МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
Кафедра IT-инжиниринг

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой
PhD, доцент
_____ .С. Картбаев
«____» _____ 2019г.

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Разработка ИС мониторинга и анализа интернет-трафика на основе протокола Netflow

Специальность 5В060200 – «Информатика»

Выполнила Якубчак М.М. Группа ИНФ-15-2
Научный руководитель ст. преподаватель Абсатарова Б.Р.

Консультанты:
по экономической части: к.э.н., доцент_____А.И.Бекишева
«02» 05 2019г.

по безопасности жизнедеятельности: д.т.н., ст. преп._____Ш.Ш.Бекбасаров
«____» _____ 2019г.

по применению
вычислительной техники: магистр, ст. преп._____М.Н.Майкотов
«____» _____ 2019г.

Нормоконтролер: ст. преп. _____Ж.К.Алимсеитова
«22» 05 2019г.

Рецензент: д.т.н., проф. _____Б.С.Ахметов
«____» _____ 2019г.

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Институт систем управления и информационных технологий

Кафедра IT-инжиниринг

Специальность 5В060200 – «Информатика»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Якубчак Милане Михаиловне

Тема работы: Разработка ИС мониторинга и анализа интернет трафика на основе протокола Netflow

Утверждена приказом по университету № 124 от «26» октября 2018 г.

Срок сдачи законченного проекта «01» июня 2019 г.

Исходные данные к работе (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): требования заказчика к функциональной части и пользовательскому интерфейсу приложения, нормативные и законодательные акты, внутриорганизационная документация, литературные и интернет-источники.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта:

а) анализ сетевого протокола;
б) выбор и настройка компонентов сети;
в) конфигурирование коллектора данных;
г) создание приложения в среде Visual Studio;
д) вопросы безопасности жизнедеятельности и охраны труда;
е) оценка экономической эффективности системы.

Перечень графического материала (с точным указанием обязательных чертежей): представлены 11 таблиц, 20 иллюстраций.

Основная рекомендуемая литература:

1 Таненбаум Э.С., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер,2012. — 960 с.

2 Куроуз Д.Ф., Росс К.В. Компьютерные сети. Нисходящий подход – М.: Эксмо,2016 – 912 с.

3 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010. — 944 с.

Консультации по работе с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Экономическая часть	Бекишева А.И.	19.03–02.05.19	
Безопасности жизнедеятельности	Бекбасаров Ш.Ш.	2.04–29.04.19	
Программная часть	Майкотов М.Н.	10.05.19	
Нормоконтролер	Алимсеитова Ж.К.	01.03.2019–15.05.2019	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Анализ сетевого протокола	11.02.2019-01.03.2019	Выполнено
Выбор и настройка компонентов сети	04.03.2019-29.03.2019	Выполнено
Конфигурирование коллектора данных	01.04.2019-12.04.2019	Выполнено
Сбор данных с маршрутизатора	15.04.2019-03.05.2019	Выполнено
Создание приложения в среде Visual Studio	06.05.2019-13.05.2019	Выполнено

Дата выдачи задания «24» октября 2018 г.

Заведующий кафедрой _____Т.С. Картбаев

Научный руководитель проекта_____Б.Р. Абсатарова

Задание принял к исполнению студент _____ М.М. Якубчак

Аңдатпа

Желі мониторингі - желінің бағытталған әсерінің бір бөлігі, ол белгілі бір бағдарламаға сәйкес жүзеге асырылады уақтылы қателіктерді және ақауларды жедел анықтау мақсатында.

Дипломдық жобада Netflow хаттамасына сәйкес осы желілік хаттаманың жіктемесі, жұмыс құрылымы, желі мониторингінің қолдану саласы толғырақ қарастырылды. Mikrotik желілік жабдықтардың маркасына ерекше назар аударылады: тарихы, нарықтағы бәсекеге қабілеттілігі, маршрутизаторлар мүмкіндігі.Осы жұмыстың практикалық бөлімінде желілік құрылғыны баптау, сервер – коллекторі роутердан мәліметтер жинау және бағдарламаға шолу жүргізіледі, бұл желі инженерлеріне жиналған деректердің ішінен қазіргі уақытта қажет нәрселерді жылдам іздеуге көмектеседі.Келесі тарауларда ақпараттық жүйенің экономикалық тиімділігін, сондай-ақ жүйе әкімшіліктерінің желі инфрақұрылымын іс жүзінде бақылайтын бөлмедегі кондиционерді кейіннен таңдауымен аспирациялық жүйені есептеуді қарастырады.

Аннотация

Мониторинг сети – это часть целенаправленного воздействия на сеть, которое осуществляется по какой-то заранее заданной программе с целью своевременного обнаружения в ней неисправностей и ошибок с быстрой реакцией на них.

В дипломном проекте продробно рассматривается область применения мониторинга сети, в частности по протоколу Netflow, класиификация данного сетевого протокола, структура работы. Особое внимание уделяется бренду сетевого оборудования Mikrotik: история возникновения, конкурентоспособность на рынке, возможности маршрутизаторов. В практической части данной работы производится настройка сетевого оборудования, сервера – коллектора для сбора данных от роутера и производится обзор программы, которая помогает сетевым инженерам быстрее искать среди собранных данных те, что необходимы в данный момент. В следующих главах рассматривается экономическая эффективность внедрения данной информационной системы, а также расчет аспирационной системы с последующим выбором кондиционера в помещении, откуда системные администраторы собственно и производят мониторинг сетевой инфраструктуры.

Abstract

Network monitoring is a part of the targeted impact on the network, which is carried out according to some predetermined program in order to timely detect faults and errors in it with a quick response to them.

In the thesis project, the area of application of network monitoring, in particular, according to the Netflow protocol, the classification of this network protocol, the structure of the work, is considered in detail. Particular attention is paid to the brand of network equipment Mikrotik: the history of emergence, competitiveness in the market, the possibility of routers. In the practical part of this work, the network equipment is configured, the server is a collector for collecting data from the router and a review of the program is made, which helps network engineers to quickly find among the collected data that are needed at the moment. The following chapters consider the economic efficiency of the implementation of this information system, as well as the calculation of the aspiration system with the subsequent choice of an air conditioner in the room, from which system administrators actually monitor the network infrastructure.

Содержание

Введение

В те времена, когда сети строились в основном на основе шинной топологии мониторинг трафика был не сложной задачей. Сети в то время имели разделяемую среду передачи, что упрощало в разы наблюдение за ними. Такая технология позволяла просто подсоединить к сети одно устройство, которое и следило за проходящим трафиком. Но времена идут, повышаются требования к такой характеристике сети, как пропускная способность, происходит развитие технологии коммутации пакетов. Эти факторы обусловили переход от разделяемой среды передачи к высокосегментированным топологиям. Теперь общий трафик нельзя прослушать из одной точки. Чтобы получить полную картину, необходимо производить мониторинг каждого порта. Из-за большого количества соединений типа «точка-точка» устанавливать приборы для мониторинга крайне неудобно, да и большое количество таких приборов превращает задачу мониторинга в дорогостоящую. Вдобавок сами коммутаторы и маршрутизаторы имели сложную архитектуру, и скорость обработки и передачи пакетов становилась важным фактором, определяющим производительность сети. Поэтому единственным реальным решением данной задачи является осуществление мониторинга трафика непосредственно внутри активного сетевого оборудования (в частности маршрутизаторов).

Целью проекта является разработка информационной системы мониторинга и анализа интернет трафика на основе протокола Netflow.

Задачи работы:

– изучение основ протокола Netflow;

– принцип работы и функционирования протокола;

– классификация протокола;

– реализация мониторинга;

– анализ трафика с помощью программы;

При написании проекта будет протестировано решение для анализа трафика, которое хранит информацию о пакетах в базе данных MySQL и с помощью C# выгружает данные в наиболее читабельном виде.

1 Теоретическая часть

1.1 Область применения системы

Мониторинг и управление компьютерной сетью является важной и обязательной задачей как для сетевого инженера, так и для системного администратора, ведь на данный момент 9 из 10 компаний имеют свою локальную сеть. На первый взгляд рядовому сотруднику может показаться, что в работе сетевого инженера нет ничего сложного: администратор сети получает сообщения от пользователей сети о неисправностях и проводит работы по их устранению. Такие работы принято называть реактивной поддержкой.

Реактивный подход недостаточен для обслуживания крупных сетей, ведь количество сообщений о неисправностях может увеличиваться лавинообразно, а это может привести к отказу критичных сетевых сервисов. Корпоративная сеть в настоящее время является бизнес-критичным инструментом. Любой, даже пятиминутный простой сети может отрицательно повлиять на доходы компании, поэтому перед сетевыми инженерами стоит задача избежать подобных случаев.

Для предотвращения непредвиденного отказа сети инженер должен применять комплексный и структурированный подход к задаче управления сетью, включающий, в том числе, выполнение проактивных действий.

Итак, в общем случае, задача управления компьютерной сетью может быть разделены на две составляющие:

а) структурированные работы – запланированные работы по поддержке сети;

б) реактивные работы – работы по устранению выявленных неполадок.

Безусловно, в реальной сетевой инфраструктуре свести к нулю реактивные работы не представляется возможным, однако, структурированный подход при управлении сетью позволяет минимизировать такие работы. Кроме того, структурированный подход позволяет более эффективно выявлять и устранять уязвимости в компьютерных сетях.

Существуют определённые модели (ITIL, FCAPS, TMN, Cisco Lifecycle Services), описывающие задачу поддержки IT-инфраструктуры в целом или сетевой инфраструктуры в частности. Использование таких моделей как основ при разработке собственной структурированной схемы управления сетью не является моветоном. Мировой опыт показывает, что процедуры, описанные в стандартизованных моделях во многих случаях избыточны.

Можно выделить основные пункты, которые требуется выполнять в рамках решения задачи управления сетью и какую роль в управлении сети играет каждый из предложенных пунктов.

Обеспечение доступа к сетевым устройствам для управления ими. Безусловно, сетевой инженер должен иметь возможность в любой момент

времени подключиться к сетевому устройству, чтобы внести изменения в настройки или посмотреть телеметрическую информацию. Основной инструмент управления сетевым устройством - командная строка (CLI), однако, практически все современные сетевые устройства предоставляют удобный графический интерфейс (GUI).

Существует широкий спектр программного обеспечения, с помощью которого можно одновременно управлять сразу несколькими устройствами и/или технологиями.

Следует отметить, доступ к сетевым устройствам необходим не только для сетевого инженера, но и для системы мониторинга. Кроме того, при решении задачи обеспечения доступа к сетевым устройствам крайне важно соблюдать надлежащий уровень безопасности.

Управление сетью в больших территориально – распределенных сетевых инфраструктурах может быть организовано как по тем же каналам, по которым передается пользовательский трафик, так и по специально выделенным каналам, что в какой-то степени уменьшает риск сильной нагрузки на основной канал передачи данных.

Мониторинг сетевой инфраструктуры можно разбить на следующие компоненты:

– мониторинг сетевых устройств;

– мониторинг каналов передачи данных.

В свою очередь, задача мониторинга сетевых устройств может быть разбита на следующие подпункты:

– сбор системных сообщений – логов устройства;

– мониторинг доступности и телеметрии сетевого устройства;

– оповещение инженера об изменениях в сети;

Постоянный мониторинг сетевой инфраструктуры позволяет сетевому инженеру получать всю необходимую информацию о сети в режиме реального времени. Кроме того, мониторинг помогает определить рабочий уровень (baseline) для параметров сетевых устройств и каналов передачи данных. Для различных сетевых инфраструктур границы допустимых значений параметров могут варьироваться. Так, например, для одной сетевой инфраструктуры загрузка процессора маршрутизатора на периметре сети в нормальном режиме работы не превышает 10%. В другой сети, аналогичный маршрутизатор работает постоянно и стабильно с нагрузкой 30 – 40%. При этом, хотя загрузка маршрутизатора во втором случае относительно высокая, все сервисы и бизнес-критичные приложения работают нормально. В таком случае сетевой инженер может принять предложенные значения за показатель нормального режима работы сетевого устройства. При превышении данных значений, сетевой инженер видит, что в сети происходит аномалия, возможны возникновения проблем в работе сервисов и приложений, следовательно, требуется оперативное вмешательство: поиск причины превышения допустимых показателей и устранение источника проблемы.

Мировой опыт инженеров показывает, что мониторинг в рамках описанных выше задач является необходимым и достаточным для поддержания работы сетевой инфраструктуры на надлежащем уровне. При аккуратном соблюдении изложенных выше пунктов, сетевой инженер сможет справиться практически с любой сетевой проблемой в сжатые сроки. Многие сетевые неполадки могут быть устранены проактивно.

Если учтены не все предложенные пункты, сетевой инженер в какой-либо момент времени обязательно столкнётся с ситуацией нехватки информации для решения очередной проблемы, а это в разы увеличивает ее время решения, так как проходится в экстренном порядке добавлять недостающие средства мониторинга. А в некоторых случаях, даже после произведенных манипуляций есть риск, что сетевой инженер после установки нового инструмента мониторинга не всегда сможет корректно интерпретировать новые данные, ведь у него нет информации о том, как сеть работала раньше, какие показатели считать нормальными, а какие аномальными.

Замена устаревшего или вышедшего из строя оборудования. С течением времени надёжность сетевых устройств падает. Устаревшее оборудование подвержено новым видам атак, поэтому представляет уязвимость для сетевой инфраструктуры в целом. Кроме того, устаревшее оборудование с определённого момента времени перестаёт отвечать постоянно возрастающим требованиям по функциональности производительности. Таким образом, сетевой инженер должен иметь исчерпывающую информацию о моделях используемых сетевых устройств и проводить замену оборудования на более современные устройства при необходимости.

Обновление программного обеспечения сетевых устройств. Производители сетевого оборудования постоянно разрабатывают новые операционные системы и новые версии систем для устройств. Как правило, выход новой версии программного обеспечения обусловлен исправлением уязвимостей операционной системы, исправлением багов в коде, увеличением производительности, а также добавлением нового функционала.

Резервное копирование конфигураций сетевых устройств. Конфигурация устройства имеет такую неприятную особенность, как сброс при внезапном отказе устройства. Сетевой инженер должен заменить вышедшее из строя устройство аналогичным, имеющим такие же настройки. Безусловно, задача замены отказавшего устройства значительно упрощается и ускоряется, если сетевой инженер имеет резервную копию конфигурации. Все современные устройства имеют возможность быстро «слить» файл с конфигурацией на какой-либо локальный сервер. Конфигурационный файл может понадобиться так и при отказе какой-либо функции устройства после перенастройки оборудования. Такая ситуация может произойти как по вине сетевого инженера (человеческий фактор), так и по вине производителя программного обеспечения (проявляется баг). Тем не менее, работоспособность сервиса должна быть восстановлена в сжатые сроки. При

наличии резервной копии рабочей конфигурации сетевой инженер может быстро провести процедуру отката.

Поддержка документации сетевой инфраструктуры. Как правило, первоначальная документация сетевой инфраструктуры создаётся на этапах проектирования и внедрения. Однако в процессе эксплуатации вносятся многочисленные изменения в настройки сетевых устройств, в топологию сети и т.д. Имея под рукой такой документ во многом упрощает жизнь сетевых инженеров и практически минимизирует человеческий фактор, когда данные и информация о сети может потеряться посредством того, что человек, который ее знал, забыл ее.

При организации управления сетевыми устройствами необходимо выбрать тип построения схемы управления, а также обеспечить правильную и безопасную настройку самих устройств для обеспечения подключения к ним с целью настройки.

На данный момент можно выделить несколько типов управления сетевым оборудованием. К наиболее часто описываемым методам относятся управление внутри полосы передачи трафика (in-band) и вне полосы передачи трафика (out-of-band). Кроме классического подхода существует несколько альтернативных вариантов управления сетевым оборудованием

Первый тип управления in-band предполагает передачу трафика управления оборудованием (Telnet, SSH, HTTPs и пр.) и трафика мониторинга (Syslog, SNMP, Netflow и пр.) по тем же физическим каналам и портам на сетевом оборудовании, где передаётся и обычный пользовательский трафик т.е. одна и та же сеть обеспечивает передачу всех данных. Безусловно при настройке оборудования необходимо на логическом уровне сегментировать трафик управления и остальной трафик. Это можно сделать, используя виртуальные сети (VLAN), списки доступа (ACL), межсетевые экраны и прочее. Но, как было отмечено ранее, «физика» остаётся одной. Основной полюс такого решения – простота. Но за простоту, как это обычно бывает, приходится платить. Главный минус данного варианта заключается в том, что если сеть полностью парализована, например, паразитным трафиком, доступ к устройствам тоже теряется и локализовать проблему удаленно становится практически невозможно. Это затруднит диагностику и исправление ситуации в работе сети. Чтобы этого не произошло, необходимо на сетевом оборудовании настроить разные уровни качества обслуживания трафика (QoS). Для трафика управления и мониторинга потребуется выделить минимально необходимую полосу пропускания, с приоритетом, позволяющим его передавать, даже если сеть перегружена, предварительно его промаркировав. Однако такой подход не даёт 100% гарантии и усложняет настройку оборудования. Также есть вероятность, что устройство по какой-то причине автоматически заблокирует порт, и удалённый доступ к нему пропадёт (например, коммутатор Cisco может перевести порт в состояние err-disabled). Также можно просто по ошибке заблокировать порт, через который идёт трафик управления, тем самым потеряв доступ на само устройство.

Второй тип управления out-of-band предполагает передачу трафика управления по отдельным физическим каналам связи т.е. строится вторая сеть, которая обслуживает передачу трафика управления. На каждом сетевом устройстве выделяет отдельный порт для подключения к этой сети. Обычно используется выделенный коммутатор, к которому подключается вся инфраструктура управления (машина администратора, Syslog-сервер, Netflow-коллектор и прочее). При такой организации, администратор сети практически всегда будет иметь доступ на сетевое оборудование, даже если основная сеть полностью отказала. Безусловно основными минусами являются необходимость использования отдельного оборудования, а также дополнительных настроек. Ещё стоит обратить внимание, что при организации out-of-band управления всегда требуются отдельные каналы связи. Когда оборудование стоит в одной серверной, это не является большой проблемой. Всегда можно найти дополнительные патч-корды. Но если оборудование разнесено по зданию или находится на территориально распределённых площадках, вопрос с выделенными каналами становиться критичным. Как это часто бывает, дополнительные медные или оптические трассы проложить достаточно проблематично, если они не были изначально предусмотрены. Также стоит обратить внимание на необходимость наличия на сетевом оборудовании дополнительных портов для подключения к сети управления. Очень часто в маршрутизаторах присутствует всего два физических интерфейса, которые обычно уже заняты.

