/Internet Protocol |
| UDP | – User Datagram Protocol |
| VLAN | – Virtual Local Area Network |
| VoIP | – Voice over Internet Protocol |
| VPN | – Virtual Private Network |

**ВВЕДЕНИЕ**

**Проблема и актуальность темы исследования.** Современное общество потребляет информацию, производимую цифровыми средствами связи и вычислительной техники. Значительная часть информации находится в необработанном состоянии, их принято называть данными. Если данные воспринимаются как фиксированные факты, то информация – это некий алгоритмический набор, лежащий в основе этих данных.

Существует разрыв между возможностями обработки данных и их объемом, и этот разрыв постоянно растет. По мере лавинообразного роста объемов данных, доля полезных для человека знаний, которые могут быть получены из этих данных, уменьшается. Зачастую в этих больших объемах данных скрыта полезная информация, которую, к сожалению, редко применяют.

В финансовой сфере, сфере экономики, здравоохранении, торговле и других отраслях специалисты по аналитике вручную анализируют и преобразовывают данные в полезную информацию. Такой подход является трудозатратным, времязатратным и субъективным процессом. Data Mining, археология данных и обработка шаблонов данных, извлечение знаний, интеллектуальный анализ данных – все эти термины относятся к концепции поиска полезной информации в данных. На семинаре в 1989 году была предложена фраза «Knowledge Discovery in Databases» (KDD). KDD - это обобщенный процесс извлечения полезных знаний из данных, тогда как интеллектуальный анализ – это особый этап в процессе, предполагающий использование алгоритмов для поиска полезной информации. В последние годы интеллектуальный анализ приобрел популярность в области информационной безопасности (ИБ).

Как известно, на протяжении многих поколений люди, при поддержке национальных законов, манер и обычаев, защищали свое имущество и частную жизнь используя замки, ограждения, подписи. Современные информационные системы электронны и автоматизированы. Получив контроль над ними, злоумышленники смогут отключать военные системы управления, скомпрометировать каналы связи, «заморозить» банковские счета, удалить данные со спутников, производить манипуляции со светофорами. Поэтому создание технологий обеспечения ИБ для обнаружения сетевых атак и вторжений является одной из критически важных, сложных и наиболее ответственных задач для инженеров в XXI веке [1].

Начиная от мелких компаний и заканчивая крупными корпорациями, выделяются значительные суммы денег для защиты информационных активов от доступа к ним и распространения. Нанимается целый штат сотрудников по информационной безопасности, который круглосуточно мониторит состояние корпоративной сети телекоммуникаций (КСТ), с целью выявления всевозможных сбоев, отказов, коллизий и инцидентов ИБ. Идентификация и оценка подобных состояний имеет решающее значение по нескольким причинам:

‒ это может помочь в своевременном обнаружении угроз безопасности. Раннее обнаружение вредоносного трафика может предоставить возможность предотвратить или смягчить последствия атаки. Это может помочь снизить риски уничтожения данных, финансовых потерь и ущерба репутации;

‒ это может дать представление о характере и масштабах атаки. Понимание характеристик вредоносного трафика, таких как его происхождение, поведение и закономерности, может помочь в разработке эффективных контрмер и превентивных мер;

‒ идентификация и оценка вредоносного трафика могут позволить улучшить общую систему безопасности организации. Выявляя уязвимости в сети, организации могут предпринять шаги по улучшению своей инфраструктуры и процессов безопасности;

‒ это будет способствовать оперативному выявлению неисправностей с сетевым оборудованием и каналами связи, которые непосредственно влияют на эффективность бизнес-процессов в КСТ.

В КСТ сетевой трафик состоит из большого количества информационных сетевых пакетов, меняющихся во времени. Данные сетевых пакетов образуют статистические параметры, анализируя которые можно контролировать состояние КСТ. Эти статистические данные представляются в виде временных рядов, которые в рамках данного исследования предлагается представлять в виде кортежей значений сетевых пакетов (КЗСП). Обработка КЗСП используется для обнаружения опасных и безопасных состояний системы, профилактического обслуживания, выявления подозрительных событий в сегментах сети. В связи с этим, возникает необходимость разработки моделей и методов, основанных на обработке КЗСП, в целях предотвращения нарушения функционирования устройств и своевременного выявления угроз информационной безопасности (ИБ).

Современная тенденция такова, что большие объемы конфиденциальной информации о сотрудниках, заказчиках, продуктах, финансовых результатах хранятся в базах госструктур, корпораций, медицинских учреждений, финансовых институтах. Имеются риски репутационных, финансовых потерь и юридических последствий при попадании информации в руки киберпреступников и бизнес-конкурентов, поэтому рассматриваемому вопросу стоит уделить серьезное внимание. Организациям крайне важно иметь надежные механизмы обнаружения и оценки вредоносного трафика для обеспечения безопасности и целостности своих сетей. Данные факторы определяют **значимость** и **актуальность** решаемых задач в рамках данного исследования.

**Научная проблема** заключаетсяв разработке моделей, методов и алгоритмов интеллектуального анализа данных сетевого трафика в корпоративных сетях телекоммуникаций с целью повышения точности выявления диструктивных информационных воздействий.

**Степень изученности и разработанности темы исследования.** Вопросы выявления аномальных ситуаций в информационных системах были освещены в работах многих исследователей, таких как Лебедев И.С., Увалиева И.М., Семенов В.В., Бельдеубаева Ж.Т., Сухопаров М.Е., Салахутдинова К.И., Dhanabal L., Shantharajah Dr. S.P., Дьяконов А., Reddy A.L.N., Ashibani Y., Kwon D.W., Mahmoud Q.H., Shamir A., Ko K., Kim S., Salehi H., Burgueño R., Vannucci M., Pedersen T. и других.

Многообразие элементов интернета вещей, большое число объектов, протоколов взаимодействия в сетевом трафике, технологий обработки данных, неоднородность форматов, постоянно меняющаяся архитектура, изменения конфигурации и совершенствование атак вызывают проблемы с оперативным обнаружением и реагированием на возникаемые впоследствии инциденты ИБ. В условиях постоянных изменений в КСТ существующие подходы и методы не всегда эффективны.

**Объектом диссертационного исследования** являются КСТ, посредством которых может осуществляться передача данных, оказывающих деструктивное информационное воздействие.

**Предметом диссертационного исследования** являются модели и методы обработки сетевого трафика, позволяющие идентифицировать и вычислять деструктивные информационные воздействия.

**Целью диссертационного исследования** является повышение качественных показателей полноты и точности идентификации вредоносного трафика в корпоративных сетях телекоммуникаций за счет применения технологии Data Mining.

**Задачами диссертационного исследования**,решаемымидля достижения поставленной цели, являются:

* определение типов угроз информационной безопасности, возникающих в КСТ;
* разработка модели признакового пространства сетевого трафика за счет выделения наиболее информативных признаков из КЗСП;
* разработка метода повышения качественных показателей (полноты и точности) идентификации вредоносного трафика за счет применения сегментирования выборки данных;
* разработка методики идентификации и оценки вредоносного трафика на основе предложенной модели и метода.

В ходе проведения работ, планируется опубликовать не менее четырех статей в отечественных и зарубежных журналах с требуемым уровнем по процентилю и квартилю, и участие в не менее двух конференциях по профилю исследуемой темы.

**Методы исследования.** Для решения поставленных задач были использованы: методы аппроксимации данных и сокращения размерности, метод анализа главных компонент для выявления наиболее информативных признаков данных, метод сегментирования выборки для уменьшения вычислительных затрат и улучшения качественных показателей идентификации; методы машинного обучения для обработки данных и оценивания качества предложенных модели и метода; методы описательной статистики для визуализации и интерпретации данных.

**Методология** исследования заключается в постановке задачи выявления и оценки вредоносного трафика, ее формализации, выявления противоречий в науке и практике, формировании моделей, методов их разрешения, основанных на методах выявления наиболее информативных признаков, сегментирования выборки и совокупной методики идентификации и оценки вредоносного для КСТ сетевого трафика.

**Научная новизна** заключается в использовании оригинальных ансамблевых подходов к обработке информационных последовательностей, отличающихся от известных применением предварительного сегментирования выборки данных, обучения моделей обработки на сегментах данных, выявления свойств и назначения моделей с наилучшими показателями на выделенных сегментах, что в комплексе повышает полноту и точность идентификации опасных и безопасных состояний и событий в информационной системе.

**На защиту выносятся следующие положения:**

1. Модель формирования признакового пространства сетевого трафика, представленного в виде кортежа значений информационной последовательности сетевых пакетов, отличающаяся от известных использованием ряда отобранных наиболее информативных характеристик, что позволяет сократить размерность признакового пространства при обработке методами машинного обучения.
2. Метод повышения качественных показателей (полноты и точности) идентификации вредоносного трафика, отличающийся от известных сегментированием выборки, учитывающем воздействующие факторы, что позволяет формировать ансамбли обрабатывающих алгоритмов, имеющих лучшие показатели на отдельных сегментах.
3. Методика идентификации вредоносного трафика, отличающаяся от известных использованием модели формирования признакового пространства и метода сегментирования выборки данных, что дает возможность формировать многоуровневые модели обработки, осуществляющие анализ данных и назначение на сегмент моделей с лучшими показателями, полученными в процессе обучения.

**Теоретическая и практическая значимость работы.** Предлагаемые модель, метод и методика являются основой научно-методического аппарата, направленного на повышение полноты и точности идентификации событий ИБ в сетевом трафике. Практическая реализация является дополнением к существующим системам мониторинга корпоративных сетей телекоммуникации, позволяющим повысить эффективность выявления деструктивных воздействий в КСТ. Использование разработанной методики позволит выявлять из сетевого трафика угрозы ИБ, которые могут привести к негативным последствиям. При этом, методика не требует значительных вычислительных затрат, минимизирует риски инцидентов и повышает оперативность специалистов по ИБ компаний.

**Апробация результатов исследования.** Результаты диссертационной работы были апробированы на научных семинарах кафедры «Информационные системы» НАО «Казахский агротехнический исследовательский университет им. С. Сейфуллина» и на следующих международных научных конференциях:

‒ международная научно-теоретическая конференция «Сейфуллинские чтения - 17: «Современная аграрная наука: цифровая трансформация», посвященная 30-летию Независимости Республики Казахстан» (Астана, 2021);

‒ международная конференция «The 14th International Symposium on Intelligent Distributed Computing» (Италия, 2021);

‒ международная научно-теоретическая конференция «Сейфуллинские чтения – 18 (2) на тему «Наука ХХІ века – эпоха трансформации», посвященная 65-летию КАТУ им. С. Сейфуллина» (Астана, 2022);

‒ международная научная конференция «Математическая логика и компьютерные науки», ЕНУ им. Л.Н. Гумилева (Астана, 2022);

‒ ІХ Международная научно-техническая конференция студентов, магистрантов и молодых ученых «Творчество молодых – инновационному развитию Казахстана» (Усть-Каменогорск, 2023).

**Личный вклад соискателя.** Все научно-экспериментальные результаты и положения, выносимые на защиту, получены автором самостоятельно, под руководством научных консультантов. В частности, экспериментальная оценка модели признакового пространства, метода повышения качественных показателей идентификации вредоносного трафика и методики идентификации вредоносного трафика была выполнена лично автором исследования.

**Соответствие диссертационного исследования паспорту научной специальности.**

Диссертационная работа соответствует образовательной программе «8D06101 – Аналитика больших данных».

**Обоснованность и достоверность результатов** диссертационной работы подтверждается полученными результатами проведенных в рамках данного исследования экспериментов, их сравнительным анализом с результатами аналогичных экспериментов и публикациями в рецензируемых журналах, а также практической апробацией предложенной методики.

**Внедрение результатов работы.**

От АО «КазТрансОйл» был получен акт об оценке результатов диссертационной работы на реальных данных сетевого трафика. Акт подтверждает применение теоретических наработок исследования в практической среде - корпоративной сети телекоммуникаций (Приложение А).

**Публикации по теме диссертационного исследования.** В рамках исследования были опубликованы 13 научных работ (Приложение Б), из них 3 статьи, входящие в базу данных Scopus (ж**урнал «Научно-технический вестник информационных технологий, механики и оптики» -** Cite Score 7; книжная серия «Studies in Computational Intelligence» (Springer) - Cite Score 26; журнал «Indonesian Journal of Electrical Engineering and Computer Science» - Cite Score 47), 3 статьи в изданиях, рекомендованных уполномоченным органом МНВО РК (журнал «Известия Национальной академии наук Республики Казахстан. Серия физико-математическая», журнал ««Вестник ВКТУ им. Д. Серикбаева», журнал «Вестник КазАТК»), 5 – в трудах международных конференций, 2 статьи в других изданиях. Получено 1 свидетельство о государственной регистрации программы для ЭВМ (Приложение В).

**Структура и объем диссертационного исследования.** Текст диссертационной работы состоит из следующих структурных элементов: титульный лист; содержание; нормативные ссылки; определения; введение; основная часть, включающая четыре главы; заключение; список использованных источников, содержащий 70 наименований; три приложения, содержащие копии акта оценки результатов на реальных данных, свидетельства о государственной регистрации программы для ЭВМ, и списка публикаций. Общий объем диссертации – 109 страниц. В работе представлено 50 рисунков и 14 таблиц.

**Во введении** выносится научная проблема, на решение которой направлено диссертационное исследование, определяются значимость и актуальность, степень изученности и разработанности темы исследования. Сформулированы объект и предмет, цель и задачи, методы и методология, научная новизна исследования и положения выносимые на защиту. Представлена теоретическая и практическая значимость работы и апробация результатов исследования. Приводятся данные по соответствию диссертационного исследования паспорту научной специальности. Показана обоснованность и достоверность результатов. Представлена информация по внедрению результатов диссертационной работы и по научным публикациям.

**Первый раздел** исследования охватывает описание корпоративных сетей телекоммуникаций. Приводятся ее качественные характеристики, типы сетевых подключений, описание компонентов КСТ – сетевого оборудования, которые являются потенциальными целями злоумышленников и которые наиболее подвержены угрозам ИБ. Далее, представлено описание распространенных типов угроз ИБ в КСТ и их сфера влияния. Дано перечисление активов компаний, приводится определение уязвимости и риска безопасности.

Cделан обзор международных и отечественных научных исследований. Нынешняя тенденция научных работ по обнаружению аномальных данных в сетевом трафике показала растущий интерес научного сообщества к статистическим методам, методам машинного обучения, нейронных сетей, и методам глубокого обучения. В разделе проведен обзор некоторых используемых в компаниях систем обеспечения безопасности. Приведена статистика по национальному индексу кибербезопасности, разделенная на подкатегории, и по количествам инцидентов ИБ за 2019-2023 годы. Линия тренда на графике инцидентов показала увеличение количества кибератак в 2023 году на 56,2%, что является негативной тенденцией и, возможно, показателем возросшей заинтересованности в атаках (совершенствования методов атак, неэффективности используемых систем обеспечения ИБ в компаниях и др.), и низкого уровня цифровой грамотности населения, статистика по которой была также представлена для ознакомления.

**Второй раздел** охватывал предлагаемые в рамках исследования следующие решения.

*Модель признакового пространства сетевого трафика.*

Приводится подробное описание сетевого трафика, ее состав, типы и параметры. Так как сетевой трафик состоит из множества сетевых пакетов, дано наглядное представление сетевого пакета, его характеристики и описание полей.

В работе предложено анализировать не отдельные пакеты, а сеансы связи, в виде информационных последовательностей сетевых пакетов - ИПСП, и затем моделировать их в виде кортежей значений признаков данных сеансов связи – КЗСП.

Сформулировано формальное определение задачи разработки модели признакового пространства. Показаны количественные характеристики сетевого трафика и основные формулы для выполнения количественных оценок трафика. Представлено формализованное описание метода главных компонент, применимо к первой задаче исследования. Разработан алгоритм его работы.

*Метод повышения качественных показателей идентификации вредоносного трафика.*

Представлено формализованное описание постановки задачи. Предполагалось, что на анализируемые данные оказывают воздействие факторы. Для интерпретации таких факторов необходимо анализировать выборку сетевого трафика автоматическими методами. Такими методами могут выступать методы поиска точек разладки и перегиба сигнала (если удастся представить всю анализируемую выборку в виде сигнала) и метод обнаружения дрейфа концепта.

Приводится формализованное описание метода сегментирования выборки с учетом воздействующих на него факторов. Разработан алгоритм сегментирования данных с учетом факторов и схема постоянно обучающейся двухуровневой модели, которая позволит при изменении свойств данных уменьшить временные затраты на обучение.

*Методика идентификации вредоносного трафика.*

В методике идентификации вредоносного трафика предлагается разработать классифицирующий алгоритм, который, с учетом влияния фактора, сопоставляет конкретный объект своему классу опасности, по анализу признакового описания. По предлагаемой методике, представлено формализованное описание; разработана блок-схема, которая, учитывая воздействие факторов, сегментирует исходную выборку, затем производит посегментную классификацию алгоритмами классификации машинного обучения и проводит сравнительный анализ полученных результатов с результатами классификации всей выборки, без разделения на сегменты.

Также, приводится формализованное описание разработанного ансамбля классификаторов, которое может быть использовано отдельно, для всей выборки, как альтернативный вариант, либо как классификатор после сегментирования данных.

**В третьем разделе** приводится экспериментальная оценка предлагаемых во втором разделе аналитических решений. Так как значительная часть экспериментов была проведена на публичном наборе данных NSL-KDD, приведено подробное описание данного набора и его атрибутов.

Представлено описание эксперимента по применению метода МГК для проверки ее эффективности при достижении цели исследования – повышения показателей точности идентификации - цель была достигнута. Удалось улучшить точность классификации двух методов МО - DecisionStump и NaiveBayes на 4 и 11% соответственно, путем преобразования признаков выборки в главные компоненты и последовательным исключением компонент с меньшим влиянием.

Приводится анализ применения сегментирования для повышения точности идентификации. Проведенным экспериментом удалось показать, что сегментированием возможно улучшить показатели качества классификаторов ориентировочно на 5%, нежели классифицировать всю выборку целиком. Метод обладает преимуществами борьбы с нежелательными шумами и выбросами, и позволяет создавать в пространстве объектов локализованные компактные подмножества.

Произведен анализ применения бэггинга для задач идентификации и оценки вредоносного трафика, на основе алгоритмов классификации REP Tree, Random Tree, Random Forest, Hoeffding Tree, Naïve Bayes, показал 99% точность идентификации вредоносного трафика на наборе данных NSL-KDD. Преимуществом данного метода явилось то, что классификаторы можно настроить для разных видов аномалий и событий, а возникаемый разброс ответов можно сглаживать разработанным ансамблем. Еще одним преимуществом данного решения является то, что каждый алгоритм классификации может адаптироваться к разным условиям функционирования КСТ.

Представлен эксперимент с применением многослойной нейронной сети на реальном сетевом трафике, выборка которой содержала около 17 тысяч записей сеансов связи с 31 атрибутами. Данные были предварительно размечены инструментом nDPI, чтобы обучить ею нейронную сеть. По результатам эксперимента удалось получить точность классификации сетевого трафика – 95%. Наилучшие результаты показали нейронные сети с параметрами 128-128-128 и 128/256/128 с функцией активации tanh и 128/32/128 с функцией активации relu. Остаток сетевого трафика, который не удалось в точности соотнести к определенному приложению можно считать аномальным и потенциально вредоносным, требующим дальнейшего исследования.

**В четвертом разделе** предлагаются рекомендации к применению предложенных решений в КСТ, по проведенному исследованию. Разработана схема применения решений в КСТ с детализированным описанием шагов. Представлена схема реагирования на инциденты, при использовании предложенных рекомендаций в КСТ. Также представлены рекомендации по созданию архитектуры безопасности, взятые из стандартов ITU-T. Приводятся «вырезки» из нормативно-правовых актов РК по обеспечению ИБ.

# **1 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ ТЕЛЕКОММУНИКАЦИЙ**

* 1. **Описание исследуемых объектов**

Для обеспечения производственной деятельности организаций, управления их технологическими процессами, разворачиваются корпоративные сети телекоммуникаций.

Корпоративная сеть телекоммуникаций (КСТ) – это сложная система взаимосвязанных устройств и каналов связи, которые обеспечивают обмен информацией внутри организации. КСТ являются важным компонентом современных бизнес-операций, позволяя компаниям общаться, сотрудничать и обмениваться информацией со своими сотрудниками, клиентами и партнерами.

КСТ может состоять из двух частей: локальной сети (LAN) и глобальной сети (WAN), рисунок 1.

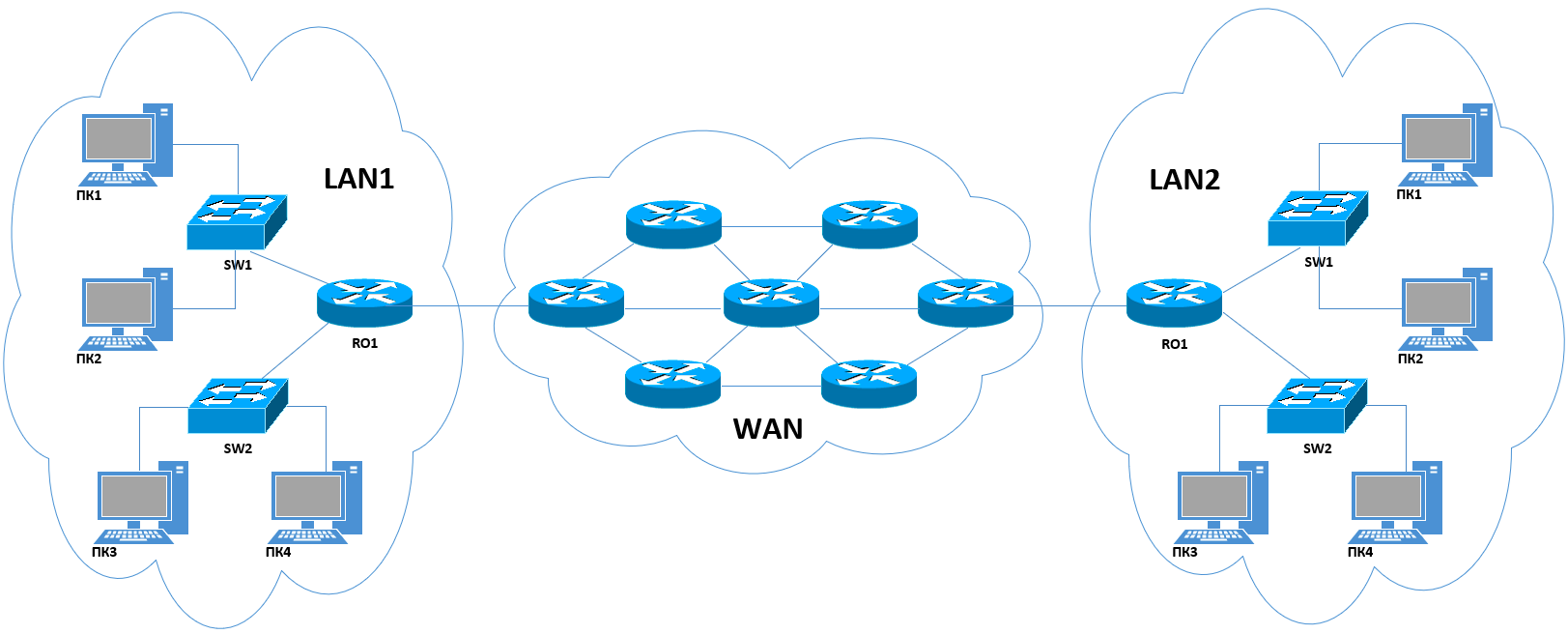


Рисунок 1 – Схема КСТ

LAN – это внутренняя сеть внутри корпоративного офиса или здания. Она соединяет различные устройства, такие как компьютеры, принтеры и серверы, друг с другом. Локальная сеть обычно подключается к глобальной сети через маршрутизатор или коммутатор, что позволяет устройствам в локальной сети взаимодействовать с другими устройствами за пределами здания.

WAN – это внешняя сеть, которая соединяет вместе несколько локальных сетей, филиалов/подразделений организации. Обычно она используется для подключения географически разнесенных офисов. Подключения к глобальной сети могут осуществляться с помощью различных технологий, таких как выделенные линии, виртуальные частные сети или MPLS. Глобальные сети обычно более сложны, чем локальные сети, и для них требуются специализированные устройства, такие как маршрутизаторы, брандмауэры и балансировщики нагрузки.

Характеристики КСТ [2] представлены в таблице 1.

Таблица 1 – Характеристики КСТ

|  |  |
| --- | --- |
| Характеристика | Описание |
| Масштабируемость | КСТ спроектированы таким образом, чтобы быть масштабируемыми, то есть способны обслуживать растущее число пользователей, устройств и приложений без ущерба для производительности или надежности. Это достигается за счет использования таких технологий, как виртуализация, облачные вычисления и программно-определяемые сети (SDN) |
| Надежность | Ожидается, что КСТ будут высоконадежными, с минимальными простоями или перерывами в обслуживании. Это достигается за счет использования избыточного оборудования, резервных источников питания и механизмов отработки отказа, которые обеспечивают бесперебойное обслуживание |
| Безопасность | КСТ должны быть высокозащищенными, в безопасности должны быть конфиденциальные корпоративные данные, предотвращая несанкционированный доступ, утечку данных или кибератаки. Это достигается за счет использования брандмауэров, систем обнаружения и предотвращения вторжений, а также технологий шифрования |
| Гибкость | КСТ должны быть гибкими, вмещающими целый ряд различных устройств, приложений и протоколов связи. Это достигается за счет использования стандартизированных протоколов, таких как TCP/IP, и возможности поддержки различных коммуникационных технологий, включая проводные и беспроводные сети, VPN и решения для удаленного доступа |
| Мониторинг и управление | КСТ требуют постоянного мониторинга и управления для обеспечения оптимальной производительности, обнаружения и предотвращения угроз безопасности, а также устранения неполадок по мере их возникновения. Это достигается за счет использования инструментов управления сетью и программного обеспечения, которые обеспечивают отображение производительности и безопасности сети в режиме реального времени |

КСТ могут иметь различные типы подключений в зависимости от требований и нужд организации. Типы соединений в КСТ можно разделить на три основных типа: соединения точка-точка, многоточечные соединения и коммутируемые соединения.

Соединения «точка-точка» - это выделенные соединения, которые связывают два устройства или местоположения вместе, рисунок 2. Эти соединения используются для передачи данных между двумя определенными точками и обычно используются для высокоскоростных приложений, требующих низкой задержки и высокой надежности. Примерами соединений «точка-точка» являются арендованные линии, линии T1 и линии T3.



Рисунок 2 – Соединение “точка-точка”

Многоточечные соединения позволяют нескольким устройствам взаимодействовать друг с другом по одному соединению, рисунок 3. Эти подключения обычно используются для приложений, требующих совместного использования данных между несколькими устройствами, таких как видеоконференции или общий доступ к файлам. Примерами многоточечных подключений являются виртуальные частные сети (VPN), сети ретрансляции кадров и сети в режиме асинхронной передачи (ATM).

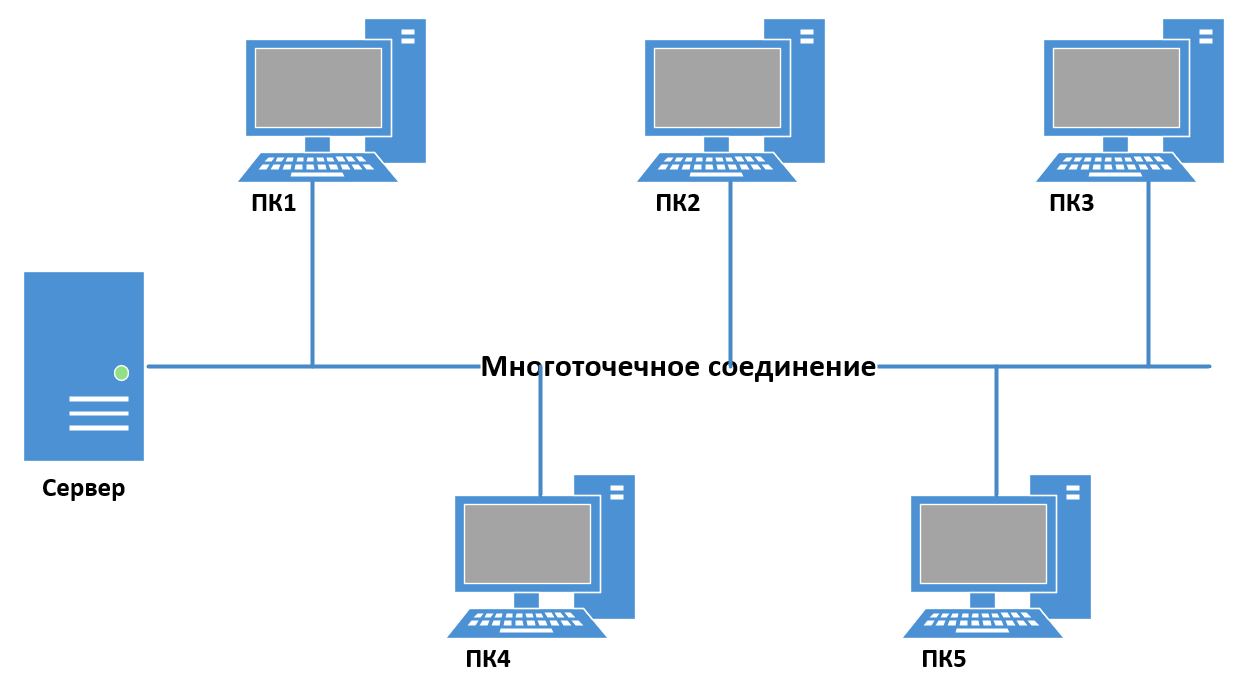


Рисунок 3 – Многоточечное соединение

Коммутируемые соединения используют коммутационное устройство для соединения нескольких устройств вместе по мере необходимости. Эти подключения используются, когда количество устройств, которым необходимо взаимодействовать друг с другом, неизвестно или когда количество устройств, которым необходимо взаимодействовать друг с другом, часто меняется. Пример коммутируемого соединения представлен на рисунке 4.

