МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

02.03.03 Математическое обеспечение и администрирование информационных систем
(код и наименование направления подготовки, специальности)

Мобильные и сетевые технологии
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Разработка методики обнаружения сетевых атак с помощью поведенческого анализа трафика»

Обучающийся А.С. Филиппов
(Инициалы Фамилия) (личная подпись)

Руководитель к.т.н., доцент, О.В. Аникина
ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Консультант А.В. Егорова
ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Аннотация

Тема выпускной квалификационной работы - «Разработка методики обнаружения сетевых атак с помощью поведенческого анализа трафика»

Цель ВКР — Разработка методики и применение её в информационной системе для обнаружения сетевых атак при помощи поведенческого трафика.

Актуальность данной работы заключается в том, что система будет защищаться автоматически, путём анализа трафика, который в неё поступает, исходя из этого её можно будет встроить в любую информационную среду для предотвращения сетевых атак.

Объектом исследования данной выпускной работы будут являться существующие методики поведенческого анализа трафика.

Результат выполнения выпускной квалификационной работы имеет практическую ценность и может быть использован для предотвращения сетевых угроз в качестве готового решения построения ИС, а также принципов и концепций методики.

Квалификационная работа содержит 40 страниц текста, 4 рисунка, 1 таблицу, 21 источник, включая 7 на иностранном языке.

Abstract

The title of the graduation work is – “Development of methods to detect network attacks using behavioral analysis of traffic”.

The graduation work consists of an explanatory note on 38 pages, introduction, including 4 figures, 1 tables, the list of 20 references including 7 foreign sources.

Much attention is given to the question of how you can analyze behavioral traffic and what it takes.

The aim of the work is to give some information about development of a methodology and its application to the information system to detect network attacks using behavioral traffic.

The relevance of this work is that the system will be protected automatically by analyzing the traffic, which comes into it, based on this it can be built into any information environment to prevent network attacks.

The object of the study of this graduate work will be the existing methods of behavioral analysis of traffic.

The result of the graduate qualification work has practical value and can be used to prevent network threats as a ready-made solution for the construction of IS, as well as the principles and concepts of the methodology. The scope of the resulting methodology can be both commercial and government

Оглавление

Введение

Разработка поведенческого анализа трафика для предотвращения сетевых атак требуется в силу того, что в наше время доступ к информации о том, как вести атаку на тот или иной информационный ресурс имеет любой с доступом в интернет. Любой человек с минимальными техническими знаниями, может взять готовое решение, написанное другим человеком и совершить сетевую атаку на какую-то информационную систему. Наше время — это время перевода всё в информационное русло и информационную среду.

В традиционных системах в рамках работы над анализом сетевого трафика используется зачастую человеческий ресурс, а именно специалист сидит и через мониторинг отслеживает получаемый сервером трафик, а также действия пользователей в ИС. Подобный процесс можно автоматизировать в силу того, что у каждого вида атаки и преступной деятельности в сфере информации есть определенный паттерн поведения. Например, у DDoS атаки имеется паттерн поведения в виде множественных запросов с одного и того же IP-адреса. ИС можно спроектировать так, чтобы она была готова в автоматическом режиме выявлять подобные паттерны внутри трафика и принимать какие-либо контрмеры, либо предоставлять информацию требуемому лицу внутри ИС.

Таким образом, разработка поведенческого анализа трафика позволит предотвратить совершение сетевой атаки при помощи анализа действий пользователей в ИС. Что позволит выявлять и предотвращать попытки несанкционированного доступа и иных противоправных действий.

В современном мире использование информационных систем очень сильно увеличилось, и почти каждая маленькая компания имеет у себя внутри информационную систему, а некоторые даже делают системы

позволяющие что-то купить онлайн. Такие системы при атаках теряют не только возможность взаимодействия с ИС, но и прибыль.

Цель данной ВКР — разработка методики поведенческого анализа трафика для предотвращения сетевых атак. Разработанная методика построения ИС и её методы помогут сфокусировать внимание специалистов по информационной безопасности на потенциально опасном трафике, а также предотвратить попытки несанкционированного доступа от пользователей.

Для достижения поставленных целей работы требуется:

- изучить варианты взаимодействий с основной массой информационных систем;

- изучить потенциальные возможности для совершения попыток несанкционированного доступа;

- разработать методику обнаружения подобных попыток для предотвращения сетевых угроз внутри ИС;

- выполнить экспериментальное тестирование методики для выявления достоинств и недостатков.

Метод исследования — анализ существующих систем, которые используют поведенческий анализ трафика не только в сфере безопасности, но и в целом. А также определение требований к новой системе, выявление её недостатков и преимуществ.

Глава1 Исследование области анализа трафика и анализ существующих разработок

1.1 Исследование понятия трафик

Трафик в компьютерных системах представляет собой поток данных, который передается между устройствами в сети. Трафик может включать в себя различные типы данных, такие как текстовые документы, изображения, видео, аудио и другие формы мультимедиа.

Уровни трафика напрямую зависят от используемой модели сетевой архитектуры. Модель сетевой архитектуры в свою очередь определяет структуру и функции, которые выполняются на каждом уровне сетевого протокола для обмена данными между устройствами в сети. Она также определяет правила, по которым устройства взаимодействуют друг с другом, и формат данных, которые передаются между устройствами на каждом уровне. Существует несколько моделей сетевой архитектуры, но самой распространенной является модель OSI (Open Systems Interconnection) или модель семи уровней. Каждый уровень модели OSI имеет свои функции и выполняет определенные задачи в процессе передачи данных в сети. Эти уровни включают следующие.

Физический уровень (англ. «Physical Layer») - этот уровень определяет физические характеристики среды передачи данных, такие как электрические, оптические или радио характеристики. Он также определяет форматы данных, которые передаются через кабели или беспроводные среды.

Канальный уровень (англ. «Data Link Layer») - этот уровень управляет доступом к физической среде и обеспечивает надежную передачу данных между двумя устройствами. Он также обрабатывает ошибки, возникающие при передаче данных.

Сетевой уровень (англ. «Network Layer») - этот уровень управляет маршрутизацией данных в сети и определяет путь, который данные должны пройти от отправителя к получателю.

Транспортный уровень (англ. «Transport Layer») - этот уровень обеспечивает передачу данных между приложениями, работающими на разных устройствах в сети. Он также обеспечивает контроль над процессом передачи данных и гарантирует, что данные доставляются в нужном порядке.

Сеансовый уровень (англ. «Session Layer») - этот уровень управляет установлением и поддержкой соединения между устройствами во время передачи данных.

Уровень представления (англ. «Presentation Layer») - этот уровень определяет формат данных, которые передаются между устройствами в сети, и обеспечивает их совместимость.

Прикладной уровень (англ. «Application Layer») - этот уровень определяет протоколы используемые приложениями для обмена данными в сети.

Трафик может находится как внутри сети, так и между сетями, включая Интернет. Содержимое трафика зависит от протокола, который используется в передаче данных.

Например, в трафике, передаваемом по протоколу HTTP (англ. «Hypertext Transfer Protocol»), содержатся запросы и ответы, отправляемые между веб-браузером и веб-сервером. Эти запросы и ответы могут содержать информацию о запрашиваемой веб-странице, используемых кукисах (англ. «Cookies»), заголовках запросов и ответов, и так далее.