В случае если у нас территориально распределённая сеть, организовать управление out-of-band в удалённом офисе, особенно, если его топология достаточно проста, становится сложным и не оправданным с точки зрения цены. Поэтому появляется гибридный вариант управлению сетью: out-of-band для центрального офиса и in-band для удалённых офисов. Точно такая же схема может быть использована, если сеть распределена по зданию и в силу отсутствия дополнительных межэтажных соединений, организовать везде out-of-band управление становится сложно.

Хотелось бы отметить ещё один вариант управления сетью, который в большей степени можно отнести к out-of-band – использование консольного сервера. В этом случае каждое сетевое устройство подключается к консольному серверу, через который происходит управление оборудованием. Самым большим преимуществом данного варианта является то, что возможность прямого подключения к устройству есть всегда, даже когда оно не корректно загрузилось. Но такой вариант управления не всегда удобен и приемлем, потому что устройство должно находиться только на небольшом расстоянии от консольного сервера, например, в одной серверной комнате, а это условие не всегда реализуемо на предприятии. Еще необходимо отметить, что такое подключение к устройствам нельзя использовать для мониторинга сетевого оборудования. К минусам также можно отнести скорость передачи консольного кабеля, из-за низкой скорости вывод большого количества информации может продолжаться достаточно много времени.Известны такие

случаи, когда вывод информации производился в течении 30 минут, а для оперативного решения проблемы это слишком много.

Помимо консольного сервера, как альтернативный вариант, можно иметь специально выделенный ноутбук с консольным кабелем т.е. минимальный комплект, позволяющий подключиться к сетевому оборудованию по консоли. Такой вариант позволит при необходимости достаточно оперативно дойти до устройства и подключится к нему. Обычно в нужный момент, нет или ноутбука под рукой или консольного кабеля с переходником.

Такой тип управления, как управление из облака является в некотором роде гибридным типом. Одним из примеров управления сетевым оборудование из облака, является концепция, реализованная в линейке продуктов Cisco Meraki. Все устройства этой марки (а туда входят и коммутаторы, и устройства безопасности, а также решения по построению беспроводной сети) автоматически после установки подключаются в облако Cisco. Для управления этой структурой сетевому инженеру необходимо подключиться к облачному порталу. Главным недостатком данной схемы является тот факт, что если пропадает связь с облаком, управлять устройствами не получится. Это существенно повышает требования к надёжности и количеству Интернет-каналов. Стоит отметить, что такой тип управления ещё не набрал популярности. Но в свете облачного тренда, видимо, мы туда дошагаем достаточно быстро.

Концепция программно-конфигурируемых сетей является одной из наиболее развивающихся на рынке сетевых технологий. Она предполагает полное отделение функций управления устройствами и контроля трафика от функций передачи данных. То есть за управление всеми сетевыми устройствами и логику контроля за трафиком (например, протоколы маршрутизации, служебные протоколы, vlan) отвечает некое централизованное программное устройство (контроллер), а сетевые устройства занимаются только передачей трафика. С одной стороны, плюсы подхода налицо: это удобное управление всей сетью, с очень гибким функционалом (дополнительные функции реализуются программно). Однако, сейчас только начинают появляться сетевые устройства с поддержкой данной технологии и функционал их пока крайне ограничен, перспективность такого подхода будет определена в ближайшие годы.

В идеале настройка сетевого оборудования для обеспечения функций управления и мониторинга должна советовать рекомендация производителя оборудования. Пароли должны иметь достаточную степень надёжности. Для удалённого подключения должны такие протоколы как, SSH и HTTPs. Доступ к устройству должен быть ограничен. Список таких рекомендаций можно продолжать достаточно долго. При этом есть ещё рекомендации по корректной настойке каждого протокола управления, рекомендации по настройке качества обслуживания (QoS), рекомендации по снятию телеметрии с оборудования и т.д. Если открыть хоть одну рекомендацию по настройке

перечисленных выше параметров, можно увидеть, что она занимает не одну страницу, но данная настройка важна.

Краткий перечень рекомендаций, который можно расширить или дополнить, обратившись к документации на оборудование:

– Для удалённого подключения рекомендуется использовать такие защищенные протоколы, как SSH и HTTPs. Уже практически каждому известно, что в трафике, который передается через протокол telnet логин и пароль передаются в открытом виде, что не есть хорошо.

– Степень надежности учетных записей, предназначенных для входа на активные сетевые устройства, должна быть выше среднего. Дефолтные учётные записи лучше удалить. Все пароли должны храниться в конфигурации в защищённом и зашифрованном виде.

– Весь трафик мониторинга и управления, передаваемый по открытым каналам должен быть зашифрован: либо с помощью vpn соединения, либо с использованием защищенных протоколов, таких как snmpv3, sftp, scp.

– Доступ к устройству должен быть ограничен только для определённого круга пользователей. Например, на оборудовании Cisco это можно сделать с помощью списков доступа (ACL).

– На устройствах должна быть настроена синхронизация времени. Время лучше не прописывать вручную, а настроить связь устройства с ntp-сервером. Это позволит более точно определять монеты, когда производилась попытка легитимного или не легитимного подключения.

– Все подключения и вводимые команды рекомендуется логировать. Особенно это актуально в случае управления устройством несколькими людьми.

– Каждый пользователь должен подключаться, используя свою уникальную учётную запись.

Настройка уровней доступа на устройствах также является важной частью конфигурирования. При подключении должно выводиться сообщение о том, что доступ разрешён только авторизованным пользователям.

Как было отмечено ранее, кроме рекомендаций, касающихся непосредственного управления устройствами, существуют такие же рекомендации по безопасной настройке различных протоколов (например, EIGRP, OSPF и пр.), обеспечивающих работу сети. Например, рекомендуется всегда включать логирование изменений состояния протокола (добавление/удаление маршрутов и пр.), а также аутентификацию между устройствами при установление соседственных отношений.

Также есть целый набор рекомендаций по настройке качества обслуживания (QoS) трафика управления и мониторинга. Туда же можно отнести вопросы фильтрации и ограничения скорости для того или иного протокола с целью предотвращения атаки типа «отказ в обслуживании».

К мониторингу сетевых устройств можно отнести сбор системных сообщений, мониторинг доступности и телеметрии сетевого устройства, а

также оповещение инженера об изменениях в сети. Для сбора с устройств системных сообщений практически на всех устройствах присутствуют syslog сообщения. Сбор телеметрических данных производится с использованием протокола SNMP. Также можно настроить систему уведомлений для инженера, которая будет посылать ему уведомления об изменениях в сети. Мониторинг каналов связи организуется по средствам протокола Netflow или его аналогов. Далее каждый этап будет рассмотрен более подробно.

Логи визуализируют процесс работы сетевого устройства, отображают его состояние. Выполнение системой какого-либо действия отражается соответствующим системным сообщением – логом. Существуют различные уровни детализации системных сообщений. Как правило, в зависимости от уровня детализации информации в логах на оборудовании существуют различные уровни логирования. Для оборудования Cisco Systems представлены 8 уровней: от уровня 0 (Emergencies – сообщения о неработоспособности системы) до уровня 7 (Debugging – отладочные сообщения).

Оборудование предоставляет следующие возможности по выводу логов: на консоль устройства (console logging), в локальный буфер устройства (buffer logging), в терминальную линию (monitor logging) и на внешний сетевой накопитель – выделенный Syslog-сервер. В роли последнего может выступать централизованная система мониторинга.

При включении логирования нужно быть крайне внимательным. Существуют некоторые нюансы, невыполнение которых может привести к отказу устройства и/или необходимости его перезапуска.

Первый нюанс касается вывода в консоль или на терминальную линию логов высокого уровня детализации, в частности – уровень 7. Особенно данный пункт касается ситуации, при которых инженер активирует дополнительную трассировку какого-либо сервиса командой debug. Сетевое устройство может генерировать слишком большое количество сообщений в единицу времени, всё процессорное время будет затрачено на вывод данных сообщений на экран. Устройство может «зависнуть» и перестать выполнять свою главную функцию – маршрутизировать и коммутировать сетевой трафик. При необходимости просмотра логов высокого уровня детализации рекомендуем выводить сообщения в локальный буфер.

Второй нюанс касается вывода лог-сообщений в локальный буфер. На сетевых устройствах Cisco локальный буфер выделяется из общего пула оперативной памяти. Если мы запросим слишком большой объём памяти под лог-буффер, устройству может испытывать нехватку оперативной памяти, что в свою очередь, может привести к «зависанию» устройства, незапланированной перезагрузке. Отдельно стоит выделить настройку логирования на межсетевых экранах Cisco ASA. Распределение лог-сообщений по уровням для многих случаев не является оптимальным. Например, сообщения, связанные с работой списков доступа (ACL) на

устройстве или с правилами трансляции IP-адресов (NAT) могут иметь уровни от 2 до 6.

Можно с уверенность сказать, что и при стабильном и нормальном режиме работы устройства нельзя исключать вывод лог-сообщений высокого уровня критичности. В связи с этим, некоторые разработчики операционных систем для сетевых устройств ввели расширенные возможности по оптимизации и настройке системы логирования на устройстве.Инженер имеет возможность изменить уровень для любого лог-сообщения. Кроме того, администратор может создавать списки системных сообщений, объединяя в группы интересующие события. Например, для отладки и мониторинга работы сервиса VPN, сетевой инженер может создать список, в который будут попадать только лог-сообщения, связанные с работой данного сервиса, и отправлять на выделенный Syslog-сервер только настроенный список. Кроме того, устройство Cisco ASA может отправлять списки лог-сообщений по электронной почте. Для любого сетевого устройства системные лог-сообщения являются главным, а в некоторых случаях и единственно доступным инструментом поиска проблем и неисправностей. При проведении диагностики сетевой проблемы, инженер, после проверки корректности конфигурации, первым шагом должен посмотреть логи сетевых устройств. Вероятность выявления причины проблемы по системному логу крайне велика.

Системные сообщения незаменимы при расследовании сетевых проблем, моменты проявления которых непредсказуемы.

Помимо решения сетевых проблем, хотелось бы отметить ещё одну область применения системных сообщений. Лог-сообщения можно использовать совместно со встроенным в операционную систему устройств Cisco редактором автоматических сценариев Cisco EEM (Embedded Event Manager). Данный функционал позволяет создавать скрипты для автоматического изменения конфигураций устройств. Лог-сообщение может выступать триггером запуска скрипта.

Протокол SNMP – Network Management Protocol – является стандартом для обмена управляющей информацией между сетевыми устройствами и системой управления сетью (NMS – Network Management System). С точки зрения мониторинга сети протокол SNMP является незаменимым средством сбора телеметрической информации с сетевых устройств.

Сбор телеметрических показателей сетевых устройства является неотъемлемым компонентом управления компьютерной сетью. Телеметрическая информация позволяет сетевому инженеру искать «узкие места» в сетевой топологии, предотвращать возможные отказы, отслеживать причины сетевых проблем, определять рабочие уровни для показателей сетевых устройств, выявлять аномалии в работе сети.

К наиболее важным датчикам телеметрии устройств относятся такие показатели, как загрузка процессора устройства, загрузка оперативной памяти, работа систем питания, охлаждения, температура устройства.

Перечисленные показатели телеметрии рекомендуется отслеживать на любом сетевом устройстве. Кроме того, на устройствах, в зависимости от возложенного функционала, рекомендуется включать мониторинг дополнительных параметров. Так, для устройств, терминирующих VPN-подключения, рекомендуется опрашивать соответствующие SNMP OID. Для многих сетевых устройств важно знать текущую загрузку сетевых интерфейсов. Данная информация поможет достаточно точно оценить загрузку каналов передачи данных в сетевой инфраструктуре. Есть даже ряд проблем, возникающих в сети, поиск причин и устранение которых просто неосуществимы без предварительного сбора и анализа телеметрии устройств, собранной по протоколу SNMP. Например, ситуации, когда связь пропадает не полностью, а частично, либо же качество связи настолько ухудшается, что становится неприемлемым для определенных сетевых приложений.В большинстве случаев при возникновении подобных проблем сетевой инженер не может получить практически никакой информации посредством проверки конфигураций сетевых устройств или просмотром лог-сообщений. В результате таких первичных проверок создаётся впечатление, что вся сетевая инфраструктура работает корректно и безотказно. Но при этом постоянно поступают жалобы от конечных пользователей о том, что «видео не грузится», «телефония работает плохо и качество голоса неприемлемо».

Наиболее вероятной причиной возникновения подобных проблем является возросшая нагрузка на сетевые устройства и/или на каналы передачи данных. С помощью NMS, собирающего телеметрию сетевых устройств по SNMP, легко оценить динамику изменения нагрузки на сетевые устройства. Вполне вероятно, что на пути следования проблемного потока данных, находятся одно или несколько сетевых устройств, загруженных сверх меры. После обнаружения таких устройств инженер сможет сделать вывод о том, являются ли данные узлы «узким местом» сетевой топологии, либо данные устройства подвержены какому-то аномальному нежелательному влиянию (вирусная активность, нелегитимный трафик больших объёмов и т.д.). Если устройство оказалось «узким местом», сетевой инженер должен поднять вопрос о замене оборудования на более производительную модель. Если высокая загрузка является аномалией – требуется дальнейшее расследование.

Например, с помощью данных, полученных по SNMP, мы можем локализовать «паразитный трафик», загружающий сетевое оборудование. Средствами SNMP можно опрашивать OID устройств, отвечающих за загрузку сетевых интерфейсов. Если «перегруженным» устройством является коммутатор, велика вероятность, что на паре его интерфейсов мы сможем увидеть аномально высокий уровень загрузки. Во многих случаях подобные рассуждения актуальны и для маршрутизаторов. После выявления пары интерфейсов инженер может уточнить, какие устройства подключены к данным портам. Возможно, для подтверждения выдвинутой гипотезы также отключить эти интерфейсы на время и посмотреть, снизится ли загрузка сетевого устройства и улучшится ли в конечном итоге качество связи. Таким

образом, сбор информации по SNMP помогает выявить причину проблемы, расследовать которую другими средствами не представляется возможным.

Необходимо отметить, проблема с ухудшением качества связи может проявляться не только вследствие сверхмерной загрузки сетевого оборудования, но и в результате высокого уровня утилизации каналов связи. Опять же, опрос по SNMP OID устройства, содержащего информацию о загрузке сетевых интерфейсов, помогает выявить и косвенно определить загрузки подключенных к интерфейсам каналов. Простейший пример. К интерфейсу высокопроизводительного маршрутизатора Cisco подключен WAN-канал. Пропускная способность канала по договору с провайдером составляет 10 Мбит/с. Пользователи, опять же, периодически испытывают проблемы с качеством связи по этому каналу. С помощью сбора информации по SNMP мы определили, что на протяжении всего времени использования канала загрузка интерфейса маршрутизатора, к которому канал подключен, не превышала 3 Мбит/с. Однако с некоторого момента времени наблюдается загрузка 10-12 Мбит/с, что превышает пропускную способность канала. Очевидно, проблема в чрезмерном уровне утилизации WAN-канала. В данной ситуации дальнейшее расследование проблемы средствами SNMP затруднительно: нужно определить качественный состав трафика в канале, то есть IP-адреса отправителей/получателей протоколы и используемые порты. Описанная задача решается с помощью протокола NetFlow.

Протокол NetFlow разработан компанией Cisco Systems. С точки зрения проблемы управления сетью данный протокол является незаменимым инструментом для мониторинга загрузки каналов передачи данных.

Конечно, протокол NetFlow не может получать информацию непосредственно с канала (витой пары или оптической линии) – данные снимаются с устройств, подключенных непосредственно к интересующему сегменту. NetFlow поддерживается многими сетевыми устройствами. По NetFlow могут отправлять информацию маршрутизаторы, коммутаторы и межсетевые экраны Cisco. NetFlow является проприетарным протоколом Cisco Systems, однако, следует отметить, существует и открытый аналог данного протокола – sFlow. SFlow реализован в современных моделях сетевых устройств многих производителей сетевого оборудования – HP, Zyxel и т.д.

Архитектура NetFlow крайне проста и состоит из двух компонентов: сетевое устройство, отправляющее информацию о проходящем через него трафике, и NetFlow-коллектор. Последний является сборщиком и анализатором информации, полученной по NetFlow.

Принцип действия протокола заключается в следующем. На сетевом оборудовании при открытии очередной сессии передачи данных формируется информация о данной сессии, называемая поток (flow). Поток содержит в себе такую информацию, как количество передаваемых байт, входной и выходной интерфейс для сессии, IP-адреса источника/приёмника, порты источника/приёмника, номер протокола IP, параметры QoS и т.д. Потоки аккумулируются на сетевом устройстве и отправляются в сторону NetFlow-

коллектора в UDP-датаграммах. NetFlow-коллектор агрегирует полученную информацию, проводит анализ и формирует удобные отчёты и графики. Один из популярных NetFlow-коллекторов – NetFlow Analyzer, но существуют коллекторы и других производителей. С помощью протокола NetFlow сетевой инженер получает полную картину трафика на каналах. Инженер может просматривать качественный состав трафика (IP-адреса, порты, приложения) в любом сегменте сети, а также оценивать, какой процент пропускной способности канала занимает тот или иной поток.

1.2 Виды протокола Netflow

NetFlow — открытый частный протокол, который был разработан Cisco с целью отслеживания трафика сети. Netflow позволяет анализировать сетевой трафик, базируясь на сеансах и делает запись о каждой операции TCP/IP.

Строение данной системы построена с помощью сенсора, коллектора и анализатора:

– с помощью сенсора собираются данные по передаваемому трафику. Обычно их ставят в узлах сети, они обычно расположены на граничных маршрутизаторах сегментов анализируемой сети.

– коллектор получает информацию от сенсоров и собирает ее. Далее данные отправляются в файл для последующей обработки. Стоит заметить, что различные коллекторы отправляют данные и сохраняют их в разных форматах.

– анализатор, или как ее принято называть, система обработки, читает данные файлы и формирует их в отчеты, которые более понятны и удобны для человеческого восприятия, но эта система должна быть совместима с тем форматом данных, в которых ее предоставил коллектор для обработки. Но обычно коллектор и анализатор в более новых системах объединены в одном.

Обычно коллектор и анализатор являются частями одного программного комплекса, который работает на сервере.

Необходимо сразу выяснить одну вещь – коллектор и его соответствующий анализатор являются пассивными элементами системы. Сенсор отправляет данные о трафике коллектору, тот принимает, анализатор фильтрует и анализирует полученную информацию и заполняет базу данных на сервере. При верно работающем сервере нам нет необходимости собственноручно подключать устройства, которые нужно отслеживать на сервере. В то время как сенсор шлет отчеты остальные элементы системы занимаются своими задачами: коллектор принимает и отправляет в отчет, а анализатор анализирует полученные данные. Пока сенсор шлет отчеты, коллектор их принимает, анализатор регистрирует. Во время отключенного сенсора, он просто скрывается из режима «онлайн» текущей статистики.