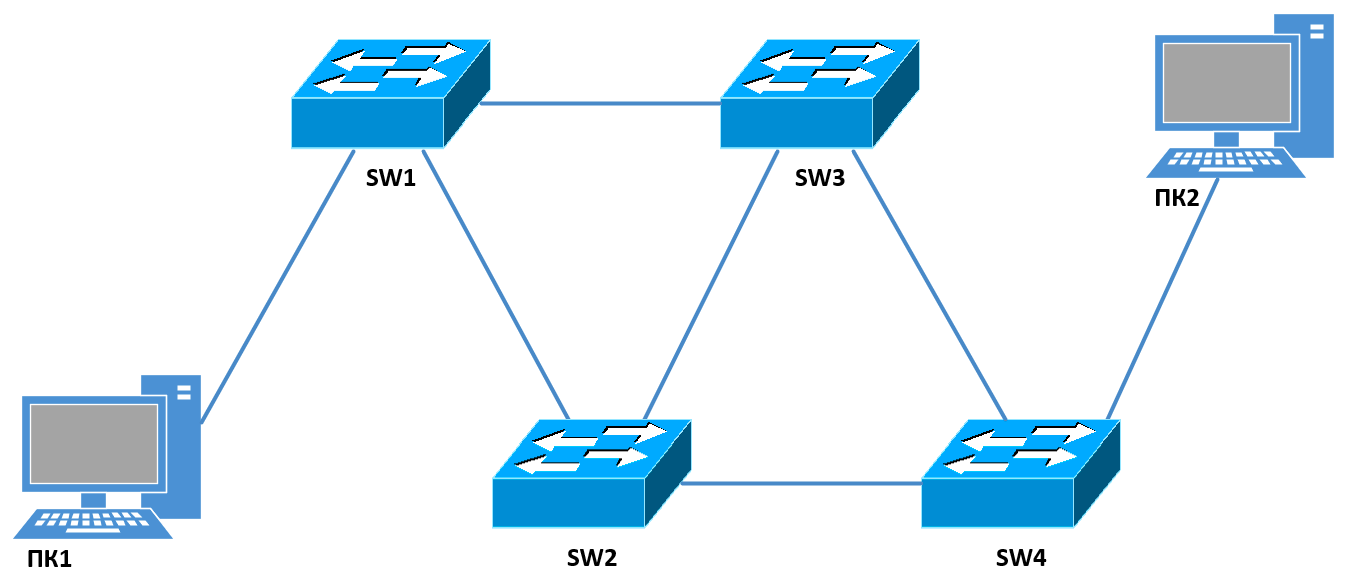


Рисунок 4 – Коммутируемое соединение

Типовую схему КСТ в пределах локальной сети одного офиса можно представить следующим образом, рисунок 5.

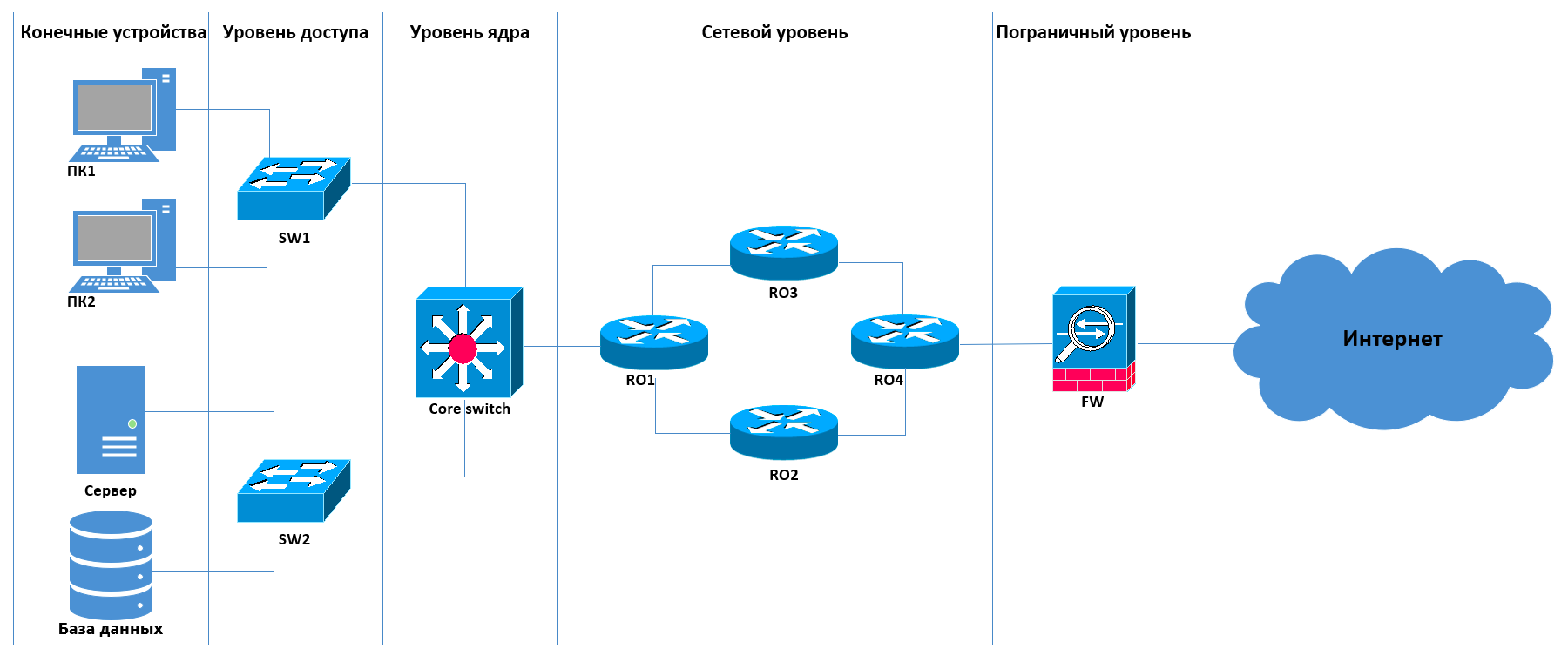


Рисунок 5 – Типовая схема КСТ в пределах локальной сети одного офиса

Согласно схеме, к конечным устройствам относятся персональные устройства пользователей, серверное оборудование и базы данных. К уровню доступа относятся Layer 2 (L2) коммутаторы, обеспечивающие передачу данных конечным устройствам. Устройства осуществляют передачу информационных пакетов исходя из таблиц коммутации – таблиц сопоставления интерфейсов коммутатора к MAC-адресам устройств. К уровню ядра относятся высокопроизводительные Layer 3 (L3) коммутаторы с поддержкой маршрутизации, которые осуществляют оперативную передачу данных между всеми коммутаторами уровня доступа, и, при необходимости, направляют трафик на вышестоящие уровни. К сетевому уровню относятся маршрутизаторы, которые предоставляют выход корпоративных сервисов «наружу» - к сетям IP VPN от провайдеров, к сетям других подразделений компании. Маршрутизаторы перенаправляют данные между различными сетями, исходя из таблиц маршрутизации, сопоставляющих адреса назначения с интерфейсами, через которые необходимо отправить данные до следующего маршрутизатора. К пограничному уровню относятся устройства, которые расположены на границе между внутренней сетью - КСТ и внешней – сетью Интернет. Преимущественно в пограничном уровне устанавливают межсетевые экраны (брандмауэры, фаерволы) и балансировщики нагрузки.

Компоненты КСТ представлены в таблице 2.

Соединения между устройствами разных уровней обеспечивают передачу данных. Устройства каждого из уровней могут принимать, изменять и передавать информацию.

Таблица 2 – Компоненты КСТ

|  |  |
| --- | --- |
| Компонент | Описание |
| Серверы | Компьютерные системы, которые предоставляют услуги клиентским компьютерам в сети. Они могут использоваться для различных целей, таких как хранение файлов и общий доступ к ним, запуск приложений и управление сетевыми ресурсами. Серверами могут быть физические или виртуальные машины, которые выполняются на главном компьютере. Обычно они подключаются к сети с помощью кабелей Ethernet или беспроводных соединений |
| Коммутаторы | Сетевые устройства, которые соединяют различные устройства в сети. Они пересылают пакеты данных между устройствами на основе их MAC-адресов. Коммутаторы могут быть управляемыми или неуправляемыми, в зависимости от их конфигурации и возможностей. Управляемые коммутаторы предлагают более продвинутые функции, такие как качество обслуживания (QoS) и виртуальные локальные сети (VLAN), которые позволяют лучше контролировать сетью |
| Маршрути заторы | Сетевые устройства, которые соединяют вместе различные сети. Они используют таблицы маршрутизации для определения наилучшего пути передачи пакетов данных из одной сети в другую. Маршрутизаторы могут использоваться для подключения корпоративной сети к сети Интернет или для соединения различных филиалов компании вместе. Они также могут предоставлять функции безопасности, такие как защита брандмауэром и подключение к виртуальной частной сети (VPN) |
| Брандмауэры (межсетевые экраны) | Устройства безопасности, которые отслеживают и контролируют входящий и исходящий сетевой трафик. Имеются брандмауэры программного и аппаратного исполнения. Они обеспечивают контроль доступа к ресурсам сети, предоставляют VPN доступ удаленным сотрудникам, могут выступать в роли каналообразующего оборудования (IPsec) |
| Балансировщики нагрузки | Устройства распределения сетевого трафика между серверами. Они могут быть использованы для повышения производительности и доступности веб-приложений и других сетевых служб. Балансировщики нагрузки могут быть аппаратными или программными и могут быть сконфигурированы для работы с различными протоколами и приложениями |

Таким образом, устройства каждого из уровней КСТ являются потенциальной целью злоумышленников. При получении доступа на одно из устройств, возможно получить доступ и на другие. Понятно, что наибольшему риску подвержено пограничное устройство. Оно должно обеспечивать защиту от внешних угроз, обладать функциями фильтрации, маршрутизации, шифрования данных, маскирования внутренних адресов и другими полезными компонентами. Но вполне вероятно, что угрозы могут исходить и внутри КСТ, это и вредоносные программы, невольно переносимые пользователями на личных съемных носителях, отсутствие последних обновлений программного обеспечения (ПО), ошибки конфигурации, в том числе и преднамеренные случаи угроз. Более подробно описание угроз ИБ представлено в следующем разделе.

## **1.2 Угрозы информационной безопасности**

Стоит понимать, что угрозы информационной безопасности существуют всегда, и они не имеют границ. Проблемой является содержание критичных сегментов инфраструктуры и активов организаций в максимально безопасном состоянии, защищенном от несанкционированного доступа, взлома и компрометации; постоянного мониторинга и устранения уязвимостей в системах хранения, обработки и передачи информации.

Под угрозами безопасности понимаются потенциальные нарушения целостности, конфиденциальности и доступности информации. Примерами угроз могут быть:

‒ потасовка данных и/или маскирование себя за другое лицо;

‒ отказ в обслуживании сервисов иоборудования;

‒ уничтожение информации с баз накопления и обработки данных, кража информации;

‒ несанкционированное изменение или стирание информации, файлов настроек сетевого оборудования, сервисов и приложений;

‒ несанкционированное распространение информации.

Классификация угроз может быть представлена как:

‒ активные/пассивные;

‒ преднамеренные (явные)/непреднамеренные (случайные).

К активным угрозам относятся нарушения доступности и работоспособности системы. Пассивная угроза применяется для целей разведки, без нарушения состояния системы. Прослушивание телефонных разговоров является примером пассивных угроз.

Целенаправленно реализованная злоумышленником угроза называется преднамеренной угрозой или атакой. Такие угрозы имеют следующие вариации, от применения известных бесплатных инструментов для просмотра содержимого информации либо конфигурации сетевого оборудования до использования новых неизвестных инструментов для проведения изощренных атак. Сбой сетевого оборудования и ПО имеет непреднамеренный характер, поэтому относится с случайным угрозам.

На рисунке 6 представлены распространенные виды угроз ИБ в КСТ.

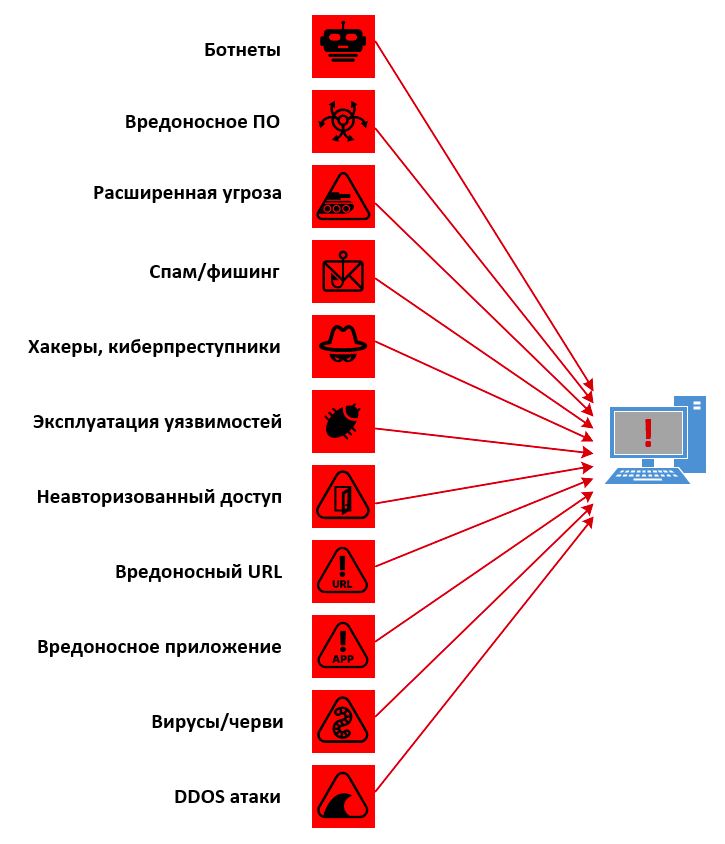


Рисунок 6 – Распространенные виды угроз ИБ в КСТ

Описание угроз ИБ в КСТ представлено в таблице 3.

Таблица 3 – Описание угроз ИБ в КСТ

|  |  |
| --- | --- |
| Угроза | Описание |
| 1 | 2 |
| Вредоносное ПО | Тип программного обеспечения, предназначенного для нарушения работы, повреждения или получения несанкционированного доступа к компьютерной системе. Вредоносное ПО может распространяться через вложения электронной почты, зараженные веб-сайты или загрузки программного обеспечения. После установки на компьютер или в сеть вредоносное ПО может украсть конфиденциальную информацию, зашифровать данные с целью получения выкупа или использовать зараженный компьютер в качестве ботнета для запуска дальнейших атак. Для защиты от вредоносных программ компаниям следует внедрить антивирусное программное обеспечение, брандмауэры и сегментацию сети |
| Продолжение таблицы 3 | |
| 1 | 2 |
| Фишинг | Разновидность атаки социальной инженерии, которая использует мошеннические электронные письма, текстовые сообщения или телефонные звонки, чтобы обманом заставить пользователей раскрыть конфиденциальную информацию, такую как учетные данные для входа в систему или финансовые данные. Фишинговые атаки часто используют поддельные веб-сайты, имитирующие законные, для кражи пользовательской информации. Чтобы предотвратить фишинговые атаки, компаниям следует регулярно проводить обучение своих сотрудников по вопросам безопасности и внедрять двухфакторную аутентификацию |
| Атаки типа "отказ в обслуживании" (DoS) | DoS-атаки нарушают нормальное функционирование компьютера или сети путем переполнения их трафиком или запросами. Эти атаки могут быть запущены путем отправки большого количества запросов на сервер, перегружая его возможности обработки, или путем использования уязвимостей в сетевых протоколах. Для защиты от DoS-атак компаниям следует внедрять системы обнаружения и предотвращения вторжений, ограничивать доступ к критически важным ресурсам и использовать методы балансировки нагрузки |
| Угрозы со стороны инсайдеров | Данные виды угроз исходят от сотрудников или других инсайдеров, которые имеют доступ к конфиденциальной информации и могут злоупотреблять ею или украсть ее. Эти угрозы могут быть преднамеренными, например, когда сотрудник крадет конфиденциальную информацию, чтобы продать ее конкуренту, или непреднамеренными, например, когда сотрудник случайно делится конфиденциальной информацией с неуполномоченными лицами. Чтобы снизить уровень инсайдерских угроз, компаниям следует внедрить средства контроля доступа, отслеживать активность пользователей и применять политики обработки и удаления данных |
| Расширенные постоянные угрозы (РПУ) | Это целенаправленные атаки, которые остаются незамеченными в течение длительного времени и предназначены для получения стабильного доступа к сети. РПУ часто используют сложные методы, такие как фишинг-рассылка, эксплойты нулевого дня и каналы управления, чтобы избежать обнаружения. Для защиты от РПУ компаниям следует внедрять передовые меры безопасности, такие как анализ угроз, сегментация сети и системы предотвращения вторжений |

Это лишь несколько примеров многочисленных угроз, с которыми сталкиваются КСТ. Компании должны сохранять бдительность и внедрять комплексную стратегию безопасности для защиты своих активов.

К активам компании, подлежащим защите, относятся:

‒ коммуникационные услуги и услуги вычислительной техники;

‒ пользовательская и служебная информация, файлы конфигураций и иные данные компании;

‒ сотрудники;

‒ оборудование и помещения [3].

Реализацию потенциальных возможностей бизнеса и получение максимальной выгоды от инвестиций невозможно осуществить без обеспечения информационной безопасности. Информация из представленного списка является основным активом, который, в отличие от других активов организации, имеет самое высокое значение. В результате этой возрастающей взаимосвязанности, информация на сегодняшний день подвергается растущему числу и широкому кругу опасностей и уязвимостей [4].

Уязвимость безопасности – это недостаток или слабое место, которые могут быть использованы для нарушения системы или информации, которую она содержит. Если уязвимость существует, то угроза может быть успешно реализована, если не будут приняты эффективные меры противодействия.

К рискам безопасности относятся меры неблагоприятных последствий, которые могут возникнуть в результате использования уязвимости и реализованной угрозы. Хотя считается, что риски не могут быть полностью устранены, важной целью принимаемых мер обеспечения безопасности является снижение риска до минимально опасного уровня.

## **1.3 Обзор научных исследований**

Идентификация вредоносных данных относится к задачам выявления аномалий. Международный и отечественный опыт показывает существенный интерес научного сообщества к исследованию проблемы обнаружения аномальных, потенциально вредоносных для организаций данных в сетевом трафике с использованием статистических методов, методов глубокого обучения и машинного обучения [5, 6].

Методы классификации машинного обучения [7-9] часто применяются для обнаружения аномалий в сетевом трафике. Эти методы включают обучение модели на большом наборе данных и использование модели для выявления необычных паттернов или моделей поведения в новых данных. Основной проблемой использования этих методов является чувствительность алгоритмов машинного обучения к свойствам обучающих данных, поэтому необходимым условием проведения качественной оценки является предварительная обработка «сырых» данных.

На рисунке 7 представлен процесс анализа данных методами машинного обучения.

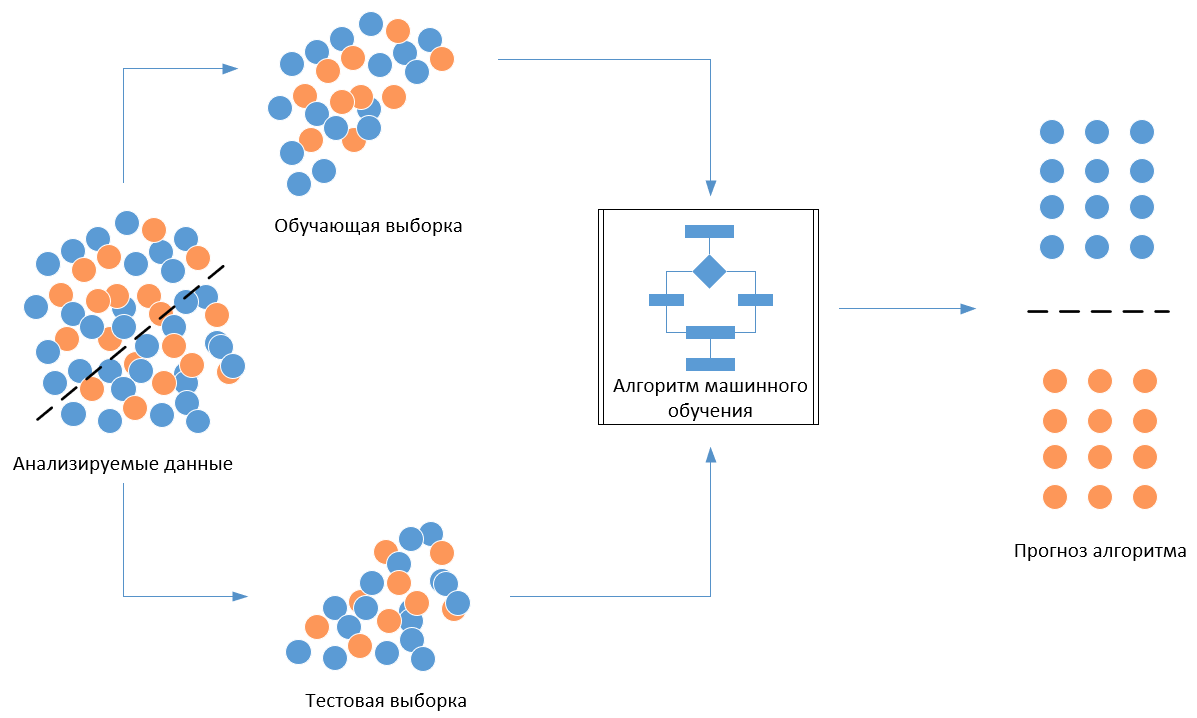


Рисунок 7 – Процесс анализа данных методами машинного обучения

Имеются исследования по применению методов кластеризации машинного обучения для определения текущего состояния ИБ устройств интернета вещей [10]. Данный метод предполагает группировку анализируемого множества по соответствующим кластерам, согласно заданным критериям. Одним из недостатков данных методов является выбор подходящего критерия, от которого напрямую зависит дальнейшая обработка данных.

Методы кластеризации принято делить на два типа (рисунок 8), иерархические (рисунок 9) и неирархические (рисунок 10).



Рисунок 8 – Типы кластеризации

Пример иерархической кластеризации представлен в виде дендрограммы, рисунок 9.

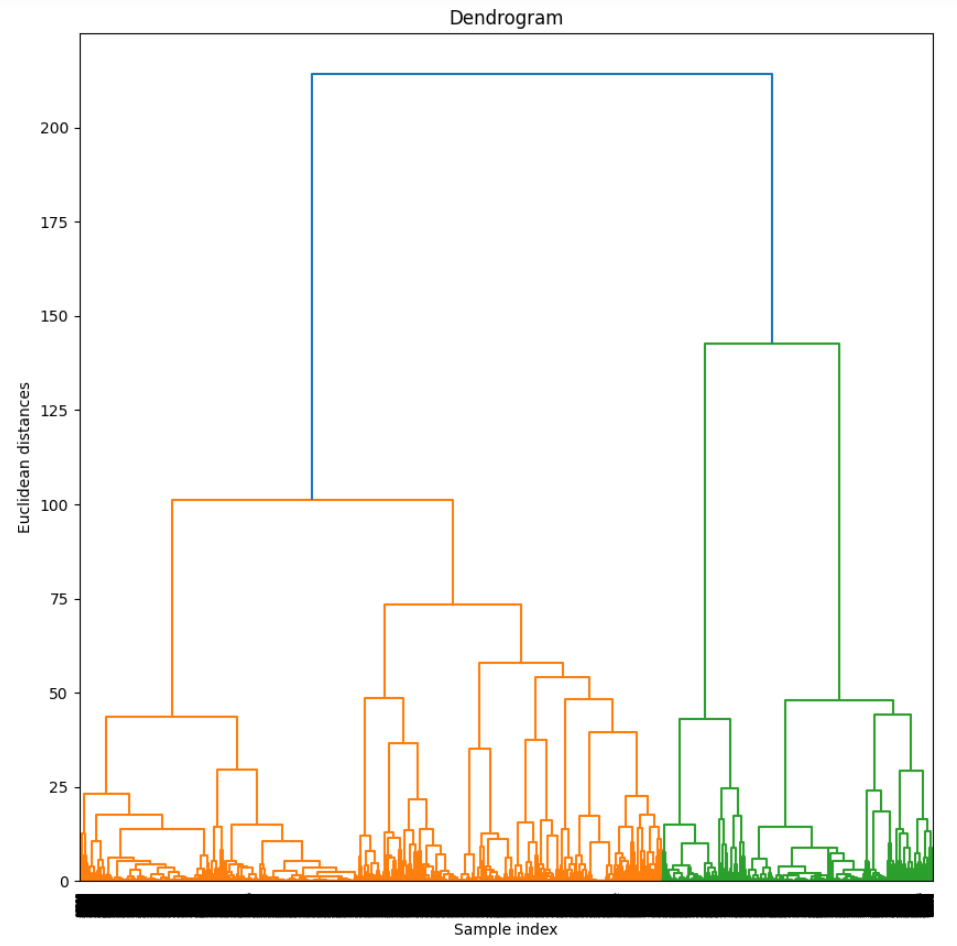


Рисунок 9 – Пример иерархической кластеризации

Пример неиерархической кластеризации представлен на рисунке 10.

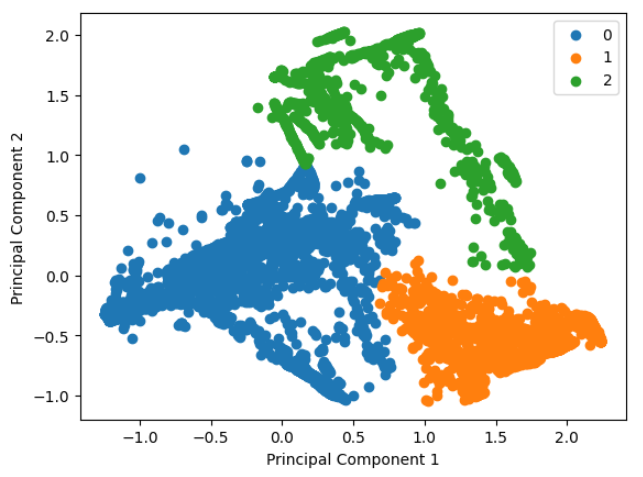


Рисунок 10 – Пример неиерархической кластеризации

Также, использование нейронных сетей [11-13] является примером методов для обнаружения вредоносного трафика. Они могут изучить сложные взаимосвязи и закономерности в данных. Схема нейронной сети представлена на рисунке 11.

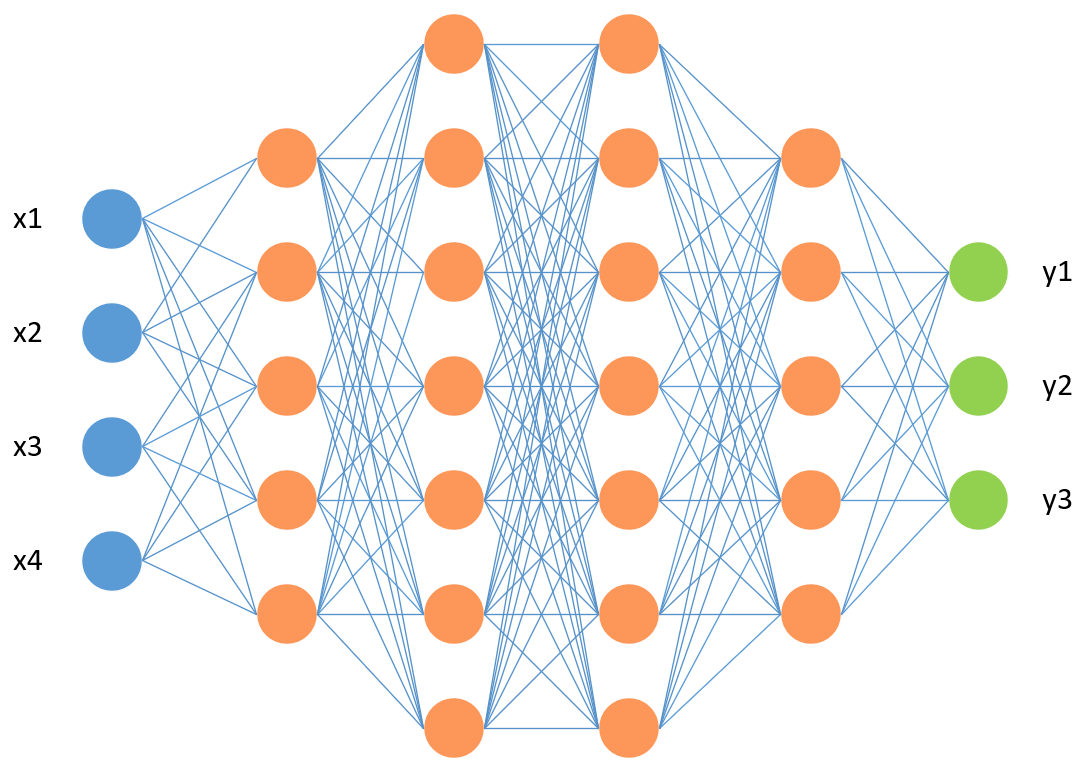


Рисунок 11 – Схема нейронной сети

Хотя скорость работы нейронных сетей и самообучаемость находятся на высоком уровне, имеются и недостатки, связанные с разработкой самой модели. Требуется довольно много времени для настройки его параметров. Также, по результатам оценки нейронной сети невозможно определить, каким образом он пришел к тому или иному решению, - нет строгого обоснования результатов.

Методы, основанные на правилах [14, 15], также могут использоваться для обнаружения аномалий в сетевом трафике. Эти методы включают в себя определение набора правил или пороговых значений, которые запускают оповещение при выполнении определенных условий. Например, может быть определено правило для запуска предупреждения, если количество неудачных попыток входа в систему превышает определенный порог в течение указанного периода времени. Примером основанного на правилах метода обнаружения аномалий является использование Snort в работе [16], как системы обнаружения вторжений с открытым исходным кодом, которая использует набор предопределенных правил для обнаружения различных типов сетевых угроз.

Одним из распространенных подходов к обнаружению аномалий в сетевом трафике являются статистические методы, применение которых описано в работах [17, 18]. Они включают в себя анализ статистических свойств данных о сетевом трафике для обнаружения необычных паттернов или моделей поведения. Примерами статистического метода обнаружения аномалий является использование скользящих средних [19, 20] и экспоненциального сглаживания [21], для выявления нехарактерных для легитимного трафика тенденций, рисунок 12.

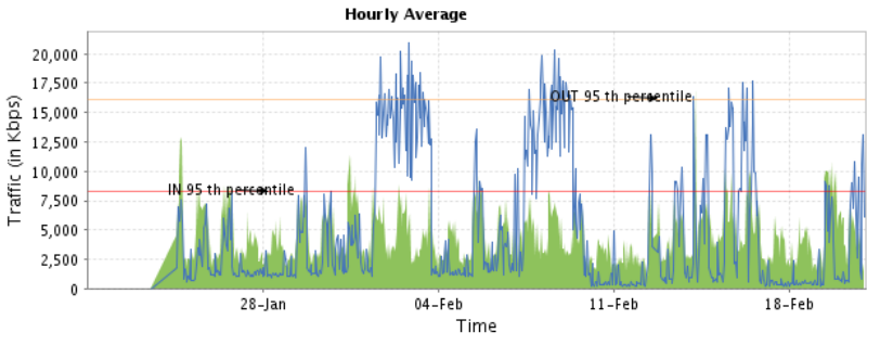


Рисунок 12 – Пример выявления выявления нехарактерных для легитимного трафика тенденций

При обнаружении аномалий в сетевом трафике ученые сталкивается с рядом проблем, включая высокую размерность [22] и сложность сетевых данных, динамический характер сетевого трафика [23] и наличие зашумленных и неполных данных. Поэтому, ученые рекомендуют тщательно сбалансировать соотношение между ложноположительными и ложноотрицательными результатами, чтобы не пропустить реальные аномалии и свести к минимуму ложные срабатывания.

По типам исследуемых данных, наиболее распространены исследования по выявлению DDoS-атак [24, 25] и активность ботнета [26, 27].