Если же речь идет о трафике, передаваемом по протоколу FTP (англ. «File Transfer Protocol»), то внутри этого трафика содержится информация о передаваемых файлах, такая как имена файлов, размеры, даты создания и так далее.

Кроме того, внутри трафика может быть информация о маршрутизации пакетов, используемых протоколов, таких как IP (англ. «Internet Protocol») или TCP (англ. «Transmission Control Protocol»), а также о протоколах безопасности, таких как SSL (англ. «Secure Sockets Layer») или TLS (англ. «Transport Layer Security»). Каждый из этих протоколов влияет на содержимое трафика.

Помимо протокола в трафике передаётся содержимое, которое зависит от протокола. Содержимое, например, это какие-то данные, отправляемые пользователем через веб-сайт, электронные письма, файлы, загружаемые на сервер, и т.д. Помимо содержимого в трафике может быть информация о конкретных устройствах, которые передают данные. Например, это может быть IP-адрес отправителя и получателя, информация о типе и версии операционной системы, типе и версии браузера и т. д.

Еще один важный аспект трафика — это метаданные, такие как время передачи, длительность соединения, количество переданных данных и т. д. Эти метаданные могут быть использованы для мониторинга и анализа сетевой активности, а также для оптимизации производительности системы.

1.2 Анализ трафика

Анализ трафика является важным инструментом для администраторов сети, аналитиков и специалистов по безопасности, которые работают с компьютерными сетями. Анализ трафика может использоваться для различных целей [1].

Отслеживание использования ресурсов сети: в данной реализации анализ трафика позволяет администраторам узнать, какие приложения и устройства используют большую часть сетевых ресурсов, и определить возможные узкие места в инфраструктуре.

Диагностика проблем с сетью: в данной реализации анализ трафика позволяет помочь выявить и исправить проблемы в работе сети, такие как перегрузки, пакетные потери или задержки, которые могут повлиять на производительность и работу приложений.

Оптимизация сети: анализ трафика позволяет администраторам оптимизировать настройки сети для улучшения производительности и безопасности.

Обнаружение вредоносных программ: анализ трафика может помочь выявить вредоносные программы и другие угрозы безопасности, которые могут находиться в сети.

Повышение безопасности сети: анализ трафика позволяет специалистам по безопасности выявить уязвимости в сети и принять меры для устранения их, а также защитить сеть от атак.

Мониторинг пользовательской активности: В данной реализации анализ трафика может помочь администраторам отслеживать активность пользователей в сети, что может быть полезно для контроля использования ресурсов, обеспечения соблюдения правил и политик безопасности.

Анализ трафика применяется в различных областях, где необходимо управлять и обеспечивать безопасность сетей, а также оптимизировать их производительность. Некоторые примеры применения анализа трафика включают в себя:

Корпоративные сети. В данной области анализ трафика используется администраторами сетей, чтобы управлять и осуществлять мониторинг корпоративной сети, обеспечивать безопасность и оптимизировать производительность и контроль использования ресурсов [3].

Интернет-провайдеры. В данной области анализ трафика используется для мониторинга и управления своими сетями, обеспечения качества обслуживания и оптимизации производительности.

Кибер-безопасность: В данной области анализ трафика необходим специалистам по кибер-безопасности для выявления и предотвращения угроз безопасности, таких как вредоносные программы, кибер-атаки, утечки данных и другие.

Разработка сетевых приложений. В данной области применение анализа трафика используется разработчиками сетевых приложений для определения проблем в работе сетевого кода и оптимизации производительности приложений [7].

Маркетинг. В данной области применение анализа трафика используется маркетологами для изучения поведения пользователей в Интернете, определения предпочтений и потребностей пользователей и анализа эффективности рекламных компаний.

Исходя из выявленных целей и применяемости анализа трафика, можно сказать, что анализ трафика является важным инструментом для управления и обеспечения безопасности сетей, а также для оптимизации их производительности [8].

Говоря об анализе трафика следует упомянуть, что с развитием технологий также развиваются и виды анализа трафика. Связано это с тем, что появляются такие технологии как: облачные вычисления, интернет-вещи, 5G и многие другие. С появлением этих технологий возникают новые требования к анализу трафика.

Изначально анализ трафика происходил вручную или с помощью специализированных программных инструментов, которые были разработаны и поддерживались вручную. В то время, когда интернет-соединения были медленными и трафик был намного меньше, чем сегодня, этот подход мог бы быть достаточным.

Однако с развитием интернета, объёмы трафика значительно выросли, а спектр используемых протоколов стал более разнообразным. В связи с этим, стали возникать новые требования к технологиям анализа трафика.

Сегодня существуют мощные системы анализа трафика, которые используют методы машинного обучения и искусственного интеллекта, а также способны обрабатывать огромные объёмы данных в режиме реального времени.

1.3 Виды анализа трафика

Исходя из задачи того, что нужно получить при анализе трафика выбирается определенный вид анализа. Иными словами, определенный вид анализа трафика — решает определенную задачу. Существует несколько видов анализа трафика.

Анализ пакетов (англ. «Packet analysis») - это процесс анализа сетевого трафика на уровне отдельных пакетов. Аналитики используют этот метод для отслеживания и идентификации различных типов трафика, а также для выявления проблем в сетевой инфраструктуре.

Анализ потоков (англ. «Flow analysis») - это метод анализа сетевого трафика на основе потоков данных, которые проходят через определенную точку в сети. Этот метод позволяет аналитикам получить информацию о трафике, связанном с конкретными приложениями и устройствами, а также о трафике, связанном с конкретными пользователями.

Анализ протоколов (англ. «Protocol analysis») - это метод анализа сетевого трафика на основе протоколов, используемых для передачи данных. Аналитики используют этот метод для изучения работы конкретных протоколов, выявления потенциальных проблем с протоколами и для повышения безопасности сетевой инфраструктуры.

Анализ контента (англ. «Content analysis») - это метод анализа содержимого сетевого трафика, такого как текстовые данные, изображения и видео. Этот метод используется для выявления нежелательного контента, такого как спам, вредоносное ПО и другие угрозы безопасности.

Поведенческий анализ трафика (англ. «Behavioral analysis») - это метод анализа сетевого трафика, который позволяет выявлять необычные или вредоносные действия пользователей и устройств в сети на основе их поведения.

Исходя, из приведенных типов можно сделать вывод, что использоваться различные технологии анализа трафика могут для различных целей, в зависимости от потребностей сетевого администратора или аналитика. Поведенческий анализ трафика в свою очередь используется в основном для изучения поведения пользователей в сети, а именно для анализа того, как они используют ресурсы сети, какие запросы они отправляют, какие сайты посещают, как долго они находятся на каждой странице и каким образом они взаимодействуют с веб-сайтами и приложениями.

1.4 Формирование требований к системе для поведенческого анализа трафика

Для того, чтобы информационная система, нацеленная на поведенческий анализ трафика поведения пользователей в сети работала корректно, требуется составить основные требования к системе [2]. Рассмотрим требования подробнее.

Высокая скорость обработки: система должна быть способна обрабатывать большие объемы данных в режиме реального времени.

Гибкость: система должна быть гибкой и масштабируемой, чтобы соответствовать требованиям различных видов анализа поведения пользователей в сети.

Совместимость: система должна быть совместимой с различными типами сетевых устройств и форматами сетевых данных.