NetFlow использует UDP или SCTP для передачи данных о трафике коллектору. Известно то, что коллектор слушает порт 2055, 9555 или 9995 (или тот порт, который был указан непосредственно при настройке).

Сенсор выделяет из проходящего трафика потоки, характеризуемые следующими параметрами:

– адрес источника;
– адрес назначения;
– порт источника для UDP и TCP;
– порт назначения для UDP и TCP;
– тип и код сообщения для ICMP;
– номер протокола IP;
– сетевой интерфейс (параметр ifindex SNMP);
– IP Type of Service.

Потоком считается набор пакетов, проходящих в одном направлении. Когда сенсор определяет, что поток закончился (по изменению параметров пакетов, либо по сбросу TCP — сессии), он отправляет информацию в коллектор. В зависимости от настроек он также может периодически отправлять в коллектор информацию о все еще идущих потоках. Это очень важный момент — при настройке сенсора можно самостоятельно решить, по каким параметрам отосланная на коллектор информация будет объединена в отчетах

Для разностороннего анализа трафика традиционно применяются несколько основных технологий — классический сетевой анализ, SNMP и NetFlow. Все они демонстрируют разный подход к вопросу учета трафика, используют принципиально разные способы получения информации. В итоге разные результаты, отличающиеся полнотой и характером информации.

Классический сетевой анализ для развертывания на сети требует некоторых затрат, аппаратных и экономических, и оправдан бывает не всегда. Особенно это касается корпоративных сетей (даже относительно крупных), целесообразнее применять такой анализ в сетях масштаба оператора связи, провайдера, поскольку он способен дать исчерпывающую информацию о потоках информации не только от пользователей, но и магистральных. Для сетей корпоративных такая информация окажется избыточной, и потребуется хороший специалист для ее анализа. Поэтому в крупных сетях обычно применяют протокол SNMP –простой протокол управления сетями.

Принцип и основная идея состоит в том, что отправляются короткие запросы на интерфейсы сетевых устройств, а потом уже на основании ответов получают информацию о сети. SNMP также предоставляет информацию и данные о загрузке процессора и памяти, он не направлен чисто на анализ трафика, а широко ориентирован.

NetFlow в свою очередь идеально подходит для сбора всей возможной информации именно о трафике, в разрезе пользователей, подсетей, потоков от конкретных приложений и т.д. Сенсор аппаратно встроен в оборудование

маршрутизации, и ему доступны все процессы обработки. Информации для анализа сенсор NetFlow выдает в значительном объеме, в ней содержится буквально все — от адресации источника и получателя до используемых протоколов и интерфейсов, метки времени и т.д. Поэтому NetFlow наиболее эффективен для учета трафика, в том числе поиска узких мест в сети, выявления основных потребителей и т.д.

Flexible NetFlow — это новейшая технология NetFlow. Flexible NetFlow расширяет возможности первоначального протокола NetFlow, позволяя настраивать параметры анализа трафика в соответствии с конкретными требованиями сетевого администратора. Технология Flexible NetFlow позволяет создавать более сложные настройки для анализа трафика и экспорта данных с помощью компонентов настройки, которые можно использовать повторно.

Flexible NetFlow работает с форматом экспорта 9 версии, его особенностью является работа на шаблонах, которые обеспечивают возможность расширить формат нужной записи и также обновить NetFlow без изменения уже существующего формата. Важно отметить, что много полезных команд Flexible NetFlow были введены вместе с версией Cisco IOS 15.1. На рисунке 1.1 изображен пример сети с анализатором трафика.

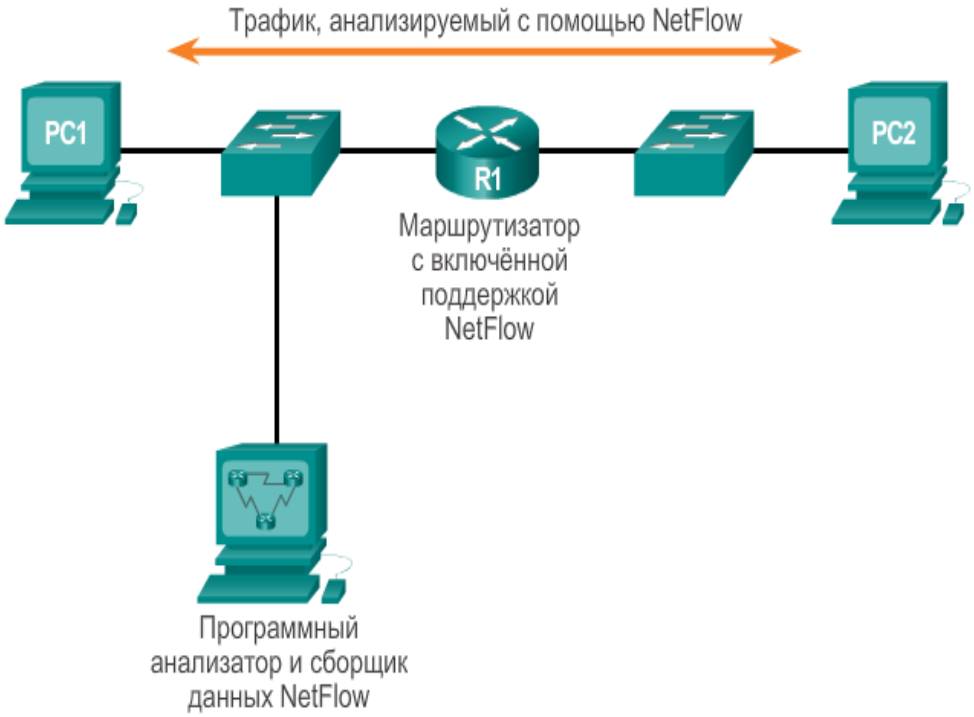


Рисунок 1.1 – Пример реализации сети

Flexible NetFlow поддерживает больше различных параметров в записях данных о потоках. Flexible NetFlow позволяет администратору определять записи для кэша контроля потока Flexible NetFlow, выбирая определяемые пользователем дополнительные и обязательные поля для настройки сбора данных в соответствии с конкретными требованиями. Записи для кэша контроля потока Flexible NetFlow называются определяемыми пользователем записями. Значения в дополнительных полях добавляются к потокам для предоставления дополнительной информации о трафике в потоках (рис. 2.2). При изменении значения дополнительного поля новый поток не создаётся.

Если NetFlow для получения данных о потоке обрабатывает каждый пакет, сохраняет его параметры в NetFlow Cache, а затем экспортирует их в NetFlow Collector, то протокол sFlow базируется на анализе статистической выборки пакетов.

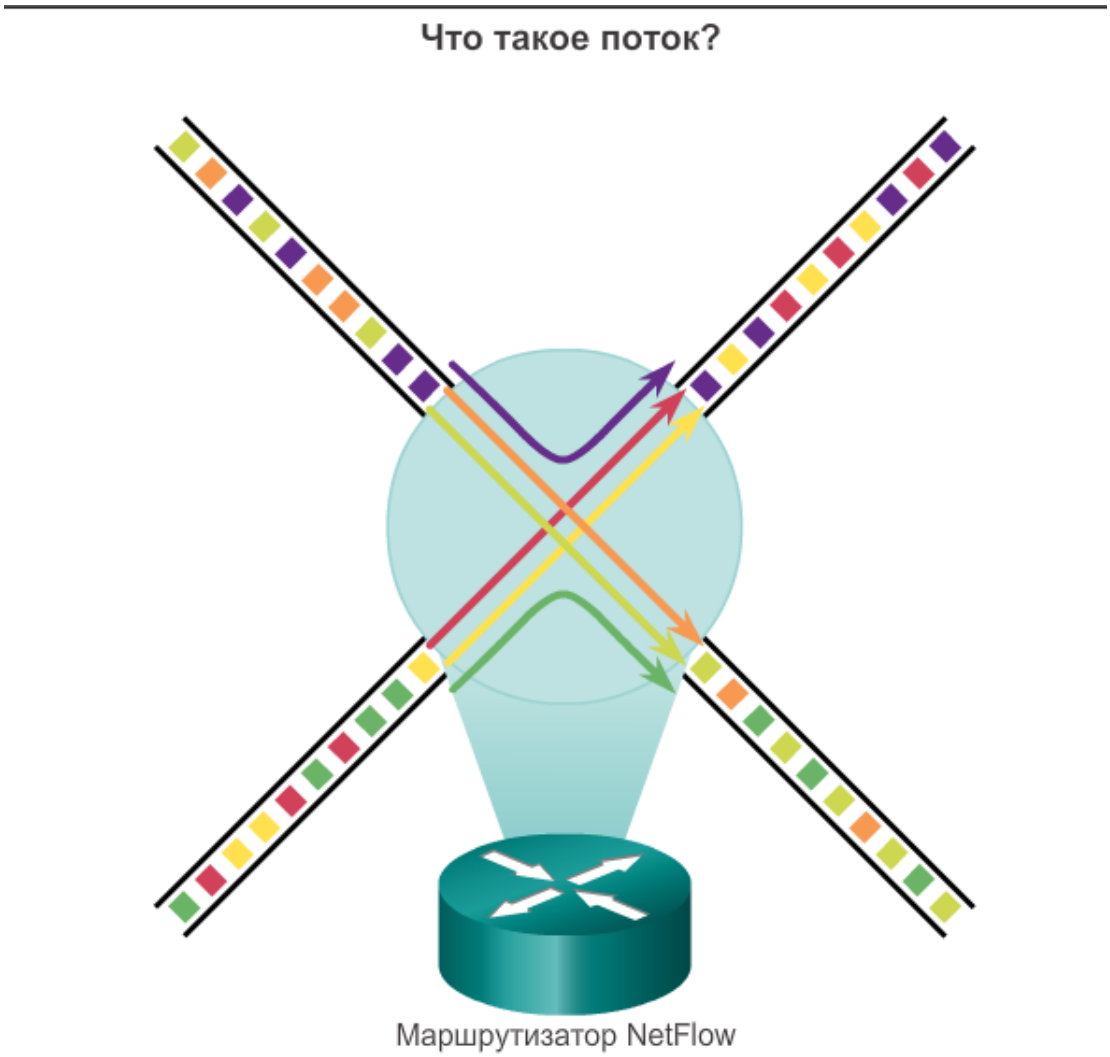


Рисунок 1.2 – Маршрутизатор Netflow и поток данных

Впервые этот метод продемонстрировала HP на выставке Telecom'91. Однако широкое распространение данная технология получила только в последние годы, что было вызвано появлением высокоскоростных сетей и переходом к коммутации пакетов. Рассмотрим суть метода оценки трафика по выборке пакетов на конкретном примере.

Пусть по сети передается 1 млн пакетов. Случайная выборка 25% трафика дает 2500 пакетов. Если 1000 из них представляет определенный класс трафика v, например голосовой трафик, то уместен вопрос об оценке количества пакетов этого класса в общем трафике. Он будет содержать по меньшей мере 1000 пакетов класса v, поскольку они попали в выборку. Максимально возможное же их число – 998 500, потому что в выборке имеются 1500 неголосовых пакетов. Вообще говоря, такие значения возможны, однако крайне маловероятны. Наиболее правдоподобным будет предположение, что часть голосовых пакетов в общем трафике близка к таковой в выборке, т. е. примерно 40%. Погрешность оценки вычисляется с помощью статистических методов.

Программный модуль, реализующий функции агента sFlow, работает как часть управляющего ПО, располагающегося на сетевом устройстве. Когда выбирается пакет, его заголовок извлекается и помещается в дейтаграмму или детализированную карту передачи пакета по сети, которая включает заголовок, адреса и порты отправителя и получателя, статистику интерфейса и другую информацию, необходимую для анализа трафика на уровнях OSI от второго до седьмого. Сформированная дейтаграмма сразу же направляется по сети в sFlow Collector. Один коллектор может обрабатывать данные более чем от 20 тыс. портов.

Выборка пакетов в типичном случае выполняется с помощью коммутирующих или маршрутизирующих заказных специализированных микросхем (ASIC) со скоростью, которую позволяют физические соединения. Записывается также состояние элементов коммутационных и маршрутных таблиц, связанных с каждым пакетом выборки.

Следует отметить, что sFlow, по сравнению с другими перечисленными вариантами, потребляет мало ресурсов процессора, памяти и полосы пропускания, что является немаловажным фактором при выборе технологии, по которой будет проводиться мониторинг трафика в высокоскоростных сетях.

1.3 Структура работы протокола

Принцип действия протокола заключается в следующем. На сетевом оборудовании, при открытии какого-либо сеанса передачи данных, складывается информация о предоставленном сеансе, именуемая потоком (flow).

Сведения о потоке включают различную информацию, такую как, количество передаваемых байтов, входной и выходной интерфейсы для

сеанса, тип и код сообщения для ICMP, IP-адреса отправителя/получателя, порты (UDP и TCP) отправителя/получателя, номер протокола IP, параметры QoS и т. д. Выше перечисленные сведения о потоках накапливаются на сетевом устройстве и отправляются коллектору NetFlow в виде датаграмм UDP.

После получения информации коллектор обрабатывает её, анализирует и создаёт удобные для восприятия отчеты и графики.

Существуют различные коллекторы NetFlow от разных фирм, такие как NetFlow Analyzer, Scrutinizer, PRTG Network Monitor и другие. У каждой программы есть свои плюсы и минусы.

Протокол NetFlow предоставляет полную картину трафика в каналах, что позволяет увидеть качественный его состав (IP-адреса, порты, приложения) в любом сегменте сети. NetFlow дает нам проанализировать, какую долю пропускной способности канала (в процентном соотношении) занимает какой-нибудь поток.

NetFlow применяется в различных областях, но вот три ключевых: мониторинг трафика, анализ поведения сети, проведение аудитов сетевой инфраструктуры. Компании провайдеры связи особенно заинтересованы в учете трафика. При проведении аудита NetFlow помогает собирать полную и детальную информацию о реальном трафике и загрузке сети.

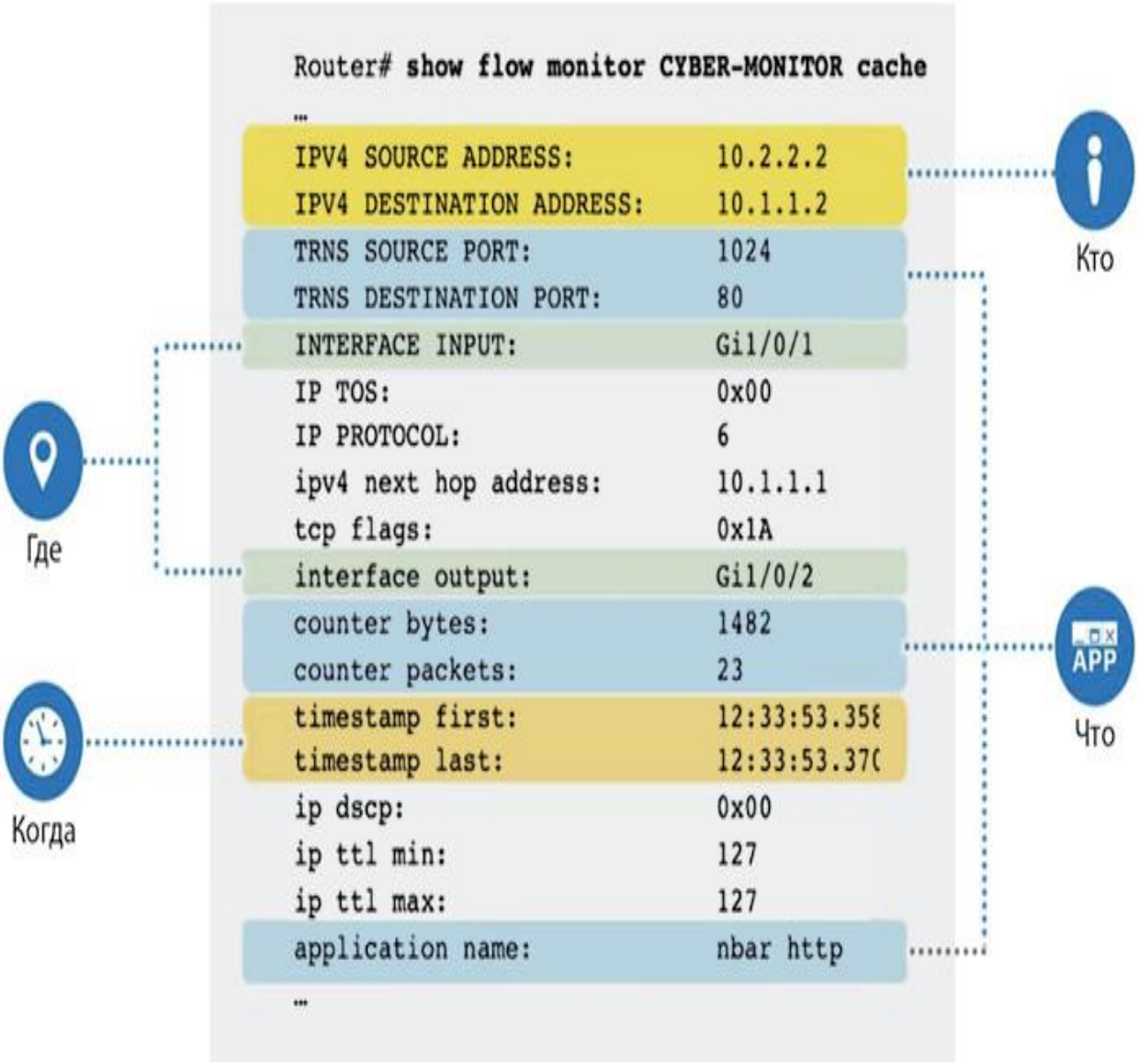


Рисунок 1.3 – Запись Netflow

1.4 Обзор производителя сетевого оборудования

В 1996 году группой инженеров с целью продажи оборудования на развивающихся рынках была основана компания Mikrotīkls Ltd. (в переводе с латышского — «Маленькие сети», известны под торговой маркой MikroTík, произносится как [микрот`ик]). В настоящее время она разрабатывает и продаёт аппаратное и программное обеспечение для подключения к Интернету в большинстве стран мира. Компания расположена в столице Латвии - Риге. В данный момент в компании работает более 280 сотрудников.

История компании:

- 1996 г. – основание компании MikroTik.
- 1997 г. – выход первой RouterOS для x86.
- 2002 г. – выход RouterBOARD.
- 2006 г. – проведение первого MUM в истории в г. Прага.

