Разработка программного обеспечения для мониторинга характеристик трафика в корпоративной компьютерной сети

Е.Е. Истратова, А.Е. Смирнов, Е.В. Глинин

***Аннотация* — В статье представлены результаты разработки и исследования программного обеспечения для мониторинга характеристик трафика в корпоративной компьютерной сети. Для реализации программного обеспечения предварительно был проведен анализ предметной области, выполнен обзор существующих решений, определена актуальность работы, на их основе было разработано программное обеспечение для мониторинга характеристик трафика в корпоративной компьютерной сети. В процессе работы были изучены различные инструменты и программное обеспечение для решения поставленной цели, разработан удобный пользовательский интерфейс, позволяющий за минимальное количество действий получить необходимую информацию о трафике, разработана база данных для хранения сессий захвата входящих и исходящих информационных потоков. Разработка программного продукта для мониторинга характеристик трафика в корпоративной компьютерной сети была выполнена с помощью объектно-ориентированного языка программирования C#. В рамках работы было проведено сравнение разработанного программного решения с четырьмя другими программами-аналогами, установленными в той же сети. Сравнение проводилось для входящего и исходящего трафика. В качестве критериев сравнения выступали показатели количества подключений и объема трафика. Результаты проведенных исследований позволили сделать вывод о том, что разработанный программный продукт можно применять для процессов мониторинга и планирования передачи данных в корпоративной сети компании.**

***Ключевые слова* — сетевой трафик, мониторинг трафика сети, программное обеспечение, корпоративная компьютерная сеть.**

I. Введение

Одной из базовых особенностей планирования и последующей разработки корпоративной сети компании является анализ характеристик сетевого подключения, основанный на проводимом периодически мониторинге сетевого трафика. Анализ сетевого трафика при передаче данных представляет собой один из ключевых параметров систем связи. Причиной этого является то, что его моделирование позволяет достаточно точно оценить и спрогнозировать динамику изменения трафика, выявить методы повышения качества обслуживания сети и оптимизировать расходы на операторов связи.

Оценка отдельных характеристик сетевого трафика может осуществляться как на основе реальных экспериментальных данных, так и при помощи процесса моделирования физических величин и механизмов. Причем оба эти направления могут быть реализованы при помощи анализа сетевого трафика в современных корпоративных компьютерных сетях. Для решения данной задачи необходимы сбор, обработка и анализ таких статистических показателей, как объем передаваемых данных и скорость данной передачи. Сбор подобной статистики осуществляется различными программными средствами.

II. Обзор программного обеспечения для сбора и анализа сетевого трафика

Применение корпоративных сетей позволяет оптимизировать работу за счет обеспечения совместного доступа к серверным программам, ресурсам и оборудованию, а также за счет ускорения обмена информацией и данными между сотрудниками. Таким образом, эффективность всего предприятия напрямую зависит от эффективности работы его корпоративной сети. Для учета и планирования роста сетевого трафика, анализа характеристик сетевого подключения целесообразно использовать специальные средства его мониторинга, называемые снифферами.

Согласно проведенному исследованию [1], ключевые характеристики сетевого подключения могут быть оценены, исходя из реальных экспериментальных данных или при помощи процесса моделирования. Причем оба эти способа могут быть реализованы за счет анализа сетевого трафика в современных информационных сетях. Для решения данной задачи необходимы сбор, мониторинг и анализ сведений о состоянии сети в процессе передачи данных. Сбор подобной статистики может осуществляться различными программными средствами.

В статье [2] предлагается решение для анализа сетевого трафика в операционных системах Windows, а также дается описание его инструментов, позволяющих выявить определенную избыточность сетевой активности. Кроме того, в исследовании представлены

Статья получена: 21 июля 2021.

Истратова Евгения Евгеньевна - Новосибирский государственный технический университет, (email:istratova@mail.ru)
Смирнов Алексей Евгеньевич - Новосибирский государственный технический университет, (email:alleex@inbox.ru)
Глинин Евгений Вадимович - Новосибирский государственный технический университет, (email:eugeny.glinin@yandex.ru)

результаты сравнительного анализа данного решения с наиболее распространёнными программными продуктами, выполняющими функции мониторинга сетевого трафика.