Надежность: система должна быть надежной и безопасной, чтобы защитить данные от несанкционированного доступа и потерь.

Аналитические возможности: система должна предоставлять широкий спектр аналитических инструментов, позволяющих обнаруживать аномалии и выявлять связи между различными видами поведения пользователей.

Удобство использования: система должна быть простой и удобной в использовании различных пользователей, включая сетевых администраторов, инженеров, аналитиков и менеджеров.

Возможность интеграции: система должна предоставлять возможность интеграции с другими системами и приложениями для обеспечения более широкого использования и анализа данных.

Поддержка больших объемов данных: система должна быть способна обрабатывать большие объемы данных и хранить их в соответствующем формате.

Поддержка алгоритмов машинного обучения: система должна предоставлять возможность применять алгоритмы машинного обучения для обнаружения аномалий и предсказания будущего поведения пользователей в сети.

Также для эффективности подобной системы требуется составить еще и функциональные требования к системе:

Сбор данных. Информационная система должна иметь возможность собирать данные о сетевом трафике, а также хранить их для последующего анализа.

Идентификация и аутентификация пользователей: для анализа поведения пользователей в сети необходимо иметь возможность их идентифицировать и аутентифицировать.

Классификация трафика. Система должна уметь классифицировать трафик по типу протокола, источнику и назначению, чтобы обеспечить более точный анализ.

Анализ и обработка данных. Информационная система должна иметь возможность проводить анализ данных с целью выявления аномалий в поведении пользователей, а также обрабатывать данные для создания отчетов и визуализации результатов.

Мониторинг и уведомление. Система должна обеспечивать мониторинг сетевого трафика в режиме реального времени и уведомлять о возможных аномалиях и нарушениях безопасности.

Интеграция с другими системами: информационная система для поведенческого анализа трафика должна иметь возможность интеграции с другими системами безопасности и управления сетью.

Соответствие законодательству: система должна соответствовать требованиям законодательства в области защиты персональных данных и конфиденциальности.

Удобства использования: система должна быть удобной и простой в использовании, чтобы обеспечить эффективную работу аналитиков и специалистов по информационной безопасности.

1.5 Обзор и анализ существующих систем

На рынке информационных технологий уже существуют готовые системы для задач поведенческого анализа трафика. Особенность выбора той или иной готовой системы заключается в том, что некоторые из них предназначены для использования в корпоративной среде, в то время как другие предназначены для использования в крупных провайдерах сетевых услуг[4]. Некоторые из известных систем для поведенческого анализа трафика.

Bro – это система для анализа трафика, разработанная в университете Калифорнии в Беркли. Она может анализировать трафик на всех уровнях

OSI-модели и предоставляет возможность создавать свои собственные сценарии анализа трафика.

Snort – это система обнаружения вторжений, которая также может использоваться для анализа трафика. Она может обнаруживать и блокировать различные виды атак, включая атаки на основе подписок и атаки на основе содержимого.

Wireshark – это популярная система для анализа трафика, которая предоставляет детальную информацию о каждом пакете трафика, включая заголовки и данные. Wireshark также позволяет фильтровать трафик, чтобы отобразить только определенные типы пакетов.

Argus – это система, которая может анализировать большие объемы трафика и предоставлять информацию о поведении пользователей, включая информацию о времени и длительности соединения, исходящие и входящие IP-адреса и порты.

NetWitness – это система для поведенческого анализа трафика, которая может обнаруживать и предотвращать атаки, а также отслеживать вредоносное поведение пользователей и утечки конфиденциальной информации.

Splunk – это платформа для анализа данных, которая может использоваться для анализа трафика. Она может анализировать различные источники данных, включая трафик, и предоставлять визуализацию для анализа данных.

NTA (Network Traffic Analysis) - эта система обеспечивает обнаружение сетевых угроз, анализ трафика и обнаружение аномальных поведений пользователей в режиме реального времени. Использует алгоритмы машинного обучения для автоматического обнаружения аномалий и предоставляет детальные отчеты для дальнейшего анализа.

Выбор системы зависит от конкретных требований и задач, потому что каждая система имеет свои особенности и недочеты. Теперь поговорим о

каждой системе с точки зрения анализа поведенческого трафика и особенностей работы.

Bro – имеет открытый исходный код, позволяет анализировать трафик в режиме реального времени и обеспечивает обширные возможности по анализу трафика, такие как сбор метаданных, сигнатурное обнаружение, анализ содержимого пакетов и другие. Система Bro имеет широкие возможности для настройки и расширения, и может быть интегрирована с другими инструментами.

Snort – это инструмент для обнаружения вторжений на основе правил, который может быть использован для анализа сетевого трафика. Snort использует базу данных правил для обнаружения аномалий в трафике, включая известные атаки, а также события, которые могут указывать на новые угрозы. Snort также может работать в режиме реального времени и поддерживает множество протоколов.

WireShark – поддерживает множество протоколов и может показывать содержимое пакетов, которые передаются по сети. Также позволяет просматривать детали каждого пакета и проводить фильтрацию и поиск по трафику.

Argus – может анализировать трафик в режиме реального времени, а также анализировать сохраненные данные. Система собирает метаданные о трафике и может выполнять анализ с использованием различных алгоритмов и моделей.

NetWitness – может анализировать трафик в режиме реального времени. Использует множество методов для анализа трафика, включая сбор метаданных, анализ содержимого пакетов и использование машинного обучения для обнаружения аномалий.

Splunk – Собирает и анализирует данные в реальном времени. Данная система легко масштабируется и может быть интегрирована с другими системами для автоматического сбора и обработки данных. Предоставляет

мощный поиск и анализ данных, что ускоряет процесс обработки и поиска необходимой информации. Splunk визуализирует данные для пользователя. Обеспечивает высокий уровень безопасности при работе с конфиденциальной информацией.

NTA – может анализировать трафик с помощью различных методов, включая анализ сигнатур, машинное обучение и поведенческий анализ. Может обнаруживать угрозы, включая вредоносное ПО, атаки DdoS, кражу данных и другие типы атак на сетевую инфраструктуру. Предоставляет визуализацию трафика. Интегрируется в другие системы. Может помочь в анализе производительности сети, выявляя проблемы с пропускной способностью и другими проблемами, которые могут повлиять на качество обслуживания. Также данная система может предоставлять подробные отчеты, которые могут быть использованы для анализа и оптимизации работы сети и систем безопасности.

Опишем недостатки каждой из систем.

Bro – ограниченная поддержка протоколов, что может ограничить его способность обнаруживать аномалии в трафике. Также требует достаточно высокой мощности обработки, что может потребовать больших затрат на оборудование.

Snort – Низкая точность обнаружения, что может привести к ложным срабатываниям или пропускам. Также не поддерживает динамическое создание правил, что ограничивает его способность адаптироваться к новым угрозам. Не имеет интегрированной системы хранения и анализа данных

WireShark – Не имеет встроенной системы обнаружения аномалий и требует ручного анализа трафика для выявления угроз, работает на уровне пакетов, что может усложнить анализ сетевых протоколов, работающих на более высоких уровнях.

Argus – Не имеет встроенной системы обнаружения аномалий и требует ручного анализа трафика для выявления угроз. Требует дополнительной настройки для работы с новыми сетевыми протоколами.

NetWitness – сложная настройка и использование, что требует опытных специалистов. Высокая стоимость лицензии и обслуживания.