– 2011 г. – начата официальная продажа в РФ.
– 2012 г. – проведение первого MUM в РФ.
Плюсы и минусы производителя сетевого оборудования:
Минусы:
– требует понимания того, что делаешь;
– нет многих полезных опций. Например, WINS-сервера;
– мало учебных материалов;
– информация на английском языке;
– плохая техническая поддержка;
– отсутствие сертификации ФСТЭК;
– не поддерживает проприетарные протоколы других вендоров (EIGRP и др.);
– не маршрутизирует более 80 Gbps.
Плюсы:
– стоимость;
– функциональность;
– стабильность;
– свободное получение обновлений;

Одним из продуктов MikroTik является RouterOS — сетевая операционная система на базе Linux. RouterOS предназначена для установки на маршрутизаторы MikroTik RouterBOARD. Также данная система может быть установлена на ПК или виртуальную машину.

RouterOS поддерживает следующий функционал:
Статическая и динамическая маршрутизация на базе: RIP, OSPF, BGP, MPLS и др.

– Виртуальные сети:
  – VPN site-to-site и client-to-site: PPTP, PPPoE, SSTP, OpenVPN, L2TP.
  – VPN site-to-site: EoIP, IPIP, GRE, VLAN и др.
– Беспроводные сети:
  – 802.11 a/b/g/n/ac;
  – Проприетарные протоколы: Nstream и Nv2.
– Прочее: QoS, брандмауэр, DHCP клиент и сервер, HotSpot и др.
– Многое другое.

Операционная система имеет несколько уровней лицензий с возрастающим числом функций. Кроме того, существует программное обеспечение под названием WinBox, которое предоставляет графический интерфейс для настройки RouterOS. Доступ к устройствам под управлением RouterOS возможен также через FTP, Telnet, и SSH. Существует API, позволяющий создавать специализированные приложения для управления и мониторинга.

WISP (Wireless Internet Service Provider) –Интернет провайдер беспроводного доступа в Интернет.

CPE (customer-premises equipment) - телекоммуникационное оборудование, устанавливаемое в помещении абонента.

История версий:

– RouterOS v3: январь 2008 — октябрь 2009 (основана на ядре Linux 2.4.31)

– RouterOS v4: октябрь 2009 — март 2011 (основана на ядре Linux 2.6.26)

– RouterOS v5: март 2011 — сентябрь 2013 (основана на ядре Linux 2.6.35)

– RouterOS v6: май 2013 — н. в. (основана на ядре Linux 3.3.5)

Обновления выпускаются в трех ветках:

– Long-term (ранее - bugfix only) – только исправление ошибок. Новый функционал отсутствует.

– Stable (ранее – Current) – исправление ошибок и новый функционал, который, в свою очередь, может внести новые ошибки.

– Testing (ранее - Release Candidate) – тестовая версия, которая содержит самый последний функционал и является потенциально нестабильной. Не рекомендуется к использованию в рабочей среде.

– Development – версии для разработчиков.

RouterBOARD — аппаратная платформа от MikroTik, представляющая собой линейку маршрутизаторов под управлением операционной системы RouterOS.

WebFig – это интерфейс управления RouterOS через веб-браузер. Для доступа в адресной строке браузера надо указать IP-адрес маршрутизатора. В настройках по умолчанию такой доступ разрешен.

Консоль (интерфейс командной строки, CLI - Command Line Interface) используется для доступа к маршрутизаторам MikroTik для настройки и управления средствами текстового терминала. Доступ к консоли может быть получен с помощью серийного порта, протоколов Telnet и SSH или окна терминала в утилитах WinBox или WebFig. Если RouterOS установлена на компьютер, то доступ может быть получен с помощью монитора и клавиатуры. Консоль также может быть использована для написания скриптов.

Консоль позволяет управлять настройками маршрутизатора используя текстовые команды. Поскольку существует много доступных команд, они разделены на группы, организованных соответственно иерархическим уровням меню графического интерфейса. Название уровня меню отражает информацию о конфигурации, доступную в соответствующем разделе.

Ввиду того, что существует огромное количество возможных команд, они разбиты по группам, организованным по принципу иерархического меню. Наименование уровня меню отображает конфигурационную информацию доступную в данной секции.

Преимущества командной строки:

– некоторые операции можно выполнить только из консоли;

– соединение возможно при самых низких скоростях соединения.

2 Практическая часть

2.1 Обзор сети и ее компонентов

Каждая компания имеет определенный характер решаемых задач, который чаще всего и формулирует требования к конфигурации локальной сети. От числа сотрудников зависит количество рабочих станций. Не маловажную роль играет внутренняя иерархия компании. Для фирмы с горизонтальной структурой оптимальным решением является простая одноранговая сеть, потому что все сотрудники должны иметь доступ к данным друг друга. Напротив, фирме с вертикальной структурой больше подойдет вариант сети с выделенным сервером, потому что в этом случае должно быть точно известно, какой сотрудник к какой информации должен иметь доступ, а к какой нет. В таком варианте сети существует возможность администрирования и определения прав доступа.

В данном случае на предприятии имеется 19 рабочих станций и файловый сервер с разграниченным доступом к информации, которые уже объединены в локальную сеть. В зависимости от типа сети при проектировании обычно возникает вопрос об ограничении длины кабельного сегмента. Если рассматривать ситуацию, когда сеть охватывает несколько этажей здания, встает вопрос об использовании репитеров и коммутаров. В ситуации с нашей организацией вся сетевая инфраструктура располагается на одном этаже здания, и расстояние между сегментами сети не настолько велико, чтобы использовать репитеры. Логическая схема исходной сети компании приведена на рисунке 2.1.

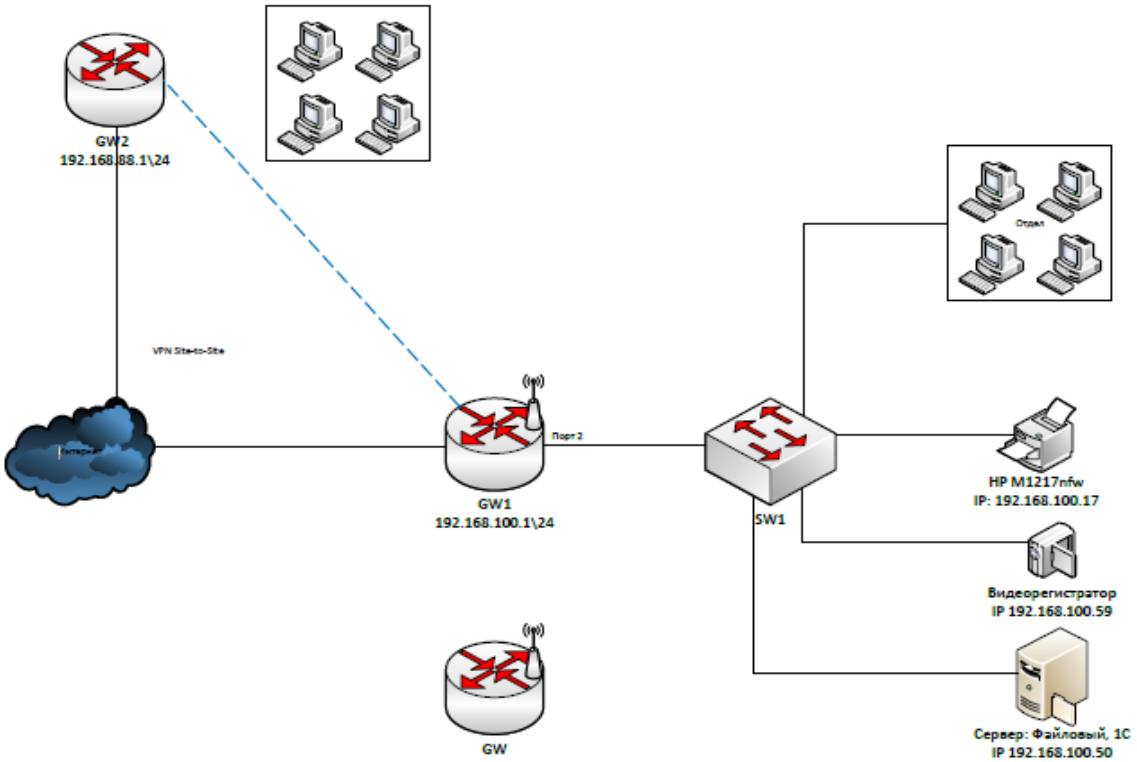


Рисунок 2.1 – Схема сети

Для стабильной работы в роль маршрутизатора исполняет Mikrotik RB951Ui-2HnD (рис.2.2). Это высокопроизводительный Wi-Fi роутер как для офиса, так и для дома. В качестве процессора используется Atheros AR9344 с частотой 600 МГц, а вкупе с 128 Мб оперативной памяти маршрутизатор показывает себя вдвое мощнее, чем устройства этой же серии, но выпущенные раньше. Роутер оборудован 5-ю Ethernet портами. Еще есть возможность получать питание по технологии PoE и запитывать по этой же технологии другое устройство уже через пятый порт.

Рисунок 2.2 – Внешний вид маршрутизатора

Маршрутизатор поставляется в комплекте с предустановленным программным комплексом Mikrotik RouterOS с лицензией четвертого уровня, что делает работу с устройством удобнее и быстрее. RouterOS может иметь как консольный вид (рис. 2.3), так и графический (рис. 2.4). По функционалу эти два интерфейса идентичны, поэтому какой использовать – дело лишь вкуса.

Данный маршрутизатор полностью соответствует требованиям сети и обеспечивает ее бесперебойную и качественную работу. В своем ценовом сегменте данный вариант также является предпочтительным.

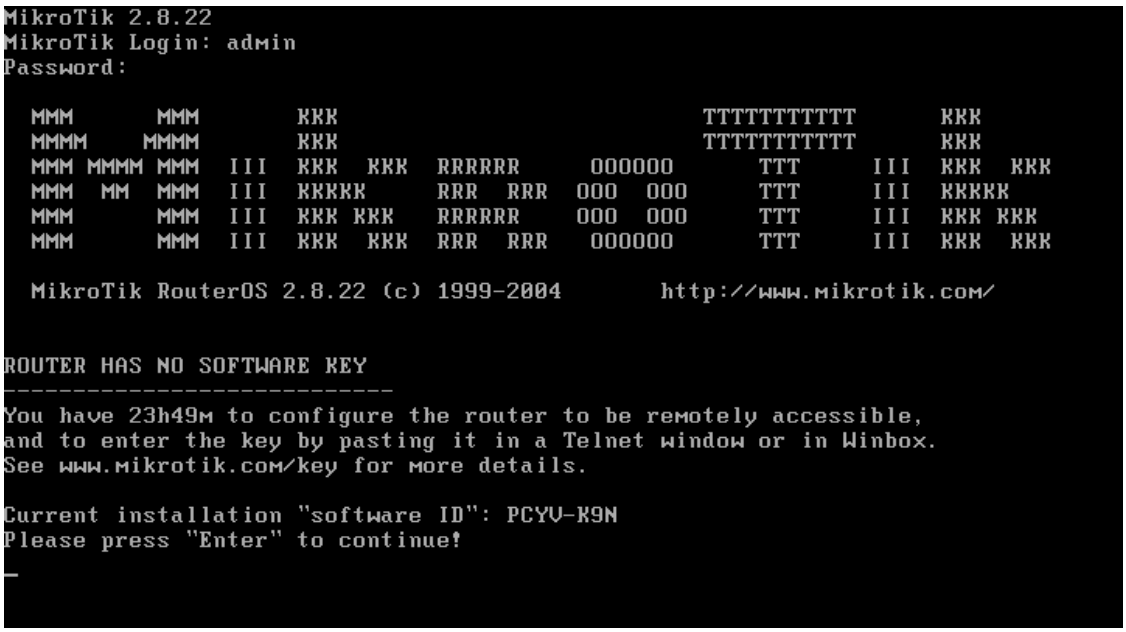


Рисунок 2.3 – Консольный вариант RouterOS

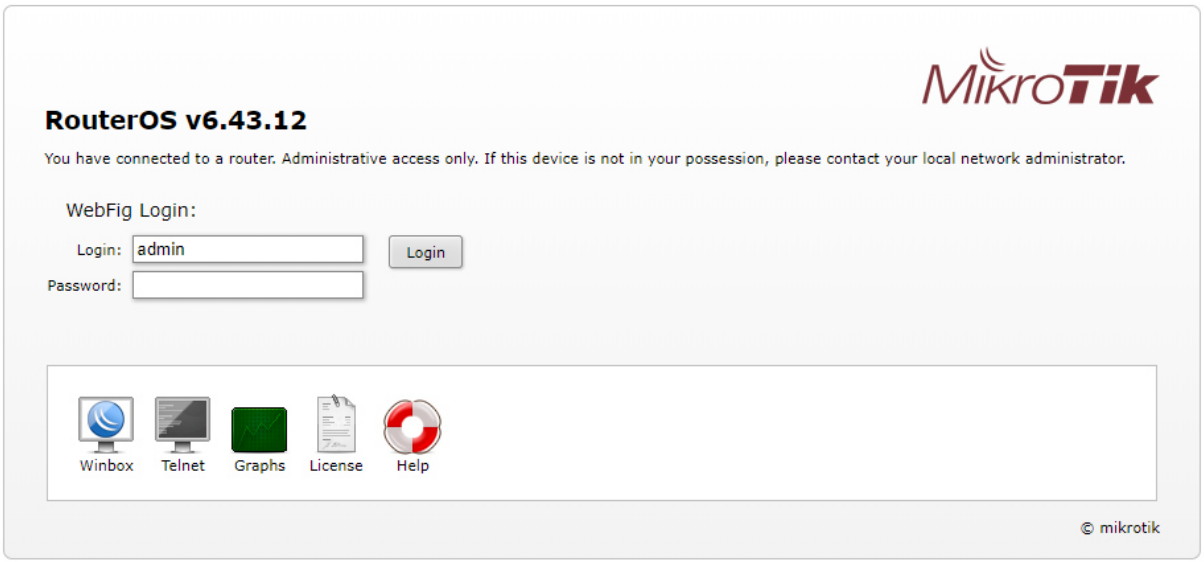


Рисунок 2.4 – Графический вариант RouterOS

Помимо маршрутизатора, к сетевым устройствам данной сети относится еще и коммутатор (свич). Свич – это сетевое устройство, которое обеспечивает соединение узлов сети для организации единой системы доступа пользователей со своих рабочих станций к сетевым ресурсам. Для коммутации в сети компании используется свич марки Cisco Catalyst 2960 (рис. 2.5).

Cisco Catalyst 2960 - новое семейство коммутаторов второго уровня с фиксированной конфигурацией, которое позволяет подключать рабочие станции к сетям Fast Ethernet и Gigabit Ethernet на скорости среды передачи, удовлетворяя растущие потребности в пропускной способности на периферии

сети. Для агрегации применяются комбинированные гигабитные uplink-порты, которые могут объединяться в единый канал по технологии GigabitEtherChannel.

Данная серия коммутаторов ориентирована в первую очередь на предприятия малого и среднего бизнеса. По сравнению с популярной серией коммутаторов Catalyst 2950 модели семейства 2960 обеспечивают более широкий набор функций обеспечения безопасности и качества обслуживания, а также управление полосой пропускания. В коммутаторах серии Catalyst 2960 для облегчения процесса конфигурирования была предусмотрена функция Smartports, которая позволяет выполнить основные настройки порта коммутаторов, основываясь на его назначении. Cisco Catalyst 2960 обеспечивают потребность в передаче данных со скоростью 100 Мбит/сек и 1 Гбит/сек, позволяют использовать LAN сервисы, например, для сетей передачи данных, построенных в филиалах корпораций. Семейство Catalyst 2960 позволяет обеспечить высокую безопасность данных за счет встроенного NAC, поддержки QoS и высокого уровня устойчивости системы.

Рисунок 2.5 – Коммутатор Cisco Catalyst 2960

К основным характеристикам данной модели можно отнести:

-высокий уровень безопасности, усовершенствованные списки контроля доступа (ACL);

-встроенные порты двойного назначения, функционирующие как для меди, так и оптоволокна. Каждый такой порт имеет встроенный порт 10/100/1000 Ethernet и порт SFP Gigabit Ethernet порт. При этом одновременно активным может быть только один из портов;

-организация контроля сети и оптимизация ширины канала с использованием QoS, дифференцированного ограничения скорости и ACL.

Чтобы обеспечить безопасность сети коммутатор использует несколько методов аутентификации пользователя, технологии шифрации данных,

организацию разграничения доступа к сетевым ресурсам на основании идентификатора пользователя, порта или же MAC-адреса.

Cisco Catalyst 2960 является лидером по соотношению цена/производительность. У данного коммутатора высокий уровень безопасности, встроена энергосберегающая технология, что не мало важно для офисного здания. Сетевым администраторам быстро и легко находить и устранять проблемы в сети благодаря поддерживаемой функцией Loopback Detection и диагностики кабеля.

Локальная сеть обеспечивает физическое соединение рабочих станций с файловым сервером, удаленных друг от друга, и состоит из:

а) сервера;

б) 19 персональных компьютеров;

в) сетевого кабеля;

г) сетевых адаптеров;

д) 1 коммутаторов;

е) 1 маршрутизатора.

Линия связи между сегментами сети предназначена для передачи текстовой информации, а именно различных документов для работы сотрудников, поэтому требования к пропускной способности линии связи не критичны и должны составлять не менее 500 Кбит/с.

Локальная сеть должна обеспечивать:

- обмен информацией между сегментами сети;
- работу программного обеспечения в сетевом режиме;
- совместное использование доступа в Интернет.

При построении локальной сети было учтено, что сеть не сложна в модификации и не зависит от работы одной из рабочих станций.

2.2 Настройка сетевого оборудования

Для того, чтобы реализовать на практике систему контроля интернет-трафика, необходимо выполнить следующие задачи:

– включить на внешнем интерфейсе Mikrotik захват NetFlow - статистики;

– отправить полученную статистику в NAS (например, в службу flow-tools, через flow-capture);

У Mikrotik есть своя реализация протокола Netflow, которая полность совместима со стандартом Cisco и называется Mikrotik Traffic Flow. С помощью Traffic Flow сетевой администратор может выявлять проблемы, которые могут возникнуть в сети, анализировать и оптимизировать общие характеристики сети. Поскольку Traffic Flow совместим полностью с Cisco Netflow, то он может в той же степени использоваться утилитами, разработанными для Netflow.

Traffic Flow поддерживает следующие версии Netflow:

- version 1 – первая версия протокола, рекомендуется использовать только в том случае, когда отсутсвуют альтернативы;

- version 5 – улучшенная версия первой версии Netflow;

- version 9 – новая версия, которая позволяет добавлять новые поля и типы записей благодаря шаблонному исполнению.