В заключение отметим, что каждое проведенное исследование может внести весомый вклад при реализации систем обнаружения аномалий, которые являются важным инструментом для сетевых администраторов и специалистов по безопасности. Они помогают обнаруживать необычное поведение и события в сетевом трафике, выявляют угрозы безопасности и проблемы с производительностью сети. С появлением машинного обучения и методов глубокого обучения точность и эффективность систем обнаружения аномалий продолжают повышаться.

* 1. **Обзор систем по обеспечению информационной безопасности**

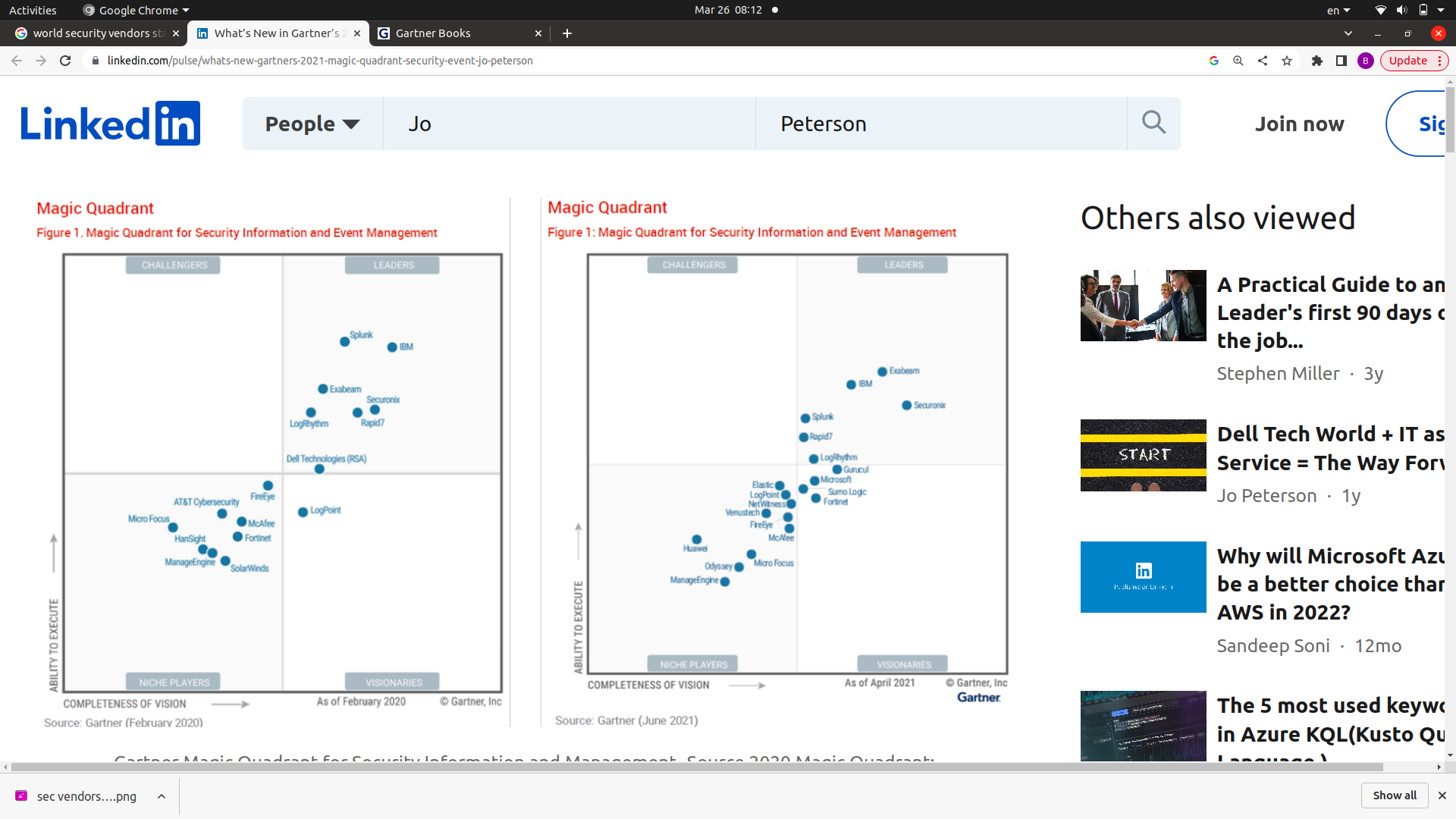
На сегодняшний день глобальный рынок машинного обучения достиг объема $7,3 млрд. По прогнозам аналитиков, к 2024 году эта цифра увеличится до $30,6 млрд. Совокупный годовой темп прироста составит 43%. По данным MMC Ventures, сегодня каждая десятая крупная компания уже использует искусственный интеллект, чат-боты и машинное обучение. Крупнейшими игроками на рынке являются Amazon, Google, Baidu, SAS Institute, Microsoft и Hewlett-Packard [28]. К примеру, Google использует преимущества алгоритмов машинного обучения и предоставляет клиентам ценный и индивидуальный опыт. Машинное обучение уже встроено в его сервисы, такие как Gmail, Google Assistant, Google Translate, Google Search и Google Maps [29].

Существуют множество продуктов по обеспечению ИБ, на основе методов интеллектуального анализа данных. Ниже приводится несколько наиболее популярных решений.

Решение компании IBM - IBM Security Intelligence with Big Data нацелено на анализ информационных потоков компании - всего сетевого трафика, в частности, данных корпоративной почты, систем документооборота, социальных сетей. Разработчики утверждают, что анализ подобного рода данных позволяет в кратчайшие сроки выявлять недовольных сотрудников, которые могут способствовать утечкам информации компании. Кроме анализа используемых сервисов и приложений, IBM Security Intelligence анализирует служебные сообщения сетевого оборудования для идентифицирования аномалий в сети. Основана данная система на БД Hadoop, с графическим интерфейсом для визуализации [30].

Компания Splunk, разработчик программного обеспечения для анализа данных, обладает программой, обрабатывающей разнородные массивы данных с большим объемом, получаемых от IoT-компонентов, с целью улучшения производительности, минимизации последствий от сетевых атак, выявления неполадок в ИТ-инфраструктуре, формирования бизнес-аналитики, оптимизации производственных процессов организаций и контроля за нарушениями ИБ [31].

Компания McAfee имеет облачное решение McAfee ESM Cloud, которое позволяет клиентам создать центр управления безопасностью (SOC), способный принимать данные или выполнять поиск и масштабирование правил сопоставления событий [32].



а б

Рисунок 13 – Магический квадрант по ИБ и управлению инцидентами, лист 1



в

Рисунок 13, лист 2

В соответствии с рисунком 13, согласно статистике исследовательской компании Gartner [33, 34], в лидерах по разработке и реализации систем обеспечения ИБ в 2020 году был IBM, в 2021 году – Exabeam, в 2022 году – Microsoft.

Эти и другие системы нашли широкое применение среди крупных компаний, в том числе и отечественных. В компаниях применяют технологии и системы обеспечения безопасности компаний SAS Institute, Microsoft, Cisco Systems, Hewlett-Packard, IBM, Huawei и др.

* 1. **Обзор состояния информационной безопасности в Республике Казахстан**

В нашей стране вопросу обеспечения информационной безопасности уделяют особое внимание. Об этом можно судить по утверждению приоритетных направлений поддержки и финансирования госпрограмм и принимаемым законопроектам - законы Республики Казахстан - «О национальной безопасности»; «О персональных данных и их защите», «О государственных секретах», Концепция Развития цифровой экосистемы на 2022-2027 года («Киберщит-2»); Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023-2029 годы.

В целях содействия в безопасном использовании информационных ресурсов и систем ИКТ с 2010 года функционирует аналитическое подразделение KZ-CERT, которая позиционируется как национальная Служба реагирования на компьютерные инциденты. KZ-CERT является участником следующих международных служб и организаций: OIC-CERT (Организация исламского взаимодействия Служб реагирования на компьютерные инциденты), TI (Надежный представитель для служб безопасности и реагирования на инциденты), FIRST (Форум групп реагирования на инциденты и обеспечения безопасности) [35].

На отечественном рынке действуют специализированные компании по выявлению причин и рисков возникновения ИБ-инцидентов, инструментальному аудиту КСТ по оценке ее защищенности (методы «white hat», «grey hat», «black hat»), на соответствие КСТ стандартам ИБ. Разработаны отечественные программные средства антивирусной защиты.

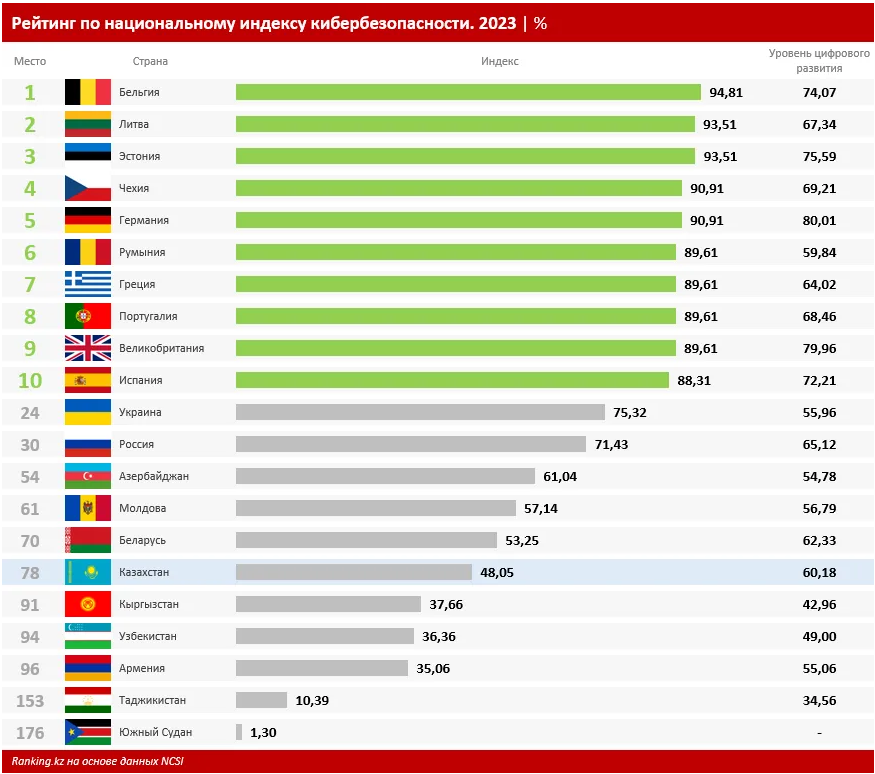


Рисунок 14 – Рейтинг по национальному индексу кибербезопасности

Согласно статистике, рисунок 14, Казахстан занял 78-е место из 176, по рейтингу национального индекса кибербезопасности среди стран-участников. Назначенный РК индекс в 48,05% (из 100%), показывает довольно низкий уровень защищенности. Уровень цифрового развития населения составляет 60,18%. Индекс показывает уровень готовности стран противостоять киберугрозам и относится к глобальным оперативным индексам [36]. Такие данные приводит [ranking.kz.](https://ranking.kz)

Cетевая готовность, индекс развития ИКТ и глобальный индекс кибербезопасности являются тремя категориями, составляющими основу оценки стран. Эти категории делятся на подкатегории, их 12. В подкатегории военных киберопераций РК присвоили 0%, борьбы с киберпреступностью – 44%, реагирования на киберинциденты – 50%, управления киберкризисами – 20%, защиты персональных данных – 100%, электронной идентификации и трастовых услуг – 89%, защиты основных услуг – 17%, защиты цифровых сервисов – 0%, вклада в глобальную кибербезопасность – 17%, образования и профессионального развития – 89%, анализа и информации о киберугрозах – 60%, в сфере разработки политики кибербезопасности присвоили 57% [36].

Данные статистики не являются индикатором уровня защищенности от угроз информационной безопасности, а лишь отражают соответствие международным стандартам и нормам.

## **Обзор проблемы обеспечения информационной безопасности**

Хотя ведется большая работа по обеспечению ИБ, факты и статистические данные говорят об обратном. По итогам января–сентября 2023 года в Казахстане было зафиксировано 18,5 тысяч кибератак – это на 56,2% больше, чем годом ранее, рисунок 15.

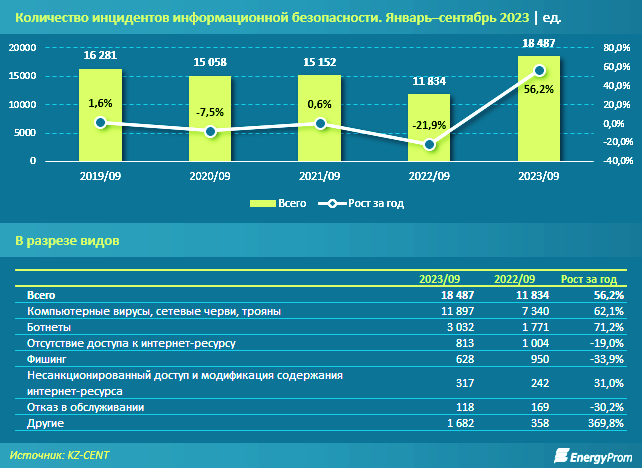


Рисунок 15 – Количество инцидентов информационной безопасности

Большая часть кибератак в прошлом году пришлась на заражение компьютеров вредоносными вирусами, сетевыми червями и троянами: 3 тыс. случаев, годовой рост – на 71,2%.

Часто наблюдались также такие инциденты, как ботнеты (3 тыс. случаев), отсутствие доступа к интернет-ресурсу (813 случаев), фишинг (628 случаев), несанкционированный доступ и модификация содержания интернет-ресурса (317 случаев), отказ в обслуживании (118 случаев) [37].

Пренебрегая соображениями безопасности при использовании ресурсов сети Интернет и социальных сетей, пользователи подвергают себя повышенному риску компрометации, несанкционированному использованию или модификации личных данных, разглашению данных мошенникам и преступникам [35].

Большинство пользователей не применяют специализированные программы для защиты своих персональных устройств. Наряду с этим, отсутствие базовых знаний функционирования вредоносных программ (особенно непреднамеренное обращение к «фишинговым» интернет-страницам, скачивание нелицензионного программного обеспечения (ПО)) и цифровая грамотность на низком уровне в вопросах защиты личных данных приводят к инцидентам ИБ, а персональные устройства становятся орудиями неправомерных воздействий.

Основными причинами возникновения угроз в сфере ИБ в РК являются:

* низкая цифровая грамотность населения, рисунок 16, работников сферы информационно-коммуникационных технологий (ИКТ) и менеджмент компаний по вопросам обеспечения ИБ;
* нарушение пользователями услуг и субъектами информатизации предъявляемых требований нормативных документов и стандартов по сбору, хранению и передаче информации;
* сбои сетевого оборудования, непреднамеренные ошибки сотрудников компаний, оказывающие негативное влияние функционирование информационных систем (ИС), ПО и другие компоненты ИКТ;
* деструктивные воздействия исполнителей сообществ и международных преступных групп по хищению данных в банковской сфере, по нарушению функционирования технологических процессов энергетики, промышленности и в сфере информационно-коммуникационных услуг;
* деятельность спецслужб иностранных государств, разведывательных структур, экономически и политически заинтересованных лиц, террористических организаций, оказывающих воздействие на сетевую и информационную инфраструктуры коммерческих и государственных учреждений РК в разведывательных и подрывных целях [35].

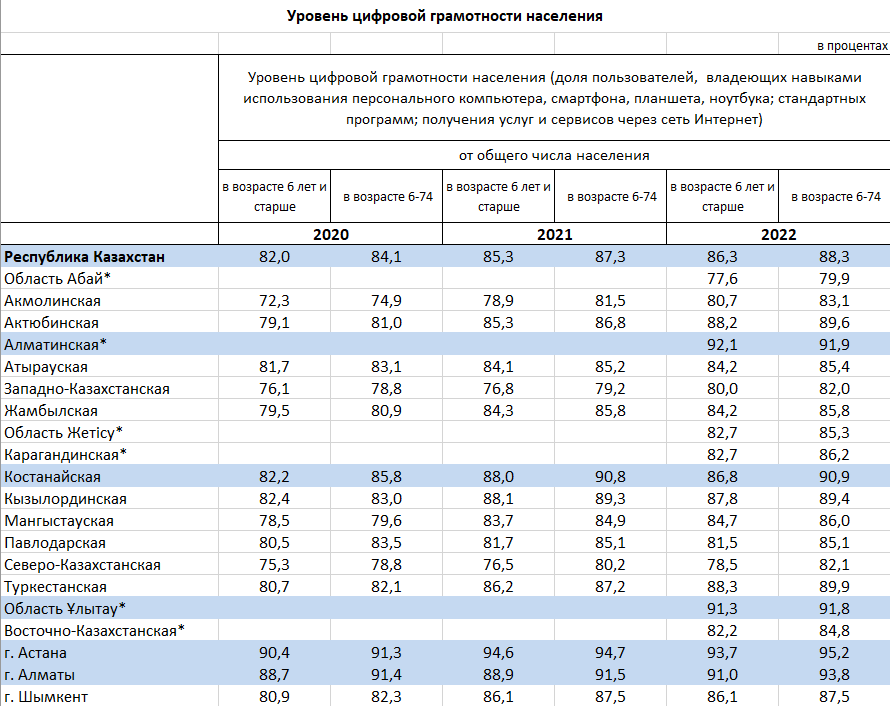


Рисунок 16 – Уровень цифровой грамотности населения Республики Казахстан

Приведенные негативные факторы эксплуатируется злоумышленниками, и приводят к прогрессированию существующих и появлению новых видов атак, «заражающих» вредоносными ПО устройства пользователей. Согласно статистике международной компании по разработке ПО Positive Technologies, 14% из всех обнаруженных атак составили атаки, направленные против частных лиц. Логины и пароли составляют основную часть украденных данных. 34% всех атак были направлены против юридических лиц с осуществлением атак троянов-шифровальщиков – известного вредоносного ПО (ВПО). Администраторы и разработчики шифровальщиков имеют собственные веб-сайты, где публикуют сумму выкупа и угрожают владельцам раскрытием и распространением их информации в случае отказа уплаты выкупа.

Злоумышленники постоянно модернизируют свои приемы обхода механизмов защиты, встроенных в операционные системы (далее – ОС), и антивирусов. С начала 2020 года были обнаружены попытки эксплуатирования ранее неизвестной уязвимости CVE-2020-0601 в Windows CryptoAPI для подписи вредоносного ПО. Уязвимостью CVE-2020-0601 можно обойти механизм проверки сертификатов. Также, имеются факты обнаружения ВПО FakeChmMsi, которое двукратно использует технику DLL hijacking для распространения сетевого трояна Gh0st, и это затрудняет обнаруживаемость ВПО антивирусами. Еще одним примером является ВПО SysUpdate. Оно является разработкой Bronze Union и используется злоумышленниками для доставки на контролируемые ими системы другого зловреда для заражения и атаки. Зачастую, такой зловред не могут обнаружить антивирусы, ввиду неизвестного формата [38].

Наряду с этим, существующие системы для обнаружения вредоносного трафика используют сигнатурный подход, что подразумевает идентификацию вирусных программ на основе известных свойств вируса – его сигнатур. Хотя большинство компаний по разработке систем обеспечения безопасности хранят свою базу сигнатур в секрете, основная часть сигнатур находится в открытом доступе, и злоумышленники хорошо осведомлены ими. Чтобы обходить ограничения, злоумышленники постоянно модифицируют свои программы и методы взлома, и сигнатурный подход уже не работает [39], а пока узнают о новом виде вируса или атаки, и компании выпустят обновления своих систем, пройдет немало драгоценного времени, которого будет достаточно, чтобы скомпрометировать данные и «замести следы». Таким образом, полагаясь исключительно на обнаружение на основе сигнатур, организации могут оказаться уязвимыми перед новыми и неизвестными угрозами.

Кроме того, злоумышленники могут использовать различные методы уклонения, чтобы обойти системы обнаружения на основе сигнатур, такие как полиморфное вредоносное ПО, обфускация и шифрование. Полиморфное вредоносное ПО может менять свой внешний вид каждый раз, когда оно заражает новую систему, что затрудняет его обнаружение с помощью систем, основанных на сигнатурах. Запутывание включает в себя изменение кода вредоносного программного обеспечения, чтобы затруднить его обнаружение. Шифрование также может использоваться для сокрытия вредоносного кода, что затрудняет обнаружение систем, основанных на сигнатурах.

**Выводы по разделу 1**

Несмотря на имеющееся на данный момент количество решений, имеется ряд недостатков, связанных с обеспечением ИБ систем КСТ.

Традиционные методы обнаружения угроз и реагирования на них основываются на идентификации кибер ‒ «отпечатков пальцев», сигнатур вредоносного ПО, чтобы предотвратить заражение системы. В течение многих лет эта форма обнаружения угроз и реагирования на них была эффективна против большинства вирусов и киберугроз, но в современном мире они становятся все более уязвимыми для новых и постоянно развивающихся форм вредоносных программ. Как следствие, существующие системы обеспечения ИБ в КСТ не могут полностью гарантировать защищенность активов компаний от внешних и внутренних угроз.

Увеличение объемов данных и рост сложности программного обеспечения не позволяет производить обработку и поиск аномалий в «ручном» режиме. Миллионы сетевых пакетов за одни сутки и десятки тысяч сеансов связи просто невозможно проанализировать вручную. Специалисты занимаются лишь развертыванием систем обеспечения безопасности с предустановленными политиками, донастройкой параметров (при возникновении проблем с работой корпоративных сервисов) и реагированием на выборочно предлагаемые системой сигнатурные инциденты.

Развитие «индустрии» разработки вредоносных программ, приводящее к тому, что ежедневно появляются тысячи различных модификаций вирусов, которые могут функционировать в системе как легитимное приложение, в разы усложняет работу специалистам по ИБ. Многие распределенные виды «грубых» атак легко обнаруживаются статистическими методами, но узкоспециализированные вирусы, которые применяют «мягкую» силу, могут пребывать в системе продолжительное время, оставаясь незамеченными.

Появление специфических программ, использующих уязвимости, основанные на сетевых пакетах, - это подмена IP-адресов, отсутствие шифрования данных (telnet, FTP), «отравление» кэша в DNS и другие, показывают необходимость обработки не только хранимых в системе данных, но и данных, передаваемых по сети, – сетевой трафик.

Все это приводит к тому, что для решения обозначенных проблемных вопросов необходимо применять методы искусственного интеллекта, обладающие как большей точностью, так и лучшей производительностью.

Для выявления новых видов атак необходимо разрабатывать альтернативные методы и приемы защиты информации, предполагающие использование средств интеллектуального анализа данных. Параллельно, необходимо прорабатывать вопросы совершенствования существующих решений, комбинируя их между собой для повышения эффективности выявления всевозможных аномалий в сети.

# **МОДЕЛИ И МЕТОДЫ ИДЕНТИФИКАЦИИ И ОЦЕНКИ ВРЕДОНОСНОГО ТРАФИКА**

## **2.1 Общая постановка задачи исследования**

В связи с развитием информационных технологий огромные объемы данных, описывающих функционирование систем и устройств, представлены в виде временных рядов и информационных последовательностей.

Информационная последовательность ­ характеризуется в каждый момент времени состоянием . Имеются модели обработки , осуществляющие отображение *,* во множество опасных и безопасных состояний *.* В ходе функционирования информационная система подвергается внешним и внутренним деструктивным воздействиям. В результате меняются различные характеристики , например, количество сообщений в сети, их частота появления, соотношения служебных и информационных сообщений. В связи с этим, при определении деструктивного информационного воздействия возникает задача разделения последовательности на сегменты и назначения на сегмент модели функционал качества которой на выбранном сегменте максимален по сравнению с другими моделями:

Таким образом, на каждый сегмент назначается модель, имеющая лучшие значения показателя качества.

Для формальной постановки и решения задачи в работе введены обозначения, представленные в таблице 4.

Таблица 4 – Обозначения

|  |  |
| --- | --- |
| Обозначение | Физический смысл обозначения |
| 1 | 2 |
|  | модель сетевого трафика |
|  | множество объектов наблюдения, исходная выборка |
|  | множество характеристик |
|  | множество последовательностей объектов наблюдения |
|  | количество объектов в выборке |
|  | кортеж значений признаков |
|  | количество признаков |
|  | класс состояния |
|  | опасный, безопасный |
|  | модель |
|  | выборка после МГК |
|  | кортеж значений информативных признаков |
|  | количество наиболее информативных признаков |
|  | значение признака |
|  | среднее значение |
| Продолжение таблицы 4 | |
| 1 | 2 |
|  | стандартное отклонение |
|  | стандартизированное значение признака |
|  | ковариационная матрица |
|  | собственное значение матрицы ковариации |
|  | собственный вектор матрицы ковариации |
|  | отсортированная по убыванию матрица собственных векторов |
|  | главный компонент |
|  | -ная главная компонента |
|  | итоговая матрица главных компонент |
|  | редуцированное уменьшенное пространство признаков |
|  | функция потерь |
|  | индикатор ошибок |
|  | множество факторов |
|  | воздействующий фактор |
|  | количество факторов, количество сегментов |
|  | подмножество, сегмент |
|  | множество моделей |
|  | количество моделей |
|  | индикаторная функция принадлежности |
|  | функция, вычисляющая свойства сегмента |
| , | пороговые значения |
|  | функционал качества модели |
|  | момент изменения характеристик наблюдаемого процесса |
|  | функция классификатора |
|  | классифицирующие алгоритмы |
|  | весовая матрица |
|  | значения весов |
|  | функция принадлежности |
|  | дополнительная функция классификатора |
|  | коэффициент регуляризации |
|  | функция регуляризации |
|  | количество состояний системы |
|  | -тое состояние |
|  | множество состояний системы |
|  | решающее правило (бэггинг) |
|  | функция для разбивки пространства на две непересекающиеся области |
|  | индекс обученных базовых классификаторов |
|  | функция апостериорной вероятности |
|  | функция для определения результирующего класса |
|  | Момент времени |

## **2.2 Модель признакового пространства сетевого трафика**

Выявление и оценка вредоносного трафика имеет первостепенное значение для обеспечения безопасности и целостности сети. Вредоносный трафик может исходить из различных источников, включая киберпреступников, хакеров и инсайдеров, и может вызывать целый ряд угроз безопасности, таких как несанкционированный доступ, утечка данных и компрометация системы.

Согласно отчету Verizon, 70% утечек данных происходят по вине внешних участников, а остальные 30% - по вине инсайдеров [40]. Вредоносный трафик может принимать различные формы, включая вредоносные программы, ботнеты, фишинговые атаки и атаки типа «отказ в обслуживании» (DoS).

Сетевой трафик относится к потоку данных между устройствами в сети. Состав и параметры сетевого трафика варьируются в зависимости от типа сети и типов устройств и приложений, использующих сеть, рисунок 17.

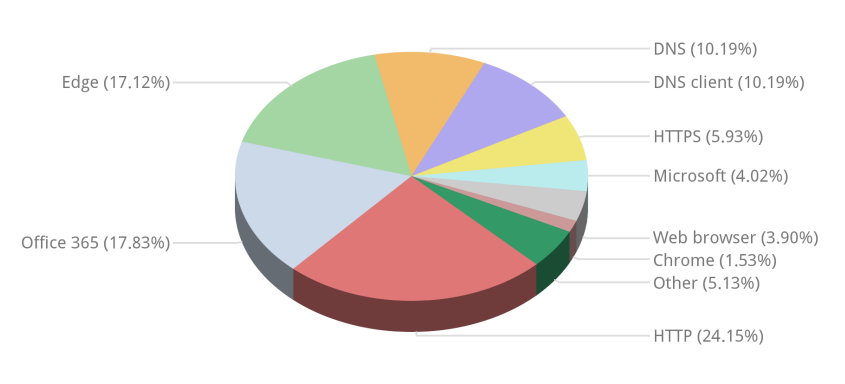


Рисунок 17 – Пример статистики используемых приложений

в локальной вычислительной сети КСТ

Состав сетевого трафика также может быть описан в терминах его протокола, полезной нагрузки и заголовка. Протокол относится к правилам и процедурам, регулирующим обмен данными между устройствами в сети. Примеры протоколов включают TCP/IP, HTTP и FTP. Полезная нагрузка относится к фактическим передаваемым данным, таким как содержимое веб-страницы или сообщения электронной почты. Заголовок содержит метаданные о данных, включая адреса источника и назначения, порядковый номер и контрольную сумму.

В дополнение к этим параметрам сетевой трафик также может характеризоваться частотой и продолжительностью соединений, типами передаваемых пакетов и объемом трафика, генерируемого отдельными устройствами или приложениями, рисунок 18.

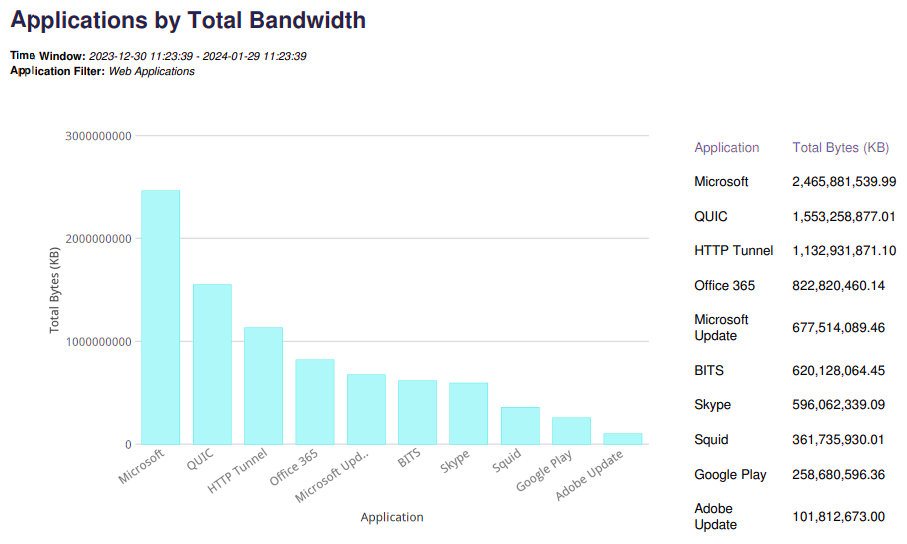


Рисунок 18 – Объем трафика, генерируемого отдельными устройствами или приложениями

Сетевой трафик можно разделить на два основных типа: локальный и удаленный трафик. Локальный трафик относится к данным, которыми обмениваются устройства в локальной сети, например компьютеры в одной локальной сети. Удаленный трафик относится к данным, которыми обмениваются устройства в различных сетях, например компьютеры, получающие доступ к веб-сайту через Интернет.

Сетевой трафик может быть дополнительно классифицирован на различные типы в зависимости от характера обмениваемых данных. Некоторые распространенные типы сетевого трафика включают:

Трафик электронной почты, которыми обмениваются почтовые серверы и клиенты.

Веб-трафик, которыми обмениваются веб-серверы и клиенты, таким как веб-страницы, изображения и видео.

Трафик при передаче файлов, которыми обмениваются устройства при загрузке файлов с сервера.

Голосовой и видео трафик, которыми обмениваются во время голосовых и видеозвонков, например, совершаемых через приложения VoIP (передача голоса по IP).