Splunk - Высокая стоимость лицензии и обслуживания. Требуется настройка и адаптация для работы с новыми протоколами и угрозами.

NTA – ограниченные возможности для анализа SSL – трафика, что может привести к упущению важных угроз, требует настройки и интеграции с другими системами для полноценного анализа трафика.

Выводы по главе 1

Таким образом, в рамках первой главы было проведено исследование существующих разработок в рамках поведенческого анализа трафика с выявлением их достоинств и недостатков. Полученные данные можно будет использовать в рамках разработки собственной методики.

Глава 2 Разработка методики и тестирование

2.1 Определение целей и области применения

Любые методики имеют конечного потребителя на которого они нацелены и чьи задачи они решают [16]. Конечным потребителем методики по поведенческому анализу трафика для предотвращения сетевых угроз может быть широкий круг организаций и индивидуальных пользователей, которые желают обеспечить безопасность своих сетей и данных. Ниже приведены примеры конечных потребителей.

Корпорации и предприятия: Крупные организации и компании, особенно те, которые хранят и обрабатывают большие объемы конфиденциальных данных, могут использовать методику поведенческого анализа трафика для защиты своей сетевой инфраструктуры от различных угроз, включая внедрение вредоносного программного обеспечения, несанкционированного доступа и утечку данных.

Провайдеры услуг безопасности: Компании, предоставляющие услуги безопасности сети, могут использовать методику поведенческого анализа трафика как часть своего арсенала инструментов для обнаружения и предотвращения сетевых угроз. Они могут предлагать эту услугу своим клиентам в качестве дополнительного уровня защиты и мониторинга.

Государственные организации: Государственные учреждения и организации могут использовать методику поведенческого анализа трафика для обеспечения безопасности своих сетей и защиты критической инфраструктуры от кибер-угроз. Это может включать военные организации, правительственные агентства и органы правопорядка.

Индивидуальные пользователи: Даже индивидуальные пользователи могут использовать методику поведенческого анализа трафика, чтобы защитить свои домашние сети и персональные данные от кибер-угроз.

Некоторые антивирусные программы и бренды межсетевых экранов включают в себя функциональность поведенческого анализа для обнаружения аномальной активности и предотвращения угроз.

Главная цель методики заключается в том, чтобы предотвращать сетевые атаки внутри системы по архитектуре «клиент — сервер» при помощи поведенческого анализа трафика.

2.2 Выявление основных концепций и принципов методики

Концепции в подобной методике продиктованы техническими потребностями ИС для того, чтобы реализовать предотвращение сетевых угроз при помощи поведенческого анализа трафика. Исходя из исследования выше, можно сделать вывод, что требуется внедрить в методику следующие принципы и концепции.

Работа с трафиком в режиме реального времени. Данная концепция методики говорит о том, что все процессы, которые происходят с трафиком происходят в реальном времени. Таким образом, данная методика приобретает плюс в виду скорости реакции персонала на наличие какой-либо угрозы в сети.

Полная интеграция в сервер. Данная концепция говорит о том, что интеграция модуля в сервер происходит прямо в ядре сервера, что одновременно сказывается плохо на интегрируемости самой системы, но в тоже время хорошо сказывается на доступе к ресурсам и защищенности, ведь не приходится проводить мост между модулями подвергая данные опасности.

Анализ поведения пользователей в системе. Основная идея этого концепта заключается в анализе текущего трафика и сравнении его с предварительно определенными профилями поведения пользователей. Алгоритмы анализа могут использовать методы машинного обучения и

статистического моделирования для выявления аномальных паттернов или отклонений от типичного поведения.

Выявление аномалий: Основной принцип этой мтеодики заключается в обнаружении аномалий в трафике и поведении пользователей. При анализе трафика и сравнении с профилями поведения система ищет необычные, подозрительные или аномальные паттерны, которые могут указывать на наличие сетевых угроз, таких как вторжения или злоумышленная активность.

Оповещение и реакция: Когда система обнаруживает аномалии или подозрительную активность, она генерирует уведомления или предупреждения, чтобы операторы или администраторы сети могли принять соответствующие меры. Реакция может включать блокирование подозрительного трафика, исключение пользователя из сети или другие превентивные действия.

Сбор и регистрация данных. Этот концепт предполагает сбор и регистрацию данных о сетевом трафике пользователей. Это может быть достигнуто с помощью системы журналирования (логирования) сетевой активности, сетевых датчиков или анализаторов пакетов, которые захватывают и регистрируют информацию о трафике.

Конфиденциальность и защита данных: Важным принципом при использовании методики по поведенческому анализу трафика является обеспечение конфиденциальности и защиты данных пользователей. Система должна соблюдать соответствующие нормы безопасности и правила обработки данных, чтобы гарантировать, что личная информация пользователей не будет использоваться неправомерно или может попасть в неправильные руки.

Постоянное совершенствование. Методика по поведенческому анализу трафика должна быть подвергнута постоянному совершенствованию и обновлению. Угрозы и способы атак постоянно развиваются, поэтому

необходимо следить за новыми трендами и технологиями, а также активно совершенствовать методику для обеспечения более эффективной защиты сети и пользователей.

2.3 Подготовка ИС для тестирования

В рамках данной работы требуется протестировать разработанную методику на информационной системе архитектуры «клиент — сервер».

Архитектура «клиент-сервер» - это модель организации компьютерных систем, в которой функциональность разделена между клиентами и серверами, которые взаимодействуют друг с другом через сеть. В этой модели клиент — это устройство или программа, которая запрашивает и получает доступ к ресурсам или услугам, а сервер — это устройство или программа, которая предоставляет эти ресурсы или услуги. В данной архитектуре клиенты обычно выполняются на конечных устройствах, таких как персональные компьютеры, смартфоны или планшеты, и обладают ограниченными ресурсами. Серверы, с другой стороны, обычно представляют собой более мощные и высокопроизводительные системы, способные обрабатывать больший объем данных и обеспечивать доступ к общим ресурсам.

Клиенты и серверы взаимодействуют посредством сети, такой как локальная сеть (англ «LAN») или интернет. Клиенты отправляют запросы на сервер, а серверы обрабатывают эти запросы и возвращают ответы клиентам. Взаимодействие между клиентами и серверами осуществляется по определенным протоколам, таким как HTTP (протокол передачи гипертекста) для веб-приложения или SMTP (простой протокол передачи почты) для электронной почты. Примеры архитектуры «клиент-сервер» включают в себя веб-серверы, где веб-браузеры (клиенты) запрашивают веб-страницы у сервера, и сервер базы данных, где клиенты отправляют запросы

на получение или изменение данных в базе данных, которые обрабатываются сервером. Эта модель позволяет более эффективно организовывать и распределять ресурсы, а также обеспечивает возможность централизованного управления и обновления системы [11].

Задачей сервера в архитектуре «клиент-сервер» является выдача клиенту по уровню допуска определенной информации. В рамках работы с поведенческим анализом трафика, требуется работать с данными ориентированными на конкретного пользователя. Каждый пользователь является опасной точкой в системе. Поведенческий анализ трафика, направлен на то, чтобы обрабатывать эти опасные точки системы. Для того, чтобы выполнить поведенческий анализ трафика сервер должен предоставить нам возможность идентификации пользователей в системе [13].

Главной задачей сервера будет являться хранение какой-то конфиденциальной информации и предоставления к ней доступа, например, такой информацией могут являться сами логи потенциальных атак.