Для того, чтобы начать сбор статистики о трафике необходимо сначала включить Traffic Flow и определиться с интерфейсом, с которого, собственно, и будет производиться сбор. Делается это при помощи комбинации следующих команд:

/ip traffic-flow set enabled=yes interfaces=WAN

После включения Traffic Flow и определения с интерфейсом, с которого нужно получать информацию о потоках, необходимо настроить хост назначения (коллектор), который будет получать данную информацию. Производится настройка следующей командой:

/ip traffic-flow target add dst-address=<192.168.50.100> port=9091 v9-template-timeout=1m version=5

Можно производить сбор траффика как с одного интерфейса, так и с нескольких (в этом случае названия интерфейсов следует указать через запятую). В данном случае идет сбор с интерфейса WAN, через который идет выход локальной сети в интернет.

В качестве порта был выбран порт 9091. При работе буду использовать версию v5 протокола Netflow. IP-адрес 192.168.50.100 является адресом сервера-коллектора. Можно указать несколько коллекторов, используя разные версии протокола и номера UDP портов.

После этого маршрутизатор начнет отправлять данные о потоках на коллектор.

2.3 Конфигурирование сервера

Далее, в качестве операционной системы, на которой следует установить Flow-Tools, была выбрана FreeBSD (рис. 2.6). FreeBSD - это современная операционная система для настольных компьютеров, ноутбуков, серверов и встраиваемых систем с поддержкой большого количества платформ.

В основе FreeBSD лежит операционная система 4.4BSD-Lite Калифорнийского Университета с некоторыми усовершенствованиями из 4.4BSD-Lite2. Также она косвенно базируется на 386BSD (BSD Net/2, перенесённой на платформу i386TM Уильямом Джолитцем (William Jolitz)), хотя от того первоначального кода осталось очень мало.

FreeBSD используется компаниями, интернет-провайдерами, научными работниками, профессионалами в вычислительной технике, студентами и рядовыми пользователями по всему миру для работы, образования и отдыха.

Цель проекта FreeBSD - предоставить быструю и стабильную операционную систему общего назначения, которую можно использовать в любых целях без каких-либо ограничений.

Настройка Flow-Tools на FreeBSD производится следующими командами:

 # Установка NetFlow сенсора:

```
pkg install flow-tools
```

 # Настройка запуска:

```
echo 'flow_capture_enable="YES"' >> /etc/rc.conf.local
echo 'flow_capture_flags="-N-2"' >> /etc/rc.conf.local
```

 # Запуск:

```
service flow_capture start
```

Результат выполнения команд можно увидеть на рис. 2.7. По рисунку видно, что служба запущена без ошибок и ей присвоен PID = 799. Это значит, что flow-tools успешно установлены, и система готова принимать пакеты данных от маршрутизатора.

Рисунок 2.6 – Окно приветствия ОС

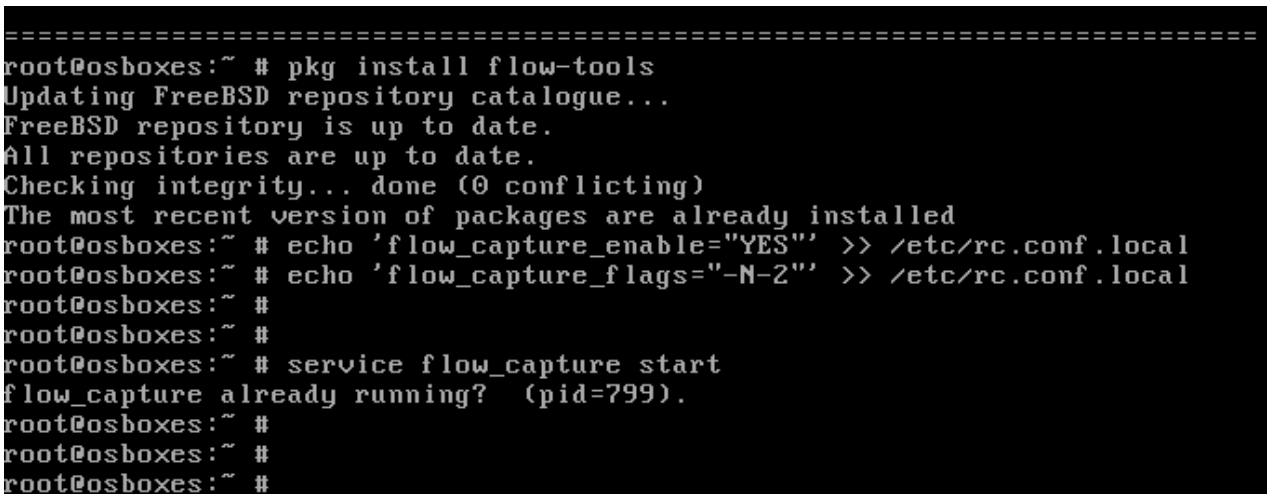


Рисунок 2.7 – Результат команд

В качестве базы данных, в которой будет храниться информация, собранная коллектором, была выбрана MySQL. MySQL – это одна из самых популярных и самых распространенных СУБД (система управления базами данных) в интернете. Она не предназначена для работы с большими объемами информации, но ее применение идеально, например, для интернет сайтов, как небольших, так и достаточно крупных.

MySQL отличатся хорошей скоростью работы, надежностью, гибкостью. Работа с ней, как правило, не вызывает больших трудностей. Поддержка сервера MySQL автоматически включается в поставку PHP.

Немаловажным фактором является ее бесплатность. MySQL распространяется на условиях общей лицензии GNU (GPL, GNU Public License).

Задача длительного хранения информации очень часто встречается в программировании Web-приложений: подсчёт посетителей в счётчике, хранение сообщений в форуме, удалённое управление содержанием информации на сайте и т.д.

Приложение на PHP, использующее для хранения информации базу данных (в частности MySql) всегда работает быстрее приложения, построенного на файлах. Дело в том, что базы данных написаны на языке C++, и написать на PHP программу, которая работала бы с жёстким диском эффективнее базы данных - задача неразрешимая по определению, поскольку программы на PHP в принципе работают медленнее, чем программы на C++, так как PHP - интерпретатор, а C++ - компилятор.

Таким образом, основное достоинство базы данных заключается в том, что она берёт на себя всю работу с жёстким диском и делает это очень эффективно.

В операционной системе FreeBSD установлен пакетный менеджер pkg, с помощью него и производится установка новых компонентов в систему

Установка и подготовка СУБД MySQL для импорта NetFlow данных:

Установим, запустим и настроим MySQL сервер:
pkg install mysql56-server

Запуск службы
echo 'mysql_enable="YES"' >> /etc/rc.conf service mysql start

Начальная настройка СУБД:
mysql_secure_installation

Установим Perl-модули для работы скрипта с СУБД:
pkg install p5-DBI p5-DBD-mysql

Входим в СУБД и создаем базу и пользователя для работы с ней:
mysql -u root –p

Далее необходимо создать саму базу данных и пользователя для нее:

mysql> create database data_netflow;
mysql> grant insert,create,update,select,delete on data_netflow.* to nflow_user@'localhost' identified by '1613local';
mysql> flush privileges;
mysql> exit;

После успешного выполнения вышеизложенных команд можно с уверенностью сказать, что СУБД установлена на операционной системе FreeBSD. Вывод команды, отображающей список созданных информационных баз можно увидеть на рисунке 2.8.

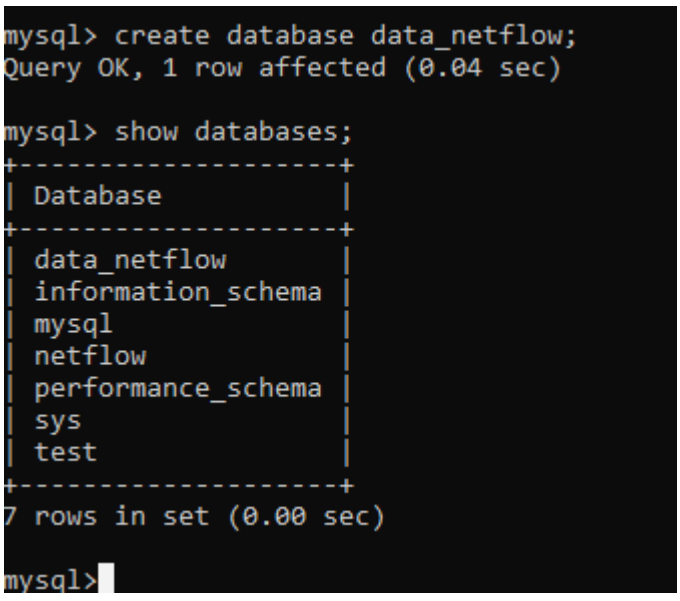


Рисунок 2.8 – Просмотр списка баз

2.4 Работа в среде Visual Studio

Microsoft Visual Studio — линейка продуктов компании Microsoft, включающих интегрированную среду разработки программного обеспечения и ряд других инструментальных средств. Данные продукты позволяют разрабатывать как консольные приложения, так и приложения с графическим интерфейсом, в том числе с поддержкой технологии Windows Forms, а также веб-сайты, веб-приложения, веб-службы как в родном, так и в управляемом кодах для всех платформ, поддерживаемых Windows, Windows Mobile, Windows CE, .NET Framework, Xbox, Windows Phone .NET Compact Framework и Silverlight.

Visual Studio включает в себя редактор исходного кода с поддержкой технологии IntelliSense и возможностью простейшего рефакторинга кода. Встроенный отладчик может работать как отладчик уровня исходного кода, так и отладчик машинного уровня. Остальные встраиваемые инструменты включают в себя редактор форм для упрощения создания графического интерфейса приложения, веб-редактор, дизайнер классов и дизайнер схемы базы данных. Visual Studio позволяет создавать и подключать сторонние дополнения (плагины) для расширения функциональности практически на каждом уровне, включая добавление поддержки систем контроля версий исходного кода (как, например, Subversion и Visual SourceSafe), добавление новых наборов инструментов (например, для редактирования и визуального проектирования кода на предметно-ориентированных языках программирования) или инструментов для прочих аспектов процесса разработки программного обеспечения (например, клиент Team Explorer для работы с Team Foundation Server).

12 ноября 2014 года было объявлено, что «Visual Studio 2015» принято в качестве окончательного варианта имени продукта.

Visual Studio 2015 предоставляется в трёх редакциях: бесплатной Community Edition, объединяющей все Express-версии, и платных Professional Edition для небольших проектов и Enterprise Edition для крупных проектов.

Visual Studio предоставляет доступ к целому ряду других утилит, которые позволяют просматривать и изменять различные аспекты компьютера или сети, не покидая среды разработки. Благодаря этим инструментам, можно просматривать выполняющиеся службы и активные соединения с базами данных, заглядывать в таблицы на сервере SQL Server и даже посещать веб-сайты с использованием окна Internet Explorer.

Visual Studio позволяет получать доступ к документации MSDN прямо из среды IDE. В случае, например, возникновения сомнений по поводу предназначения того или иного ключевого слова во время работы с текстовым редактором, можно выделить это ключевое слово и нажать клавишу <F1>, в результате чего Visual Studio автоматически подключится к MSDN и отобразит подходящие разделы справки. Аналогично, если нужно посмотреть,

что означает та или иная ошибка компиляции, потребуется выделять сообщение с ошибкой и нажать <F1>.

Также Visual Studio содержит графические редакторы и конструкторы XML, обеспечивает поддержку разработки программ Windows, ориентированных на мобильные устройства, поддержку разработки программ Microsoft Office и Windows Workflow Foundation, содержит встроенную поддержку рефакторинга кода и инструменты визуального конструирования классов.

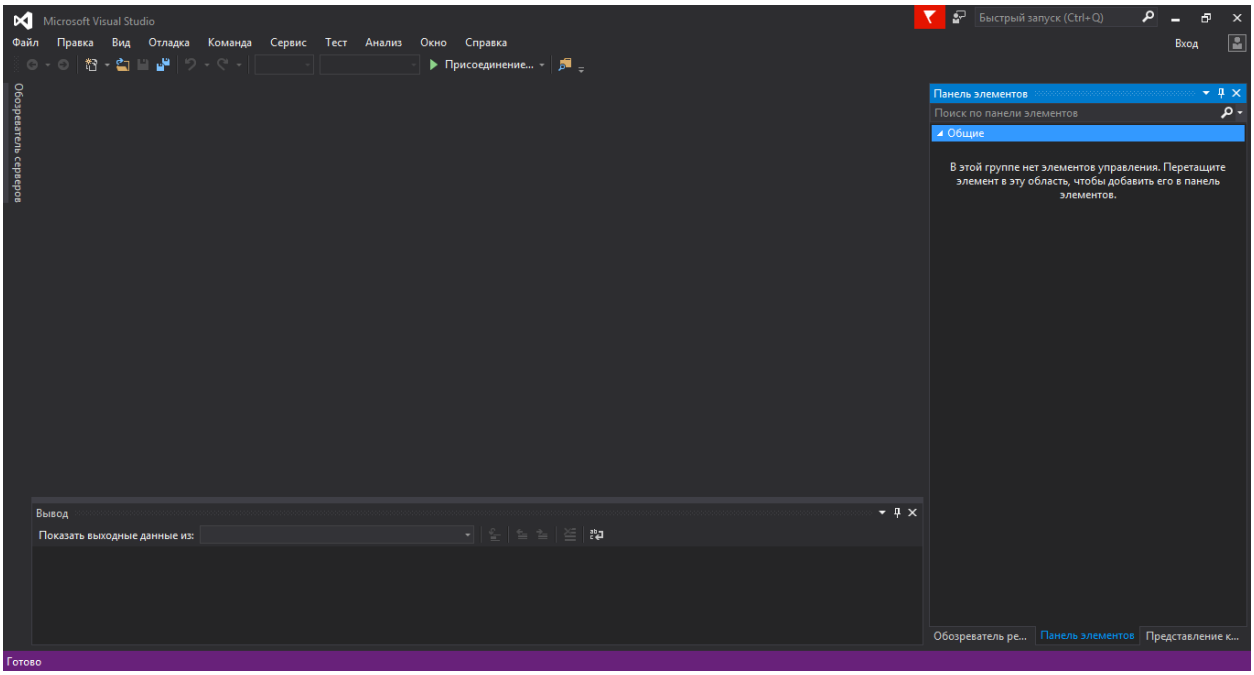


Рисунок 2.9 – Начальное окно программы

После установки Visual Studio можно приступать к созданию первого проекта. В Visual Studio редко когда требуется начинать с пустого файла и добавления в него кода C#. Разумеется, возможность создания пустого проекта приложения существует. Это нужно, если действительно возникла потребность в написании кода с нуля, либо при создании решения, которое должно содержать в себе несколько проектов.

Вместо этого, необходимо просто указать Visual Studio, проект какого типа должен быть создан, и среда автоматически сгенерирует файлы и код C#, образующие соответствующий указанному типу проекта каркас. Далее останется добавить в этот каркас собственный код.

При разработке приложения с пользовательским интерфейсом, наподобие приложения Windows, библиотеки элементов управления Windows или приложения ASP.NET, нужно использовать окно Design View (Конструктор). В этом окне предлагается визуальное представление того, как будет выглядеть форма. Обычно окно Design View применяется в сочетании с еще одним окном, которое называется Toolbox (Панель инструментов). В этом

окне отображается огромное количество компонентов .NET, которые можно перетаскивать в разрабатываемое приложение, как показано на рисунке 2.10

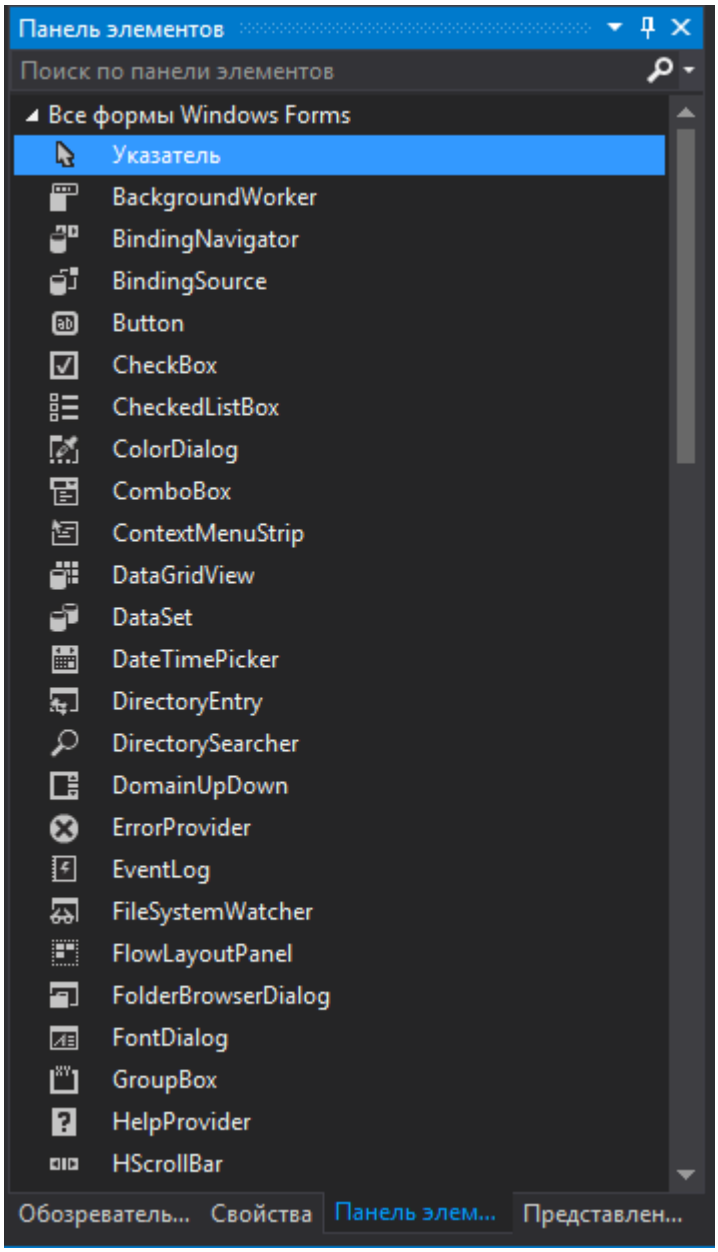


Рисунок 2.10 – Панель управления

Окно Properties (рис.2.11) тоже берет свое начало еще из старой IDE-среды Visual Basic. Как известно классы .NET могут реализовать свойства. На самом деле, базовые классы .NET, которые представляют формы и элементы управления, имеют множество свойств. Эти свойства определяют внешний вид и поведение, например, Width, Height, Enabled (указывающее, разрешен ли ввод в данном элементе управления) или Text (текст, отображаемый в данном элементе управления), и Visual Studio известно о многих из них. Окно Properties позволяет редактировать начальные значения большинства таких

свойств для тех элементов управления, которые Visual Studio обнаруживает при чтении исходного кода.