Cетевой трафик измеряется в [битах](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82), [байтах](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%B9%D1%82), [килобайт](https://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%BB%D0%BE%D0%B1%D0%B0%D0%B9%D1%82)ах (КБ), [мегабайт](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B3%D0%B0%D0%B1%D0%B0%D0%B9%D1%82) (МБ), гигабайтах (ГБ) и т.д.

Трафик классифицируется как:

* внешний (за пределами определённой сети, чаще всего - [интернет](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)-трафик);
* внутренний (в пределах определённой сети, чаще всего [локальной](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C));
* входящий (информация, поступающая из внешней сети);
* исходящий (информация, поступающая во внешнюю сеть).

В компьютерных сетях сетевой трафик чаще всего инкапсулируются в сетевые пакеты, рисунок 19, которые характеризуют нагрузку в сети.

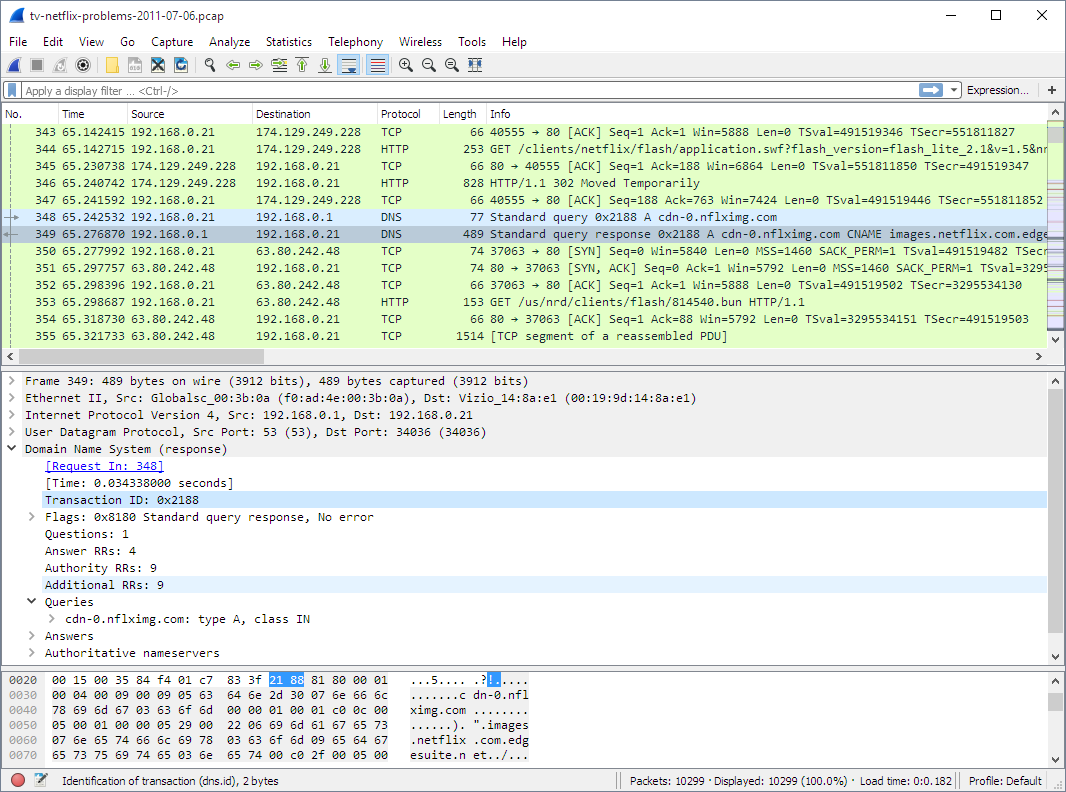


Рисунок 19 – Вид сетевого пакета с анализатора трафика Wireshark

Формат сетевого пакета включает в себя заголовок, состоящий из 12 полей, общая длина которых равна 160 бит, поле параметров переменной длины и поле данных, рисунок 20.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 4 | 5 8 | 9 16 | 17 19 | 20 32 |
| 1. Версия | 2. Длина заголовка | 3. Тип сервиса | 4. Общая длина | |
| 5. Идентификация | | | 6. Флаги | 7. Смещение фрагмента |
| 8. Время жизни | | 9. Протокол | 10. Контрольная сумма заголовка | |
| 11. IP-адрес источника | | | | |
| 12. IP-адрес получателя | | | | |
| 13. Параметры IP | | | | |
| 14. Данные | | | | |

Рисунок 20 – Формат сетевого пакета

Описание полей сетевого пакета [41] представлено в таблице 5.

Таблица 5 – Описание полей сетевого пакета

|  |  |  |
| --- | --- | --- |
| Поле пакета | Длина (биты) | Описание |
| 1 | 2 | 3 |
| Версия | 4 | Версия протокола IP (IPv4 или IPv6) |
| Длина заголовка (HLen) | 4 | Количество 32-битных слов в заголоске (минимальное значение равно 5) |
| Тип сервиса (TOS) | 8 | Набор флагов, указывающих на качество запрашиваемой или предоставляемой услуги. |
| Общая длина | 16 | Общая длина IP-пакета в байтах (заголовок + данные) |
| Продолжение таблицы 5 | | |
| 1 | 2 | 3 |
| Идентификация | 16 | Уникальный идентификатор, назначаемый отправителем для повторной сборки фрагментированных пакетов |
| Флаги | 3 | Набор флагов, указывающих, можно ли фрагментировать пакет или это последний фрагмент |
| Смещение фрагмента | 13 | Смещение текущего фрагмента в исходном пакете (измеряется блоками по 8 байт) |
| Время жизни (TTL) | 8 | Максимальное количество переходов (маршрутизаторов), которые может пройти пакет, прежде чем он будет отброшен |
| Протокол | 8 | Протокол используемый данным пакетом (имеется ввиду TCP или UDP) |
| Контрольная сумма заголовка | 16 | Контрольная сумма, которая проверяет целостность заголовка IP |
| IP-адрес источника | 32 | IP-адрес источника |
| IP-адрес получателя | 32 | IP-адрес получателя |
| Параметры IP | переменной длины | Необязательные поля, которые могут включать дополнительную информацию или инструкции по обработке пакета |
| Данные | более 64 | Полезные данные |

Исходя из сказанного выше, в общем виде, модель сетевого трафика определяется кортежем:

где – множество объектов наблюдения (сетевых пакетов);

– множество характеристик;

– метод поиска наиболее информативных компонент.

В IP-сети трафик между любой парой узлов источник-назначение обычно следует по одному и тому же пути. При этом, в пределах одного сеанса, между этими узлами фактически может передаваться от десятков до нескольких тысяч сетевых пакетов. По единичным пакетам достаточно сложно выявить угрозы ИБ, - необходимо анализировать целый сеанс связи – информационные последовательности сетевых пакетов (ИПСП) между конкретными узлами источника и назначения.

В предлагаемом исследовании под информационной последовательностью сетевых пакетов (ИПСП) понимается однонаправленный поток сетевых пакетов [42], относящихся к конкретному экземпляру некоторого пользовательского приложения в пределах одного сеанса и который использует общий набор полей IP-заголовка: IP-адрес источника, IP-адрес назначения, протокол и порты источника/назначения.

### 2.2.1 Постановка задачи

Концепция ИПСП важна для анализа и управления сетевым трафиком, поскольку она позволяет сетевым администраторам отслеживать поведение сетевого трафика и выявлять потенциальные проблемы, такие как узкие места, угрозы безопасности и проблемы с производительностью.

В рамках данного исследования, ИПСП принято моделировать в виде кортежа значений признаков (параметров, атрибутов) данной информационной последовательности (КЗСП). В качестве таких признаков могут быть использованы: количество пакетов, размер, комбинация флагов сообщений, длительность сеанса, время между прибытиями сетевых пакетов, и др.

Основываясь на концепции ИПСП, формализованную постановку задачи исследования можно определить следующим образом.

Выборка объектов, сеансов связи (ИПСП), , – количество объектов в выборке, представленных в виде КЗСП и отражающее состояние ИБ КСТ.

Класс состояния ИБ КСТ , который может быть опасным или безопасным .

Необходимо соотнести объект к своей группе – классу опасного или безопасного состояния , путем анализа значений объектов:

(2)

Данная задача относится к задаче классификации. Так как классов всего два, к данным будет применяться бинарная классификация.

Алгоритм решаемой задачи представлен на рисунке 21.

Сложно охватить весь объем данных, так как изучение больших объемов данных является дорогостоящим процессом, требующим значительных временных затрат, а также неизбежно приводит к ошибкам, связанным с человеческим фактором. Поэтому достаточно рассмотреть выборку объектов - часть из всей генеральной совокупности ИПСП.

В зависимости от набора данных и от условий появления объектов наблюдения и возможностей по съему значений характеристик от регистрирующих устройств возможно получение различных признаков (атрибутов), описывающих состояние ИБ КСТ.

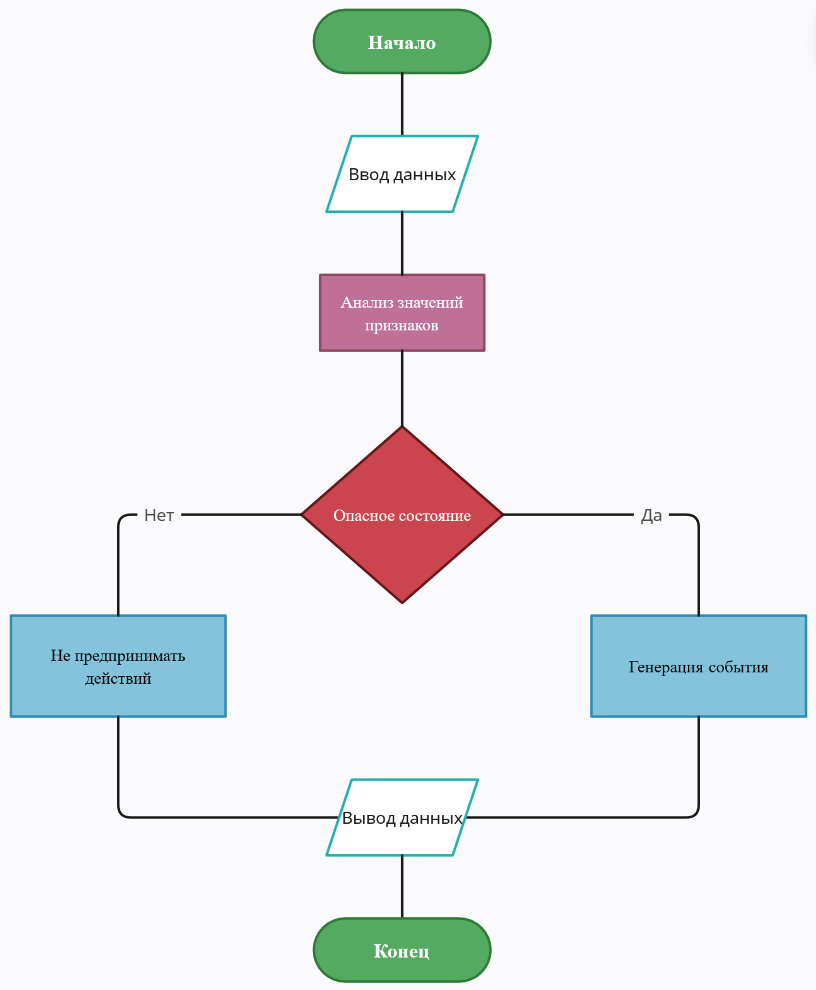


Рисунок 21 – Алгоритм решаемой задачи

В качестве типовых признаков вредоносного трафика могут быть:

* коды сетевых протоколов, информирующих об ошибках;
* несовпадение контрольной суммы сетевого пакета (CRC);
* неправильный размер сетевых пакетов (MTU);
* разрыв TCP соединения (TCP Reset);
* большое количество DNS записей;
* изменение топологии STP;
* присутствие в сетевом трафике сигнатур исполняемых файлов;
* подозрительные флаги;
* соединения с управляющими серверами;
* попытки несанкционированного подключения;
* поведенческие характеристики, определяемые для различных шаблонных последовательностей пакетов и их содержимого, и др.

2.2.2 Количественные характеристики сетевого трафика

Для решения задачи идентификации вредоносного сетевого трафика необходимы количественные параметры.

Каждый (ИПСП) обладает множеством признаков (представленных в виде КЗСП) *.* Имеет место отображение ,, где могут характеризовать время начала сеанса, количество переданных пакетов в сеансе, продолжительность сеанса и т.д., а также использоваться для вычисления таких характеристик как, например, частота появления.

Опишем распространенные ситуации в КСТ.

Необычно высокий или низкий объем трафика по сравнению с историческими или ожидаемыми уровнями трафика может указывать на аномальный трафик [43]. Увеличение объема трафика может указывать на DDoS-атаку, в то время как уменьшение объема трафика может указывать на проблемы с подключением к сети или сбои в обслуживании.

Диаграмма, показывающая зависимость объема передаваемого по сети трафика от времени показана на рисунке 22.

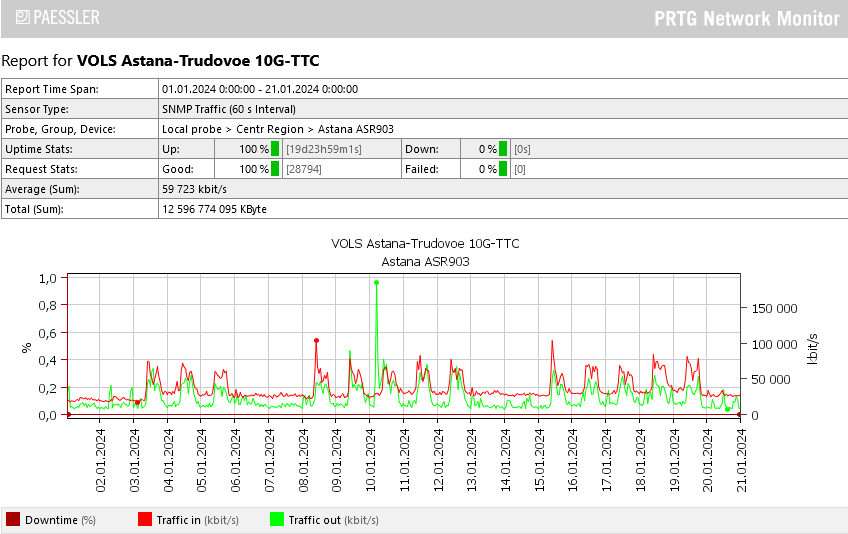


Рисунок 22 – Диаграмма зависимости объема передаваемого по сети трафика от времени

Необычное использование протоколов, такое как использование нестандартных протоколов [44] или неожиданные номера портов, может указывать на аномальный трафик (рисунок 23). Это может свидетельствовать о вредоносном ПО или активности ботнета, который пытается избежать обнаружения.

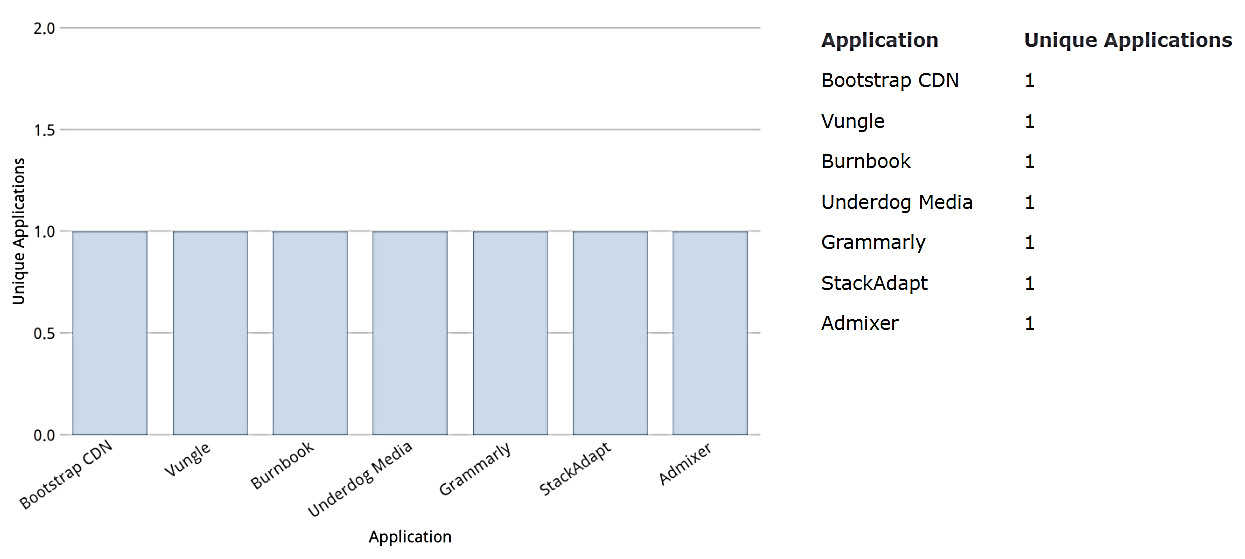


Рисунок 23 – Выявление уникальных приложений

Необычные схемы передачи трафика между IP-адресами источника и назначения могут указывать на аномальный трафик. Например, большие объемы трафика с одного IP-адреса источника (рисунок 24) на несколько IP-адресов назначения могут указывать на попытку сканирования или рекогносцировки.

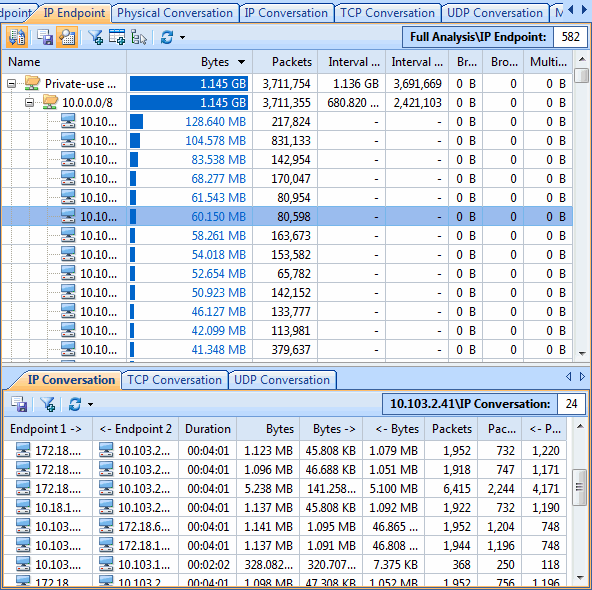


Рисунок 24 – Выявление больших объемов трафика

Высокая скорость пакетов в секунду (PPS), рисунок 25, может свидетельствовать о DDoS-атаках [45], в то время как низкая скорость PPS может указывать на проблемы с подключением к сети или перегрузку.

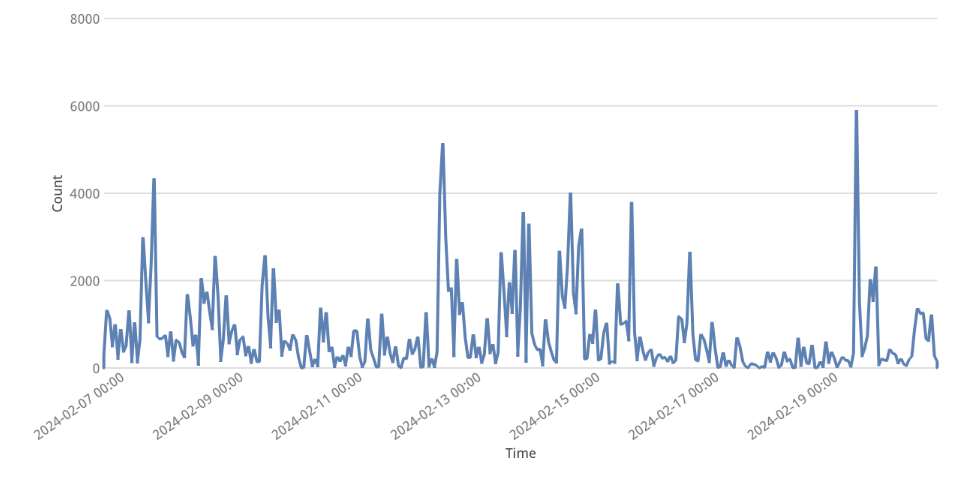


Рисунок 25 – Количество передаваемых пакетов за единицу времени

Необычно продолжительные или короткие сеансы могут указывать на аномальный трафик. Это может свидетельствовать о различных типах атак, таких как slowloris [46] или SYN-флуды.

Также, среднее значение и стандартное отклонение [47] могут использоваться для выявления точечных аномалий в сетевом трафике. Точки данных, отклоняющиеся от среднего значения более чем на три стандартных отклонения, могут считаться аномальными.

Одной из немаловажных параметров является энтропия, которая измеряет случайность или непредсказуемость данных. В сетевом трафике энтропия может использоваться для выявления аномалий [48], таких как сканирование сети и атаки. Высокие значения энтропии могут указывать на то, что трафик не является типичным для сети.

Параметр скользящая средняя рассчитывается путем усреднения определенного количества прошлых точек данных. Если текущая точка данных значительно отклоняется от скользящей средней, это его также можно считать аномальным.

Приведем несколько распространенных формул для нахождения параметров:

Максимальное значение трафика:

Минимальное значение трафика:

Пиковое значение трафика:

Среднее значение трафика:

– непрерывное время

– дискретное время

Коэффициент пачечности трафика (берстность):

Средняя длительность пика:

СКО трафика:

Рассмотренные показатели позволяют осуществить количественные оценки. В дальнейшем, применяя методы математической статистики, методов МО, применительно к рассмотренным показателям, возможно решение задачи классификации, распознавания, предсказания, в целях идентификации нормального и аномального (вредоносного) сетевого трафика.

2.2.3 Поиск информативных признаков

Информативными признаками называется полезная информация, полученная из исходной информации. Ответственной задачей исследователя является выявление наиболее информативных признаков из анализируемых данных, ввиду неодинаковой равнозначности признаков для целей надежной классификации. Вводится понятие «информативности» для количественного измерения параметра. От информативности признака зависит окончательный результат классификации данных [49].

Наряду с этим, анализ всего признакового пространства требует больших вычислительных затрат, а избыточность данных может приводить к переобучению модели. Причиной тому является чрезмерно большое количество обрабатываемых признаков. Данное явление принято называть «проклятием размерности» или «проклятием Беллмана», в честь придумавшего данный термин математика Ричарда Э. Беллмана.

В связи с этим, имеется необходимость в уменьшении размерности признакового пространства, путем выделения наиболее информативных и исключения менее информативных признаков.

Опишем постановку задачи.

Имеется выборка объектов, рисунок 26, описывающих сетевой трафик, , , где – – мерное пространство признаков. Задача уменьшения размерности состоит в получении представления этой выборки в пространстве уменьшенной размерности , при .

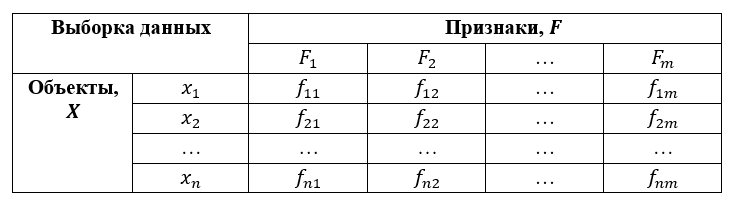


Рисунок 26 ‒ Шаблон исходной выборки объектов

Существенно качественное признаковое пространство позволяет получить использование метода главных компонент (МГК). Основная суть метода заключается в выявлении отношений данных, преобразовании существующих данных на основе найденных отношений и их количественном определении.

В этом случае отношения называются главными компонентами и определяются как линейные комбинации, которые имеют максимальную дисперсию, но с ограничениями - (а) вектор линейных весов, определяющий каждый компонент, должен иметь единичную длину, (б) компоненты ортогональны друг другу (т. е. некоррелированны) и (c) каждый компонент должен иметь максимально возможную дисперсию с учетом ограничений (a) и (b) [50].

Блок-схема работы МГК представлена на рисунке 27.

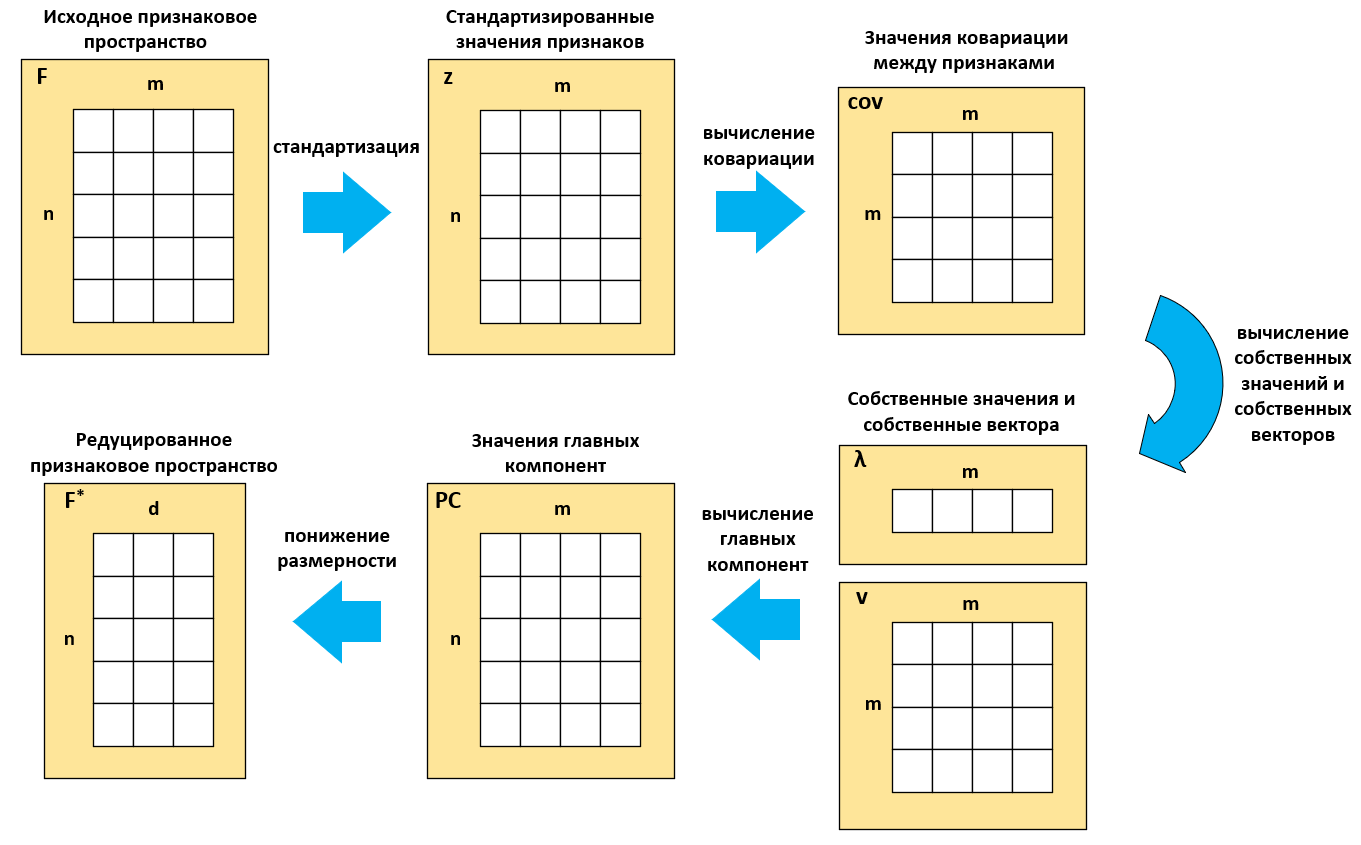


Рисунок 27 – Блок-схема работы МГК

Опишем последовательность действий.

1. Для исходного признакового пространства , – количество признаков:

где – значение – го признака – го объекта, необходимо вычислить среднее значение и стандартное отклонение каждого из признаков по формулам (4) и (5).

2. Чтобы избежать эффектов масштабирования, перед анализом переменные нормализуются. В противном случае переменные с большой дисперсией будут доминировать в анализе и искажать результаты.

Для нормализации данных необходимо вычислить отношение разности значения каждого признака и его среднего значения на стандартное отклонение, (6).

где ‒ стандартизированное значение – го признака – го объекта.

Тогда стандартизированные значения признаков будут иметь вид (7):

В результате получаем стандартизированные значения по каждому значению признаков таким образом, чтобы их средние значения равнялись 0, а стандартные отклонения 1.

3. Вычислить ковариацию между стандартизированными значениями всех признаков (8), для выявления линейной зависимости. Для этого необходимо вычислить все ковариации между двумя возможными значениями стандартизированных значений признаков (9) и поместить их в квадратную матрицу (10). Необходимо отметить, что чем выше значение ковариации между признаками, тем выше зависимость между ними.

Формула (8) вычисления ковариации:

Все возможные значения признаков:

Матрица ковариации:

4. Вычислить собственные значения и собственные вектора матрицы следующим образом.

Имеется квадратная матрица и пусть будет ненулевым вектором, для которого выполняется равенство (11):

для некоторого скалярного значения . Тогда, будет называться собственным значением матрицы , а – собственным вектором матрицы соответствующим собственному значению .

В конечномерном пространстве равенство является эквивалентным следующему матричному равенству (12):

Следовательно, является собственным значением матрицы в том случае, когда , а является корнем многочлена , называемого характеристическим многочленом матрицы . Определение собственных векторов , соответствующих собственным значениям , сводится к нетривиальному решению однородной системы уравнений.

Далее, полученные собственные значения и соответствующие им собственные вектора многочлена отсортировываются по убыванию, т.е. и .

Получим отсортированную матрицу собственных векторов (13):

где

, , ,

5. Нахождение главных компонент. Данная задача сводится к произведению стандартизированных значений (7) к отсортированной матрице векторов (13), выходит следующее (14):

Итого получилось отсортированных по убыванию главных компонент, где

6. Понижение размерности.

Разработаны десятки различных методов выбора необходимого числа компонент. Все используемые методы являются эвристиками, то есть ни один из них не может быть доказан и каждый может иметь смысл в определенных обстоятельствах. По этой причине общий совет состоит в том, чтобы использовать эти различные правила в качестве отправной точки, а затем выбрать ряд компонентов, чтобы результирующие компоненты казались действительными.

Одним из наиболее распространенных методов выбора необходимого числа компонент является критерий Кайзера. В PCA критерий Кайзера отбрасывает компоненты, собственные значения которых меньше 1 (когда данные стандартизированы). Более 1 собственного значения предполагает, что соответствующий компонент объясняет большую дисперсию, чем одна переменная, учитывая, что переменная отвечает за единицу дисперсии [51].

Тогда, следуя критерию Кайзера исключаем компоненты, собственные значения которых меньше 1, и получаем итоговую матрицу главных компонент (16).

(16)

Далее проектируем выборку на оставшиеся главные компоненты:

(17)

Редуцированное уменьшенное пространство признаков будет иметь вид: , где

А исходная выборка в признаковом пространстве преобразуется во множество в редуцированном пространстве , где

На рисунке 28 представлен шаблон выборки объектов после применения МГК.