Для реализации идентификации пользователей в системе можно использовать различные методы аутентификации и хранение информации о пользователях. Иными словами, требуется добавить процесс регистрации и аутентификации, а при попытках доступа к тому или иному ресурсу проводить процесс авторизации. Также помимо этого стоит добавить ролевую модель на сервер. Для этого требуется определить роль пользователей в системе и разграничить их права на основе этих ролей.

Некоторые пользователи могут иметь более привилегированный доступ, чем другие [10]. Например, администраторы системы могут иметь доступ к административным функциям, которые обычным пользователям недоступны. На рисунке 1 представлена базовая схема архитектуры «клиент-сервер».

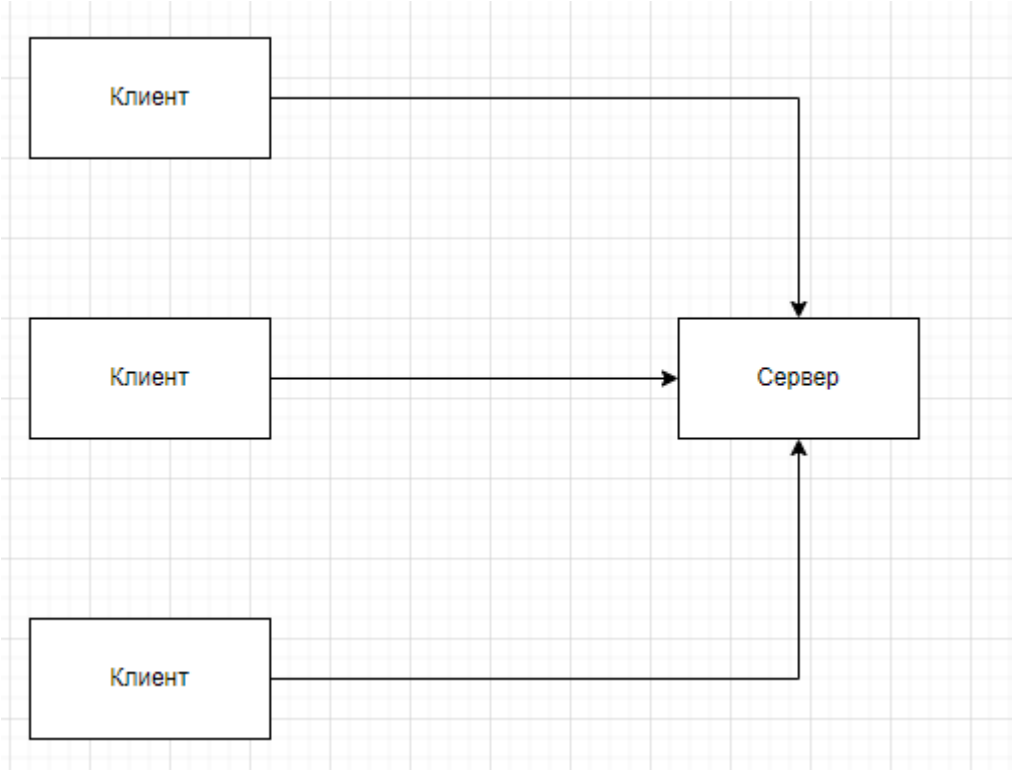

Рисунок 1 — Схема архитектуры «клиент-сервер»

Исходя из этого в рамках ИС требуется реализовать программный код для сервера, который будет взаимодействовать с базой данных, а также реализовать программный код клиента для обращения к серверу [20].

Для хранения данных требуется спроектировать базу данных. Требуется хранить данные пользователей, данные посещений и данные взаимодействия с системой [19]. На рисунке 2 представлена полученная база данных.

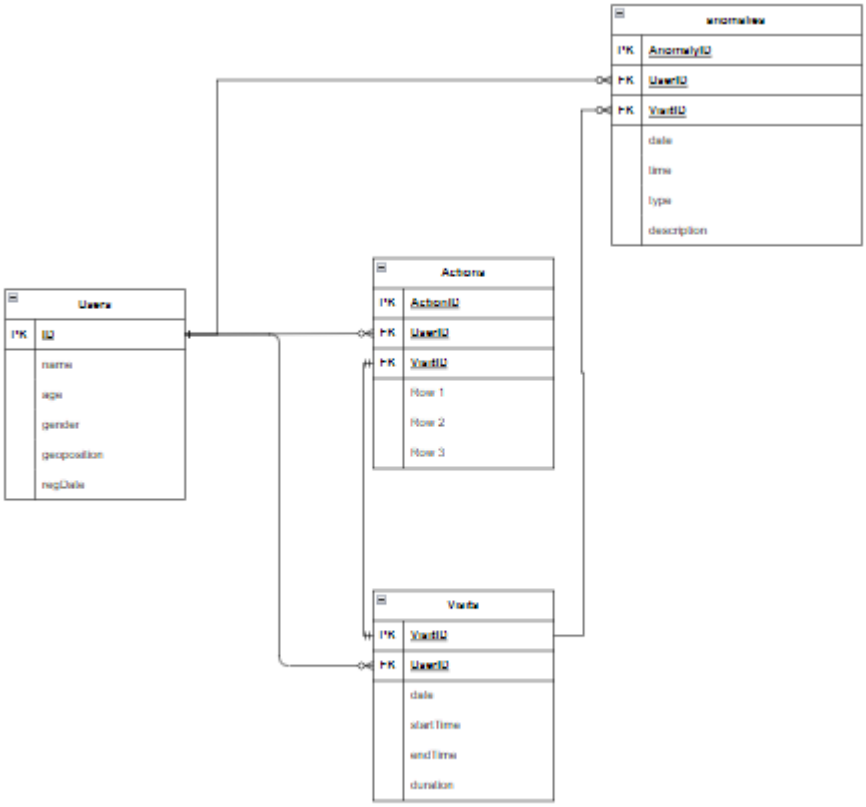

Рисунок 2 — Схема базы данных

На основе данных требований было выполнено проектирование базы данных для хранения необходимой информации [9].

В рамках разработки тестовой информационной системы на основе полученных принципов и концепций требуется использовать язык Java. На нем будет реализован программный код сервера, который в будущем можно полностью сделать модульным для полной интеграции в ИС потребителя. В рамках работы с данным языком программирования можно выделить следующий ряд основных технологий [13].

Java Servlet Api: является стандартной технологией Java для создания серверных приложений. Она предоставляет набор классов и интерфейсов для разработки и обработки HTTP-запросов. Servlet-контейнер, такой как Apache Tomcat или Jetty, обеспечивает запуск и управление сервлетами [17].

JavaServer Pages (JSP): является технологией Java для создания динамических веб-страниц с использованием Java-кода и HTML-шаблонов. JSP-страницы также выполняются на сервере и могут быть развернуты вместе с сервлетами на контейнере сервлетов [15].

JavaServer Faces (JSF): является компонентным фреймворком для разработки пользовательских интерфейсов веб-приложений. Он предоставляет набор готовы компонентов и API для управления состоянием пользовательского интерфейса. JSF-приложения также запускаются на контейнере сервлетов.