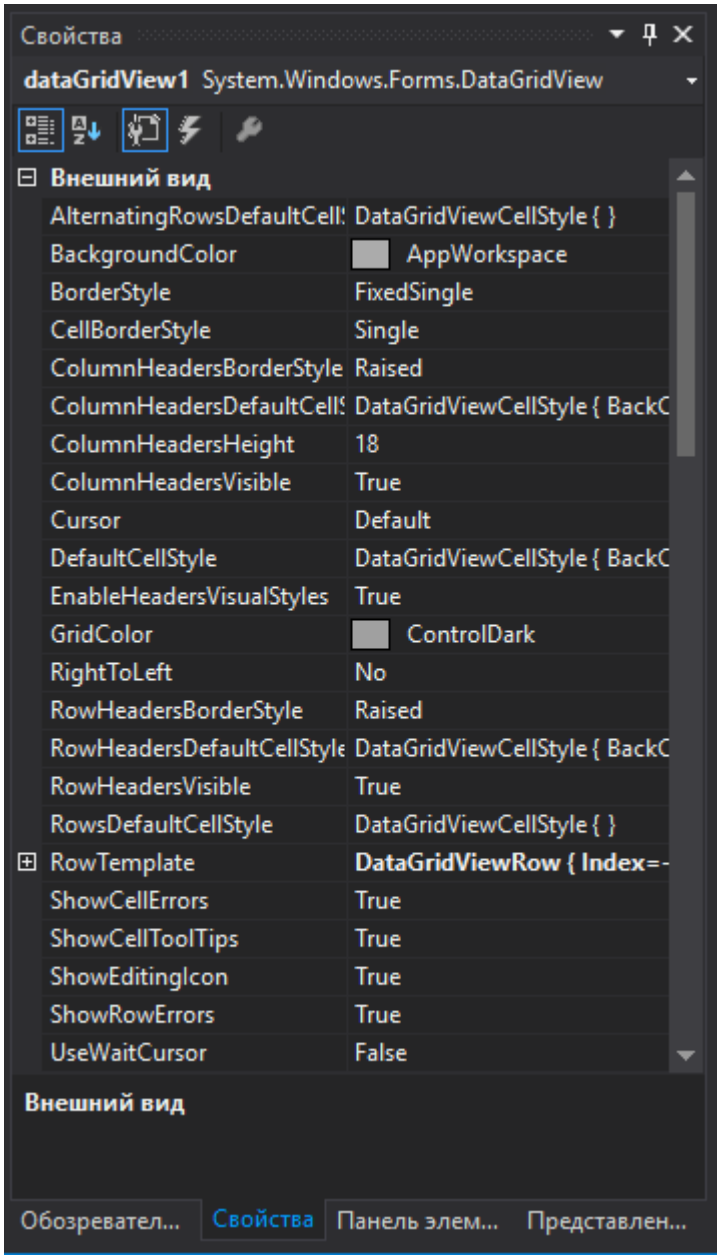


Рисунок 2.11 – Вкладка «Свойства»

В качестве языка программирования был выбран язык C#. C# — это изящный объектно-ориентированный язык со строгой типизацией, позволяющий разработчикам создавать различные безопасные и надежные приложения, работающие на платформе .NET Framework. C# можно использовать для создания клиентских приложений Windows, XML-веб-служб, распределенных компонентов, приложений клиент-сервер, приложений баз данных и т. д. Visual C# предоставляет развитый редактор кода, удобные конструкторы пользовательского интерфейса,

интегрированный отладчик и многие другие средства, которые упрощают разработку приложений на языке C# для платформы .NET Framework.

Синтаксис C# очень богат, но при этом прост и удобен в изучении. Характерные фигурные скобки C# мгновенно узнаются всеми, кто знаком с C, C++ или Java. Разработчики, знающие любой из этих языков, обычно очень быстро начинают эффективно работать в C#. Синтаксис C# упрощает многие сложности C++, но при этом предоставляет отсутствующие в Java мощные функции, например обнуляемые типы значений, перечисления, делегаты, лямбда-выражения и прямой доступ к памяти. C# поддерживает универсальные методы и типы, которые обеспечивают более высокий уровень безопасности и производительности, а также итераторы, позволяющие определять в классах коллекций собственное поведение итерации, которое может легко применить в клиентском коде. Выражения LINQ создают очень удобную языковую конструкцию для строго типизированных запросов.

Процесс построения в C# проще по сравнению с C или C++, но более гибок, чем в Java. Отдельные файлы заголовка не используются, и нет необходимости объявлять методы и типы в определенном порядке. Исходный файл C# может определить любое число классов, структур, интерфейсов и событий.

2.5 Интерфейс программы

Была поставлена задача, написать удобный графический интерфейс для вывода данных из базы данных MySQL. Системному администратору должно быть удобно искать необходимую сетевую информацию, отображать по фильтрам. В конечном счете было написано 2 формы:

- форма с авторизацией;
- форма программы.

Форма авторизации (рис. 2.12) состоит из двух элементов TextBox, трех элементов Label и одной кнопки Button. По нажатию кнопки происходит сверка введенных аутентификационных данных с теми, что прописаны в файле enter.txt. При введении неправильных учетных данных выходит сообщение «Неверный логин или пароль». При введении пароля включена функция скрытие пароля от посторонних глаз, поэтому в работающем состоянии данная форма выглядит так, как на рисунке 2.13. С листингом данной формы можно ознакомиться в приложении Б.

Помимо формы с авторизацией, код которой представлен в приложении Б присутствует основная форма программы Form1.cs (рис. 2.14). На данной форме количество элементов побольше, чем на предыдущей. Львиную долю занимает DataGridView, который предназначен для вывода таблицы из базы данных MySQL. Данный элемент управления имеет огромное число настроек. Исполняющий код файла Form1.cs представлен в приложении В.

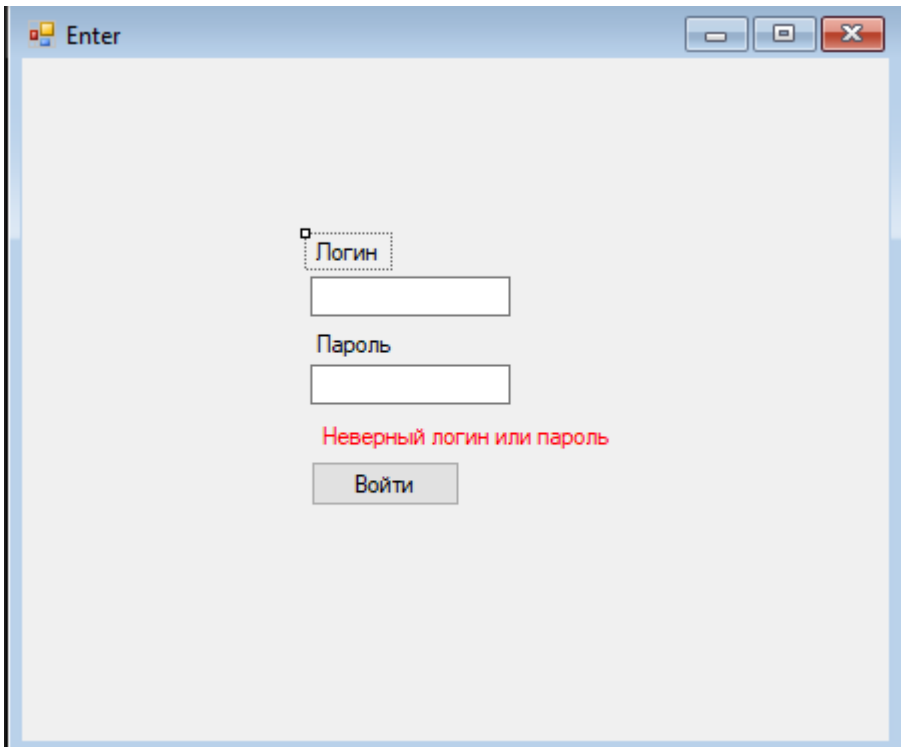


Рисунок 2.12 – Форма Enter.cs

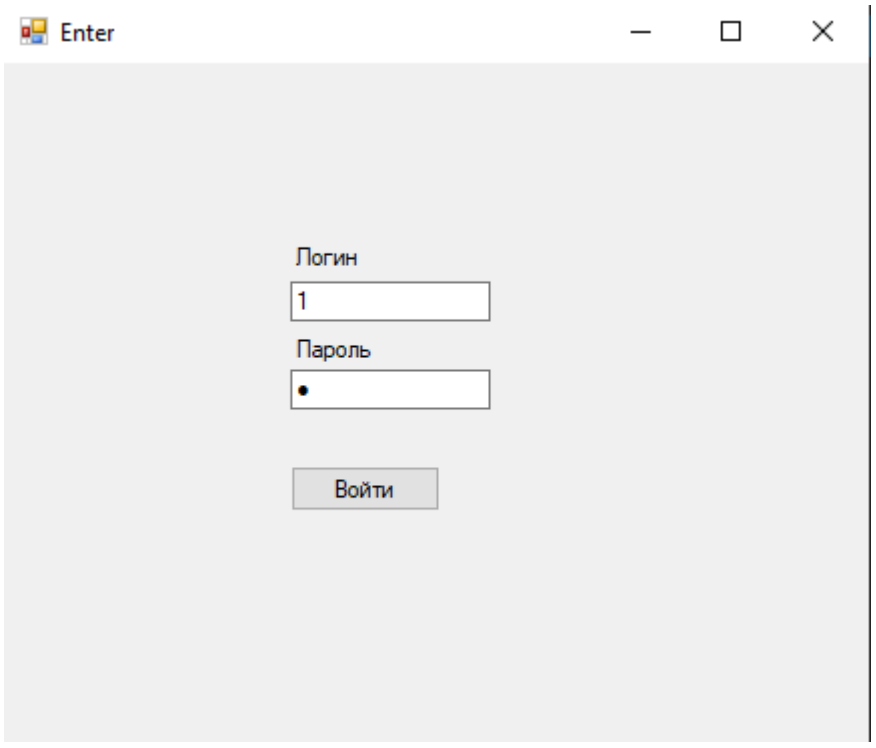


Рисунок 2.13 – Форма enter.cs работе

После успешного входа в приложении вторая форма автоматически откроется. Поиск с указанием фильтров помогает быстрее найти нужную информацию. Можно указать как дату, так и сервер, если он известен, так и протокол передачи данных.

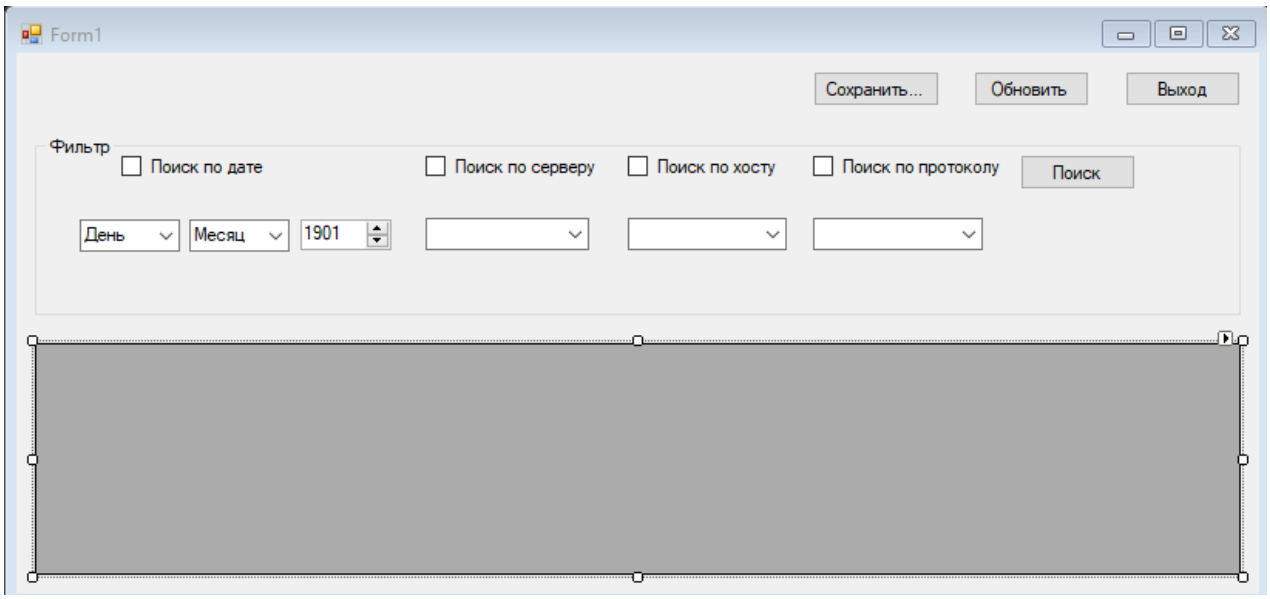
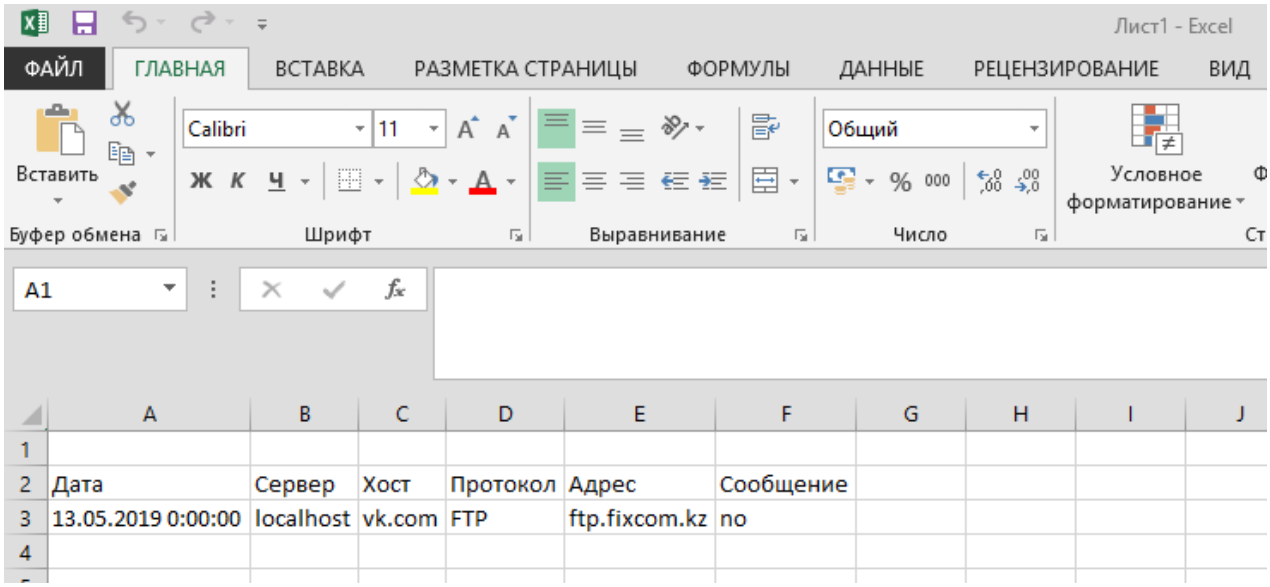


Рисунок 2.14 – Форма Form1.cs

Кнопка «Обновить» обновляет информацию и подгружает новую из базы данных. Если нажать на кнопку «Сохранить…», то можно получить выгрузку текущего отчета в excel-файл (рис. 2.15). Кнопка «Выход» возвращает к предыдущей форме с авторизацией.



	A	B	C	D	E	F
1						
2	Дата	Сервер	Хост	Протокол	Адрес	Сообщение
3	13.05.2019 0:00:00	localhost	vk.com	FTP	ftp.fixcom.kz	no
4						

Рисунок 2.15 – Вывод в excel

Скрин работы программы представлены на рисунке 2.16.

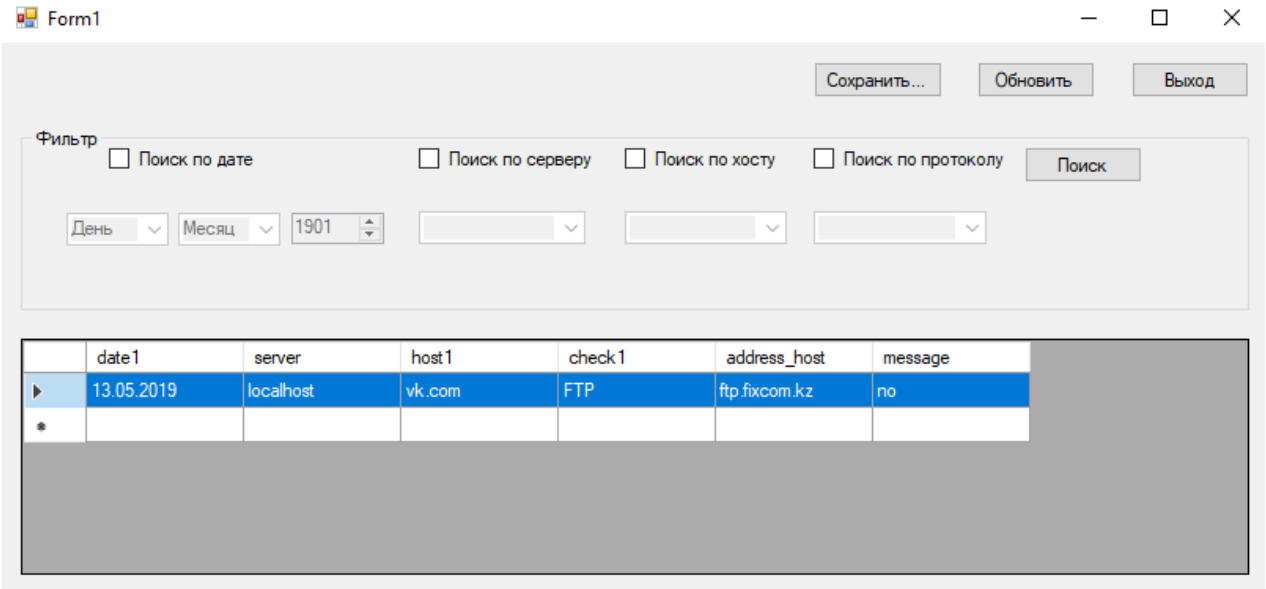


Рисунок 2.16 – Скрин работы программы

3 Безопасность жизнедеятельности

3.1 Анализ условий труда

В дипломном проекте проектируется информационная система учета интернет-трафика, которая представляет собой настроенную локальную сеть и программу для мониторинга, с которой будут работать it-инженер. Сотрудник будет производить мониторинг из помещения длиной $A = 4{,}2$ м и шириной $B = 3$ м, высота потолка $H = 3$ м. Площадь помещения составляет 12,6 м^2. В данном офисе практически отсутствует шум, потому что в нем находятся только компьютеры с периферийными устройствами и люди, а приборы, выделяющие большое количество шума (такие как производственные станки и т.д.), отсутствуют. В помещении присутствует окно, выходящее на запад, площадью примерно 3 м^2. Окно обрамлено металлическим переплетом, загрязнение на стеклах незначительное. Для защиты от чрезмерного поступления света во второй половине дня предусмотрено наличие жалюзи. Искусственное освещение осуществляется энергосберегающими лампочками в количестве 3-х штук. Поэтому можно сделать вывод, что с освещением, как с естественным, так и с искусственным, в помещении всё отлично – поступает оптимальное количество света для работы. Помимо инженера, который будет работать с написанной программой, в офисе находятся еще 2 человека. Кондиционер, который установлен, не справляется с нагрузкой и в помещении температура не соответствует нормам. Отсутствие систем, поддерживающих температуру в допустимых значениях или не способных осуществлять воздухообмен в должном количестве негативно сказывается на работе сотрудников, а в некоторых случаях может привести к некоторым болезням. Поэтому будет производиться расчет вентиляции и воздухообмена, необходимого для конкретно этого помещения, также подберется кондиционер, способный обеспечить данный офис необходимым потоком воздуха и поддерживать температуру в оптимальных пределах как в теплое, так и в холодное времена года.