Статья [3] рассматривает разнообразие инструментов, применяемых для решения практических задач, связанных с анализом трафика. В настоящее время спектр инструментов очень широк – при этом каждый из них использует собственные алгоритмы разбора трафика и оперирует над своим внутренним представлением разобранных сетевых пакетов.

В литературном источнике [4] приводится сравнительный анализ основных из существующих на сегодняшний день методов анализа сетевого трафика. Если необходимо проанализировать небольшой трафик, то для этого рекомендуется использование бесплатных программ-снифферов. Если же речь идет о больших данных, то предполагается применение совокупности статистических методов или нейронной сети. Кроме того, анализ с помощью нейронных сетей – довольно перспективное и развивающееся направление, которое на сегодняшний день себя довольно хорошо зарекомендовало.

В работе [5] рассмотрены различные анализаторы сетевых протоколов с точки зрения применяемых в них способов перехвата сетевого трафика, а также продемонстрированы примеры практического применения программного инструмента Wireshark с учетом его ключевых преимуществ и недостатков.

В статье [6] рассмотрены проблемы анализа сетевого трафика, приведена их актуальность, а также изучены различные методы сбора пакетов через сеть Интернет, такие как: фильтрация и создание потоков для последующего анализа. По итогам исследования было получено системное представление о процессе анализа сетевого трафика.

В работе [7] был проведен анализ сетевого трафика локальной сети при помощи снифферов. На основании проведенного изучения основных понятий и определений компьютерных сетей, анализаторов трафика, назначения и принципа работы анализаторов трафика был проведен обзор и настройка анализатора трафика Wireshark.

В литературном источнике [8] приведен пример разработки программы, позволяющей захватывать сетевые пакеты, проходящие через выбранный сетевой интерфейс, что позволяет пользователю просматривать заголовки и содержимое пакетов.

В статье [9] предлагается новая объектная модель данных для углубленного анализа сетевого трафика. В отличие от модели, используемой большинством современных сетевых анализаторов, например, в Wireshark и Snort, предлагаемая модель поддерживает повторную сборку потока данных с последующим синтаксическим анализом. Программный продукт также предоставляет удобный универсальный механизм привязки парсеров, что позволяет разрабатывать полностью независимые парсеры. Кроме того, предлагаемая модель позволяет обрабатывать модифицированные - сжатые или зашифрованные — данные, что составляет основу инфраструктуры для глубокого анализа сетевого трафика.

Поскольку количество приложений, основанных на использовании сети Интернет, увеличивается, то трафик становится все более сложным. Таким образом, задача улучшения качества обслуживания и безопасности сети становится все более и более важной. В литературном источнике [10] изучается применение машины опорных векторов в идентификации трафика при классификации сетевого трафика. Посредством методов сбора данных и генерации признаков и методов проверки характеристик сетевого трафика машина векторов применяется в качестве классификатора с использованием возможности поддержки, а параметры и функции ядра машины векторов поддержки настраиваются и выбираются на основе перекрестных методов. Использование метода перекрестной проверки для получения наиболее разумной статистики при классификации и определении точности распознавания скорректированной машины опорных векторов позволяет избежать ситуации, когда точность классификации машины опорных векторов нестабильна или статистика неточна. В результате исследования была реализована система классификации и идентификации трафика на основе машины опорных векторов. Конечная скорость распознавания зашифрованного трафика составила 99,31%, что позволило преодолеть основные недостатки традиционной идентификации трафика и обеспечило достаточно надежную точность.