Spring Framework: Spring является одним из наиболее популярных фреймворков разработки приложений на Java. Он предоставляет широкий набор функциональных возможностей, включая управление зависимостями, инверсию управления, аспектно-ориентированное программирование программирование и т. д. Spring предоставляет также средства для создания серверных приложений, такие как Spring MVC для создания веб-приложений и Spring Boot для прощенного развертывания [5].

Java EE (Java Enterprise Edition): представляет собой спецификацию и набор технологий для разработки и развертывания корпоративных приложений на Java. Java EE включает в себя различные спецификации, такие как EJB (Enterprise JavaBeans), JPA (Java Persistence API), JMS (Java Message Service) и другие. Контейнеры приложений Java EE, такие как Apache TomEE, Glassfish и WildFly, предоставляют среду выполнения для развертывания и выполнения Java EE приложений [6].

Все эти инструменты обширны и функциональны, но в рамках задачи тестирования они слишком многовесны. Для тестирования существует эмуляция поведения реального сервера. Такая как: Mock-сервер, который представляет из себя инструмент для эмуляции или имитации поведения реального сервера или сервиса в контролируемой среде тестирования или разработки. Он не является полноценным сервером, а скорей представляет

собой специальный компонент или инструмент, который помогает в разработке и тестировании клиентского кода или интеграции с внешними сервисами, также на основе тестирования на Mock-сервере, можно протестировать анализ трафика при помощи поведенческого подхода.

Дальше требуется разработать имитацию сервера, работающего с HTTP-запросами. Данная система будет имитацией корпоративной сети, основанной на работе с внутренними веб-сайтами, связь с которыми устанавливается посредством HTTP-запросов. Таким образом, мы сможем идентифицировать какой пользователь пытается пройти авторизацию на какой ресурс в нашей сети, обрабатывать и собирать подобную информацию.

Вся имитация сервера будет представлена в одном файле расширения Java с классом «App». Данный класс будет обеспечивать сразу несколько основных задач сервера: обработка запросов от клиентов, работа с базой данных, обработка данных. На рисунке 3 представлена UML диаграмма класса App на стороне сервера [12].

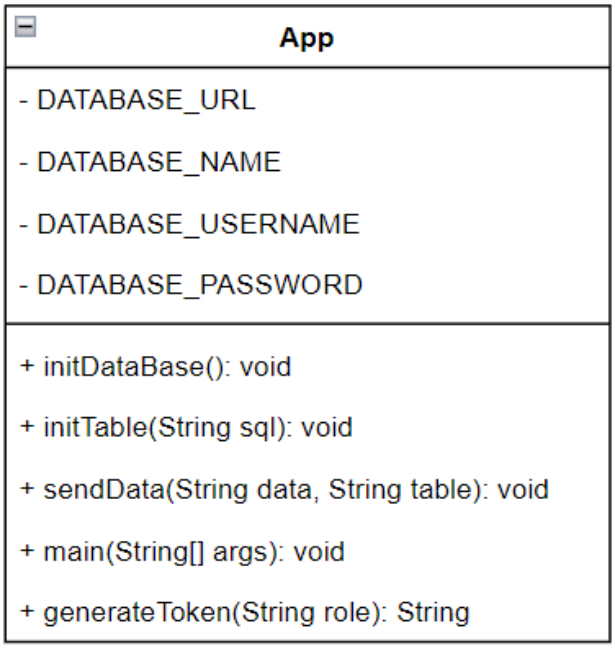

Рисунок 3 — Диаграмма класса App

Также помимо класса App внутри данного файла присутствует класс, который будет отвечать за хранение локального трафика, а также за его анализ. Это класс «BehavioralAnalysis» [14]. На рисунке 4 представлена схема полученного класса «BehavioralAnalysis».

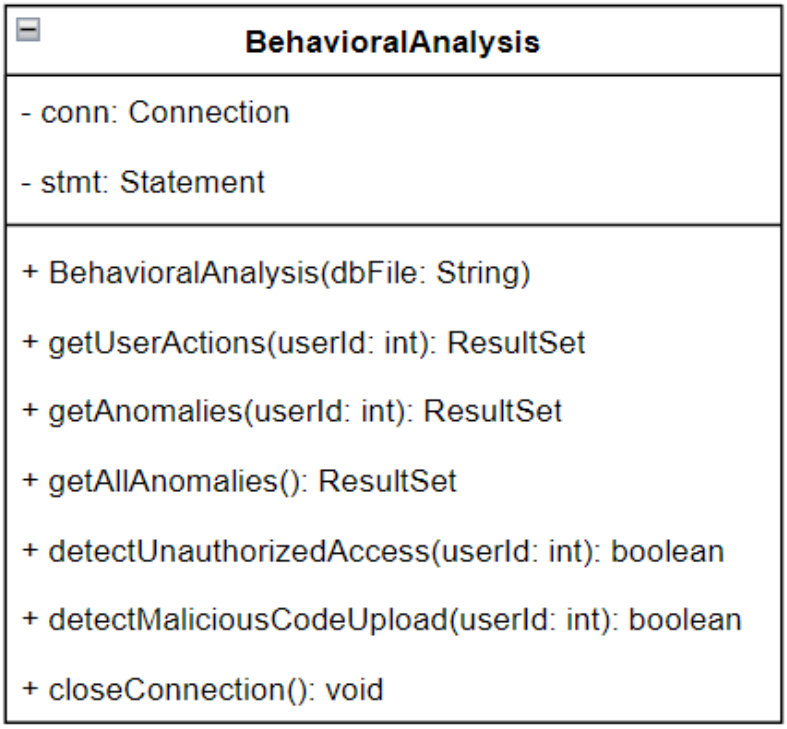

Рисунок 4 — Диаграмма класса «BehavioralAnalysis»

Конечный клиент зависит от потребительского продукта в которую будет интегрироваться полученная ИС или модуль по выявленной ранее методики.

2.4 Тестирование методики внутри ИС

Для оценки эффективности в будущем для не прикладных задач требуется выполнить определение метрики, по которой будет рассчитываться эффективность. В рамках данной выпускной работы метрикой

эффективности будут являться: точность обнаружения аномалий, ложные срабатывания, полнота обнаружения и время отклика.

Для того, чтобы узнать являются ли эти критерии выполненными, требуется использовать несколько подходов:

- подготовка тестовых данных;

- имитация реальных условий.

В рамках тестирования по имитации реальных условий мною были сделаны действия со стороны клиента, которые делает большинство людей, работающих в офисе. А именно я просто перемещался имитации по корпоративной сети. После чего все данные успешно появились в базе данных.

В рамках тестирования по тестовым данным, я подготовил заготовленные в базе данных данные и отдал команду системе выполнить их проверку. В результате получил данные по несанкционированному доступу, который пытался совершить при сборе тестовых данных.

Данные полученные во время тестирования:

- точность обнаружения аномалий: 200 аномалий вызвано, 180 нашлись;

- ложные срабатывания: 200 аномалий вызывано, не соответствуют данным;

- полнота обнаружения: реальных аномалий 250, обнаружено 230;

- общее время отклика на 1 единицу трафика: 0,5 секунд.

Выводы по главе 2

Таким образом, в рамках второй главы была разработана методика на основе исследования проведенного в первой главе. А также было проведено тестирование с использованием нескольких подходов полученной методики в испытательных условиях.

Глава 3 Анализ эффективности полученной методики

3.1 Эффективность полученной методики

При разборе эффективности полученной методики следует учитывать особенности процесса тестирования. Процесс тестирования был выполнен с прозрачными данными в рамках тестирования базовой работоспособности. На оценку эффективности напрямую влияют следующие факторы [21].