3.2 Расчет вентиляционной системы

Для лучшей наглядности исходные данные помещения были представлены в виде таблицы 3.1.

Таблица 3.1 – Исходные данные

Город		Алматы
Параметры помещения		Длина-4,2 м, ширина – 3 м, высота – 2,5м
Оборудование	количество	6
	Мощность $P_{об}$, кВт/ч	0,1
	КПД	0,8
мощ. N ос.уст., Вт/м^2		9,5
Вид источников света		Энергосберегающие лампы
Окна	Кол-во	1
	площадь 1 окна, м^2	3,045
	Расположение	З
	Вид	Жалюзи, металлический переплет, загрязнение незначительное
Расчетное время суток, ч.		12-13
Температура, ^{0} С	Летом	24
	Зимой	20
Вид положения работы		Сидя

В помещениях различного назначения действуют в основном тепловые нагрузки, возникающие снаружи помещения (наружные); а также тепловые нагрузки, возникающие внутри зданий (внутренние).

Наружные тепловые нагрузки представлены следующими составляющими:

– теплопоступления или теплопотери в результате разности температур снаружи и внутри здания через стены, потолки, полы, окна и двери.

– разность температур снаружи здания и внутри него летом является положительной, в результате чего имеет место приток тепла снаружи во внутрь помещения; и наоборот – зимой эта разность отрицательна и направление потока тепла меняется;

– теплопоступления от солнечного излучения через застекленные площади; данная нагрузка проявляется в форме ощущаемого тепла;

– теплопоступления от инфильтрации.

В зависимости от времени года и времени суток наружные тепловые нагрузки могут быть положительными.

Теплопоступления и теплопотери в результате разности температур определяются по формуле (3.1):

$$Q_{огр} = V_{пом} \cdot X_o \cdot (t_{Нрасч} - t_{Врасч}), \quad Вт \tag{3.1}$$

где $V_{пом}$ – объем помещения, $м^3$

X_o – удельная тепловая характеристика, $Вт/м^3\,^0C$

$$X_o = 0.42 \quad Вт/м^3\,^0C,$$

$t_{Нрасч}$ – наружная температура. Для холодного периода – средняя температура самого холодного месяца в 13 часов, для теплого периода – средней температуре самого жаркого месяца в 13 часов.

$T_{Врасч}$ – внутренняя температура, выбирается с учетом комфортных условий или технологических требований, предъявляемых к производственным процессам.

Объем помещения в данном случае равен:

$$V_{пом}=4{,}2*3*2{,}5=31{,}5\ м^3;$$

Для теплого времени года

$t_{Нрасч} = 29{,}4\ ^0C$

$t_{Врасч} = 24\ ^0C$

$$Q_{огр} = 31{,}5 \cdot 0{,}42 \cdot 5{,}4 = 71{,}442\ Вт$$

Для холодного времени года

$t_{Нрасч} = -9\ ^0C$

$t_{Врасч} = 20\ ^0C$

$$Q_{огр} = 31{,}5 \cdot 0{,}42 \cdot 29 = 383{,}67\ Вт$$

Избыточная теплота солнечного излучения в зависимости от типа стекла почти до 90% поглощается средой помещения, остальная часть отражается. Максимальная тепловая нагрузка достигается при максимальном уровне излучения, которое имеет прямую и рассеянную составляющие. Интенсивность излучения зависит от ширины местности, времени года и времени суток.

Теплопоступление от солнечного излучения через остекление определяется по формуле

$$Q_p = (q^I F_0^I + q^{II} F_0^{II}) \cdot \beta_{с.з.} \tag{3.2}$$

где q^I, q^{II} – тепловые потоки от прямой и рассеянной солнечной радиации, Вт/м^2;

F^I_o, F^{II}_o – площади светового проема, облучаемые и необлучаемые прямой солнечной радиацией, м^3;

$\beta_{с.з.}$ – коэффициент теплопропускания.

$$B_{с.з.} = 0.15$$

При отсутствии наружных затеняющих козырьков, ребер и т. Д. для периода облучения остекления солнцем, когда его лучи проникают через окно в помещение $F^I_o=F_o$; $F^{II}_o=0$,:

$$Q_p = q^I F_0 \cdot \beta_{с.з.} = (q_{вп} + q_{вр}) \cdot K_1^c \cdot K_2 \cdot \beta_{с.з.} \cdot n \cdot S_o, \quad Вт \tag{3.3}$$

$q_{вп}$; $q_{вр}$ – тепловые потоки от прямой рассеянной радиации, Вт/м^2. По таблице 3.2 для широты в 44^0 СШ после полудня в 12-13 ч. При расположении З:

$$q_{вр} = 59 \text{ Вт/м}^2;$$

Таблица 3.2 – Поступление тепла (qвп, qвр) от прямой (П) и рассеянной (Р) радиации в июле через вертикальное остекление (СН и П II-33-75)

Расчет географ. Широта	Истинное солнечное время		Вертикальное остекление до полудня							
	до полудня	после полудня	С		ЮВ		Ю		ЮЗ	
			Вертикальное остекление после полудня							
			С		ЮЗ		Ю		ЮВ	
			П	Р	П	Р	П	Р	П	Р
44	5-6	18-19	84	38	72	40	-	23	-	22
	6-7	17-18	42	70	209	86	-	55	-	44
	7-8	16-17	-	77	333	109	-	71	-	55
	8-9	15-16	-	71	398	108	66	79	-	60
	9-10	14-15	-	64	387	101	162	81	-	63
	10-11	13-14	-	60	305	86	245	84	-	67
	11-12	12-13		59	214	79	288	85	73	77
48	5-6	18-19	93	45	95	45	-	27	-	26
	6-7	17-18	35	69	237	87	-	55	-	43
	7-8	16-17	-	74	363	109	3	73	-	53
	8-9	15-16	-	70	427	112	80	81	-	60
	9-10	14-15	-	64	419	107	186	86	-	65
	10-11	13-14	-	60	352	94	271	87	7	70
	11-12	12-13		59	251	84	317	88	106	78

$F_o = nS_o = 1 \cdot 2{,}1 * 1{,}45 = 3{,}045$ м^2 – площадь светового проема, где

n – число окон;

S_o – площадь 1 окна;

K_1 – коэффициент затемнения остекления переплетами (K^T_1 – для проемов в тени).

K^T_1= 1,28;

K_2 – коэффициент загрязнения остекления.:

K_2 = 0,95.

Тогда:

$$Q_p = 65 \cdot 1{,}28 \cdot 0.95 \cdot 0.15 \cdot 3{,}045 = 36{,}1015\ Вт$$

Внутренние нагрузки в жилых, офисных или относящихся к сфере обслуживания помещениях слагаются в основном из тепла:

– выделяемого людьми;

– выделяемого лампами и осветительными, электробытовыми приборами;

– выделяемого компьютерами, печатающими устройствами фотокопировальными машинами пр.;

В производственных и технологических помещениях различного назначения дополнительными источниками тепловыделений могут быть: нагретое производственное оборудование, горячие материалы, в том числе жидкости и различного рода полуфабрикаты, продукты сгорания и химических реакций.

Теплопоступления от людей зависит от интенсивности выполняемой работы и параметров окружающего воздуха. Тепло, выделяемое человеком, складывается из ощутимого (явного), то есть передаваемого в воздух помещения путем конвекции и лучеиспусканий, и скрытого тепла, затрачиваемого на испарение влаги с поверхности кожи и из легких.

По таблице 3.3 летом при 24 ^{0}С один мужчина выделяет явного тепла 67 Вт, а общего – 102 Вт. Женщина выделяет 85% от нормы тепловыделений взрослого мужчины. Тогда выделение явного тепла в помещении составит:

$$Q^я_л = 67 * 2 + 67 * 1 * 0{,}85 = 190{,}95\ Вт.$$

А выделение общего тепла:

$$Q^о_л = 102 * 2 + 102 * 1 * 0{,}85 = 290{,}7\ Вт.$$

По таблице 3.3 зимой при 20^{0}С один мужчина выделяет явного тепла 82 Вт, а общего – 103 Вт. Тогда выделение явного тепла в помещении составит:

$$Q^я_з = 82 * 2 + 82 * 1 * 0.85 = 233{,}7\ Вт.$$

А выделение общего тепла:

$$Q^о_з = 103 * 2 + 103 * 1 * 0{,}85 = 293{,}55\ Вт.$$

Теплопоступление от осветительных приборов, оргтехники и оборудования рассчитывается следующим образом. Теплопоступление от ламп определяется по формуле (3.4):

$$Q_{осв} = \eta \cdot N_{осв} \cdot F_{пол},\ \ Вт \qquad (3.4)$$

где η – коэффициент перехода электрической энергии в тепловую (для энергосберегающей лампы η=0,25);

$N_{осв}$ – установленная мощность ламп

Мощность энергосберегающих ламп N=9,5 Вт/м^2;

$F_{пол}$ – площадь пола:

$$F_{пол} = 4{,}2 * 3 = 12{,}6\ м^2$$

Тогда:

$$Q_{осв} = 0{,}25 * 9{,}5 * 12{,}6 = 29{,}925\ Вт.$$

Тепло, выделяемое производственным оборудованием, определяется по формуле (3.5):

$$Q_{об} = N_{уст} \cdot K \tag{3.5}$$

$$Q_{об} = 0{,}1 * 0.8 * 6 = 0{,}48\ кВт.$$

Теплопритоки, возникающие за счет находящейся оргтехники, - это 30% мощности оборудования:

$$Q_{орг} = 0{,}1 * 6 * 0{,}3 = 0{,}18\ кВт.$$

3.3 Расчет теплового баланса

На основании выполненных расчетов составим баланс теплопоступлений в помещении:

$$Q_{изб} = Q_р + Q^я + Q_{осв} + Q_{об} + Q_{орг} + Q_{огр} \tag{3.6}$$

Лето:

$$Q_{изб} = 36{,}1015 + 190{,}95 + 29{,}925 + 480 + 180 + 71{,}442 = 988{,}4185\ Дж$$

Зима:

$$Q_{изб} = 36{,}1015 + 233{,}7 + 29{,}925 + 480 + 180 + 383{,}67 = 1343{,}3965\ Дж$$

Так как тепловой баланс для зимы больше летнего теплового баланса, то рассчитаем теплонапряженность воздуха по формуле (3.7):

$$Q_н = \frac{Q_{избзима} * 860}{V_{пом}} \tag{3.7}$$

Получаю следующее значение теплонапряженности:

$$Q_н = \frac{1343{,}3965 * 860}{31{,}5} = 36{,}67\ ккал/м3$$

При $Q_н$>20ккал/м^3, Δt=8 °С,

Определение количества воздуха, необходимое для поступления в помещение:

$$L = \frac{Q_{изб} * 860}{c * \Delta t * \gamma} = \frac{1343{,}3665 * 860}{0.24 * 8 * 1{,}206} = 498{,}94\ м^3/час$$

где С=0,24 ккал/(кг°С) – теплоемкость воздуха,

γ=1,206 кг/м^3 – удельная масса приточного воздуха.

Определение кратности воздухообмена:

$$N = \frac{L}{V_{пом}} = \frac{498{,}94}{31{,}5} = 15{,}839\ час^{-1}$$

3.4 Выбор кондиционера

Исходя из полученных данных, выбор пал на кондиционер сплит-системы настенного типа Midea Mission 18.

Таблица 3.3 – Основные технические характеристики настенного кондиционера Midea Mission 18

Параметр	Значение
Мощность охлаждения, BTU	18000
Потребляемая мощность при охлаждении, Вт	1740
Мощность обогрева, BTU	18500
Потребляемая мощность при обогреве, Вт	1540
ERR\COP, Вт/Вт	3,21/3,61
Расход воздуха внутренним блоком, $м^3$/ч	789/633/510
Уровень шума внутреннего блока, dB (A) (турбо/выс/сред/низ)	42,5/36/29,5
ШхВхГ внутреннего блока, мм	980x325x225
Вес внутреннего блока, кг	11,2
ШхВхГ наружного блока, мм	770x555x300
Вес наружного блока, кг	34,6
Напряжение питания, Ph/V/Hz	1/220/50

Во внешнем блоке находятся компрессор, конденсатор и вентилятор. Внешний блок можно установить на стене здания, то есть в таком месте, где горячий конденсатор может продуваться атмосферным воздухом более низкой температуры.

Внутренний блок устанавливается непосредственно в кондиционируемом помещении и предназначен для охлаждения или нагревания воздуха, фильтрации его и создания необходимой подвижности воздуха в помещении. Внутренние блоки поддерживают заданную температуру, обеспечивают равномерное распределение воздуха в помещении и работают практически бесшумно.

Функции Midea mission:

а) Фильтр высокой степени очистки;

б) Wi-Fi управление;

в) Управление кондиционером без пульта;

г) Режим комфортного сна;

д) Автоматический перезапуск;

е) Температурная компенсация;

ж) Автоматическое качание заслонки;
з) Работа при чрезвычайной ситуации;
и) Запоминание положения жалюзи;
к) Экономичный режим;
л) Обнаружение утечки хладагента;
м) 2 варианта подсоединения трубопровода;
н) Отключение звуковых сигналов.

Управление работой настенного кондиционера производится с дистанционного пульта, который позволяет задать режим работы кондиционера: обогрев, охлаждение, осушку, вентиляцию, ночной режим; задать требуемую температуру, которую должен поддерживать автоматически; выбрать режим работы вентилятора: настроить таймер, который включит или выключит кондиционер в заданное время; автоматически регулировать положение направляющих шторок и изменить таким образом направление воздушного потока.

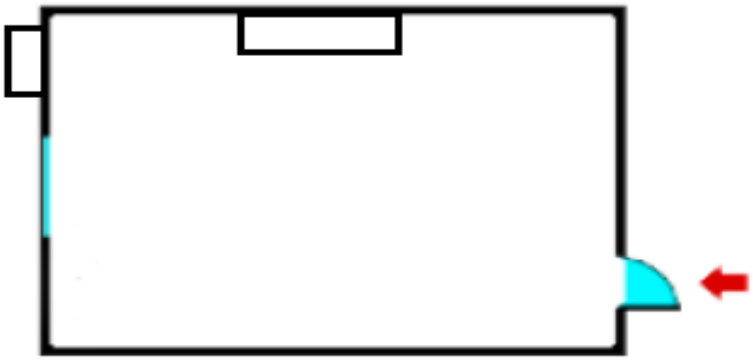


Рисунок 3.1 – Схема расположения кондиционера в помещении

4 Технико-экономическое обоснование проекта

4.1 Резюме

Расчет экономической эффективности абсолютно любого проекта является неотъемлемой частью разработки проекта, потому что нет смысла реализовывать заранее нерентабельную разработку. Затраты на реализацию любого программного средства зависят от материальных трат на ресурсы, затрат на заработную плату разработчика, включая социальные отчисления, амортизационные отчисления и др.

Информационная система, полученная в результате разработки дипломного проекта, представляет собой локальную сеть и специальное программное обеспечение, с помощью которого it-инженер реализует мониторинг сети. Данное ПО упрощает жизнь it-инженера и позволяет ему экономить своё время и материальные ресурсы компании.

4.2 Расчет затрат на разработку

Основные задачи планирования:

– определение объема предстоящих работ;

– взаимная увязка программы и установление рациональной последовательности предстоящих работ;

– установление сроков выполнения работ.

Работы по планированию сводятся к составлению перечня работ, определению их трудоемкости, расчету длительности цикла работ, обоснования сметы затрат на проведение работ.

Полный перечень работ с разделением их по этапам выполнения проекта следует оформить в виде таблицы, фрагмент которой показан в таблице 4.1.

Таблица 4.1 – распределение работ по этапам и видам и оценка их трудоемкости.

Этапы разработки ПП	Вид работы на данном этапе	Трудоемкость разработки ПП	
		Чел. х час	Час х день
Анализ требований	Формирование цели и задач проекта, выделение базовых сущностей и взаимосвязей между ними	1 х 16	8 х 2
Проектирование	Получение технических заданий, назначение требований к пользовательскому	1 х 16	8 х 2

	интерфейсу, оценка и подбор оборудования		

Продолжение таблицы 4.1

Разработка	Экспериментирование и анализ, строение прототипов, как целой системы, так и ее частей	1 х 64	8 х 8
Тестирование	Тестирование системы	1 х 40	8 х 5
Подготовка документации	Подготовка полной инструкции для работы с продуктом	1 х 16	8 х 2
Внедрение и поддержка	Установка программного обеспечения, обучение пользователей, исправление выявленных в ходе работы ошибок.	1 х 48	8 х 6
Итого трудоемкость выполнение дипломного проекта		1 х 200	8 х 25

Для определения затрат на разработку ПП нужно составить смету, которая включает следующие статьи:

– материальные затраты;
– затраты на оплату труда;
– социальный налог;
– амортизация основных фондов;
– прочие затраты.