Современные корпоративные сети состоят из нескольких типов взаимосвязанных сетей. Кроме того, в этих сетях организации используют множество систем и приложений. Операционный и управленческий персонал должен обеспечивать эффективную, надежную и безопасную операционную среду для поддержки повседневной деятельности организации. В корпоративных сетях необходимо контролировать производительность, конфигурацию, безопасность, учет и устранение неисправностей. Современные методы управления обычно предполагают использование сложных для изучения и работы инструментов. Что крайне необходимо, так это набор простых, единообразных, повсеместных инструментов для управления сетями. Для устранения этих недостатков в проведенном исследовании [11] основное внимание было уделено использованию веб-технологий и технологии Multi-Router Traffic Grapher (MRTG) для мониторинга сетевого трафика предприятия и создания отчетов. Для этого сначала были исследованы требования к мониторингу, анализу и отчетности корпоративного сетевого трафика, а затем разработаны дизайн и способ реализации веб-системы мониторинга сетевого трафика и отчетности, которая удовлетворила этим требованиям. Также в статье были представлены рекомендации для анализа корпоративного сетевого

трафика.

В статье [12] предлагается адаптивная модель системы обнаружения сетевых атак в распределенной компьютерной сети. Система обнаружения основана на различных методах интеллектуального анализа данных, позволяющих отнести сетевое взаимодействие к нормальному или ненормальному в соответствии с набором атрибутов, извлеченных из сетевого трафика. Предлагаемая модель системы обнаружения вторжений является опосредованным средством мониторинга и анализа сетевого трафика и позволяет обеспечить защиту устройств сети Интернет вещей.

Контроль телефонного трафика — также одна из задач алгоритмов управления сетью и маршрутизации. В статье [13] представлено исследование двух групп магистральных каналов, по которым передается телефонный трафик, чтобы показать, что нестабильность может возникнуть, если есть задержка в получении информации обратной связи для сетевого контроллера. Сетевой контроллер пытается сбалансировать трафик в двух группах магистралей, которые могут представлять два пути от источника к месту назначения. Анализ показывает, как такие факторы, как время удержания, коэффициент усиления регулятора и задержка обратной связи, влияют на стабильность. Также проводится моделирование случая с двумя услугами, чтобы показать, что могут возникать такие же нестабильности.

Сетевая аналитика имеет ключевое значение для правильного управления сетевыми ресурсами, поскольку скорость интернет-трафика продолжает расти. Целью статьи [14] было исследование производительности различных инструментов захвата сетевого трафика для извлечения функций и оценки производительности восьми алгоритмов машинного обучения (ML) при классификации приложений, состояния и аномалий сети. Были также рассмотрены шесть Интернет-приложений, четыре состояния персонального компьютера пользователя в сети и две аномалии сети. Сеть отслеживалась тремя инструментами захвата трафика: PRTG, Colasoft Capsa и Wireshark, а классификация проводилась с помощью Weka Toolkit. Производительность восьми классификаторов машинного обучения была определена на основе нескольких показателей. Набор функций Colasoft Capsa обеспечил высочайшую точность классификации приложений, в то время как то же самое было достигнуто с помощью функций PRTG для классификации четырех рассматриваемых состояний. Что касается классификации аномалий, алгоритмы машинного обучения показали почти аналогичное поведение классификации при использовании набора функций Colasoft Capsa или PRTG.

Так как программное обеспечение для исследования сетевого трафика существенно различается по функционалу, то целесообразно провести его предварительную классификацию.

По функциональному назначению программное обеспечение для исследования трафика в корпоративных компьютерных сетях можно разделить на следующие три группы:

1) программное обеспечение для сбора характеристик сетевого трафика;
2) программное обеспечение для мониторинга сетевого трафика;
3) программное обеспечение для анализа сетевого трафика.

На основе проведенного литературного обзора были определены наиболее распространенные программные продукты для мониторинга сетевого трафика, к которым относятся следующие: NetTraffic, NetBalancer, BitMeter, BitTally.

III. Определение критериев оценки сетевого трафика

Помимо изучения функционала программ для анализа сетевого трафика, также необходимо учитывать собираемые и анализируемые с их помощью показатели сетевого трафика, непосредственно влияющие на качество передачи данных в корпоративной сети предприятия.