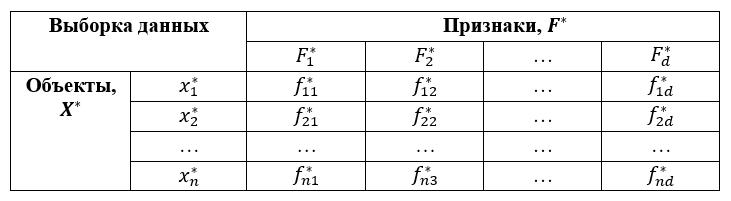


Рисунок 28 ‒ Шаблон выборки объектов после применения МГК

Блок-схема преобразования выборки до и после применения МГК представлена на рисунке 29.

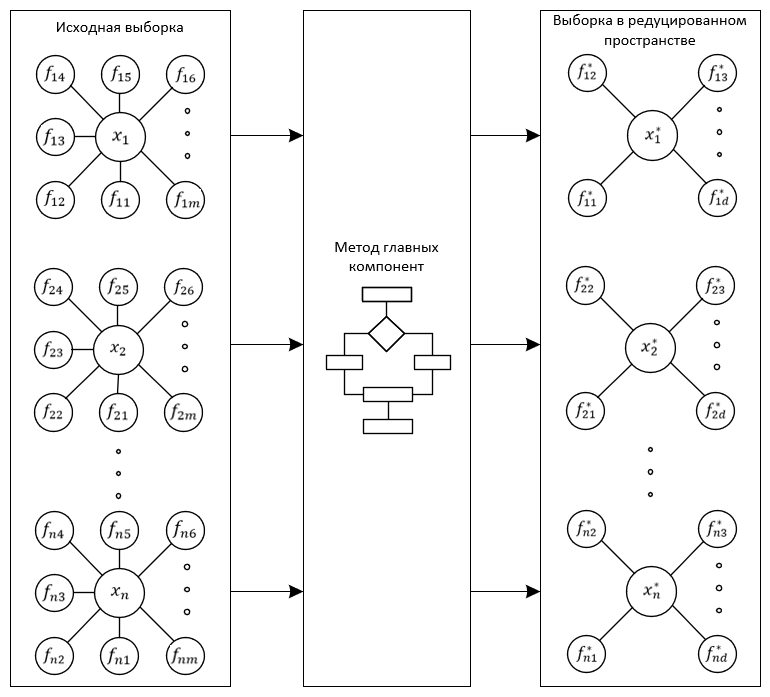


Рисунок 29 – Блок-схема преобразования выборки до и после применения МГК

Итак, метод главных компонент предполагает переход от исходного базиса к базису из собственных векторов матрицы ковариации с дальнейшим отбрасыванием проекций выборки на собственные вектора, отвечающие наименьшим собственным значениям. В базисе из собственных векторов матрица ковариации имеет диагональный вид . Таким образом, признаки, получаемые с помощью метода главных компонент, являются некоррелированными. Переход к некоррелированным признакам часто является разумным методом предобработки исходных данных. Поэтому метод главных компонент применяется и в случае [52].

На рисунке 30 представлена зависимость времени обработки от количества признаков в исследуемых данных. Это дает представление о том, что с уменьшением количества признаков уменьшается и время обработки.

Рисунок 30 – График зависимости времени обработки от количества признаков

На рисунке 31 представлена зависимость точности классификации алгоритмов машинного обучения от количества признаков. По гистограмме становится очевидным, что уменьшая количество признаков можно улучшить показатели точности классификаторов.

Рисунок 31 – Гистограмма зависимости точности от количества признаков

Алгоритм применения метода главных компонент к выборке сетевого трафика, представлен на рисунке 32.

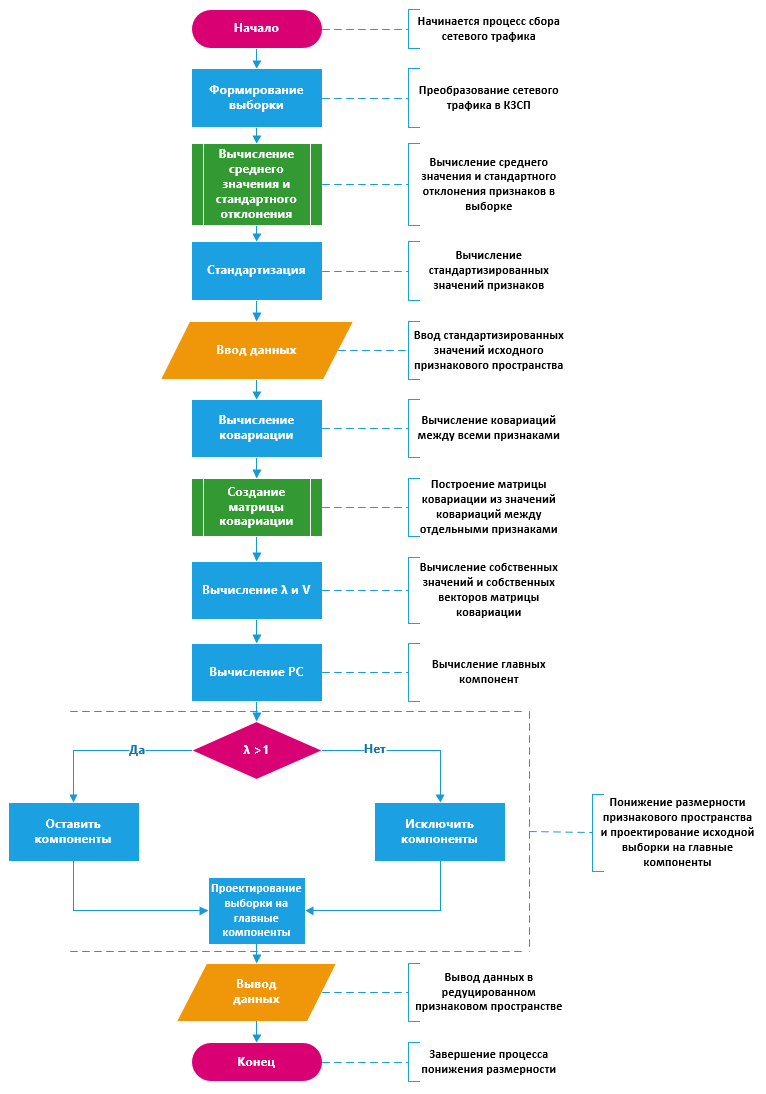


Рисунок 32 – Алгоритм применения метода главных компонент к выборке

сетевого трафика

Псевдокод алгоритма работы МГК представлен на рисунке 33.

|  |  |
| --- | --- |
| Алгоритм: *Метод Главных Компонент* | |
| *Ввод:*  // исходная выборка данных сетевого трафика  *Вывод:*  // представление выборки в редуцированном пространстве  *Начало*  *Начало*  *Для выполнить*  // вычисление выборочного среднего  // вычисление стандартного отклонения  // стандартизация значения признаков  // вычисление ковариации между признаками  // построение матрицы ковариации  *Конец*  *Начало*  Для выполнить  // вычисление собственных значений и собственных векторов  *Конец*  *Начало*  *Если то*  Оставить собственных значений и соответствующие им собственные вектора  *Иначе*  Исключить собственных значений и соответствующие им собственные вектора  *Для выполнить*  // проектирование выборки на выбранные направления  *Конец*  *Конец* |

Рисунок 33 – Псевдокод работы МГК

**2.3 Метод повышения качественных показателей (полноты и точности) идентификации вредоносного трафика**

2.3.1 Постановка задачи

Формирование выборки для анализа в задачах по машинному обучению вызывает определенные проблемы. Свойства и состав сетевого трафика могут изменяться при функционировании КСТ. Примером может служить вариативность объемов данных в рабочее и нерабочее время. Наряду с этим, неоднородность признакового пространства, на формирование которого влияют структура и различные типы сообщений, вызывает сложности для алгоритмов классификации. Однотипные сообщения, но с наличием разных флагов, могут быть индикаторами разных событий в КСТ. Также, может выявляться изменчивость распределений и диапазонов значений.

Такая выборка данных не всегда может показательно описать состояние системы. Данный факт может повлиять на качество результатов алгоритмов МО и приводить к разбросу ответов.

Для решения данных проблем исходная выборка объектов сетевого трафика , была преобразована во множество объектов с наиболее информативными значениями признаков , .

Следовательно, кортеж значений имеет множество параметров. В процессе функционирования КСТ возможно увеличение частоты служебных и информационных сообщений с разными флагами в течение определенного момента времени. К примеру, о несанкционированных попытках подключения может судить нетипичное увеличение сетевых пакетов с флагом <SYN>. Впоследствии, специалистами по ИБ необходимо проверить легальность обнаруженных попыток подключения к сети. Появляется возможность выявления аномальных и нормальных состояний, на основе использования количественных характеристик на размеченной по классам опасности выборке, собранную на опыте предыдущего промежутка времени (недели, месяцы, годы).

Введем параметр , которая может быть опасным состоянием КСТ или безопасным.

являются количественными значениями (атрибутами, признаками). Анализируя значения ставится задача точного сопоставление конкретных объектов из множества к классу состояния - нормального или аномального .

Для решения поставленной задачи имеется возможность сегментирования выборки. Формальное описание сегментирования представляется в следующем виде.

Дано множество объектов выборки , определенных в метрическом пространстве. Анализ и сравнение объектов осуществляется с помощью функции , вычисляющей расстояние между объектами. Каждому объекту сопоставляется ответ , предопределенный на множестве ответов.

Однако возникают изменения распределений, целевых переменных, диапазонов, размаха и частоты выборки сетевого трафика в различных локальных сегментах сети. Это вызывает необходимость введения функции разделения множества , которая объекту назначает свою метку подмножества.

В итоге множество разделяется на подмножества и , в таком виде, чтобы каждое подмножество содержало объекты схожие по, а сами множества различались. При объединении подмножеств должно получиться множество , и пересечения подмножеств быть не должно.

, где - представление обучающей выборки в виде пары значений – сегментов выборки , которая получилась при использовании функции , где – это множество значений анализируемых объектов в сегменте объектов со схожей метрикой .

Для формирования ансамблей алгоритмов, которые имеют наилучшие показатели на отдельно взятых сегментах, из множеств классифицирующих моделей необходимо определить решающую функцию для отдельно взятого сегмента , причем решающая функция должна иметь наилучшие качественные показатели для предопределенного ему сегмента.

2.3.2 Назначение моделей на сегменты при обработке трафика

Сравнение прогноза с меткой производится функцией потерь , которая определяет качественные показатели модели (16).

Для задач классификации применим следующий метод. Введем индикатор ошибок (20), как функцию по измерению потерь классифицирующего алгоритма , действующего на выборке (где - количество объектов в выборке).

Выражением (21) можно определить частоту ошибок (20) алгоритма , для анализа потерь:

Факторы оказывают воздействие на регистрируемые данные. Их можно определить явно, например, в будние дни и в выходные объем трафика разнится. Но интерпретировать их однозначно не представляется возможным, ввиду одновременного воздействия. Данный аспект обуславливает необходимость применения автоматических методов анализа данных, к которым относятся обнаружение дрейфа концепта или поиск точек разладки и перегиба сигнала [53].

Воздействие на КСТ внутренних и внешних факторов приводит к возникновению неоднородности данных.

Необходимым условием качественного повышения результатов, выдаваемых алгоритмами машинного обучения, с учетом влияния на данные изменений плотности вероятности появления тех или иных случайных событий, шумов и коллизий, выбросов данных, необходимо сегментировать множество на подмножества (сегменты) (22), учитывая влияние факторов .

Затем, необходимо минимизировать функцию потерь (23) для каждого сегмента , где оказывает влияние фактор :

Выражением (23) возможно определить свой классификатор МО для сегмента , с наилучшими значениями функции потерь, при условии заранее определенных классифицирующих алгоритмов .

Применяя предопределенные заранее классификаторы МО для каждого сегмента, имеется необходимость минимизации потерь на всей выборке:

Главным преимуществом выражения (24) является возможность выборки группы классификаторов МО с наилучшими качественными показателями для каждого предопределенного сегмента анализируемой выборки.

2.3.3 Сегментирование выборки

Модели, на основе уточненной локальной информации являются одними из распространенных направлений повышения качества классифицирующих алгоритмов [54, 55]. В большинстве задач выборку для обучения рассматривают единым множеством. Но состав кортежей данных зависит от воздействующих факторов [56]. К примеру, увеличение объемов служебных сообщений в сетевом трафике может свидетельствовать об активности лиц, инициирующих управляющие команды. Мощности, потребляемые в электросетях, зависят от уменьшения продолжительности дня в зимнее время и наоборот – в летнее. Возникают изменяющие состояние систем воздействия, зачастую в реальных КСТ. Если такие факторы возникают случайно, то их невозможно спрогнозировать и предпринять определенные шаги, для явных факторов такая возможность есть. Но, в любом случае, высока цена ошибки.

Полагая, что имеются влияющие факторы, способные изменять значения переменных анализируемых объектов, можно сформировать кортежи, полученные при воздействии данных факторов.

Тогда появляется возможность произвести сегментирование данных, при учете влияния на свойства данных факторов.

Имеется:

– анализируемые объекты данных .

– множество классифицирующих моделей.

– множество влияющих факторов, способные изменять диапазоны значений переменных. Часть факторов возможно выявить анализируя изменения структуры и свойств данных. Другая часть является связной, поддающейся аналитике, может характеризоваться цикличностью процессов. При этом, функцией принадлежности можно формализовать влияющие факторы.

– функция разбиения, которая сегментирует выборку на сегменты , в которых изменялись диапазоны значений целевых переменных под влиянием фактора .

Функция делит исходное множество на отдельные подмножества – сегменты , где – множество сегментов выборки . На отдельных сегментов делится временная последовательность. Получается разбивка данных, которую можно воспринимать как сегменты по временным последовательностям. Каждый сегмент имеет свои свойства (плотность вероятности распределения данных, частота объектов наблюдений, и т.д.). В ходе разбивки могут появиться сегменты с одинаковыми свойствами. Тогда, вводится функция , уточняющая свойства сегмента и экономящая вычислительные ресурсы. Также, появляется возможность сформировать объединением сегментов подвыборки, если значение лежит в диапазоне , где и – пороговые значения.

Каждая классифицирующая модель имеет свои качественные показатели, вычисляемые в процессе обучения, в зависимости от базовых моделей и состава данных подвыборки.

– функционал качества модели для подвыборки .

Тогда необходимо выбрать модели , которая на подвыборке данных обладает наилучшими качественными показателями:

Иллюстрация метода [57] показана на рисунке 34. На отдельные сегменты разделяется область данных. На каждый сегмент назначается собственная модель, исходя из свойств данных. На основе значений функционала качества определяется модель и ее назначение, затем и набор алгоритмов классификации. Входные данные делятся на сегменты, и рассчитываются функция потерь для классификаторов МО. Далее, на каждый сегмент назначается своя классифицирующая модель в зависимости от полученных значений.

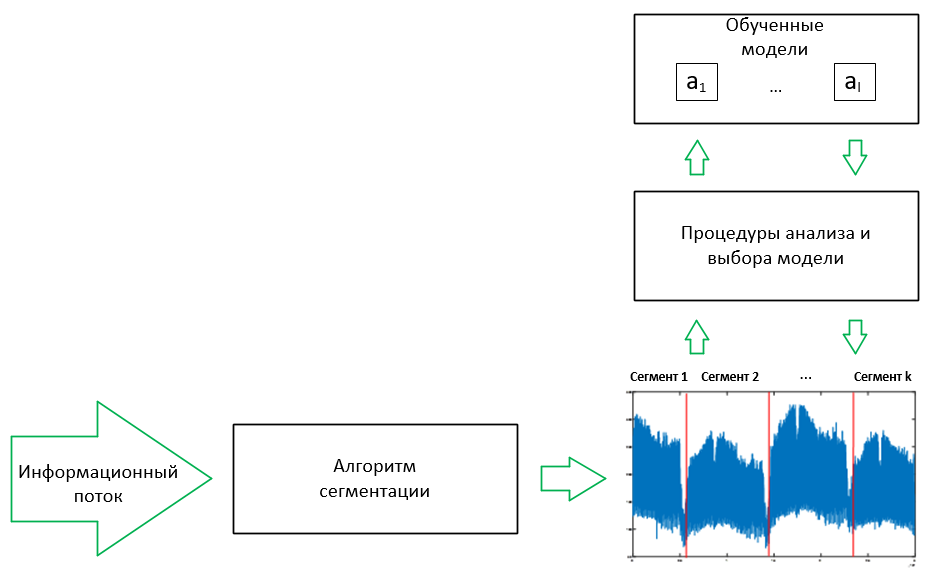


Рисунок 34 – Иллюстрация предлагаемого метода

Алгоритм сегментирования в виде блок-схемы представлен на рисунке 35.

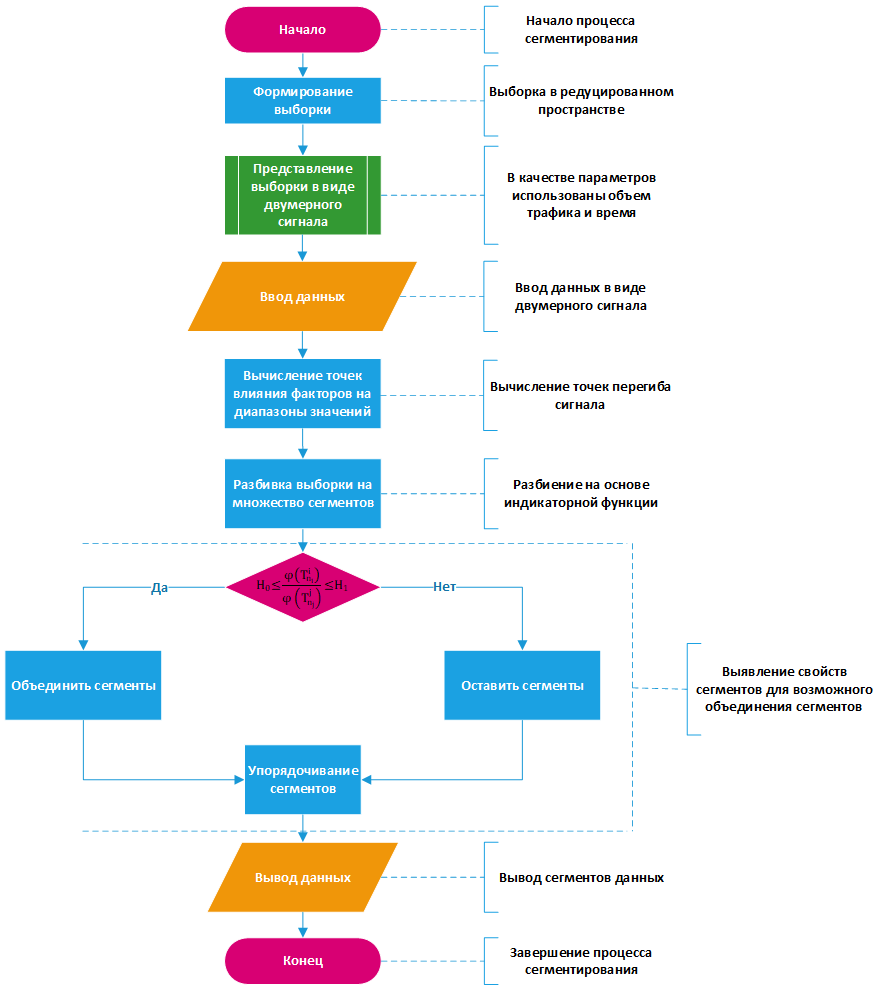


Рисунок 35 –Алгоритм сегментирования выборки данных

Таким образом, сегментирование данных лежит в основе предлагаемого метода. Для каждого сегмента назначаются наиболее подходящие классифицирующие модели, после вычисления свойств данных. Также, имеется возможность использования моделей для каждого сегмента, и данные модели будет легко интерпретировать.

При практической реализации метода возможно делить принимаемые на входе последовательности на сегменты, в режиме реального времени, наряду с анализом свойств и предобработкой поступающей информации.

Пример постоянно обучающейся модели с последовательностью шагов может быть схематично представлен как на рисунке 36.

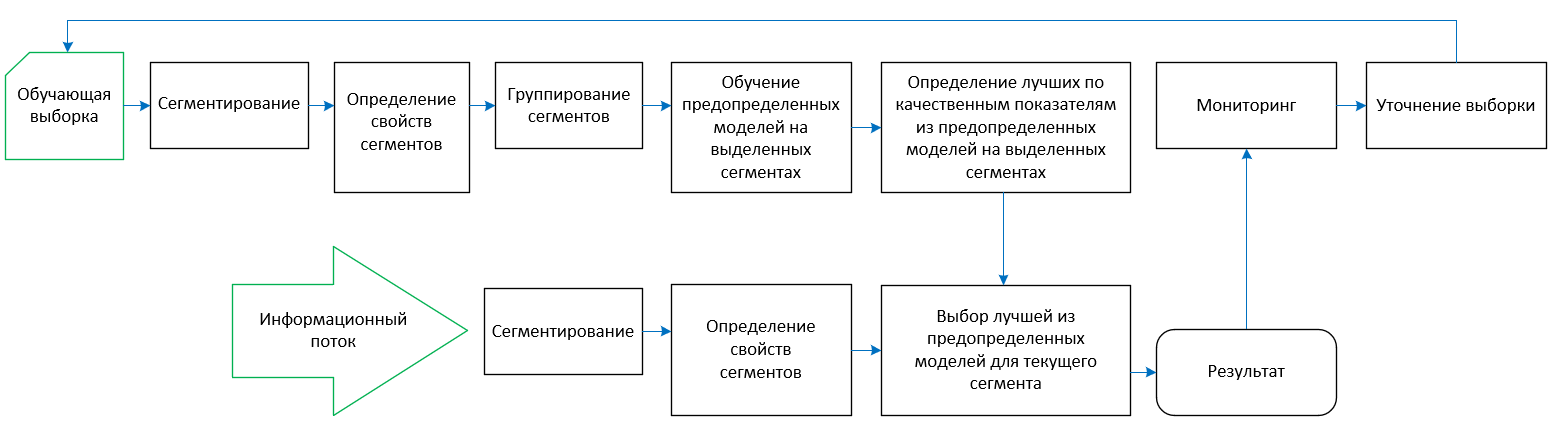


Рисунок 36 – Блок-схема постоянно обучающейся модели

с последовательностью шагов

Модель состоит из двух уровней. Первый уровень обрабатывает непрерывный информационный поток. Второй уровень ведет обучение модели.

– сформируем множество для обучения. Оно будет являться основой, чтобы выделить отдельные сегменты с разными свойствами.

Для обнаружения изменения свойств данных возможно применение процедуры поиска момента , когда меняются характеристики анализируемого процесса (изменение частоты, линии тренда и др.):

В итоге, множество разделяется на подмножества . Затем производится анализ свойств полученных подмножеств. Число подмножеств возможно уменьшить, если предопределенные параметры совпадают.

На подмножествах обучаются модели . Производится анализ качественных показателей. Определяется функция потерь для каждой модели на каждом сегменте . Данную функцию потерь нужно минимизировать, используя выражение - . Значения функции позволяют упорядочить модели и назначать модель с наилучшими качественными показателями на каждый полученный сегмент.

Процедуры выявления свойств данных и сегментирования поступающего на вход информационного потока выполняются на первом уровне постоянно обучающейся модели. Корректно назначить одну из предобученных моделей на текущий сегмент позволяет анализ найденных при обработке информационного потока свойств сегментов, и сопоставление их со свойствами подмножеств, полученных из обучающей выборки.

На последнем этапе, модель , назначенная конкретному сегменту, будет решать задачу обработки информационного потока. Анализ фактических значений и значений, полученных моделью, позволяет формировать данные для уточнения модели. Эти данные затем добавляются в выборке для обучения модели. Следовательно, реализуется постоянно обучающаяся модель, где параллельно осуществляются процессы обработки информационных потоков и обучения. Когда наблюдается изменение свойств данных, предварительно обученные модели уменьшают временные затраты на обучение, при условии использования сложных моделей регрессии или классификации.

**2.4 Методика идентификации вредоносного трафика**

2.4.1 Постановка задачи

Данные из реальных систем имеют несовершенную форму. В то же время могут изменяться свойства данных в различных областях выборки. В результате дрейфа концепта, может возникать парадокс Симпсона. Отдельные области выборки могут быть лучше классифицированы различными классификаторами.

Чтобы реализовать практические методы, становится возможным выявить ряд оказывающих влияние на свойства и структуру данных факторов. Повышение качества классифицирующих алгоритмов происходит за счет использования информации о влияющих на значения показателей факторов. Более подробно методика сегментирования выборки данных с учетов воздействующих факторов приведена в работе [58].

Постановку задачи представим в формализованном виде.

– множество анализируемых объектов, – это -мерные кортежи значений атрибутов в векторном пространстве .

Объектам ставятся в соответствие метки , разбивающие выборку на бинарное подмножество состояний - классов .

- множество факторов, влияющих на значения атрибутов.

- множество, характеризующее объекты .

При воздействии на объект в текущее время фактора определяется признаковое описание анализируемого объекта как при заданных .

Обучающее множество преобразуется в – размеченная по классам выборка, где – количество кортежей в момент, когда оказывал влияние -й фактор .

Ставится задача разработки алгоритма классификации, который учитывает влияние фактора , . Алгоритм должен учитывать влияние фактора при сопоставлении класса конкретному объекту, на основе анализа его признакового описания.

2.4.2 Описание методики

Имеется классификатор . На вход классификатора подается кортеж атрибутов . Весовая матрица будет использоваться для принятия решения. Сегментирование возможно осуществить двумя методами: применением функции принадлежности и реализацией продукционных правил.

Использование продукций для поставленной задачи классификации предполагает, что предопределенные факторы, влияющие на свойства данных, поддаются эвристике. С учетом воздействий на данные, это дает возможность сформулировать определенные правила. Например, можно сформулировать ряд продукционных правил основываясь на периодичности возникновения производственных процессов в энергетике, перерабатывающей отрасли, экономике, финансовой отрасли и др. Предикативный вид такой модели представляется в следующем виде (27):

где – алгоритмы классификации, которые для сравнения поступающих кортежей данных используют весовые матрицы;

– множество факторов, оказывающих влияние на значения переменных в анализируемой выборке;

– множество матриц весов классифицирующих алгоритмов, значения таких матриц зависят от влияющего на данные фактора в системе;

– состоящее из подмножества выборок данных анализируемое множество объектов, где каждому подмножеству назначены собственные весовые матрицы алгоритмов классификации.

Выбор значений осуществляется с помощью продукционной модели. С учетом влияния фактора определяется подмножество данных . Алгоритм классификации назначается каждому подмножеству. Происходит группировка в виде «влияющий фактор ‒ подмножество» , и определяется матрица с учетом свойств алгоритмов классификации. Реализующая данное правило продукция, представляется в виде:

Выражение (28) необходимо для использования матрицы после определения текущего воздействия .

Классифицирующий алгоритм идентифицирует поступающий на вход новый кортеж .

Это дает возможность в будущем разрабатывать правила не только для сегментирования выборок данных, но и для отбора подходящего алгоритма классификации при воздействии фактора. В этом проявляются преимущества, связанные с улучшением показателей качества алгоритмов с учетом изменений в данных.

Следующее направление основывается на функции принадлежности. Оно применяется при наличии воздействий, поддающихся аналитическому описанию (повышение объема сетевого трафика в рабочее время и уменьшение в нерабочее время, повышение объемов трафика при репликации почтовых серверов, повышение количества сетевых пакетов, направленных к конкретному компоненту системы – можно предположить о попытках воздействий и др.). С помощью функции принадлежности (индикаторной функции) могут быть обработаны приведенные выше факторы . На ее основе производится разбиение выборки данных на конечное число не пересекающихся измеримых подмножеств . Функция принадлежности подмножества , где – кортеж обучающей выборки, в простейшем случае, может быть представлена в виде:

Выражение (29) позволяет в момент действия фактора определить принадлежность элемента выборки данных подмножеству .

Анализируемая выборка состоит из подмножеств . Функциями определяется принадлежность подмножеству.

- полученное разбиение, при условии . При объединении подмножеств получается множество, без пересечений подмножеств.

На каждом из подмножеств становится возможным осуществить классификацию. Формируется обучающая и тестовая выборка с учетом влияющих факторов . Алгоритм классификации может быть дополнен функцией , в зависимости от обрабатываемого подмножества. Функция определяет по значению влияющего на подмножество фактора весовую матрицу . Тогда классифицирующий алгоритм преобразуется в вид .

Функция потерь применяется в качестве одной из мер оценки модели.

Для подмножества функция потерь находится выражением

Для данных множества средняя сумма потерь будет равна

Минимизируя среднюю сумму потерь с применением выражений (30) и (31), можно вычислить оптимальные параметры

Используя методику [58, с. 29-37], в комбинации с выражением (32), появляется возможность с учетом влияющих факторов осуществить сегментирование анализируемых множеств на подмножества.

Методика в виде блок-схемы показана на рисунке 37.

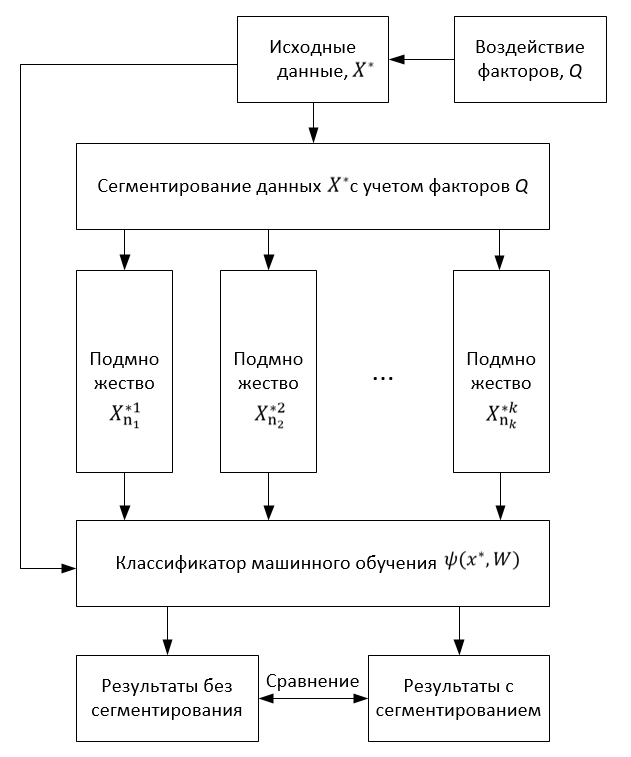


Рисунок 37 – Блок-схема методики идентификации вредоносного трафика

Экспериментальная оценка методики с результатами сравнения без сегментирования и с сегментированием будет представлена в 3 разделе исследования.

2.4.3 Описание ансамбля классификаторов

Методы машинного обучения преимущественно являются основой при анализе сетевого трафика. Положительным качеством подходов на основе МО является универсальность и автоматическое извлечение признаков, без участия эксперта. Однако современные атаки на телекоммуникационные сети и оборудование каждый раз проявляют свою уникальность и неповторимость, ввиду специфики направления ИБ. Наряду с этим, растет число шифрованных соединений (P2P-сервисов, HTTPS) с применением методов сжатия данных. Следовательно, в сети возникают проблемы, связанные с интерпретацией информационных воздействий и для разного рода атак, проблемы с извлечением анализируемых признаков, проблемы определения входных параметров, функционирования алгоритмов. В связи с этим, предлагается метод выявления в КСТ аномальных ситуаций, на основе бэггинга, которой, при практической реализации позволит сопоставлять результаты классифицирующих алгоритмов для целей анализа деструктивных воздействий.