Качество и доступность данных. Качество и доступность данных используемых для обучения и тестирования методики, имеет прямое влияние на ее эффективность. Чем более репрезентативными и разнообразными являются данные, тем лучше методика будет способна обнаруживать аномалии и правильно классифицировать активности.

Пороговые значения и настройки. Пороговые значения и настройки методики также влияют на ее эффективность. Определение правильных порогов для классификации активностей и обнаружения аномалий помогает снизить количество ложных срабатываний и улучшить точность обнаружения.

Обновление и адаптация. Эффективность методики может улучшаться с течением времени благодаря обновлениям и адаптации. Постоянный мониторинг и обновление методики на основе новых данных и развития угроз позволяют снизить вероятность пропуска аномалий и улучшить ее общую производительность.

Инфраструктура и вычислительные ресурсы. Доступность и мощность вычислительных ресурсов, а также эффективность инфраструктуры обработки данных, такой как распределенные системы или высокопроизводительные вычисления, также могут влиять на эффективность методики. Более мощные ресурсы могут обеспечить более быструю обработку и анализ больших объемов данных.

В таблице 1 представлена статистика составленная по данным полученным во время тестирования.

Таблица 1 — Оценка эффективности полученной методики

Точность обнаружения аномалий	Ложные срабатывания	Полнота обнаружения	Время отклика
90%	10%	92%	500

На основе этих данных можно сказать, что методика является эффективной, но имеет некоторые недостатки и достоинства.

3.2 Эффективность поведенческого трафика вне методики

Поведенческий анализ трафика представляет собой процесс анализа паттернов и характеристик трафика, направленного на выявление необычного или подозрительного поведения. Этот подход позволяет выявить атаки, которые не могут быть обнаружены с помощью традиционных методов, основанных на сигнатурах или известных уязвимостях.

Преимущества использования поведенческого анализа трафика включают:

- обнаружение новых и неизвестных атак: Поведенческий анализ позволяет выявлять атаки, которые не соответствуют известным сигнатурам или моделям поведения. Это особенно полезно в случае новых или эволюционирующих угроз;

- раннее обнаружение атак: Анализ поведения трафика может помочь выявить подозрительные активности на ранних стадиях, еще до того, как атака достигнет своей цели. Это позволяет принять меры по предотвращению или минимизации ущерба;

- выявление скрытых атак: Некоторые атаки могут быть скрытыми и избегать обнаружения с помощью традиционных методов. Поведенческий анализ позволяет выявить подозрительные активности, которые могут быть незаметными в отдельности, но выделяются в контексте общего поведения.

Однако, стоит отметить, что поведенческий анализ трафика также может вызывать ложные срабатывания и требовать значительных вычислительных ресурсов для анализа больших объемов данных.

В целом, эффективность поведенческого анализа трафика зависит от правильной настройки и конфигурации системы, использования соответствующих алгоритмов и моделей, а также комбинации с другими методами обнаружения и защиты сетевых угроз.

Применение поведенческого анализа трафика в сфере борьбы с сетевыми угрозами может быть осуществлено через использование различных методов и инструментов. Некоторые из них включают:

- машинное обучение: Поведенческий анализ может включать использование алгоритмов машинного обучения для построения моделей и обнаружения аномалий в сетевом трафике. Это позволяет системе "обучиться" на основе предыдущих данных и выявлять новые или необычные паттерны;

- сетевые сенсоры: Установка сетевых сенсоров и мониторинг сетевого трафика позволяет собирать данные для последующего анализа. Сенсоры могут быть размещены на различных уровнях сети для обнаружения подозрительных активностей и аномального поведения;

- анализаторы трафика: Программные инструменты для анализа трафика позволяют обрабатывать и анализировать большие объемы данных, выявлять аномалии, коррелировать информацию и предоставлять отчеты о подозрительной активности;

- интеграция с системами обнаружения вторжений (IDS) и защиты от DDoS-атак: Поведенческий анализ трафика может быть использован в

сочетании с другими системами безопасности, такими как IDS или системы защиты от DDoS-атак, чтобы обнаруживать и предотвращать различные виды угроз.

В целом, эффективность поведенческого анализа трафика в борьбе с сетевыми угрозами зависит от правильной настройки и оптимизации системы, выбора подходящих методов и инструментов, а также обновления и адаптации системы к новым и развивающимся угрозам. Комбинация поведенческого анализа с другими методами обнаружения и защиты позволяет создать более эффективную систему обеспечения безопасности сети.

3.3 Описание недостатков полученной методики

Исходя из данных по оценке эффективности и результатах при тестировании можно выделить ряд недостатков полученной методики.

Ложные срабатывания: Алгоритмы анализа поведения могут иногда давать ложные срабатывания, то есть неправильно определять определенные активности как аномалии. Это может произойти, например, когда пользователь меняет свои обычные пути или ведет нестандартную активность, которая может быть истолкована как аномалия. Ложные срабатывания могут создавать лишнюю нагрузку для операторов и приводить к потере доверия к системе.

Требуется обучение и адаптация: Методика по поведенческому анализу трафика требует обучения на предварительных данных и постоянной адаптации к изменяющимся условиям. При внесении новых типов угроз или изменении поведения пользователей необходимо проводить обновление профилей и алгоритмов анализа. Это может требовать значительных усилий и времени для поддержания актуальности методики.

Зависимость от доступных данных. Качество и эффективность методики по поведенческому анализу трафика зависит от доступных данных. Если данные недостаточны или неполные, это может снизить точность выявления аномалий и угроз. При этом сбор и хранение больших объемов данных может требовать значительных ресурсов.

Сложность настройки: Реализация методики по поведенческому анализу трафика может быть сложной задачей. Это включает выбор подходящих алгоритмов анализа, определение пороговых значений для определения аномалий, настройку системы уведомлений и реакции на обнаружение. Неправильная настройка может привести к недостаточной или избыточной защите, а также к чувствительности к ложным срабатываниям.

Соблюдение конфиденциальности: Сбор и анализ данных о поведении пользователей могут вызывать вопросы о конфиденциальности и неприемлемом мониторинге личной информации. Для успешной реализации методики необходимо обеспечить соответствие соответствующим нормам и законодательству в отношении защиты данных и конфиденциальности. Система должна использовать анонимизацию или псевдонимизацию данных и соблюдать принципы минимальной необходимости сбора и использования личной информации.

Обход защиты: Атаки на сетевую инфраструктуру могут быть направлены на обход методики по поведенческому анализу трафика. Злоумышленники могут попытаться скрыть свою активность или подделать паттерны поведения, чтобы избежать обнаружения. Это может потребовать дополнительных мер по защите и обновлению методики для обнаружения новых методов обхода.

Сложность интерпретации результатов: Анализ поведения пользователей и выявление аномалий могут предоставить большое количество данных и результатов, которые требуют тщательной интерпретации. Операторы и аналитики должны иметь достаточный опыт и

знания для правильной оценки и понимания обнаруженных аномалий, чтобы принять соответствующие меры по предотвращению угроз.

В целом, методика по поведенческому анализу трафика является ценным инструментом для предотвращения сетевых угроз. Однако она также имеет свои ограничения и недостатки, которые требуют постоянного совершенствования и внимания к конфиденциальности.