В ходе работы были выявлены основные показатели сетевого трафика, оказывающие влияние на качество подключения в корпоративной сети предприятия. К ним относятся: тип трафика (T); количество подключений (N) и объем трафика (V).

Тип трафика (T) — это количество переданных пакетов за единицу времени для конкретного протокола. Тип трафика зависит от протокола пакета. Каждый передаваемый пакет имеет в заголовке поле протокола (TCP/UDP/ICMP и т.д.). Разные протоколы отвечают за разные задачи, в основном: TCP – за гарантированную доставку пакета, UDP – за негарантированную доставку пакета (потоковое видео), ICMP – за передачу служебных данных.

Количество подключений узла корпоративной сети (N) – это количество компьютеров, с которыми происходит обмен данными. Данный параметр включает в себя: исходящий трафик, показывающий, на какое количество компьютеров идет передача данных; входящий трафик, определяющий, с какого количества узлов идет передача данных. Подозрительно большое количество подключений может означать, что компьютер в сети выполняет роль сервера раздачи (например, торрентов). Большой объем трафика при одном подключении можно интерпретировать как рабочий видеозвонок, или не относящийся к работе просмотр потокового видео.

Объем трафика (V) – объем информации, переданной и полученной в корпоративной сети.

Таким образом, целью исследования являлось проектирование программного обеспечения для мониторинга характеристик трафика в корпоративной компьютерной сети.

Для реализации указанной цели были решены задачи, связанные с анализом уже существующих программных

продуктов для изучения сетевого трафика; с определением ключевых показателей качества сетевого трафика; с разработкой алгоритма сбора характеристик сети за определенные промежутки времени; с организацией процессов хранения и визуализации результатов мониторинга сетевого трафика; с разработкой программного обеспечения для мониторинга сетевого трафика.

IV. Разработка программного обеспечения для мониторинга сетевого трафика

Предварительными этапами разработки программного обеспечения для мониторинга характеристик сетевого трафика стали определение точки сбора трафика в корпоративной сети и проектирование его алгоритма.
С целью минимизации изменений структуры корпоративной сети было принято решение о мониторинге внешнего сетевого трафика. В предлагаемой схеме компьютер с разработанным программным обеспечением устанавливается между маршрутизатором и оборудованием Интернет-провайдера. Тем самым, становится возможным осуществлять мониторинг всего проходящего по данному каналу связи сетевого трафика.

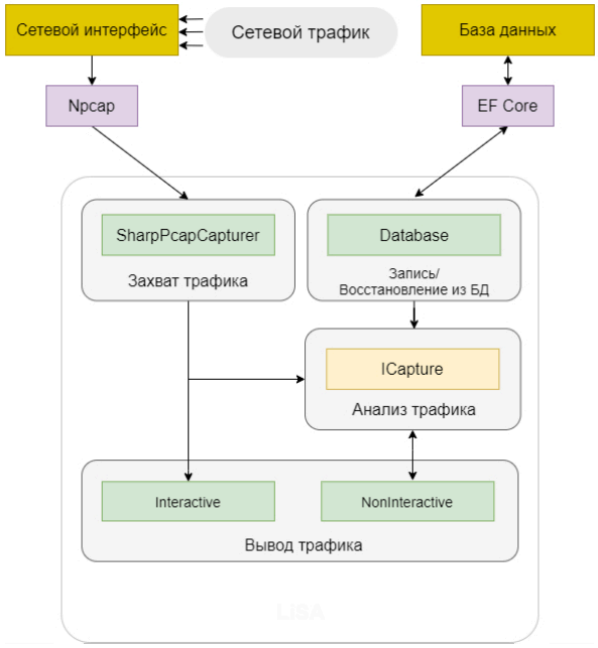

Рис. 1. Схема потока данных в разработанном программном обеспечении

На рис. 1 приведена схема взаимодействия компонентов программного обеспечения. При разработке программного продукта был определен класс Packet. Этот класс включает в себя такие поля как id, timestamp, src, dest, protocol, автоматическое свойство type. Поле id – напрямую не относится к захваченному пакету, но нужно для того, чтобы хранить объекты Packet в базе данных (требование фреймворка EFCore). Поле timestamp хранит в себе время, когда был захвачен пакет. Поля src и dest хранят адреса отправителя и получателя соответственно. Свойство type указывает на тип пакета и автоматически вычисляется на основании поля protocol.