В работе [59] показано формализованное описание построения ансамбля классификаторов МО.

Рассматривается меняющееся во времени, под внутренними и внешними воздействиями, конечное множество состояний системы .

Имеется выборка, где получены значения анализируемых признаков для - различных состояний системы, что позволяет произвести сопоставление кортежей сетевого трафика из множества каждому состоянию.

По кортежам определяется множество состояний , где -количество записей в выборке, которое отражает поведение процесса в разных состояниях.

) содержит кортеж значений признаков с длиной , где – количество признаков.

Множество бинарных классов , предварительно разбитое на подмножества опасных и безопасных , отражает множество состояний системы.

В результате, получается конечная обучающая выборка, размеченная по классам опасности и состоящая из кортежей:

Требуется для , входного кортежа значений, разработать классифицирующий алгоритм , производящий отображение , где – количество базовых алгоритмов МО в ансамбле.

На основе решающего правила алгоритма , которое вычисляется функцией , приводящей к разбиению пространства на две непересекающиеся области, определяется соответствие текущего наблюдения одному из подмножеств или :

где – пороговое значение.

Вследствие особенности реализации функции , разделяющей пространство в задачах идентификации аномалий в трафике, для классифицирующего алгоритма возникает ошибка, которая сглаживается последовательностью независимо обученных друг от друга базовых алгоритмов МО .

Тогда ответ алгоритма , с учетом бинарной классификации, позволяет определить принадлежащий бинарному множеству классов опасных и безопасных состояний класс подмножеств .

– апостериорная вероятность для -го алгоритма МО после процедуры обучения.

Вероятность принадлежности к классу поступающего на вход кортежа, при использовании по отдельности алгоритмов , будет находиться по формуле:

На основе значений функций и для бинарного подмножества и возможно определить предсказываемый ансамблем классификаторов для кортежа результирующий класс:

Следующим выражением можно реализовать ансамбль базовых алгоритмов:

где – решающее правило, позволяющее установить номер класса и определить вероятностную оценку. На рисунке 38 показана схема работы бэггинга.

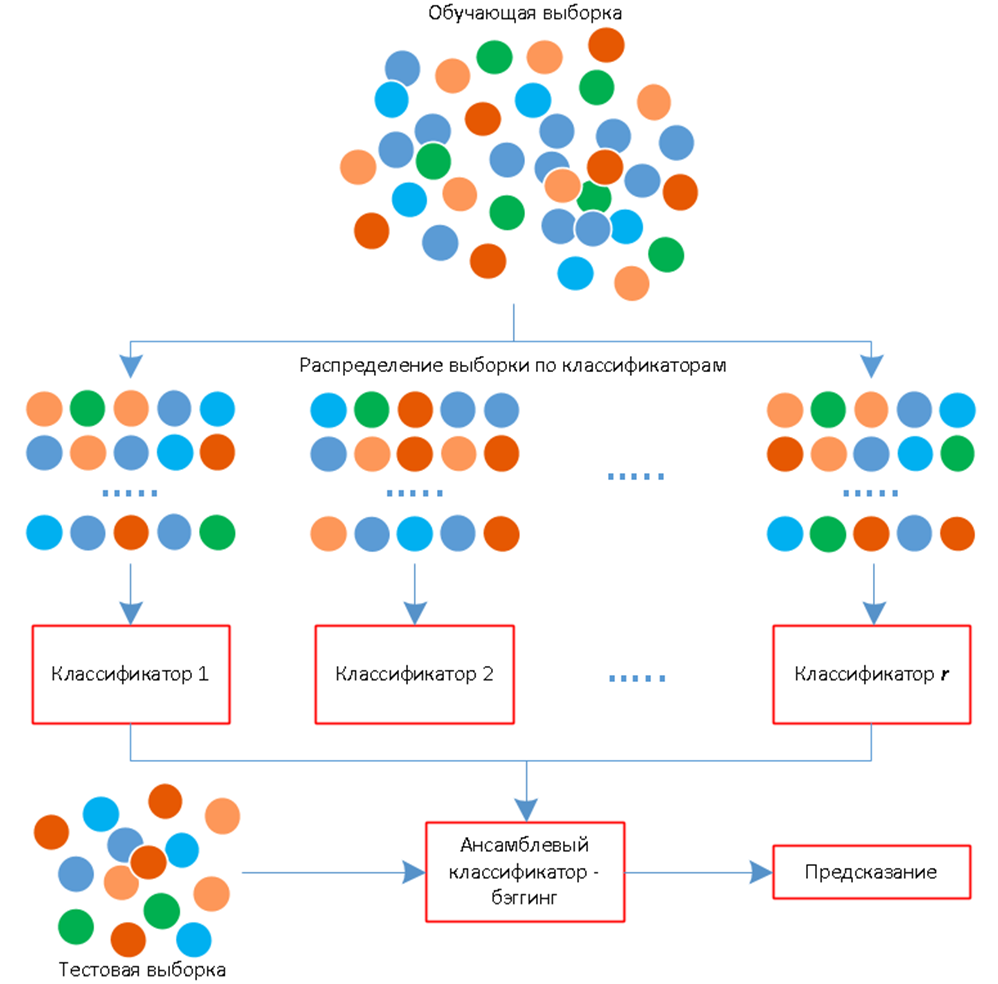


Рисунок 38 – Схема работы бэггинга

В итоге, применяемое решение основано на бинарной классификации. Обобщение формализации производится решающим правилом, которое переводит оценку в номер класса. Используется вспомогательное множество (пространство оценок) для подсчета результатов ансамбля. Для достижения разнообразия алгоритмов, включенных в ансамблевую модель, они обучаются независимо друг от друга на случайно выбранных и несбалансированных подмножествах обучающей выборки.

**Выводы по разделу 2**

В целях повышения качественных показателей идентификации сетевого трафика и снижения вычислительных затрат при реализации методов МО возможно применение описанных в разделе 2 моделей и алгоритмов.

Выявление наиболее информативных признаков методом главных компонент дает существенное уменьшение объемов обрабатываемых данных без потери полезной информации. Как следствие, исключается риск переобучения модели и недостоверности полученных результатов. Метод главных компонент является фундаментальным методом в области интеллектуального анализа данных. Преобразование многомерных данных в более низкоразмерную форму, сохраняя при этом важную информацию, в МГК достигается путем определения новых осей, называемых главными компонентами, по которым данные изменяются больше всего. Эти компоненты ортогональны друг другу, то есть они некоррелированы, что делает их мощным инструментом уменьшения размерности.

Необходимо, с учетом влияния на данные факторов, разбивать анализируемое множество на подмножества, чтобы повысить качественные показатели методов машинного обучения, на которые влияют изменения плотности вероятности возникновения событий, шумы, выбросы данных. К таким факторам относятся сезонность, неисправности оборудования, нетипичное объемы передаваемых по сети данных и др. Выявление и постоянный мониторинг таких факторов способствует более глубокому пониманию происходящих в сети процессов.

Действие факторов оказывает влияние на структуру данных. В результате становится возможным разделение множества по границам влияния факторов при помощи метода сегментирования данных. Это позволит назначать эффективные классификаторы МО на отдельные сегменты сетевого трафика. Кроме указанных преимуществ сегментирования, имеется ряд других, связанных с маркировкой данных, эффективностью управления сегментами, категоризацией атак и уязвимостей.

Далее, в рамках исследования, при решении задачи идентификации вредоносного трафика методами МО, возникает необходимость выбора лучших классификаторов. Это многоитерационный процесс. Тем более, одни классификаторы могут показать различные результаты на разных наборах данных. Необходимо искать более универсальные решения. В результате, предлагается ансамблевый метод, с применением бэггинга классификаторов, который в комплексе поможет улучшить показатели точноcти классификации, нежели использование единичных классификаторов.

Все экспериментальные оценки решений представлены в разделе 3.

## **АНАЛИЗ ПРЕДЛОЖЕННЫХ МОДЕЛЕЙ, МЕТОДОВ И АЛГОРИТМОВ К ЗАДАЧЕ ИДЕНТИФИКАЦИИ ВРЕДОНОСНОГО ТРАФИКА**

## **3.1 Представление данных**

Анализируемая выборка, отражающий дамп сетевого трафика, представляется в виде таблицы – «объекты-признаки-класс». Пример представлен в таблице 6.

Таблица 6 – Выборка в виде «объекты-признаки-класс»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Объекты, | Признаки, | | | | Класс, |
|  |  |  | … |  |  |
|  |  |  | … |  |  |
| … | … | … | … | … | … |
|  |  |  | … |  |  |

Оценка предлагаемых методов и решений, в рамках исследования, была проведена на наборе данных NSL-KDD [60]. Описание признаков данного набора представлена в таблице 7.

Таблица 7 – Описание признаков набора NSL-KDD

|  |  |  |
| --- | --- | --- |
| Название признака | Категория признака | Описание признака |
| 1 | 2 | 3 |
| Duration | Основные признаки (Basic Features), для анализа трафика общего назначения | Длительность времени сеанса связи |
| Protocol\_type | Протокол, используемый в сеансе связи |
| Service | Используемый сервис |
| Flag | Флаг |
| Src\_bytes | Количество переданных от источника получателю байтов данных, в пределах одного сеанса связи |
| Dst\_bytes | Количество переданных от получателя источнику байтов данных, в пределах одного сеанса связи |
| Land | Этот параметр принимает значение 1 если IP-адреса источника и получателя с номерами портов равны, если нет то 0 |
| Wrong\_fragment | Число ошибочных фрагментов в пределах одного сеанса связи |
| Urgent | Количество срочных пакетов (пакеты с активиро ванным битом срочности) в пределах одного сеанса связи |
| Hot | Признаки контента (Content Features), ищут подозри тельное поведение, | Количество «горячих» индикаторов данных, таких как: выполнение программ, создание программ и вход в системный каталог |
| Num\_failed\_logins | Количество неудачных попыток аутентификации |
| Продолжение таблицы 7 | | |
| 1 | 2 | 3 |
| Logged\_in | например, коли чество неудачных | Этот параметр принимает значение 1 при успешном входе в систему; 0 при неудачном |
| Num\_compromised | попыток входа. | Количество «компромиссных» условий |
| Root\_shell | Этот параметр принимает значение 1 при корневом доступе; иначе 0 |
| Su\_attempted | Этот параметр принимает значение 1 если имеется попытка использования команды «su root»; иначе 0 |
| Num\_root | Количество обращений «root» или количество операций, выполненных в качестве корневого в соединении |
| Num\_file\_creations | Количество операций по созданию файла при подключении |
| Num\_shells | Количество подсказок оболочки |
| Num\_access\_files | Количество операций с файлами контроля доступа |
| Num\_outbound\_cmds | Нумерация исходящих команд в ftp-сессии |
| Is\_hot\_login | Этот параметр принимает значение 1 если логин принадлежит к корневому или администраторскому списку; иначе 0 |
| Is\_guest\_login | Этот параметр принимает значение 1 если логин – «гость»; иначе 0 |
| Count | Характеристики трафика с привязкой к времени (Time-based Traffic Features). Трафик, основанный на времени, состоит из функций «тот же хост», которые проверяют соединения за последние 2 секунды, которые имеют тот же самый целевой хост, что и текущее соединение. В эту категорию также входят функции «тот же сервис», которые прове ряют соединения | Количество подключений за последние две секунды к тому же самому узлу назначения, что и текущее соединение |
| Srv\_count | Количество подключений за последние две секунды к той же услуге (номер порта), что и текущее соединение |
| Serror\_rate | Процент сеансов, с активацией флага (4) s0, s1, s2 или s3, среди соединений, агрегированных в сount (23) |
| Srv\_serror\_rate | Процент сеансов, с активацией флага (4) s0, s1, s2 или s3, среди соединений, агрегированных в srv\_count (24) |
| Rerror\_rate | Процент сеансов, с активацией флага (4) REJ, среди соединений, агрегированных в сount (23) |
| Srv\_rerror\_rate | Процент сеансов, с активацией флага (4) REJ, среди соединений, агрегированных в srv\_count (24) |
| Same\_srv\_rate | Процентное соотношение подключений к одной и той же услуге, среди подключений, агрегированных в сount (23) |
| Diff\_srv\_rate | Процентное соотношение подключений к различным службам, среди подключений, агрегированных в сount (23) |
| Продолжение таблицы 7 | | |
| 1 | 2 | 3 |
|  | за последние 2 секунды, имеющие тот же сервис, что и текущее соединение |  |
| Srv\_diff\_host\_rate | Характеристики трафика на базе хоста (Host-based Traffic Features). Обнаружение атак, использующих больший промежуток времени, чем 2 секунды, осуществляется с помощью функций трафика хоста, который состоит из 100 соединений и соответствует функциям трафика на основе времени. | Процент подключений, которые были к различным машинам назначения среди подключений, агрегированных в srv\_count (24) |
| Dst\_host\_count | Количество сеансов с одинаковыми IP-адресами устройства назначения |
| Dst\_host\_srv\_count | Количество сеансов с одинаковыми номерами порта |
| Dst\_host\_same\_srv\_rate | Соединения (в процентах) к одному и тому же сервису, среди подключений, агрегированных в dst\_host\_count (32) |
| Dst\_host\_diff\_srv\_rate | Соединения (в процентах) к различным службам, среди подключений, агрегированных в dst\_host\_count (32) |
| Dst\_host\_same\_src\_port\_rate | Соединения (в процентах), которые были к одному и тому же порту источника, среди соедине ний, объединенных в dst\_host\_srv\_count (33) |
| Dst\_host\_srv\_diff\_host\_rate | Соединения (в процентах), которые были к различным машинам назначения, среди подключений, агрегированных в dst\_host\_srv\_count (33) |
| Dst\_host\_serror\_rate | Соединения (в процентах), с активацией флага (4) s0, s1, s2 или s3, среди соединений, агрегированных в dst\_host\_count (32) |
| Dst\_host\_srv\_serror\_rate | Соединения (в процентах), с активацией флага (4) s0, s1, s2 или s3, среди соединений, агрегированных в dst\_host\_srv\_count (33) |
| Dst\_host\_rerror\_rate | Соединения (в процентах), с активацией флага (4) REJ, среди соединений, агрегированных в dst\_host\_count (32) |
| Dst\_host\_srv\_rerror\_rate | Соединения (в процентах), с активацией флага (4) REJ, среди соединений, агрегированных в dst\_host\_srv\_count (33) |

Здесь представлена основная информация о потоке IP, включая задействованные устройства, используемые порты и протокола передачи данных, продолжительность потока, объем передаваемых данных и др.

## **Анализ модели формирования признакового пространства сетевого трафика**

Модель признакового пространства была сформирована применением метода главных компонент. Экспериментальная оценка метода была проведена на NSL-KDD – публично распространяемом наборе данных. Выборка была поделена в пропорции 50/50 на две части: первой частью производилось обучение модели, второй частью тестировали модель. Обучение и тестирование классифицирующих алгоритмов проводилось с использованием инструмента Weka. Для оценивания моделей применялись алгоритмы NaiveBayes и DecisionStump.

Схема эксперимента представлена на рисунке 39.

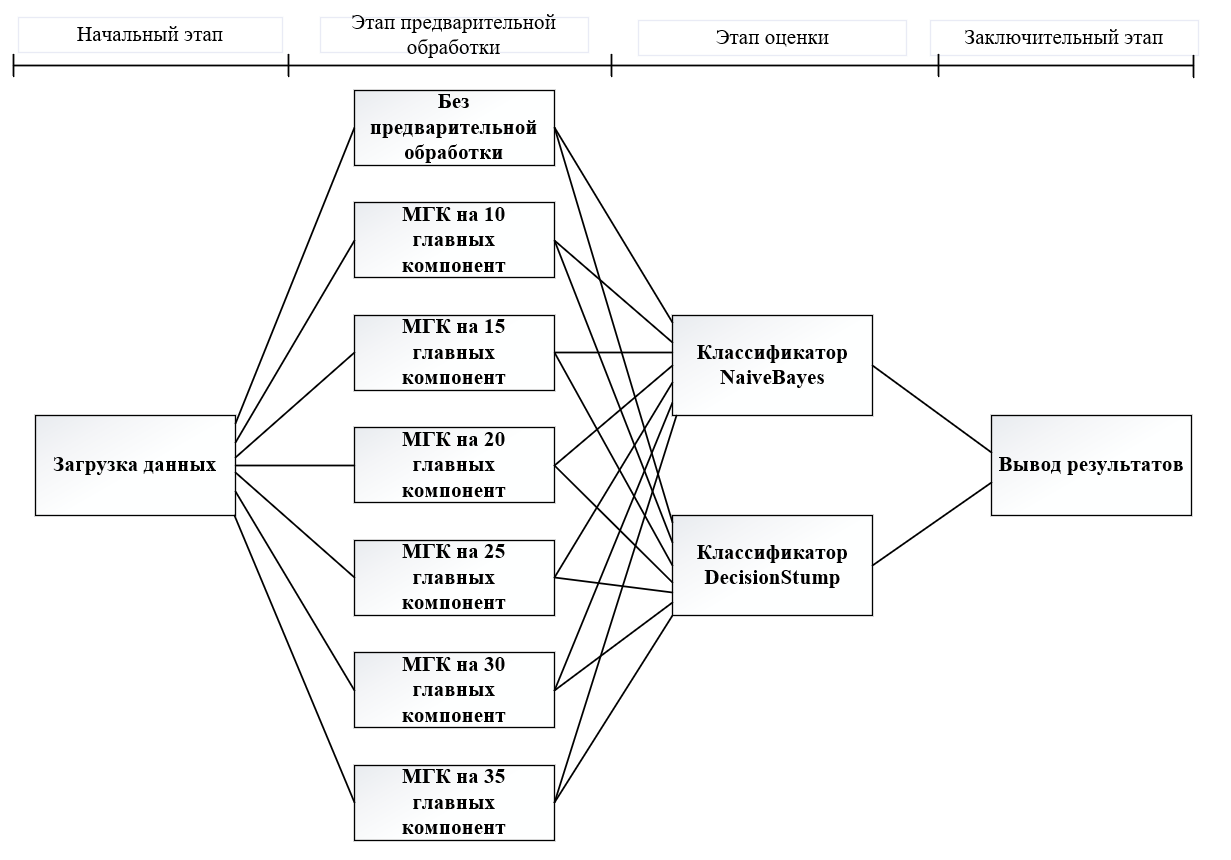


Рисунок 39 – Схема работы бэггинга

Начальный этап предполагал загрузку датасета в приложение Weka с локального репозитария. На этапе предварительной обработки использовался МГК с настройками количества главных компонент от 10 до 35. На этапе оценки была произведена классификация данных по классам опасности. На заключительном этапе произведен вывод и фиксация результатов оценки.

Результаты эксперимента представлены в таблице 8.

Таблица 8 – Результаты эксперимента с использованием МГК

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Этап предварительной обработки | Классификатор | Accuracy, % | Precision, % | Recall, % | F-Measure, % | ROC Area, % |
| Без МГК | NaiveBayes | 80.7 | 84.5 | 80.7 | 80.7 | 95.5 |
| DecisionStump | 81.4 | 84.8 | 81.5 | 81.5 | 83.2 |
| Продолжение таблицы 8 | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| МГК 10 | NaiveBayes | 87.1 | 87.6 | 87.1 | 87.2 | 94.5 |
| DecisionStump | 84.6 | 84.7 | 84.7 | 84.6 | 83.9 |
| МГК 15 | NaiveBayes | 87.2 | 87.7 | 87.3 | 87.3 | 94.5 |
| DecisionStump | 84.6 | 84.7 | 84.7 | 84.6 | 83.9 |
| МГК 20 | NaiveBayes | 86.5 | 86.8 | 86.5 | 86.6 | 94.3 |
| DecisionStump | 84.6 | 84.7 | 84.7 | 84.6 | 83.9 |
| МГК 25 | NaiveBayes | 90.0 | 90.1 | 90.0 | 90.0 | 95.3 |
| DecisionStump | 84.6 | 84.7 | 84.7 | 84.6 | 83.9 |
| МГК 30 | NaiveBayes | 86.6 | 87.9 | 86.6 | 86.7 | 95.1 |
| DecisionStump | 84.6 | 84.7 | 84.7 | 84.6 | 83.9 |
| МГК 35 | NaiveBayes | 80.7 | 85.0 | 80.8 | 80.7 | 94.9 |
| DecisionStump | 84.6 | 84.7 | 84.7 | 84.6 | 83.9 |

Гистограмма результатов МГК представлена на рисунке 40.

Рисунок 40 – Гистограмма результатов МГК

По результатам эксперимента удалось улучшить точность классификатора NaiveBayes на 11%, и классификатора DecisionStump на 4% на наборе данных NSL-KDD. Результаты подтверждают эффективность применения метода главных компонент для уменьшения признакового пространства анализируемых данных без потери качества.

## **Анализ метода повышения качественных показателей (полноты и точности) идентификации вредоносного трафика**

Метод основывается на применении сегментирования исходной выборки. Датасет NSL-KDD был использован для оценивания метода сегментирования, в рамках проведения эксперимента. Выборка NSL-KDD Test содержит в себе 22544 текстовых записей значений параметров сетевого трафика, среди которых 9711 с меткой нормального трафика, 12833 записей с меткой аномального (вредоносного) трафика. Выборка, поделенная на две части – для обучения и тестирования моделей. Структура датасета представляет собой значения 41 атрибута, таблица 7.

В целях обучения классифицирующих алгоритмов использовался свободно распространяемый инструмент Weka со стандартными настройками.

Первая часть эксперимента предполагала применение библиотеки «ruptures» [61] перед проведением сегментирования данных. На рисунке 41 показаны точки разладки и перегиба выборки NSL-KDD Test, представленного в виде двумерного сигнала.

Рисунок 41 – Определение точек разладки и перегиба, которые являются границами сегментирования, по горизонтальной оси расположено время (time), по вертикальной оси объем данных (volume), передаваемых от источника к узлу назначения в пределах одного сеанса

В итоге, выборка данных была разделена на сегменты. Каждый из которых имеет свои характеристики, относящиеся к тенденции и диапазону статистических данных. Было обучены классификаторы Hoeffding Tree (HT), OneR на всех полученных сегментах и определены значения параметров данных сегментов.

С помощью выражения (22) и рассматривая требуемый показатель качества, можно назначить свой классификатор с наилучшими показателями на конкретный сегмент.

Полученные в ходе эксперимента, при выборе наилучших классификаторов, средние значения, посегментные показатели и показатели по всей анализируемой выборке приведены на гистограммах (рисунок 42).

а

б

в

Рисунок 42 – Гистограммы результатов, лист 1

г

Рисунок 42, лист 2

Гистограммы демонстрируют возможности улучшения качества анализа выборки целиком, с применением метода сегментирования выборки, и назначая сегментам классификаторы с наилучшими характеристиками.

Сегментирование выборки обладает преимуществами борьбы с нежелательными шумами и выбросами, и позволяет создавать в пространстве объектов локализованные компактные подмножества. Сегментированием возможно улучшить показатели качества классификаторов ориентировочно на 5%, нежели классифицировать всю выборку сразу. Но, необходимо учитывать, что классификаторы МО чувствительны к свойствам данных для обучения и тестирования, и это непосредственно оказывает влияние на эффективность.

## **3.4** **Анализ методики идентификации вредоносного трафика**

NSL-KDD – набор данных, который был использован для оценки методики идентификации вредоносного трафика. Эксперимент предполагал бинарную классификацию состояний КСТ (идентификации нормального и вредоносного трафика). Формализация была обобщена переводящим оценку в номер класса решающим правилом. Пространство оценок (вспомогательное множество) было использовано для подсчета результатов предлагаемого ансамбля классификаторов МО.

Обучение моделей производится для каждого подмножества независимо, как на несбалансированных подмножествах, так и на случайно выбранных подмножествах обучающей выборки, в целях достижения различности классификаторов, входящих в ансамбль. Анализируется несбалансированная выборка для достижения показателей качества ансамбля.

Отбор классификаторов для построения ансамбля стал одним из проблемных вопросов бэггинга. Не существует строгих правил, стандартов или рекомендаций формирования обучающих выборок. Значительная часть исследований описывает задействование «слабых» алгоритмов классификации МО в ансамбле. В других исследованиях авторы рекомендуют исключать обучающие подвыборки, устойчивые к изменениям, для обеспечения необходимых условий достижения «различности» алгоритмов классификации. В работе [62] рассмотрено комбинированное применение относительно слабых и точных алгоритмов. Исследовано объединение нескольких ансамблей, в которых есть алгоритмы, неравнозначные по показателям качества [63]. Имеются подходы, предполагающие применение многоуровневого стекинга и блендинга [64, 65].

Так как нет правил, регламентирующих состав ансамбля, такая работа требует дополнительных экспериментов и исследований. Выбор нужной модели производится по сути задачи, где заранее определяется состав алгоритмов и будет затруднено его изменение. Алгоритмы классификации могут быть как слабыми, так и сильными, исходя из возможностей по обучению и формированию обучающей выборки, характеру возникающих аномалий и зависимости от условий работы системы. Поэтому возникает необходимость изучения характеристик при разных условиях.

Важной составляющей разработки эффективной модели является формирование обучающей выборки. На практике, вызывает затруднение формированию обучающих подмножеств. Не всегда получается определить необходимую вероятность появления объектов и признаков в генеральной совокупности. Данный процесс тяжело поддается прогнозированию. Проблемы при формировании подвыборок для обучения связаны с корректной интерпретацией обнаружений, и разделением штатных служебных состояний и значимых событий и закономерностей, разбалансировкой, появлением сторонних закономерностей формирования множеств для обучения, не точными значениями признаков, отсутствием объектов для обучения конкретных компонентов и всей признаковой системы [66].

Эксперимент предполагал случай использования в ансамбле комбинации слабых и сильных алгоритмов МО. Разнообразие классификаторов достигалось составом обучающей выборки. Оценка была произведена на основе алгоритмов МО, реализованных в инструменте Weka: REP Tree (REP), Random Tree (RT), Random Forest (RF), J48, Hoeffding Tree (HT), Naïve Bayes (NB).

Выборка для анализа была предварительно размечена и разделена на пару частей – тестирования и обучения. Признаковое пространство состояло из более чем 40 атрибутов. В работе [60, р. 92-95] представлено описание всех атрибутов.

Набор данных представлен в виде последовательности кортежей КЗСП, где 50% кортежей размечено как аномальный (вредоносный) и 50% – нормальный, не представляющий угрозы.

Набор, в рамках эксперимента, делился на пропорции 20/80, 40/60, 60/40 и 80/20, где первая часть пропорции обозначает количество обучающих данных, а нижняя – тестирующих.

Использовались стандартные настройки Weka при обучении классификаторов.

Выражениями (31) и (32) определялись соответствия кортежей выборки для тестирования одному из категорий нормальных или аномальных состояний.

Выборки для обучения составлялись искусственно. Вначале анализ подразумевал несбалансированность данных и для каждого алгоритма конкретные события появляются с разной частотой. Моделировалась обычная ситуация, при котором алгоритм классификации может показывать приемлемые результаты на выборке для обучения, но качественные показатели снижаются если классифицировать тестовые (реальные) данные. Это можно объяснить тем, что в ходе анализа возникают неучтенные признаки и множество для обучения не может полностью характеризовать генеральную совокупность.

Оценка алгоритмов классификации производилась параметром AUC (площадь под ROC-кривой) для тестового подмножества (рисунок 43).

a б

Рисунок 43 – Гистограммы оценки качества алгоритмов классификации по параметру AUC в пропорциях 20/80, 40/60, 60/40, 80/20 при сбалансированной (a) и несбалансированной (б) обучающей выборке

На рисунке 43 представлена бинарная классификация по классам опасности трафика. По гистограммам становится возможным выявить «сильные» и «слабые» алгоритмы, возникшие использованием несбалансированных выборок для обучения, из-за определения неправильных зависимостей, неполноты признаков и т.д.

Параметры Accuracy, Precision, Recall, F-мера были использованы для оценки алгоритмов классификации МО.

В таблице 9 приведены результаты проведенного эксперимента.

Таблица 9 – Значения параметров Accuracy, Precision, Recall и F-мера для алгоритмов классификации, %

| Алгоритмы классификации | Пропорциональные отношения обучающей  к тестирующей выборке | | | |
| --- | --- | --- | --- | --- |
| 20/80 | 40/60 | 60/40 | 80/20 |
| Accuracy | | | | |
| Naïve Bayes | 72,1 | 96,9 | 99,9 | 99,9 |
| Hoeffding Tree | 64,2 | 70,8 | 99,9 | 99,9 |
| J48 | 58,8 | 59,9 | 63,6 | 71,7 |
| Random Forest | 94,5 | 96,8 | 99,7 | 99,9 |
| Random Tree | 81,6 | 86,7 | 96,3 | 99,9 |
| REP Tree | 62,1 | 95,8 | 99,9 | 99,9 |
| Precision | | | | |
| Naïve Bayes | 73,6 | 98,9 | 99,9 | 99,9 |
| Hoeffding Tree | 70,7 | 78,0 | 99,9 | 99,9 |
| J48 | 65,1 | 66,4 | 70,4 | 79,4 |
| Random Forest | 95,6 | 98,0 | 99,9 | 99,9 |
| Random Tree | 86,0 | 91,4 | 99,1 | 99,9 |
| REP Tree | 68,3 | 98,4 | 99,9 | 99,9 |
| Recall | | | | |
| Naïve Bayes | 77,7 | 96,0 | 99,9 | 99,9 |
| Hoeffding Tree | 71,1 | 75,5 | 99,9 | 99,9 |
| J48 | 64,9 | 65,8 | 68,5 | 74,3 |
| Random Forest | 95,1 | 96,7 | 99,7 | 99,9 |
| Random Tree | 83,3 | 86,8 | 95,1 | 99,9 |
| REP Tree | 69,0 | 95,3 | 99,9 | 99,9 |
| F-мера | | | | |
| Naïve Bayes | 75,6 | 97,4 | 99,9 | 99,9 |
| Hoeffding Tree | 70,9 | 76,7 | 99,9 | 99,9 |
| J48 | 65,0 | 66,1 | 69,5 | 76,7 |
| Random Forest | 95,3 | 97,4 | 99,8 | 99,9 |
| Random Tree | 84,6 | 89,0 | 97,1 | 99,9 |
| REP Tree | 68,6 | 96,8 | 99,9 | 99,9 |

Вторая часть эксперимента предполагала реализацию ансамблевого решения (35). Производилась одновременная обработка входных данных, затем, на основании формул (33)-(35) находился класс подмножества , и далее, происходило их сравнение с размеченным множеством для тестирования.

Показатель общей точности классифицирующей последовательности и параметр AUC были выбраны для анализа ансамбля. В таблице 10 показаны результаты использования предлагаемого ансамбля классификаторов.