3.4 Описание достоинств полученной методики

У полученной системы анализа трафика в сфере предотвращения сетевых угроз, которая анализирует поведение пользователей в системе есть ряд достоинств.

Обнаружение неизвестных угроз. Поведенческий анализ трафика позволяет обнаруживать неизвестные угрозы, которые не соответствуют известным сигнатурам или шаблонам атак. Это позволяет выявлять новые, ранее неизвестные виды угроз и защищаться от них.

Адаптивность к изменяющимся угрозам: Методика может обновляться и адаптироваться к новым видам угроз и изменяющемуся поведению пользователей. Это позволяет оперативно реагировать на новые угрозы и применять соответствующие меры защиты.

Идентификация внутренних угроз: Методика может помочь вам выявить внутренние угрозы, такие как несанкционированный доступ к данным или злоупотреблением привилегиями. Анализ поведения пользователей позволяет обнаружить аномалии в их активности, свидетельствующие о возможных нарушениях безопасности.

Минимизация ложны срабатываний: С использованием поведенческого анализа трафика можно достичь более точного выявления аномалий и снижения количества ложных срабатываний по сравнению с традиционными методами. Анализ поведения позволяет учитывать контекст

и уникальные характеристики каждого пользователя, что способствует точному выявлению и предотвращению угроз.

Улучшения реакции на инциденты: Методика позволяет оперативно обнаруживать и реагировать на инциденты безопасности. Анализ поведения пользователей и обнаружение аномалий позволяют операторам системы быстро распознавать подозрительные активности и принимать меры по предотвращению дальнейших нарушений.

Мониторинг в режиме реального времени. Методика позволяет выполнять мониторинг сетевого трафика в режиме реального времени, что позволяет оперативно реагировать на угрозы и аномалии. Система анализирует и нтерпретирует данные практически в реальном времени, обнаруживая подозрительные активности и выделяя их среди обычного трафика. Это позволяет операторам сети и администраторам принимать меры по предотвращению или минимизации ущерба от потенциальных угроз незамедлительно.

Выводы по главе 3

Таким образом, в третьей главе был выполнен анализ эффективности на основе данных полученных при тестировании из главы 2. А также были выявлены достоинства и недостатки полученной методики.

Заключение

В конечном счете, любая организация или индивидуальный пользователь, который ценит безопасность своей сети и данных, может быть потребителем методики поведенческого анализа трафика для предотвращения сетевых угроз. Это может включать банки, финансовые учреждения, интернет-провайдеров, онлайн-сервисы, электронную коммерцию и другие секторы, которые нуждаются в надежной защите от кибер-атак.

Методика поведенческого анализа трафика предлагает ряд преимуществ в обнаружении и предотвращении угроз, а также в быстрой реакции на аномалии и инциденты безопасности. Ее применение позволяет выявлять новые и неизвестные угрозы, адаптироваться к изменяющимся сценариям атак, идентифицировать внутренние угрозы, минимизировать ложные срабатывания, улучшать реакцию на инциденты и обеспечивать мониторинг в режиме реального времени.

Однако, как и любая методика, у неё также есть некоторые ограничения и недостатки, которые могу включать сложность реализации и интеграции, требования к вычислительным ресурсам и возможность ложных срабатываний. Поэтому при выборе и внедрении методики поведенческого анализа трафика необходимо учитывать специфические потребности и возможности организации, а также провести тщательное тестирование и обучение персонала для достижения максимальной эффективности в безопасности.

Описанные выше достоинства и потенциальные ограничения методики должны быть учтены при принятии решения о ее применении в конкретном контексте. Всегда рекомендуется проводить комплексный анализ рисков и преимуществ, а также обратиться к экспертам в области кибер-безопасности для получения совета и поддержки при реализации данной методики.

Список используемой литературы

1. Анализ трафика как инструмент исследования вычислительной сети Учебное пособие / Славнов К.В., Барсуков О.М, Игнатов Д.В., Воронеж: ООО «Ритм», 2019. – 380 с.
2. Бауэр, К. Java Persistence API и Hibernate / К. Бауэр, Г. Кинг, Г. Грегори ; под редакцией А. Н. Киселева ; перевод с английского Д. А. Зинкевич. — Москва : ДМК Пресс, 2017. — 632 с.
3. Беленькая, М.Н. Администрирование в информационных системах : учеб. пособие для студентов вузов, обучающихся по направлению 230100 «Информатика и вычислительная техника» / М.Н. Беленькая, С.Т. Малиновский, Н.В. Яковенко. – Москва : Горячая линия – Телеком, 2011. – 399 с.
4. Блох, Дж. Эффективное программирование на Java / Дж. Блох. — Санкт-Петербург: Диалектика, 2017. - 416 с.
5. Введение в Java программирование / Виктор В. Вагнер - Киев: Диафильм. - 160 с.
6. Изучаем JAVA на примерах и задачах / Р. В. Сеттер. — Санкт-Петербург : Наука и Техника, 2016. — 240 с.
7. Информационные системы и технологии / С.А. Клейменов, В.П.Мельников, А.М. Петраков. - Москва : Академия, 2008. - 271 с.
8. Клейменов, С.А. Администрирование в информационных системах: учебное пособие для студентов вузов, обучающихся по специальности «Информационные системы и технологии» / С.А. Клейменов, В.П.Мельников, А.М. Петраков. - Москва : Академия, 2008. - 271 с.
9. Колесов Ю. Б. Моделирование систем. Объектно-ориентированный подход: учебное пособие / Ю. Б. Колесов, Ю. Б. Сениченков. СПб.: БХВ-Петербург, 2012. – 192 с

10. Купер А. Интерфейс. Основы проектирования взаимодействия. 4-е издание: Питер, 2021. – 722с.

11. Мызникова, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Мызникова. — Омск : ОмГУПС, 2017. — 82 с. — ISBN 978-5-949-41160-5.

12. Романчик В.С, Блинов И.Н. Java. Методы программирования / Романчик В.С, Блинов И.Н. - Минск: издательство «Четыре четверти», 2013. - 896 с.

13. Шелухин, О. И. Моделирование информационных систем : учебное пособие / О. И. Шелухин. — 2-е изд., перераб. и доп. — Москва : Горячая линия-Телеком, 2012. — 536 с. — ISBN 978-5-9912-0193-3.

14. Шилдт, Г. Java: Полное руководство / Г. Шилдт — Москва: Вильямс, 2018. - 960с

15. Начинаем программировать на Java / Седжвик Р., Уэйн К., Донати Дж. - Москва : Вильямс, 2020. - 496 с.

16. Beginning Java Programming: The Object-Oriented Approach / B. Baesens, A. Backiel, S. Vanden Broucke. – 1st edition, Wrox. – 2015.

17. Deitel, H. Java How to Program / H. Deitel, P. Deitel. – 9th edition, Prentice Hall. – 2015

18. Getting started with IntelliJ IDEA // O. Hudson, Birmingham: Packt Publishing, 2013. – 114p

19. IntelliJ IDEA Essentials // J. Krochmalski. – Birmingham: Packt Publishing, 2014. – 263p.

20. Network security essentials: applications and standarts / William S. - Upper Saddle River, NJ : Pearson Education, 2003 – 409p

21. Testing Computer Software. / Kaner, Falk, Nguyen. – USA: Wiley, 2nd edition, 1999. – 480p.