Для того, чтобы получать пакеты с сетевого интерфейса и базы данных был выделен интерфейс ICapture. Это позволяет без изменения кода в графическом интерфейсом работать как с базой данной, так и с сетевым адаптером. Интерфейс ICapture описывает поля Name, Network, Packets, From, To, которые отвечают за имя сессии, адрес сети, захваченные пакеты, время начала и время окончания сессии захвата пакетов. Также интерфейс описывает методы для разделения трафика на входящий, исходящий и запроса трафика в указанных временных рамках.

SharpPcapCapturer реализует интерфейс ICapturer. Этот интерфейс описывает следующие свойства:

1. Name – имя источника пакетов;
2. ReceivedCount – количество полученных пакетов.

А также методы:

1. StartCapture() – начать сессию захвата пакетов;
2. StopCapture() – остановить сессию захвата пакетов;
3. GetCapture() – получить текущую сессию захвата пакетов.

Графический интерфейс принципиально разбит на две части: Interactive и NonInteractive (интерактивный и неинтерактивный соответственно). Interactive отображает статистику во время захвата пакетов. NonInteractive – анализирует и выводит статистику по сессии захвата пакетов.

Interactive рисует диаграмму с областями по количеству полученных пакетов. Интерфейс ICapturer описывает свойство receivedCount которое хранит в себе общее количество полученных пакетов. Чтобы рисовать диаграммы, запрашивается receivedCount с периодичностью одна секунда, и разница запрошенного значения с предыдущим выводится на экран.

NonInteractive рисует три диаграммы: столбчатая диаграмма по количеству подключений, круговые диаграммы по типу трафика и диаграмма с областями по объему трафика. На вход NonInteractive получает сессию захвата пакетов (ICapture). ICapture предоставляет только методы позволяющие разделить пакеты на входящие и исходящие. Поэтому NonInteractive реализует следующий функционал для вывода графиков.

Для отрисовки по количеству подключений NonInteractive группирует пакеты по источнику и назначению и выводит на диаграмму размер этих двух. Чтобы отрисовать круговую диаграмму пакеты группируются по типу и на график выводится размер этих групп. Для отрисовки графика с областями отображающего объем трафика список пакетов делится на группы по времени захвата с определенным шагом. На график выводится размер этих групп. Размер шага -

1/60 общего времени сессии захвата пакетов.

Программа захватывает все доступные пакеты на сетевом интерфейсе и делит их на входящие и исходящие. При запуске программа запрашивает у указанного интерфейса адрес и маску, с их помощью определяет адрес корпоративной сети. С помощью адреса сети определяется направление пакета. Чтобы программа работала, она должна находиться в корпоративной сети и получать на сетевой интерфейс пакеты из этой сети.

Следующим этапом работы стал выбор программных средств для реализации программного обеспечения. Было решено разрабатывать программное обеспечение для мониторинга ключевых характеристик сетевого трафика, ориентированное на работу с операционной системой Windows 10. Для захвата пакетов была выбрана оболочка SharpPcap над библиотекой Pcap, так как она легко добавляется в приложение с помощью системы управления пакетами NuGet и позволяет захватывать пакеты со всех интерфейсов. Также был выбран графический интерфейс WinUI 3, при этом для создания диаграмм был использован фреймворк Telerik UI.

V. Исследование разработанного программного обеспечения

С помощью разработанного программного обеспечения был проанализирован тип входящего и исходящего трафика. На рис. 2 представлена схема корпоративной компьютерной сети, для которой проводилось исследование, а на рис. 3 и 4 приведены результаты ее исследования. В рамках работы было проведено сравнение разработанного программного решения с четырьмя другими программами-аналогами, установленными в той же сети. Сравнение проводилось для входящего и исходящего трафика. В качестве критериев сравнения выступали показатели – количество и объем трафика.