Таблица 10 – Значения параметров AUC, Accuracy, Precision, Recall и F-мера для алгоритмов классификации, %

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Параметры | Пропорциональные отношения обучающей к тестовой выборке | | | |
| 20/80 | 40/60 | 60/40 | 80/20 |
| для ансамбля классификаторов | | | |
| AUC | 0,8947 | 0,9696 | 0,9999 | 0,9999 |
| Accuracy, % | 95,0 | 99,7 | 99,8 | 99,9 |
| Precision, % | 96,3 | 99,9 | 99,9 | 99,9 |
| Recall, % | 96,2 | 99,6 | 99,8 | 99,9 |
| F-мера, % | 96,2 | 99,8 | 99,9 | 99,9 |

Результаты проведенного эксперимента на датасете NSL-KDD, с использованием инструмента Weka, для реализации и оценки ансамбля классификаторов, показатели 99% точности классификации сетевого трафика по классам опасности.

Основным преимуществом реализованного ансамбля классификаторов являются полученные результаты точности, сопоставимые с результатами исследований [60, р. 92-95; 67], даже на сравнительно небольшой выборке данных. В предлагаемом решении для отдельных классификаторов формируются разбалансированные выборки для обучения, что отличает его от традиционных подходов формирования множества для обучения. Данный аспект позволяет «разнообразить» используемые алгоритмы. На каждой выделенной части событий «специализируется» собственный классификатор. Классификаторы адаптируются под различные аномалии и события, а предлагаемый ансамбль сглаживает возникаемый разброс ответов.

Чувствительность классификаторов к смещению ответов может быть недостатком приведенного решения. Чтобы предупредить возможность появления данного эффекта, необходимо производить предварительный анализ данных, так как при значительном влиянии данного эффекта результаты точности ансамбля могут быть иными.

## **3.5 Анализ применения нейронной сети для классификации сетевого трафика**

Основной целью классификации сетевого трафика является облегчение администрирования сети. Классификация трафика имеет ключевую роль в обеспечении качества сервисов (QoS), планировании сети, обнаружении вторжений, мониторинге сети, анализе тенденций трафика и межсетевого экранирования.

Идея, взятая за основу метода, заключается в том, что разные используемые в КСТ сервисы и приложения, формируют сетевые транспортные потоки, значения признаков которых различаются между собой. При корректном выявлении набора статистических параметров потоков, возможно с высокой долей вероятности предсказать конкретные сервисы и приложения, которые сгенерировали данные потоки [68]. Транспортными потоками будем считать совокупность IP-пакетов в пределах одного сеанса связи, между одним и тем же источником и получателем, с совпадающими протоколами.

Для категоризации сетевых транспортных потоков по приложениям и сервисам, предлагается использовать свободно распространяемую библиотеку глубокого инспектирования пакетов nDPI.

Для проведения эксперимента были собраны реальные данные из тестовой КСТ. Признаки потоков (атрибуты) сетевого трафика, используемых для эксперимента, представлены в таблице 11.

Таблица 11 – Атрибуты потоков сетевого трафика

|  |  |
| --- | --- |
| Название признака | Описание |
| 1 | 2 |
| duration | Продолжительность потока |
| src\_ip | Адрес источника |
| src\_port | Номер порта источника |
| dst\_ip | Адрес получателя |
| dst\_port | Номер порта получателя |
| c\_to\_s\_pkts | Количество переданных пакетов внутри потока от клиента к серверу |
| c\_to\_s\_bytes | Количество переданных данных в байтах внутри потока от клиента к серверу |
| c\_to\_s\_goodput\_bytes | Количество переданной полезной нагрузки в байтах внутри потока от клиента к серверу |
| s\_to\_c\_pkts | Количество переданных пакетов внутри потока от сервера к клиенту |
| s\_to\_c\_bytes | Количество переданных данных в байтах внутри потока от сервера к клиенту |
| s\_to\_c\_goodput\_bytes | Количество переданной полезной нагрузки в байтах внутри потока от сервера к клиенту |
| data\_ratio | Соотношение между переданными клиентом и принятыми сервером пакетами внутри потока |
| iat\_flow\_min | Минимальное время между прибытиями пакетов в потоке |
| iat\_flow\_avg | Среднее время между прибытиями пакетов в потоке |
| iat\_flow\_max | Максимальное время между прибытиями пакетов в потоке |
| iat\_flow\_stddev | Стандартное отклонение времени между прибытиями пакетов в потоке |
| iat\_c\_to\_s\_min | Минимальное время между прибытиями пакетов от клиента к серверу в потоке |
| iat\_c\_to\_s\_avg | Среднее время между прибытиями пакетов от клиента к серверу в потоке |
| iat\_c\_to\_s\_max | Максимальное время между прибытиями пакетов от клиента к серверу в потоке |
| iat\_c\_to\_s\_stddev | Стандартное отклонение времени между прибытиями пакетов от клиента к серверу в потоке |
| iat\_s\_to\_c\_min | Минимальное время между прибытиями пакетов от сервера к клиенту в потоке |
| iat\_s\_to\_c\_avg | Среднее время между прибытиями пакетов от сервера к клиенту в потоке |
| Продолжение таблицы 11 | |
| 1 | 2 |
| iat\_s\_to\_c\_max | Максимальное время между прибытиями пакетов от сервера к клиенту в потоке |
| iat\_s\_to\_c\_stddev | Стандартное отклонение времени между прибытиями пакетов от сервера к клиенту в потоке |
| pktlen\_c\_to\_s\_min | Минимальная длина пакета от клиента к серверу в потоке |
| pktlen\_c\_to\_s\_avg | Средняя длина пакета от клиента к серверу в потоке |
| pktlen\_c\_to\_s\_max | Максимальная длина пакета от клиента к серверу в потоке |
| pktlen\_c\_to\_s\_stddev | Стандартное отклонение длины пакета от клиента к серверу в потоке |
| pktlen\_s\_to\_c\_min | Минимальная длина пакета от сервера к клиенту в потоке |
| pktlen\_s\_to\_c\_avg | Средняя длина пакета от сервера к клиенту в потоке |
| pktlen\_s\_to\_c\_max | Максимальная длина пакета от сервера к клиенту в потоке |
| pktlen\_s\_to\_c\_stddev | Стандартное отклонение длины пакета от сервера к клиенту в потоке |
| Class | Класс, протокол/приложение назначенное nDPI для потока |

Для начала, датасет был проанализирован с помощью ndpiReader, после чего был получен набор размеченных по приложениям потоков данных. Набор был «очищен», из него удалены избыточные метрики, потоки протоколов и приложений. Набор данных разделили в соотношении 70/30 и классифицировали с использованием многослойной нейронной сети, реализованной на Python.

Результаты эксперимента при различных параметрах нейронной сети при соотношении данных 70/30 представлены в таблице 12.

Таблица 12 – Результаты эксперимента при различных параметрах нейронной сети при соотношении данных 70/30

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Параметры НС | identity | logistic | tanh | relu |
| 1 | 2 | 3 | 4 | 5 |
| 8/8/8 | 0.84 | 0.89 | 0.90 | 0.88 |
| 32/32/32 | 0.85 | 0.92 | 0.94 | 0.93 |
| 128/128/128 | 0.84 | 0.93 | 0.94 | 0.94 |
| 8/32/128 | 0.84 | 0.91 | 0.93 | 0.92 |
| 8/128/32 | 0.84 | 0.91 | 0.92 | 0.91 |
| 8/32/8 | 0.84 | 0.88 | 0.91 | 0.91 |
| 8/128/8 | 0.84 | 0.90 | 0.89 | 0.91 |
| 32/8/128 | 0.84 | 0.91 | 0.92 | 0.92 |
| 32/128/8 | 0.85 | 0.90 | 0.93 | 0.93 |
| 32/8/32 | 0.85 | 0.91 | 0.92 | 0.92 |
| 32/128/32 | 0.84 | 0.93 | 0.94 | 0.93 |
| 128/8/32 | 0.84 | 0.92 | 0.91 | 0.92 |
| 128/32/8 | 0.84 | 0.92 | 0.94 | 0.93 |
| 128/8/128 | 0.85 | 0.91 | 0.92 | 0.93 |
| 128/32/128 | 0.83 | 0.92 | 0.93 | 0.93 |
| 8/8/8/8/8 | 0.84 | 0.88 | 0.90 | 0.90 |
| Продолжение таблицы 12 | | | | |
| 1 | 2 | 3 | 4 | 5 |
| 8/32/8/32/8 | 0.84 | 0.86 | 0.89 | 0.90 |
| 32/32/32/32/32 | 0.84 | 0.89 | 0.94 | 0.93 |
| 32/8/32/8/32 | 0.84 | 0.90 | 0.92 | 0.92 |
| 8/32/128/32/8 | 0.84 | 0.88 | 0.92 | 0.91 |
| 128/32/8/32/128 | 0.84 | 0.91 | 0.93 | 0.93 |
| 128/128/128/128/128 | 0.84 | 0.91 | 0.94 | 0.94 |
| 128/256/128 | 0.84 | 0.93 | 0.94 | 0.94 |

По полученным результатам, оставили наилучшие комбинации - число скрытых слоев/функции активации нейронной сети, таблица 13.

Таблица 13 – Наилучшие комбинации результатов

|  |  |  |  |
| --- | --- | --- | --- |
| Параметры НС | logistic | tanh | relu |
| 32/32/32 | 0.92 | 0.94 | 0.93 |
| 128/128/128 | 0.93 | 0.94 | 0.94 |
| 8/32/128 | 0.91 | 0.93 | 0.92 |
| 32/128/8 | 0.90 | 0.93 | 0.93 |
| 32/128/32 | 0.93 | 0.94 | 0.93 |
| 128/32/8 | 0.92 | 0.94 | 0.93 |
| 128/8/128 | 0.91 | 0.92 | 0.93 |
| 128/32/128 | 0.92 | 0.93 | 0.93 |
| 32/32/32/32/32 | 0.89 | 0.94 | 0.93 |
| 128/32/8/32/128 | 0.91 | 0.93 | 0.93 |
| 128/128/128/128/128 | 0.91 | 0.94 | 0.94 |
| 128/256/128 | 0.93 | 0.94 | 0.94 |

Используя параметры НС из таблицы 14 провели классификацию, но уже в соотношении данных 90/10, и получили следующие результаты, таблица 14.

Таблица 14 – Результаты эксперимента при различных параметрах нейронной сети при соотношении данных 90/10

|  |  |  |  |
| --- | --- | --- | --- |
| Параметры НС | logistic | tanh | relu |
| 32/32/32 | 0.93 | 0.93 | 0.93 |
| 128/128/128 | 0.94 | *0.95* | 0.94 |
| 8/32/128 | 0.91 | 0.94 | 0.92 |
| 32/128/8 | 0.89 | 0.93 | 0.93 |
| 32/128/32 | 0.92 | 0.94 | 0.93 |
| 128/32/8 | 0.93 | 0.92 | 0.92 |
| 128/8/128 | 0.92 | 0.94 | 0.93 |
| 128/32/128 | 0.94 | 0.94 | *0.95* |
| 32/32/32/32/32 | 0.90 | 0.94 | 0.93 |
| 128/32/8/32/128 | 0.90 | 0.94 | 0.92 |
| 128/128/128/128/128 | 0.90 | 0.93 | 0.94 |
| 128/256/128 | 0.94 | *0.95* | 0.94 |

Затем, сделали сравнение результатов в соотношениях 70/30 и 90/10, рисунок 44.

Для функции активации logistic:

a

б

в

Рисунок 44 – Гистограммы результатов классификации в соотношениях 70/30 и 90/10 c функцией активации logistic (a), tanh (б), relu (в)

По результатам эксперимента удалось получить точность классификации сетевого трафика – 95%. Наилучшие результаты показали MLP с параметрами 128/128/128 и 128/256/128 с функцией активации tanh и 128/32/128 с функцией активации relu.

Для сравнения, приведем результаты похожих исследований, и сравним их с нашими, таблица 15.

Таблица 15 – Таблица сравнения

|  |  |  |  |
| --- | --- | --- | --- |
| Исследование | Модель | Точность классифи кации, % | Набор данных |
| 1 | 2 | 3 | 4 |
| M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas and J. Lloret, "Network Traffic Classifier With Convolutional and Recurrent Neural Networks for Internet of Things," in IEEE Access, vol. 5, pp. 18042-18050, 2017, doi: 10.1109/ACCESS.2017.2747560. | CNN+RNN-2a | 96 | реальные данные из RedIRIS |
| Fatih Ertam, Engin Avcı, A new approach for internet traffic classification: GA-WK-ELM,  Measurement, Volume 95, 2017,  Pages 135-142,  ISSN 0263-2241,  https://doi.org/10.1016/j.measurement.2016.10.001 | GA-WK-ELM | 96 | реальные данные полученные из кампуса Кэмбриджского университета |
| Brian Schmidt, Ala Al-Fuqaha, Ajay Gupta, Dionysios Kountanis,  Optimizing an artificial immune system algorithm in support of flow-Based internet traffic classification, Applied Soft Computing, Volume 54, 2017, Pages 1-22, ISSN 1568-4946,  https://doi.org/10.1016/j.asoc.2017.01.016. | Naive Bayes | 95 | реальные данные |
| Sun, G., Chen, T., Su, Y. et al. Internet Traffic Classification Based on Incremental Support Vector Machines. Mobile Netw Appl **23**, 789–796 (2018). https://doi.org/10.1007/s11036-018-0999-x | SVMs | 96 | реальный набор данных из Кэмбриджского проекта Nprobe |
| Pathmaperuma MH, Rahulamathavan Y, Dogan S, Kondoz AM. Deep Learning for Encrypted Traffic Classification and Unknown Data Detection. Sensors. 2022; 22(19):7643. https://doi.org/10.3390/s22197643 | SAE, 1D CNN | 94 | публичный набор ISCX |
| Продолжение таблицы 15 | | | |
| 1 | 2 | 3 | 4 |
| Wang, P.; Ye, F.; Chen, X.; Qian, Y. DataNet: Deep learning based en-crypted network traffic classification in SDN home gateway. IEEE Access **2018**, 6, 55380–55391 | namely multilayer perceptron, stacked autoencoder, and CNN | 92 | публичный набор ISCX |
| Li, D.; Li, W.; Wang, X.; Nguyen, C.T.; Lu, S. App trajectory recognition over encrypted internet traffic based on deep neural network. Comput. Netw. **2020**, 179, 107372 | DNN | 79 | реальный мобильный трафик |
| X. Wang, S. Chen and J. Su, "Automatic Mobile App Identification From Encrypted Traffic With Hybrid Neural Networks," in IEEE Access, vol. 8, pp. 182065-182077, 2020, doi: 10.1109/ACCESS.2020.3029190. | Combination of bi-LSTM and 1D-CNN | 93 | реальный мобильный трафик полученный при использовании NetLog пользователями сети |
| B. Mohammed et al., "Edge Computing Intelligence Using Robust Feature Selection for Network Traffic Classification in Internet-of-Things," in IEEE Access, vol. 8, pp. 224059-224070, 2020, doi: 10.1109/ACCESS.2020.3037492. | EWA | 98 | реальные данные полученные из кампуса Кэмбриджского университета |
| Safari Khatouni, A., Seddigh, N., Nandy, B. et al. Machine Learning Based Classification Accuracy of Encrypted Service Channels: Analysis of Various Factors. J Netw Syst Manage **29**, 8 (2021). https://doi.org/10.1007/ s10922-020-09566-5 | RF | 97 | публичные данные NIMS2018, NIMS2019, PRI2019 |
| Наш эксперимент | MLP | **95** | публичные данные NSL-KDD |

Исходя из таблицы 15, результаты точности классификации разнятся. Это может быть связано как со структурой данных, так и с используемыми методами и инструментами. Несмотря на это, результаты предлагаемого решения позволяют соотносить сетевой трафик по сгенерировавшим их приложениям и используемым протоколам с точностью 95%. Остаток сетевого трафика, который не удалось соотнести к определенному приложению можно считать аномальным и потенциально вредоносным, требующим дальнейшего исследования.

## **Выводы по разделу 3**

В данном разделе приведены экспериментальные оценки предлагаемых методов и решений.

Уменьшение размерности.

В машинном обучении многомерные данные относятся к данным с большим количеством функций или переменных. Проклятие размерности – распространенная проблема в машинном обучении, когда производительность модели ухудшается по мере увеличения числа функций. Это связано с тем, что сложность модели увеличивается с увеличением количества функций, и найти хорошее решение становится все труднее. Кроме того, многомерные данные также могут привести к переобучению, когда модель слишком точно соответствует обучающим данным и плохо обобщается на новые данные. Данные факторы обуславливают необходимость в уменьшении размерности исследуемых данных.

Благодаря использованию МГК для уменьшения признакового пространства, удалось улучшить точность классификатора NaiveBayes на 11%, и классификатора DecisionStump на 4% на наборе данных NSL-KDD. Результаты подтверждают эффективность применения метода главных компонент для отдельных классификаторов машинного обучения.

Сегментирование данных.

Используя метод сегментирования данных стало возможным итеративно обучать и тестировать модель на разных подмножествах, а затем назначить наилучший классификатор для каждого подмножества. Этот процесс дает надежную оценку производительности модели и помогает выявить потенциальные отклонения в результатах. Метод позволил сосредоточить анализ на меньших подмножествах, более эффективно используя вычислительные ресурсы и ускоряя процесс анализа.

Различные сегменты данных могут обладать уникальными характеристиками или закономерностями, которые могут быть замаскированы при анализе всего набора данных. Сегментируя данные на основе соответствующих критериев и влияющих факторов, можно проводить индивидуальный анализ для конкретных подмножеств, получая более глубокое представление об их поведении. Сегментирование также может быть полезным для предварительной обработки данных, к примеру, для генерирования сводной статистики, выявления профиля и визуализации каждого сегмента.

В рамках исследования, используя сегментирование для обнаружения вредоносного сетевого трафика удалось повысить показатели качества классификаторов приблизительно на 5%.

Бэггинг. Данный метод коллективного машинного обучения направлен на повышение общей производительности прогностической модели. Он предполагает обучение нескольких базовых моделей на различных подмножествах обучающих данных, а затем объединение их прогнозов для получения окончательного, более надежного прогноза. Метод применим к широкому спектру базовых алгоритмов, таких как деревья решений, случайные леса, машины опорных векторов и даже нейронные сети. Это показывает гибкость метода, который справляется с вариативностью различных моделей. Существенным преимуществом бэггинга является его универсальность. Данный метод можно комбинировать с другими ансамблевыми методами, такими как бустинг, для реализации более «сильных» ансамблей, использующих преимущественные стороны различных техник.

По результатам проведенного эксперимента с применением бэггинга на публичном наборе данных NSL-KDD, с содержанием вредоносных составляющих, удалось получить точность классификации 99%.

Нейронная сеть. Класс моделей глубокого обучения, вдохновленный структурой и функциями человеческого мозга, на сегодняшний день является одним из самых передовых технологий. Он становится более популярным в различных задачах анализа данных благодаря способности извлекать сложные шаблоны и закономерности. Нейронные сети способны улавливать нелинейные взаимосвязи между переменными в данных. Это делает их подходящими для задач, в которых традиционные линейные модели могут оказаться недостаточными для представления сложных паттернов. Нейронные сети могут автоматически извлекать соответствующие функции из необработанных входных данных, уменьшая необходимость в ручном проектировании функций. Это особенно полезно при работе с данными большой размерности. Нейронные сети могут быть адаптированы к различным типам данных, включая изображения, текст, аудио и последовательные данные. Такая универсальность позволяет применять их в широком спектре задач анализа данных, от классификации изображений до обработки естественного языка. Глубокие нейронные сети состоят из нескольких уровней, что позволяет им изучать иерархические представления. Каждый уровень изучает более абстрактные объекты на основе представлений, усвоенных предыдущими уровнями, что приводит к пониманию данных на более высоком уровне. Во многих областях, таких как распознавание изображений, обработка естественного языка и распознавание речи, нейронные сети достигли самой высокой производительности, превосходящей традиционные подходы к машинному обучению.

Область нейронных сетей и глубокого обучения постоянно развивается, и исследователи разрабатывают новые архитектуры, методы оптимизации и регуляризации. Этот продолжающийся прогресс гарантирует, что нейронные сети по-прежнему будут находиться на переднем крае подходов к анализу данных.

В рамках исследования, нейронная сеть была развернута для классификации реального сетевого трафика по генерируемым приложениям. Удалось достичь точности классификации 95%. Данный эксперимент подтверждает применимость нейронной сети для классификации реальных данных. Это позволить в дальнейшем существенно сократить вычислительные ресурсы, ввиду исключения из анализируемого набора легитимных данных, сгенерированных известными приложениями, и акцентировании внимания на аномальных, потенциально вредоносных данных.

## **РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ РЕШЕНИЙ В КОРПОРАТИВНЫХ СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ**

## **4.1 Адаптирование предлагаемых решений в корпоративных сетях телекоммуникаций**

Задача выявления аномалий представляет собой идентификацию событий, наблюдений или элементов, которые могут оказать негативное воздействие. Любой тип обнаружения аномалий основывается на двух основных предположениях:

* аномалии в данных возникают очень редко;
* характеристики аномалий данных значительно отличаются от характеристик обычных экземпляров данных.

Как правило, аномальные данные связаны с какой-либо проблемой или редким событием, таким как взлом, банковское мошенничество, неисправное оборудование, структурные дефекты/сбои инфраструктуры или текстовые ошибки. По этой причине с точки зрения защиты КСТ важно выявлять фактические аномалии, а не ложные срабатывания или шум данных.

В рамках исследования предлагается блок-схема адаптирования предлагаемых решений в КСТ, рисунок 45. Схема может быть использована как для периодического проведения аудита в КСТ, так и для постоянного мониторинга сети для выявления вредоносных объектов.

Процесс адаптирования состоит из трех этапов:

1. этап сбора и обработки данных;
2. этап идентификации и оценки вредоносного трафика;
3. этап анализа результатов.

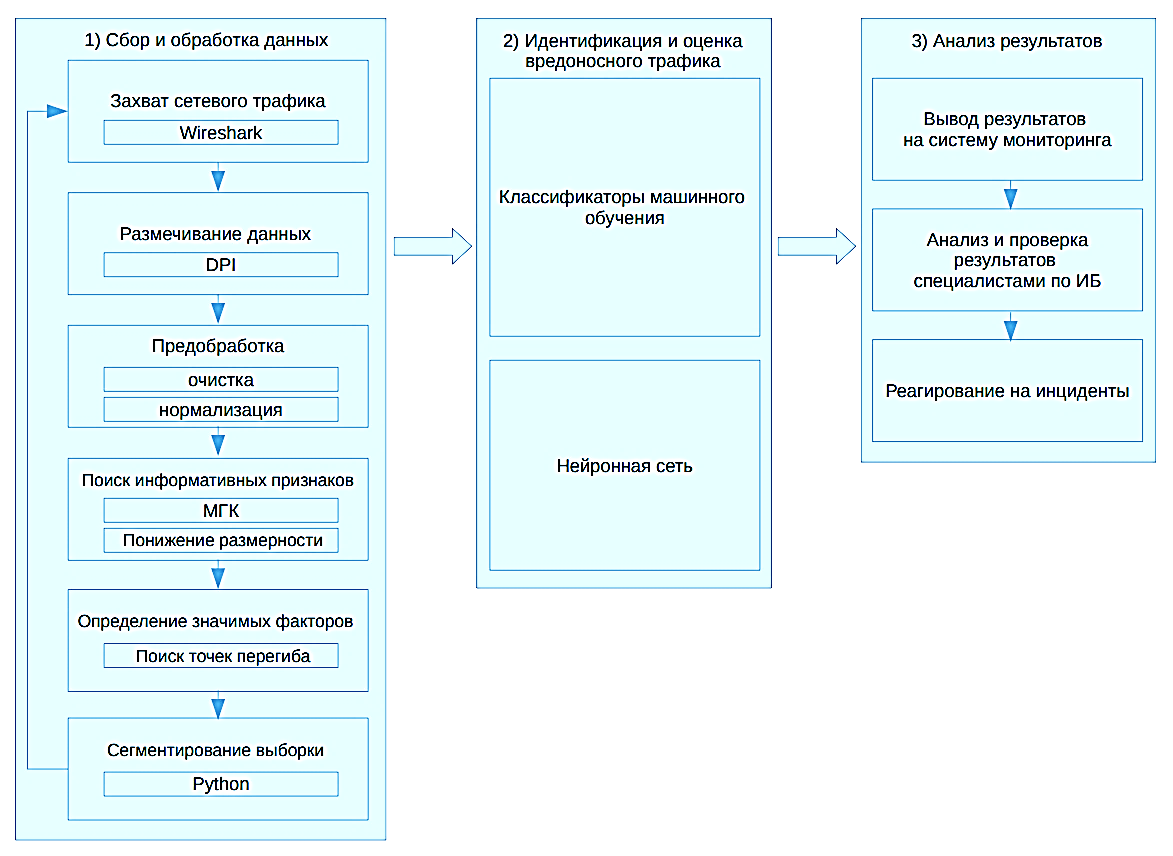


Рисунок 45 – Блок-схема адаптирования предложенных решений в КСТ

На первом этапе предлагается следующая последовательность действий.

Захват сетевого трафика.

На ПК администратора направляется спан-сессия с сетевым трафиком. С помощью свободно распространяемого инструмента Wireshark ведется захват сетевого трафика с последующей записью в файл формата .pcap.

Размечивание данных.

Для разметки данных предлагается использовать технологию глубокого инспектирования пакетов (DPI). Данная система способна по параметрам трафика точно определять приложение, которое сгенерировало данный трафик. На выходе получаем размеченные по приложениям записи. Те записи, которые DPI не смог соотнести к конкретному приложению, размечаются как Unknown (неизвестного происхождения). Так как данные виды записей представляют потенциальную угрозу, их будем относить к вредоносному трафику.

Предобработка.

Известно, что обработка данных занимает 90% времени аналитика. Но это является обоснованной необходимостью, без которого невозможно получить качественные результаты. Поэтому размеченный набор данных необходимо очистить от ошибочных записей и произвести нормализацию, то есть исключить дублирующие записи.

Поиск информативных признаков.

С использованием метода главных компонент удается выявить наиболее информативные признаки. Это повышает надежность результатов и необходимо для понижения объемов обрабатываемых данных.

Понижение размерности.

Предполагается, что в полученном наборе размеченных данных удаляем параметры с наименьшей информативностью.

Определение значимых факторов.

Идет преобразование данных в двумерный сигнал. Затем, с применением метода поиска точек разладки и перегиба, или, другими словами, точек изменения сигнала, находим точки, по которым будем разделять набор данных на части – сегменты.

Сегментирование выборки.

После определения точек перегиба, производим разделение всей выборки на подвыборки – сегменты. Точки перегиба в данном случае являются границами сегментов. Для сегментирования предполагается использование библиотек Python.

Второй этап предлагаемого решения предполагает использование классификаторов машинного обучения и нейронной сети.

Классификаторы машинного обучения.

Здесь модель пытается предсказать правильную метку заданных входных данных. При этом следует отметить, что классификация проводится для каждого сегмента в отдельности. Обученные на реальных данных классификаторы МО производят прогнозирования новых неизвестных данных.

Нейронная сеть.

Параллельно с этим, подвыборки, в виде полученных сегментов, подаются на вход нейронной сети. В решении используется многослойный перцептрон. Он имеет входные и выходные слои, а также один или несколько скрытых слоев со множеством нейронов, сложенных вместе. Хотя нейронная сеть имеет отличную от классификаторов МО структуру, она может успешно выполнять задачи классификации.

На третьем этапе проводится вывод и анализ результатов.

На систему мониторинга в режиме реального времени выводятся потенциально опасные записи, со всеми анализируемыми параметрами. Затем специалисты проверяют, действительно ли полученное оповещение представляет собой угрозу и предпринимают соответствующие меры.

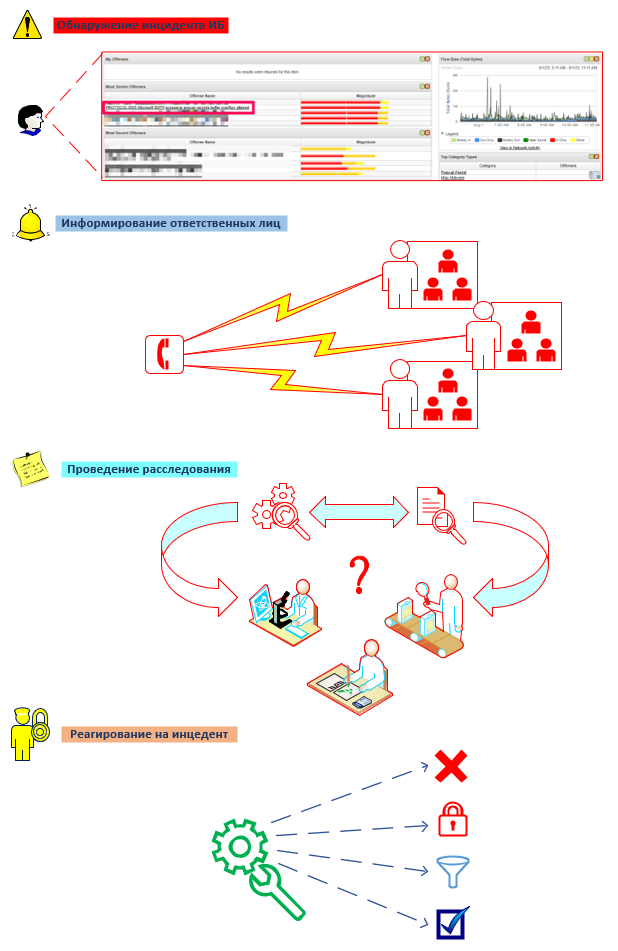


Рисунок 46 – Схема реагирования на инциденты ИБ в КСТ

В соответствии с рисунком 46, представлена схема реагирования на инциденты ИБ в КСТ.

Согласно схемы реагирования, диспетчер, который мониторит состояние различных систем, обнаруживает инцидент с системы мониторинга. Об инциденте немедленно сообщается ответственным за ИБ КСТ, делается оповещение. Ответственными лицами даются указания специалистам по ИБ по проведению расследования: выявления инициатора вредоносных данных, поиск взаимосвязей, структуру данных, критичность для активов компании и др. После проведения расследования принимается необходимое решение: удаление, блокировка, ограничение, разрешение.

## **4.2 Рекомендации ITU-T.** **Архитектура безопасности**

При развертывании КСТ, для обеспечения безопасности, следует руководствоваться признанными общемировыми стандартами и рекомендациями. Одним из таких рекомендаций является ITU-T X.805 [69], где приводится архитектура безопасности (далее ‒ АБ), которая определяется тремя основными концепциями: уровнями безопасности, плоскостями и измерениями для сквозной сети. При разделении требований безопасности по уровням и планам используется иерархический подход, так, что сквозная безопасность достигается за счет разработки мер безопасности в каждом из измерений для устранения конкретных угроз. Рисунок 47 иллюстрирует элементы этой архитектуры.