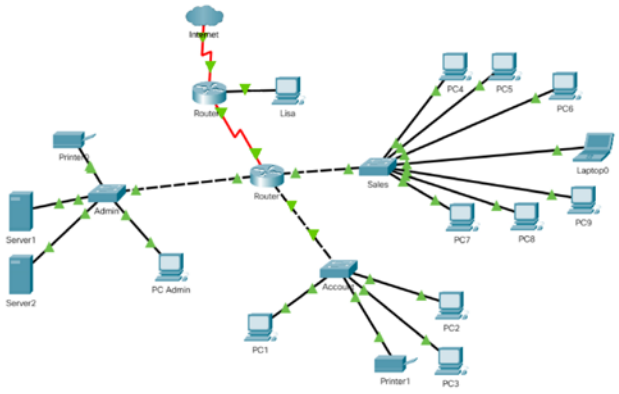

Рис. 2. Схема исследуемой корпоративной компьютерной сети

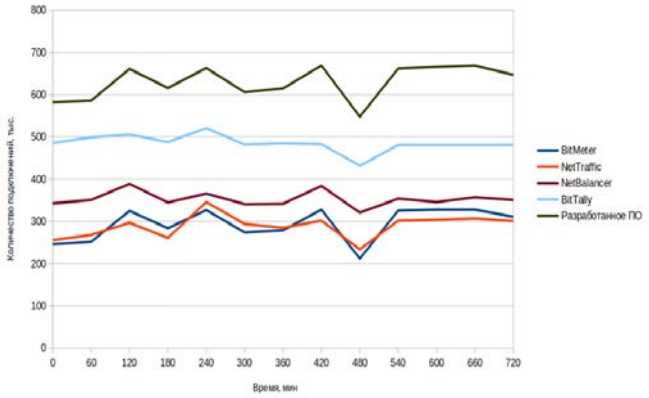

Рис. 3. Результаты исследования программного обеспечения по количеству подключений

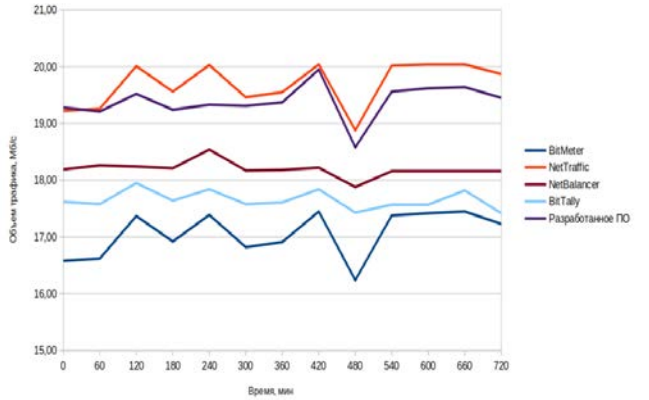

Рис. 4. Результаты исследования программного обеспечения по объему трафика

Согласно полученным данным, разработанное программное обеспечение показывает лучшие результаты. Помимо этого, в результате проведенного сравнительного анализа указанных программных продуктов можно выделить программу для мониторинга сетевого трафика NetTraffic, обладающую максимальным функционалом. Однако данный программный продукт является слишком громоздким для мониторинга трафика сетей небольших и средних предприятий. Программы NetBalancer и BitTally ориентированы на работу с небольшими сетями предприятий, но не обладают всем необходимым инструментарием для сбора необходимых характеристик сетевого трафика. Программный продукт BitMeter по своему функционалу уступает в случае повышенных требований к сбору характеристик сетевого подключения, которые предъявляются при проведении исследования сетевого трафика в корпоративных сетях или в научных целях. Таким образом, на основании результатов исследования можно сделать вывод о целесообразности разработки, так как программа по сравнению с аналогами демонстрирует лучшие результаты.

VI. Заключение

В результате работы были изучены различные

инструменты и программное обеспечение для решения поставленной цели, разработан удобный пользовательский интерфейс, позволяющий за минимальное количество действий получить необходимую информацию о трафике, разработана база данных для хранения сессий захвата входящих и исходящих информационных потоков.

Для дальнейшего развития данного программного обеспечения присутствует огромное поле возможностей. Одним из вариантов развития является применение программного обеспечения в действующей корпоративной сети, а также добавление дополнительного функционала, в соответствии с условиями работы конкретной корпоративной компьютерной сети.

Библиография

[1] Антонянц Е.Н., Амельченко А.О., Истратова Е.Е. Разработка программного обеспечения для исследования скорости передачи данных в корпоративной сети // International Journal of Open Information Technologies. 2021. Т. 9. № 2. [Электронный ресурс]. Режим доступа: http://www.injoit.ru/index.php/j1/article/view/1035.

[2] Wheeb A.H. Performance analysis of VoIP in wireless networks // International Journal of Computer Networks and Wireless Communications (IJCNWC). 2017. Т. 7. № 4. С. 1-5.

[3] Габдуллин А.Ш., Инкинин И.Ф., Сафиуллина Л.Х. Анализ сетевого трафика // Вектор развития управленческих подходов в цифровой экономике. 2020. № 2. С. 36-40.

[4] Медведев Д.О. Анализ сетевого трафика на предприятии // Доклады ТУСУР. 2017. № 3. С. 179-184.

[5] Андрианов И.А. Анализатор сетевого трафика // Вестник Брянского государственного технического университета. 2019. № 6. С. 38-49.

[6] Аронов В.Ю. Анализ характеристик сетевого трафика с помощью специализированных программ // Проблемы техники и технологии телекоммуникаций. Оптические технологии в телекоммуникациях. – 2018. – С. 104-105.

[7] Nor S.A., Alubady R., Kamil W.A. Simulated performance of TCP, SCTP, DCCP and UDP protocols over 4G network //Procedia computer science. – 2017. – Т. 111. – С. 2-7.

[8] Ivannikov V.P., Markin Y.V. Data representation model for in-depth analysis of network traffic. Program Comput Soft 42, 316–323 (2016). https://doi.org/10.1134/S0361768816050030.

[9] Zhu Y., Zheng Y. Traffic identification and traffic analysis based on support vector machine. Neural Comput & Applic 32, 1903–1911 (2020). https://doi.org/10.1007/s00521-019-04493-2.

[10] Hong J.W., Park SU., Kang YM. Enterprise Network Traffic Monitoring, Analysis, and Reporting Using Web Technology. Journal of Network and Systems Management 9, 89–111 (2001). https://doi.org/10.1023/A:1009481719707.

[11] Platonov V.V., Semenov P.O. Detection of Abnormal Traffic in Dynamic Computer Networks with Mobile Consumer Devices. Aut. Control Comp. Sci. 52, 959–964 (2018). https://doi.org/10.3103/S0146411618080217.

[12] Goodman R.M., Ambrose B.E. Stability of traffic patterns in broadband networks. J Netw Syst Manage 3, 371–380 (1995). https://doi.org/10.1007/BF02139530.

[13] Fowdur T.P., Baulum B.N. & Beeharry Y. Performance analysis of network traffic capture tools and machine learning algorithms for the classification of applications, states and anomalies. Int. j. inf. tecnol. 12, 805–824 (2020).

[14] AL-Dhief F.T. et al. Performance Comparison between TCP and UDP Protocols in Different Simulation Scenarios //International Journal of Engineering & Technology. – 2018. – Т. 7. – №. 4.36. – С. 172-176.