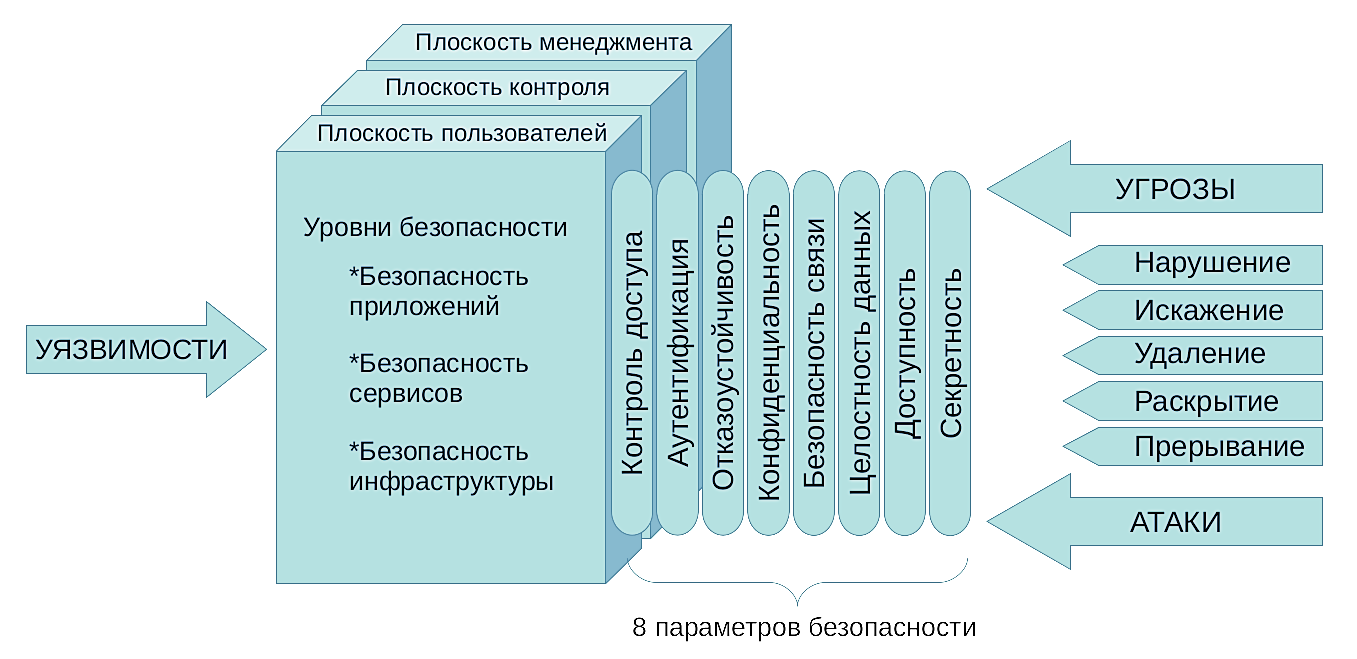


Рисунок 47 – Элементы архитектуры безопасности в рекомендациях

ITU-T X.805

Рекомендации ITU-T признают четыре типа уязвимостей:

‒ уязвимости модели угроз, возникающие в результате неспособности предвидеть грядущие угрозы;

‒ уязвимости спецификации и дизайна, которые возникают по причине упущений при разработке дизайна протокола или системы;

‒ уязвимости реализации, возникающие по причине упущений при функционировании системы или разработке протокола;

‒ уязвимости в настройках и работе, возникающие по причине неправильного применения опций в разработке, либо слабых методов и политик деплоймента, к примеру, в беспроводной сети часто отказываются использовать средства шифрования [69].

В то время как меняются угрозы ИБ, уязвимости существуют на протяжении всего жизненного цикла протоколов и систем. Уязвимости, связанные с этими протоколами и системами, могут привести к значительным последствиям по своему масштабу, ввиду широкого применения стандартизированных систем и протоколов. Следовательно, необходимо осознавать всю серьезность вопроса и предпринимать действия по выявлению уязвимостей в КСТ и их устранению.

АБ изначально создавалась как инструкция к решению глобальных проблем в сфере ИБ для провайдеров, компаний и отдельных абонентов. Она может применяться к проводным сетям Ethernet, волоконно-оптическим линиям связи, беспроводным и конвергентным сетям связи. АБ помогает при решении проблем обеспечения ИБ при мониторинге и управлении службами и приложениями сетевой инфраструктуры компаний. АБ обеспечивает всестороннюю, нисходящую, сквозную перспективу сетевой безопасности и может быть применена к сетевым элементам, службам и приложениям для обнаружения, прогнозирования и исправления уязвимостей.

АБ логически разделяет сложный набор функций безопасности сквозной сети, на отдельные компоненты архитектуры. Подобное разделение предоставляет системный подход к обеспечению безопасности, который может быть использован для разработки новых ИБ-решений и оценивания уровня безопасности реальной КСТ [69].

АБ помогает при решении проблем обеспечения сквозной безопасности:

1. К каким угрозам применять тот или иной тип обеспечения защиты?

2. Каким типам объектов и сетевого оборудования необходимо обеспечить защиту?

3. Каким действиям в сети необходимо обеспечить защиту?

Три архитектурных компонента: плоскости безопасности, уровни безопасности и измерения безопасности предлагаются для решения представленных вопросов [69].

Принципы АБ возможно применять к большому спектру сетей, в не зависимости от местоположения в стеке протоколов и применяемых сетевых технологий, и КСТ не является исключением.

Предлагаемые решения в КСТ будут выполнять роль дополнительной системы мониторинга, рисунок 48. Они будут работать аналогично существующим системам, будут анализировать тот же сетевой трафик компании, но по другим правилам.

По схеме, становится очевидным, что воздействие угроз и эксплуатацию уязвимостей можно обнаружить по сетевому трафику, так как любые манипуляции и изменения в сети отражаются в передаваемых данных и их свойствах.

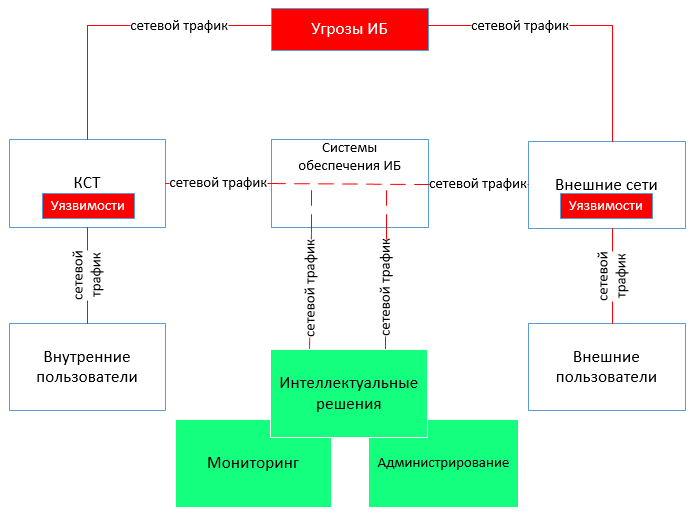


Рисунок 48 – Схема уточнения роли интеллектуальных решений в КСТ

С применением интеллектуальных решений становится возможным улучшить АБ, путем добавления нового уровня безопасности - защищенности информации. Таким образом, для КСТ, акцент архитектуры сдвигается в пользу информационных активов компании, рисунок 49.

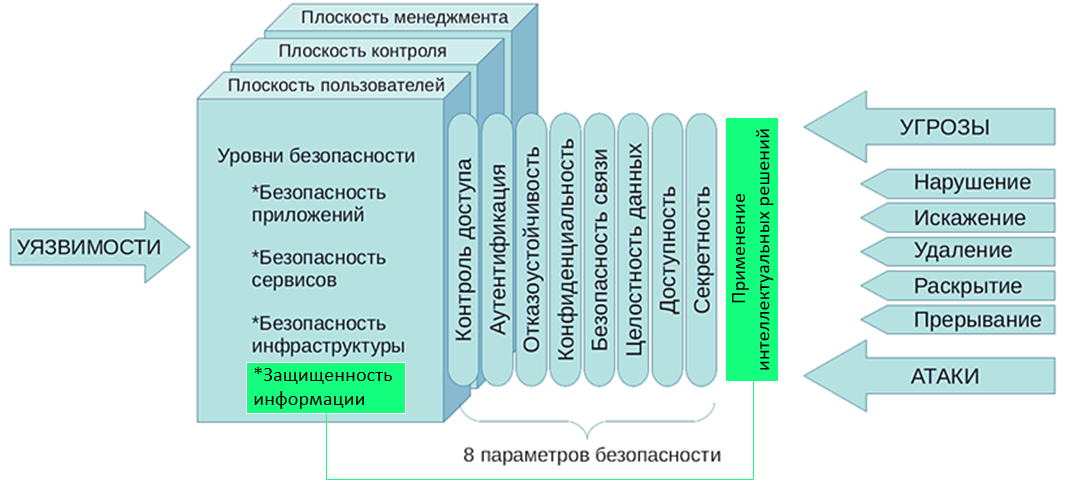


Рисунок 49 – АБ с применением интеллектуальных решений в КСТ

Известно, что современные угрозы могут быть скрыты среди пользовательских приложений и сервисов. Когда возникает инцидент ИБ, уже поздно предпринимать превентивные действия, так как информация более не конфиденциальна, целостность разрушена, и стала доступна чужим лицам. Для предотвращения инцидентов ИБ необходимо, в идеале, предугадывать дальнейшие действия угроз и просчитывать все возможные комбинации. Фантазия человека безгранична, поэтому считаем, что обе стороны имеют равные возможности. Применение интеллектуальных систем для обеспечения ИБ является обоснованной необходимостью в нынешних реалиях.

## **4.3 Рекомендации нормативно-правовых актов Республики Казахстан по обеспечению информационной безопасности**

Для обеспечения ИБ в КСТ можно руководствоваться положениями стандарта СТ РК ISO/IEC 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации».

Покажем рекомендации, наиболее эффективные для КСТ.

Для выполнения требований обеспечения ИБ осуществляется приобретение ПО и электронной продукции как товар и информационно-коммуникационная услуги из специального реестра доверенной продукции электронной промышленности и ПО, в соответствии с законодательством РК о госзакупках [70]. То есть, ПО и сетевое оборудование для КСТ необходимо закупать согласно реестра доверенного ПО и оборудования.

Собственники ПО, находящихся в реестре доверенной продукции и ПО, для учета и хранения передают исходные программные коды оператору [70].

В компаниях для контроля за инцидентами проводятся следующие мероприятия:

1) сбор информации об инцидентах ИБ, мониторинг, анализ;

2) нарушения ИБ выявляются путем анализа следующих журналов логирования:

* журналов логирования ОС;
* журналов логирования баз данных;
* журналов логирования антивирусных программ;
* журналов логирования прикладных ПО;
* журналов логирования сетевого оборудования КСТ;
* журналов логирования IDS/IPS;
* журналов логирования фильтрации приложении;

3) производится настройка синхронизации времени лог-журналов с корпоративным источником времени;

4) производится реализация процедуры информирования ответственных лиц об инцидентах ИБ реагирования на инциденты ИБ.

Требования, предъявляемые к объектам информатизации при их эксплуатировании:

1) обеспечение аутентификации;

2) обеспечение СКЗИ - средствами контроля и защиты информации;

3) обеспечение отказоустойчивости и доступности информации;

4) мониторинг обеспечения безопасного функционирования и защиты целевых устройств;

5) использование систем и инструментов реализации ИБ;

6) наличие необходимых свидетельств удостоверяющих центров.

Необходимо применять специализированные СКЗИ с параметрами, соответствующими стандартам СТ РК 1073-2007 «Средства криптографической защиты информации», с целью защиты электронных ресурсов, конфиденциальной информации, ИС и других активов компании [70].

В КСТ с целью проведения мониторинга действий сотрудников:

1) производится оперативное оповещение специалистов по ИБ о выявлении аномальной, потенциально дискредитирующей активности пользователей, при котором, впоследствии, эти действия блокируются;

2) производятся аналогичные действия при выявлении событий, инициированных обслуживающим персоналом.

ИБ события, критичные по принципам целостности, доступности и конфиденциальности, по итогам анализа журнала логирования:

1) определяются как ИБ-инциденты;

2) заносятся в базу угроз (рисков) ИБ;

3) регистрируются в службе реагирования на инциденты ИБ государственной технической службы.

Используются следующие системы и средства, на этапе опытной и промышленной эксплуатации объектов информатизации:

* обнаружения и предотвращения вредоносных программ;
* мониторинга за событиями и инцидентами ИБ;
* выявления и предотвращения вторжений;
* мониторинга за информационной инфраструктурой.

Системы предотвращения утечки информации (DLP) применяются для защиты критически важных объектов ИКТ и объектов информатизации.

Также реализуется:

* обязательное информирование сотрудников о планируемом контроле за их действиями в КСТ;
* размещение на периметре локальной сети центра мониторинга и систем обнаружения и предотвращения утечки информации [70].

Менеджментом компании инициируется проведение аудита ИБ независимыми аудиторскими командами не реже одного раза в год, для проверки эффективности используемых инструментов и систем защиты, выявления уязвимостей в сети и устройствах, упущения в конфигурации сетевых устройств. Затем, компанией принимаются к сведению все замечания аудита, которые устраняются в кратчайшие сроки.

## **Выводы по разделу 4**

В разделе 4 даны рекомендации по применению предложенных в рамках исследования решений для КСТ. Данные рекомендации требуют согласования специалистов по ИБ, с точки зрения полноты и необходимости тех или иных компонентов анализа.

В разделе представлена разработанная авторами типовая схема реагирования на инциденты ИБ в КСТ.

Предложены рекомендации ITU-T по обеспечению ИБ. Данные рекомендации определяет архитектуру сетевой безопасности и могут быть применимы для обеспечения сквозной сетевой безопасности в КСТ. Архитектура может быть применена к различным типам сетей, где требуется комплексная безопасность, независимо от используемой технологии сети. Она является основой для разработки индивидуальных подробных рекомендаций для отдельных компаний.

Следует отметить, что выявление аномальных, потенциально вредоносных для КСТ данных требует комплексного подхода. Поэтому основные общие требования к организациям по вопросам обеспечения ИБ закреплены нормативно-правовыми актами.

# **ЗАКЛЮЧЕНИЕ**

Управление информационной безопасностью в корпоративных сетях телекоммуникаций является сложным, и зависящим от внешних и внутренних факторов. В процессе эксплуатации сети, необходимо охватывать все области сетевой инфраструктуры, приложения, службы и другие объекты, включая ряд телекоммуникационных технологий (например, проводных, беспроводных или широкополосных), поддерживать широкий спектр услуг в масштабах компании, и областей обслуживания.

Учитывая масштабы охвата, каждое сетевое устройство генерирует либо передает по телекоммуникационной сети данные таких объемов, проанализировать которые в полной мере не представляется возможным, даже при наличии высокопроизводительных систем. Причиной этому является проблема проведения скурпулезных, точечных настроек оборудования так, чтобы они не повлияли на работу критичных служб и систем компании. При поиске такого «баланса» могут быть упущены «маленькие детали», которые впоследствии могут принести большие проблемы.

Поэтому, в дополнение к используемым системам, организациям необходимо внедрять дополнительные интеллектуальные средства обеспечения ИБ, с целью адекватного и полного выявления инцидентов и управления рисками ИБ. Именно здесь, Data Mining оказался неоценимым, поскольку он дает возможность обработки практически любых объемов данных сетевого трафика и улучшает подход организаций к обеспечению информационной безопасности.

Такой подход, позволяет «эшелонировать оборону», так как возникает дополнительный аналитический фильтр для выявления событий, упущенных предыдущими системами. Алгоритмы машинного обучения и статистический анализ, лежащие в основе Data Mining позволяют выявить скрытые закономерности в данных, невольно упускаемые системами ИБ и администраторами сети.

В рамках диссертационного исследовании было представлено решение на основе применения методов Data Mining для целей минимизации рисков, связанных с обеспечением информационной безопасности в пределах корпоративной сети телекоммуникаций.

Исходя из проделанной работы, можно убедиться в эффективности методов интеллектуального анализа данных при решении задач обнаружения вредоносного трафика в КСТ.

Дальнейшие исследования будут направлены на развитие академической науки по анализу данных, с целью поиска аномалий и скрытых закономерностей в сетевом трафике, с параллельной бизнес-ориентированной оценкой выдвигаемых идей и гипотез.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1 Petersen R. Data Mining for Network Intrusion Detection: A comparison of data mining algorithms and an analysis of relevant features for detecting cyber-attacks: thes. – Östersund, 2015. – 61 р.

2 Структура и функции программного обеспечения ККС // https://www.bibliofond.ru/view.aspx?id=564260. 12.10.2022.

3 XSTR-USM Unified security model (USM) – A neutral integrated system approach to cybersecurity // https://www.itu.int/dms\_pub/itu-t/opb/tut. 03.06.2022.

4 СТ РК ИСО/МЭК 27002-2009. Информационные технологии. Средства обеспечения. Свод правил по управлению защитной информации. – Введ. 2009-17-11. – Астана, 2009. – 124 с.

5 Kulambayev B., Beissenova G., Katayev N. et al. A Deep Learning-Based Approach for Road Surface Damage Detection // Computers, Materials and Continua. – 2022. – Vol. 73. – P. 3403-3418.

6 Gao Y., Yin X., He Z. et al. A deep learning process anomaly detection approach with representative latent features for low discriminative and insufficient abnormal data // Computers & Industrial Engineering. – 2023. – Vol. 176. – P. 108936.

7 Nassif A.B., Talib M.A. et al. Machine Learning for Anomaly Detection: A Systematic Review // IEEE Access. – 2021. – Vol. 9. – P. 78658-78700.

8 Thudumu S., Branch P., Jin J. et al. A comprehensive survey of anomaly detection techniques for high dimensional big data // J Big Data. – 2020. – Vol. 7, Issue 1. – P. 42-1-42-30.

9 Omar S., Ngadi Md. et al. Machine Learning Techniques for Anomaly Detection: An Overview // International Journal of Computer Applications. – 2013. – Vol. 79, Issue 2. – P. 33-41.

10 Сухопаров М.Е., Лебедев И.С. Идентификация состояния информационной безопасности устройств интернета вещей в информационно-телекоммуникационных системах // Системы управления, связи и безопасности. – 2020. – №3. – С. 252-268.

11 Staar B., Lütjen M., Freitag M. Anomaly detection with convolutional neural networks for industrial surface inspection // Procedia CIRP. – 2019. – Vol. 79. – P. 484-489.

12 AlDahoul N., Abdul Karim H., Ba Wazir A.S. Model fusion of deep neural networks for anomaly detection // J Big Data. – 2021. – Vol. 8. – P. 106-1-106-18.

13 Albuquerque Filho J.E.D., Brandão L.C.P., Fernandes B.J.T. et al. A Review of Neural Networks for Anomaly Detection // IEEE Access. – 2022. – Vol. 10. – P. 112342-112367.

14 Elfaki A.O. et al. Using a Rule-based Method for Detecting Anomalies in Software Product Line // Research Journal of Applied Sciences, Engineering and Technology. – 2014. – Vol. 7, Issue 2. – P. 275-281.

15 Duffield N., Haffner P., Krishnamurthy B., Ringberg H. Rule-Based Anomaly Detection on IP Flows // Procced. IEEE INFOCOM 2009. – Rio de Janeiro, 2009. – P. 424-432.

16 Szmit M., Wężyk R. et al. Traffic Anomaly Detection With Snort // Procced. conf. ISAT Volume: Information Systems and Computer Communication Networks. – Wrocław, 2007. – P. 1-8.

17 Vázquez F.I., Zseby T. Analysis of network traffic features for anomaly detection // Machine Learning. – 2014. – Vol. 101, Issue 1. – P. 59-84.

18 Liu H., Wang H. Real-Time Anomaly Detection of Network Traffic Based on CNN // Symmetry. – 2023. – Vol. 15, Issue 6. – P. 1205-1-1205-21.

19 Zhang M., Guo J., Li X. et al. Data-Driven Anomaly Detection Approach for Time-Series Streaming Data // Sensors (Basel). – 2020. – Vol. 20, Issue 19. – P. 5646-1-5646-16.

20 Zhou Z.G., Tang P. Improving time series anomaly detection based on exponentially weighted moving average (EWMA) of season-trend model residuals // 2016 IEEE International Geoscience and Remote Sensing Symposium (IGARSS). – Beijing, 2016. – P. 3414-3417.

21 Tang H., Wang Q., Jiang G. Time Series Anomaly Detection Model Based on Multi-Features // Comput Intell Neurosci. – 2022. – Vol. 2022. – P. 2371549.

22 Zheng J., Li J., Liu C. et al. Anomaly detection for high-dimensional space using deep hypersphere fused with probability approach // Complex Intelligent Systems. – 2022. – Vol. 8. – P. 4205-4220.

23 Ranshous S., Shen S., Koutra D. et al. Anomaly detection in dynamic networks: a survey // WIREs Computational Statistics. – 2015. – Vol. 7, Issue 3. – P. 223-247.

24 Chovanec M., Hasin M., Havrilla M. et al. Detection of HTTP DDoS Attacks Using NFStream and TensorFlow // Applied Sciences. – 2023. – Vol. 13, Issue 11. – P. 6671-1-6674-24.

25 Lopez A.D. et al. Network Traffic Behavioral Analytics for Detection of DDoS Attacks // SMU Data Science Review. – 2019. – Vol. 2. – P. 14-1-14-25.

26 Singh M., Singh M., Kaur S. Issues and challenges in DNS based botnet detection: A survey // Computers & Security. – 2019. – Vol. 86. – P. 28-52.

27 Schiller C.A., Binkley J. et al. Charter 5 – Botnet Detection: Tools and Techniques // Botnets: The Killer Web App. – Amsterdam, 2007. – P. 133-215.

28 Какие задачи бизнеса решает машинное обучение // https://kapital.kz /tehnology/90446/kakiye-zadachi-biznesa-reshayet-mashinnoye. 17.11.2020.

29 How Google uses Machine Learning to revolutionise the Internet World? // https://data-flair.training. 17.11.2020.

30 Дата майнинг для информационной безопасности // https://habr.com/ru/ companies/ibm/articles/168005. 16.11.2020.

31 Splunk // https://ru.wikipedia.org/wiki/Splunk#Система\_. 17.11.2020.

32 Материалы о Enterprise Security Manager // <https://partners.trellix.com/> enterprise/ru-ru/assets/data-sheets/ds. 17.11.2020.

33 Magic Quadrant for SIEM 2021 // https://www.exabeam.com/library/2021-gartner-magic-quadrant-for-siem. 17.11.2021.

34 Our reflections on the 2022 Gartner Magic Quadrant for Data Quality Solutions // https://www.qlik.com/blog/our-reflections-on-the-2022. 24.02.2023.

35 Постановление Правительства Республики Казахстан. Об утверждении Концепции кибербезопасности ("Киберщит Казахстана"): утв. 30 июня 2017 года, №407 // https://adilet.zan.kz/rus/docs/P1700000407. 17.11.2020.

36 В рейтинге стран по кибербезопасности РК заняла 78-е место // https://kapital.kz/tehnology/118681/v-reytinge-stran-po. 08.02.2024.

37 Опасность из глубин интернета: количество кибератак в РК увеличилось на 56% // https://energyprom.kz/ru/articles-ru/society-ru./opasnost-iz-glubin-interneta-kolichestvo-kiberatak-v-rk-uvelichilos-na-5. 08.02.2024.

38 Актуальные киберугрозы: I квартал 2020 года // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity. 12.11.2020.

39 Al Jallad K., Aljnidi M., Desouki M.S. Anomaly detection optimization using big data and deep learning to reduce false-positive // J Big Data. – 2020. – Vol. 7. – P. 68-1-68-13.

40 2019 Verizon Data Breach Investigations Report (DBIR) // https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach. 02.04.2022.

41 What is a network packet and how does it work? // https://www.techtarget.com/searchnetworking/definition/packet. 23.05.2022.

42 ITU-T Rec. E.417 (02/2005) // https://www.itu.int/rec. 16.02.2023.

43 Fillatre L., Nikiforov I., Vaton S. Optimal volume anomaly detection in network traffic flows. – 2008 // https://www.researchgate.net. 15.06.2021.

44 UBA: Detect Insecure Or Non-Standard Protocol // https://www.ibm.com/docs/en/qradar-common?topic=endpoint-uba. 06.12.2022.

45 Measuring the Magnitude of DDoS Attacks // https://ddos-guard.net/en/blog/magnitude-of-ddos-attacks. 07.12.2022.

46 Lavrova D., Semyanov P., Shtyrkina A. et al. Wavelet-analysis of network traffic time-series for detection of attacks on digital production infrastructure // SHS Web of Conferences. – 2018. – Vol. 44. – P. 00052.

47 Koren O., Koren M. et al. A procedure for anomaly detection and analysis // Engineering Applications of Artificial Intelligence. – 2023. Vol. 117, Part A. – P. 105503.

48 Bereziński P., Jasiul B., Szpyrka M. An Entropy-Based Network Anomaly Detection Method // Entropy. – 2015. – Vol. 17, Issue 4. – P. 2367-2408.

49 Голованова И.С. Методы обработки биомедицинских данных: метод. указ. – Томск, 2003. – 18 с.

50 James H. Steiger Principal Component Analysis // https://statpower.net/Content/312/R%20Stuff/PCA.html. 26.06.2023.

51 Kaiser Rule // https://docs.displayr.com/wiki/Kaiser\_Rule. 27.06.2023.

52 Уменьшение размерности в данных. Метод главных компонент // https://studizba.com/files/mmo-metody-mashinnogo-obucheniya/book. 25.05.2022.

53 Lebedev I.S. Various machine learning models application on separate segments in regression and classification problems // Informatsionno-upravliaiushchie sistemy. – 2022. – Vol. 3. – P. 9-19.

54 Atsuya O., Genki Y. Computational mechanics enhanced by deep learning // Computer Methods in Applied Mechanics and Engineering. – 2017. – Vol. 327. – P. 327-351.

55 Wong J.C., Lian H., Cheong S.A. Detecting macroeconomic phases in the Dow Jones Industrial Average time series // Physica A: Statistical Mechanics and its Applications. – 2009. – Vol. 388, Issue 21. – P. 4635-4645.

56 Lebedev I.S. Dataset segmentation considering the information about impact factors // Informatsionno-upravliaiushchie sistemy. – 2021. – Vol. 3. – P. 29-38.

57 Лебедев И.С. Адаптивное применение моделей машинного обучения на отдельных сегментах выборки в задачах регрессии и классификации // Информационно-управляющие системы. – 2022. – №3. – C. 20-30.

58 Rzayev B.T., Lebedev I.S. Segmentation of data when analyzing the state of telecommunication systems // Indonesian Journal of Electrical Engineering and Computer Science. – 2023. – Vol. 29. - №3. – P. 1473-1479.

59 Sukhoparov M.E., Lebedev I.S., Garanin A.V. Application of classifier sequences in the task of state analysis of Internet of Things devices // Computing, Telecommunications and Control. – 2020. – Vol. 13, Issue 3. – P. 44-54.

60 Bhupendra Ingre, Anamika Yadav Performance Analysis of NSL-KDD dataset using ANN // Procced. internat. conf. on Signal Processing And Communication Engineering Systems (SPACES). – Guntur, 2015. – P. 92-96.

61 Truong C., Oudre L., Vayatis N. Selective review of offline change point detection methods // Signal Processing. – 2020. – Vol. 167. – P. 107299.

62 Zhou Z.-H. Ensemble Methods: Foundations and Algorithms. – NY.: CRC Press, 2012. – 222 p.

63 Gao W., Zhou Z.-H. On the doubt about margin explanation of boosting // Artificial Intelligence. – 2013. – Vol. 203. – P. 1-18.

64 D’yakonov A.G. Solution methods for classification problems with categorical attributes // Computational Mathematics and Modeling. – 2015. – Vol. 26, Issue 3. – P. 408-428.

65 Re Matteo, Valentini Giorgio Ensemble methods: A review // In book: Advances in Machine Learning and Data Mining for Astronomy. – London,2012. – P. 563-594.

66 Kaftannikov I.L., Parasich A.V. Problems of training set’s formation in machine learning tasks // Bulletin of the South Ural State University. – 2016. – Vol. 16, Issue 3. – P. 15-24.

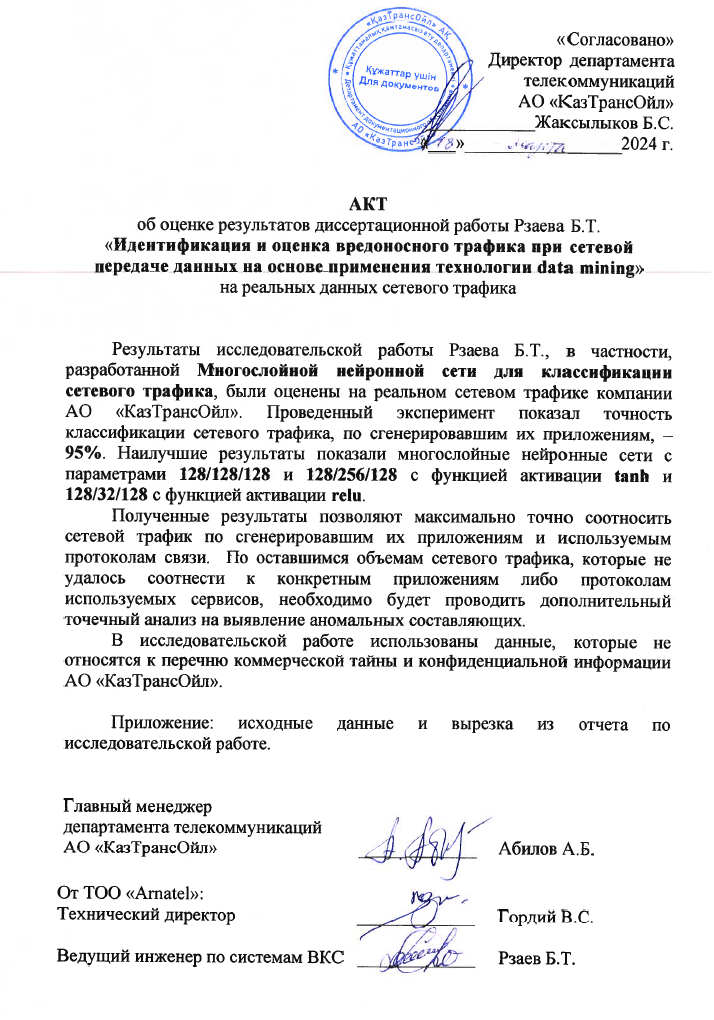
67 Yu Y., Zhou Z.-H., Ting K.M. Cocktail ensemble for regression // Procced. 7th IEEE internat. conf. on Data Mining (ICDM). – Omaha, 2007. – P. 721-726.

68 Машинное обучение вместо DPI. Строим классификатор трафика // https://habr.com/ru/post/304926. 20.06.2022.

69 X.805 : Security architecture for systems providing end-to-end communications //https://www.itu.int/rec/T-REC-X.805-200310-I/en. 11.03.2023.

70 Постановление Правительства Республики Казахстан. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: утв. 20 декабря 2016 года, №832 // https://adilet.zan.kz/rus/docs/P1600000832. 21.09.2023.

# **ПРИЛОЖЕНИЕ А**

Акт оценки результатов на реальных данных 

# **ПРИЛОЖЕНИЕ Б**

Свидетельство на программу для ЭВМ