Development of software for monitoring the characteristics of traffic in a corporate computer network

E.E. Istratova, A.E. Smirnov, E.V. Glinin

***Abstract* — The article presents the results of the development and research of software for monitoring the characteristics of traffic in a corporate computer network. To implement the software, a preliminary analysis of the subject area was carried out, a review of existing solutions was carried out, the relevance of the work was determined, on their basis, software was developed for monitoring the characteristics of traffic in a corporate computer network. In the process of work, various tools and software were studied to solve this goal, a convenient user interface was developed that allows you to get the necessary traffic information in a minimum number of actions, a database was developed to store sessions for capturing incoming and outgoing information flows. The development of a software product for monitoring the characteristics of traffic in a corporate computer network was carried out using the object-oriented programming language C #. As part of the work, the developed software solution was compared with four other analogue programs installed in the same network. The comparison was carried out for incoming and outgoing traffic. The indicators of the number of connections and the volume of traffic were used as comparison criteria. The results of the research made it possible to conclude that the developed software product can be used for monitoring and planning data transmission in the corporate network of the company.**

***Keywords* — network traffic, network traffic monitoring, software, corporate computer network.**

REFERENCES

[1] Antonyanc E.N., Amelchenko A.O., Istratova E.E. Razrabotka programmnogo obespecheniya dlya issledovaniya skorosti peredachi dannyh v korporativnoj seti // International Journal of Open Information Technologies. 2021. V. 9. № 2. http://www.injoit.ru/index.php/j1/article/view/1035.

[2] Wheeb A.H. Performance analysis of VoIP in wireless networks // International Journal of Computer Networks and Wireless Communications (IJCNWC). 2017. V. 7. № 4. P. 1-5.

[3] Gabdullin A.SH., Inkinin I.F., Safiullina L.H. Analiz setevogo trafika // Vektor razvitiya upravlencheskih podhodov v cifrovoj ekonomike. 2020. № 2. P. 36-40.

[4] Medvedev D.O. Analiz setevogo trafika na predpriyatii // Doklady TUSUR. 2017. № 3. P. 179-184.

[5] Andrianov I.A. Analizator setevogo trafika // Vestnik Bryanskogo gosudarstvennogo tekhnicheskogo universiteta. 2019. № 6. P. 38-49.

[6] Aronov V.YU. Analiz harakteristik setevogo trafika s pomoshch'yu specializirovannyh programm // Problemy tekhniki i tekhnologii telekommunikacij. Opticheskie tekhnologii v telekommunikaciyah. – 2018. – P. 104-105.

[7] Nor S.A., Alubady R., Kamil W.A. Simulated performance of TCP, SCTP, DCCP and UDP protocols over 4G network //Procedia computer science. – 2017. – V. 111. – P. 2-7.

[8] Ivannikov V.P., Markin Y.V. Data representation model for in-depth analysis of network traffic. Program Comput Soft 42, 316–323 (2016). https://doi.org/10.1134/S0361768816050030.

[9] Zhu Y., Zheng Y. Traffic identification and traffic analysis based on support vector machine. Neural Comput & Applic 32, 1903–1911 (2020). https://doi.org/10.1007/s00521-019-04493-2.

[10] Hong J.W., Park SU., Kang YM. Enterprise Network Traffic Monitoring, Analysis, and Reporting Using Web Technology. Journal of Network and Systems Management 9, 89–111 (2001). https://doi.org/10.1023/A:1009481719707.

[11] Platonov V.V., Semenov P.O. Detection of Abnormal Traffic in Dynamic Computer Networks with Mobile Consumer Devices. Aut. Control Comp. Sci. 52, 959–964 (2018). https://doi.org/10.3103/S0146411618080217.

[12] Goodman R.M., Ambrose B.E. Stability of traffic patterns in broadband networks. J Netw Syst Manage 3, 371–380 (1995). https://doi.org/10.1007/BF02139530.

[13] Fowdur T.P., Baulum B.N. & Beeharry Y. Performance analysis of network traffic capture tools and machine learning algorithms for the classification of applications, states and anomalies. Int. j. inf. tecnol. 12, 805–824 (2020).

[14] AL-Dhief F.T. et al. Performance Comparison between TCP and UDP Protocols in Different Simulation Scenarios //International Journal of Engineering & Technology. – 2018. – V. 7. – №. 4.36. – P. 172-176.