Затраты на основные и вспомогательные материалы относятся к материальным затратам. Расчет затрат на материальные ресурсы и стоимость оборудования производятся по форме, приведенной в таблицах 4.2 – 4.3

Таблица 4.2 – Стоимость оборудования и ПО

№	Наименование	Описание	Цена за единицу, тг	Сумма, тг
1	Ноутбук	Acer 5750g	75 000	75 000
2	Операционная система	Microsoft Windows 10 Pro	45 000	45 000
3	СУБД	MySQL	бесплатно	бесплатно
4	Маршрутизатор	Mikrotik	8 500	8 500

5	Принтер	Canon LBP 6030	25 000	25 000
6	Патчкорд	Cat.5e/ UTP/ LSZH/ RJ-45/ 0.3 м	320	320

Таблица 4.3 – Затраты на материальные ресурсы

№	Наименование	Описание	Цена за единицу, тг	Сумма, тг
1	Бумага	А4	1 200	1 200

Эта подглава включает затраты на технологические нужды, которые приведены в таблице 4.4. Общая сумма затрат рассчитывается по формуле (4.1).

$$З_э = \sum_{i=1}^{n} М_i * K_i * T_i * Ц, \quad (4.1)$$

С 1 января 2019 года цена на электроэнергию по тарифу ТОО «АлматыЭнергоСбыт» составляет 15,92 тенге за 1 кВтч без НДС. Цена на электроэнергию с учетом НДС составит 17,81 тенге за 1 кВтч.

Таблица 4.4 – Затраты на технологические нужды

Наименование оборудования	Паспортная мощность, кВт	Коэффициент использования мощности	Время работы оборудования для разработки ПП, ч	Цена электроэнергии тг/кВт*ч	Сумма, тг
Ноутбук	0,2	0,8	200	17,81	569,920
Принтер	0,3	0,8	40	17,81	170,976
Маршрутизатор	0,003	0,8	200	17,81	8,548
Итого затраты на электроэнергию					749,445

Эта статья затрат учитывает выплаты по заработной плате за выполненную работу, исчисленные на основании тарифных ставок и должностных окладов в соответствии с принятой в организации – разработчике системой оплаты труда. Затраты на оплату труда рассчитывают по форме, приведенной в таблице 4.5.

Общая сумма затрат на оплату труда рассчитывается по формуле (4.2).

$$З_{тр} = \sum_{i=1}^{n} ЧС_i * T_i, \quad (4.2)$$

Часовая ставка работника, рассчитанная по формуле, равняется – 600 тг /час.

Ежемесячная заработная плата начинающего инженер-программиста, который участвовал в разработке ПП = 120000 тг.

Таблица 4.5 – Затраты

Категория работника	Трудоемкость разработки ПП, чел. х ч	Часовая ставка, тг/ч	Сумма, тг
Разработчик	1 х 200	600	120 000
ИТОГО затрат на оплату труда			120 000

Отчисления на социальные нужды учитывает 9,5 % от затрат на оплату труда всех работников, однако пенсионные отчисления (10% от Зтр) не облагаются социальным налогом.

Обязательные пенсионные отчисления составят:

ОПВ = 120 000 * 10% = 12 000 (тенге).

Отсюда, сумма социального налога составит:

СН = (120 000 – 12 000) * 9,5% = 10 260 (тенге).

По статье «Амортизация основных фондов» рассчитываются амортизационные отчисления, исходя из стоимости основных используемых в процессе разработки программного продукта, сроков эксплуатации оборудования и годовой нормы амортизации.

Амортизация отчисления определяются согласно таблице 4.6. Сумма амортизационных отчислений вычисляется по формуле (4.3).

$$З_{ам} = \frac{С_{обор} * Н_а * N}{100 * 12 * t}, \quad (4.3)$$

где $Н_а$ – норма амортизации (%);

$С_{обор}$ – первоначальная стоимость оборудования;

N – время использования оборудования;

t – количество рабочих дней в месяце.

Необходимоучитывать, что в стоимость ОФ также входят затраты на такие вещи как: доставка, монтаж, установка программного обеспечения и оборудования. Норма амортизации для линейного способа начисления вычисляется по формуле (4.4).

$$Н_{ai} = \frac{100}{Т_{Hi}}, \quad (4.4)$$

Использование ОФ варьируется от 3 до 10 лет. Все используется в течении 8 лет. Программное обеспечение – 4 года. Используя формулу (4.4), заполним таблицу 4.6 для отображения амортизации основных фондов.

$$Н_{А1} = 100/8 = 12,5\%.$$
$$Н_{А3} = 100/4 = 25\%.$$

Расчеты амортизации:

$З_{ам} = (75000 \times 0,125 \times 25)/(1 \times 12 \times 24) = 813,802$ тг;
$З_{ам} = (45000 \times 0,25 \times 25)/(1 \times 12 \times 24) = 976,563$ тг;
$З_{ам} = (8500 \times 0,125 \times 25)/(1 \times 12 \times 24) = 92,231$ тг;
$З_{ам} = (25000 \times 0,125 \times 25)/(1 \times 12 \times 24) = 271,267$ тг.
$З_{ам} = (320 \times 0,125 \times 25)/(1 \times 12 \times 24) = 3,472$ тг;

Таблица 4.6– Амортизация основных фондов

Наименование оборудования и ПО	Стоимость оборудования и ПО, тг	Годовая норма амортизации, %	Время работы оборудования и ПО для разработки ПП, д	Сумма, тг
Ноутбук	75 000	12,5	25	813,802
Microsoft Windows 10 Pro	45 000	25	25	976,563
Маршрутизатор	8500	12,5	25	92,231
Принтер	25 000	12,5	25	271,267
Патчкорд	320	12,5	25	3,472
ИТОГО амортизация основных фондов				2157,335

Статья «Прочие затраты» представляет собой расходы за аренду помещения, коммунальные услуги, затраты на электроэнергию, рекламу и другие хозяйственные и организационные расходы.

Арендная плата за 1 кв.м. площади определяется:

$$А_п = С \times S \times К1 \times К2 \times К3 \times К4 \times К5 \times К6;$$

где $А_п$ – ставка арендной платы за пользование помещением;

С – базовая ставка арендной платы за имущественный наем 1 кв.м. - 1,5 МРП;

S – арендная площадь, квадратный метр;

К1 = 1,0;
К2 = 1,0;
К3 = 1,0;
К4 = 1,0;
К5 = 1,0;
К6 = 1,0.
Тогда:

$$А_п = 1,5 \times 2525 \times 13 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 48\ 237,5 \text{ тг}$$

Расходы на электроэнергию представлены в таблице 4.7

Таблица 4.7 – Затраты на электроэнергию

Наименование оборудования	Кондиционер	Освещение
Паспортная мощность, кВт	0,7	0,0095
Коэффициент использования мощности	0,8	0,7
Время работы оборудования для разработки ПП, ч	200	200
Цена электроэнергии тг/кВт*ч	17,81	17,81
Сумма, тг	1994,720	23,687
Итого затраты на электроэнергию		2018,407

При разработке информационной системы были использованы ресурсы Интернета, расходы на который составили 7300 тенге в месяц. Арендная плата за месяц составляет 48 237,5 тенге. Расходы за электроэнергию 2018,407 тенге в месяц. Итого по прочим затратам сумма составляет 57 555,907 тенге.

Рассчитав затраты, связанные с созданием информационной системы, опираясь на расчеты, полученные в пунктах 4 – 8 смета затрат была составлена и отражена в Таблице 4.8.

Таблица 4.8 – Смета затрат на разработку ПП

Статья затрат	Сумма, тг
Материальные затраты	155 020
Оплата труда	120 000

Социальный налог	10 260
Электроэнергия	749,445
Амортизация основных фондов	2 157,335

Продолжение таблицы 4.8

Прочие затраты	57 555,907
ИТОГО по смете	345 742,687

Величина возможной (договорной) цены ПП устанавливается на основе эффективности, качества и сроков её выполнения на уровне, отвечающим экономическим интересам заказчика (потребителя) и исполнителя и вычисляется по формуле (4.5).

$$Ц_д = З_{нир}\left(1 + \frac{Р}{100}\right), \quad (4.5)$$

Р–средний уровень рентабельности ПП принимается в размере 20%.

$$Ц_д = 345\ 742{,}687 * (1+0{,}2) = 414\ 891{,}224 \text{ (тенге)}.$$

Далее определяется цена реализации с учетом налога на добавленную стоимость (НДС), ставка (НДС) устанавливается законодательно. Налоговым Кодексом РК на 2019 год ставка НДС установлена в размере 12%.

Цена реализации с учетом НДС рассчитывается по формуле (4.6):

$$Цр = Цд + Цд * НДС, \quad (4.6)$$

$$Ц_р = 414\ 891{,}224 + 414\ 891{,}224 * 0{,}12 = 464\ 678{,}171 \text{ (тенге)}.$$

Рассчитанная возможная цена ПП составляет 464 678,171 тенге.

4.3 Оценка эффективности внедрения ПП

Экономическая эффективность до внедрения информационной системы рассчитывалась и осуществлялась одним работником.

Затраты на решение задачи без использования программного средства рассчитываются по формуле(4.7):

$$З_{тр} = ФЗП_р + ОТ_{з/п} \quad , \quad (4.7)$$

где $ФЗП_р$ – фонд заработной платы группы лиц, решающих данную задачу;

$ОТ_{з/п}$ – отчисления на социальные нужды (9,5%).

Фонд заработной платы работников определяется по формуле (4.8):

$$ФЗП_р = ЗП_р * N * 12 \quad , \qquad (4.8)$$

где $ЗП_р$ – оклад работника, тенге/месяц;
N – количество работников.
Оклад работника составляет 200 000 тенге в месяц
Исходя из этого, фонд заработной платы сотрудников за год составляет:

$$ФЗП_р = 120\,000 * 12 = 1\,440\,000 \text{ тг.}$$

$$ОТ_{з/п} = (ФЗП_р - ФЗП_р * 10\%) * 9{,}5\% = (1\,440\,000 - 1\,440\,000 * 0{,}1) * \\ * 0{,}095 = 123\,120 \text{ тг.}$$

Подставив полученный в формулу (8) и рассчитаем затраты на решение задач без использования программного продукта:

$$З_{тр} = 1\,440\,000 + 123\,120 = 1\,563\,120 \text{ тг.}$$

Годовые затраты машинного времени на решение задачи определяются по формуле (4.9):

$$З_м = K * q * 12 \quad , \qquad (4.9)$$

где К – количество часов использования ПК в месяц;
q – стоимость часа аренды сервера (146 тенге/час).

С учетом 8 часового рабочего дня, а также 24 рабочих дней в месяц, получаем часы использования ПК в месяц К=200 час. Исходя из этого получим:

$$З_м = 200 * 146 * 12 = 350\,400 \text{ тг.}$$

Скорость печати одного документа 0,1 минута (т.е. 0,0016 часа). Годовые затраты для печати результата с принтера $К_{печ}$ определяются:

$$З_п = t_п * N_э * q \quad , \qquad (4.10)$$

где $t_п$ – время на печать одного экземпляра;
$N_э$ – количество экземпляров в год;
q – стоимость часа машинного времени (146 тенге/час).
Учитывая, что в день примерно печатается 3 документа и 24 рабочих дней в месяце, то получим 864 экземпляров в год.
Исходя из этого, годовые затраты на печать составляют:

$$З_{п} = 0{,}0016 * 864 * 146 = 202 \text{ тг}$$

Суммарные затраты после внедренияпрограммного продукта определяются по формуле:

$$З_{ом} = З_{м} + З_{п} \quad , \qquad (4.11)$$

Подставив значения, получим:

$$З_{ом} = 350\,400 + 202 = 350\,602 \text{ тг.}$$

Экономия затрат от программного продукта определяется по формуле:

$$Э = З_{тр} - З_{ом} \quad , \qquad (4.12)$$

где $З_{тр}$ – затраты до внедрения системы;
$З_{ом}$’ – затраты после внедрения системы.
Подставив значения получим следующее:

$$Э = 1\,563\,120 - 350\,602 = 1\,212\,518 \text{ тг.}$$

Срок окупаемости программного продукта определяется по формуле (4.13):

$$Т_{ок} = С/Э \quad , \qquad (4.13)$$

где С – затраты на разработку и внедрение системы, тенге;
Э – экономия затрат от внедрения системы, тенге/год.
Подставив значения, получим:

$$Т_{ок} = 464\,678{,}171 \ /1\,212\,520 = 6 \text{ (месяца).}$$

$Е_{н}$ – нормативный коэффициент эффективности капитальных вложений ($Е_{н}$ = прибыль/затраты):

$$Е_{н} = 1\,212\,520 / 464\,678{,}171 = 2.6$$

Вывод по разделу: в результате расчета, было выявлено, что затраты на разработку и внедрение информационной системы составят $464\,678{,}171$. Данный проект окупится за 6 месяцев. Исходя из полученных данных можно сделать вывод, что проект является экономически эффективным и сэкономит средства компании в размере 1 212 520 тенге.

Заключение

Правильно настроенная система мониторинга сети позволяет существенно уменьшить время реагирования на возникшие неполадки в сети, контролировать входящий и исходящий трафик и минимизировать паразитный трафик в локальной сети.

При построении системы необходимо учитывать спецификацию сети, пропускную способность каналов связи, так как неправильно сконфигурированная система может не только не выполнять своих прямых обязанностей, а еще и испортить связь в существующей сети.

После выполненных работ можно сделать следующие выводы:

– маршрутизатор производителя Mikrotik является оптимальным вариантом для компании, входящей в сегмент малого бизнеса;

– сервер, на котором установлена FreeBSD быстро обрабатывает запросы, потому что данная операционная система оперативно взаимодействует аппаратным обеспечением компьютера;

– решение на основе NetFlow является самым бюджетным средством обнаружения вторжения, потому что не предусматривают использование отводов трафика и каких-либо методов выявления аномалий путем включения оборудования в разрыв;

– разработанное приложение для вывода данных работает стабильно и позволяет фильтровать данные в зависимости от потребностей сетевого инженера;

– в разделе БЖД было рассчитано оптимальное количество воздуха, необходимое для поступления в операторскую комнату;

– в разделе экономики были произведены расчеты, которые показали, что данный проект окупится в течении 4-х месяцев.

Список литературы

1. Таненбаум Э.С., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер,2012. — 960 с.

2. Куроуз Д.Ф., Росс К.В. Компьютерные сети. Нисходящий подход – М.: Эксмо,2016 – 912 с.

3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010. — 944 с.

4. Кузьменко, Н.Г. Компьютерные сети и сетевые технологии / Н.Г. Кузьменко. - СПб.: Наука и техника, 2013. - 368 с.

5. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. Стандарт третьего поколения / В.Г. Олифер, Н.А. Олифер.. - СПб.: Питер, 2013. - 944 с.

6. Яргер, Р.Дж. MySQL и mSQL: Базы данных для небольших предприятий и Интернета / Р.Дж. Яргер, Дж. Риз, Т. Кинг. - М.: СПб: Символ-Плюс, 2000. - 560 с.

7. Культин, Н. C# в задачах и примерах / Н. Культин. - М.: БХВ-Петербург, 2016**. -** 952 с.

8. Фленов М. Библия C# / Михаил Фленов. - М.: БХВ-Петербург, 2016. - 544 с.

9. Троелсен, Эндрю Язык программирования C# 2005 и платформа .NET 2.0 / Эндрю Троелсен. - М.: Вильямс, 2015**. -** 329 с.

10. Бекишева А.И. Методические указания к выполнению экономической части дипломной работы для бакалавров специальности 5В0703 - Информационные системы – Алматы: АУЭС, 2013.

Приложение А
(обязательное)

Техническое задание
на выполнение дипломного проекта
" Разработка ИС мониторинга и анализа интернет-трафика на основе протокола Netflow "

1 Наименование, шифр и основание для выполнения дипломного проекта (работу) (ДП).

1.1 Наименование ДП – " Разработка ИС мониторинга и анализа интернет-трафика на основе протокола Netflow ".

1.2 Основание для выполнения ДП – приказ по университету № 124 от «26» октября 2018 г.

2 Исполнитель – студентка группы ИНФ-15-2 Якубчак М.М..

3 Цель выполнения ДП и назначение работы.

3.1 Целью ДП является: разработка информационной системы мониторинга и анализа интернет-трафика, конфигурирование сетевого устройства для снятия данных о трафике, конфигурирование сервера-коллектора для сбора собранных с маршрутизатора данных, разработка программного обеспечения для удобного вывода собранных данных.

3.2 Назначение проекта – мониторинг трафика с последующим анализом, проводимым сетевым инженером, в локальных сетях.

4 Состав изделия

Информационная система должна состоять из:

4.1 коллектора данных о пакетах, передающихся в ЛС;

4.2 сенсора данных;

4.3 программного обеспечения,

5 Технические требования.

5.1 Требования к программному обеспечению (ПО) мониторинга данных.

5.1.1 ПО должно обеспечивать корректный и актуальный вывод данных из БД.

5.3.2 ПО должно производить фильтрацию выходных данных по нескольким заранее оговоренным фильтрам.

6 Этапы ДП и сроки их выполнения.

6.1 Этапы ДП и сроки их выполнения представлены в календарном плане (таблица 1).

Продолжение Приложения А

Таблица 1 – Этапы ДП и сроки их выполнения

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Анализ сетевого протокола	11.02.2019-01.03.2019	
Выбор и настройка компонентов сети	04.03.2019-29.03.2019	
Конфигурирование коллектора данных	01.04.2019-12.04.2019	
Сбор данных с маршрутизатора	15.04.2019-03.05.2019	
Создание приложения в среде Visual Studio	06.05.2019-13.05.2019	

7 Порядок приемки ДП и материалы, предъявляемые по окончании стадий ДП и в целом.

7.1 По окончании этапов и ДП в целом, прием работы осуществляется Государственной аттестационной комиссией (ГАК).

8 Требования по обеспечению сохранения государственной и военной тайны при выполнении ДП.

8.1 В период выполнения ДП требования по обеспечению сохранения государственной и военной тайны не предъявляются.

9 В процессе выполнения ДП допускается корректировка настоящего ТЗ, согласованная обеими сторонами.

Приложение Б

Листинг файла Enter.cs

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.IO;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace test
{
   public partial class Enter : Form
   {
      public Enter()
      {
         InitializeComponent();
         label5.Visible = false;
      }

      private void enter1_Click(object sender, EventArgs e)
      {

         if (password.Text != "" && login.Text != "")
         {
            string log = login.Text;
            string pass = password.Text;
            string enter = log + "\t" + pass;
            StreamReader reading = File.OpenText("enter.txt");
            string str;
            while ((str = reading.ReadLine()) != null)
            {
```

```
                if (str.Contains(enter))
                {
                    this.Hide();
                    main Form = new main();
                    Form.FormClosed += (s, args) => this.Close();
                    Form.Show();
                }
```

Продолжение Приложения Б

```
            else
                {
                    label5.Visible = true;
                }
            }
        }
        else
        {
            label5.Visible = true;
        }
    }
  }
}
```

Приложение В

Листинг файла Form1.cs

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using MySql.Data.MySqlClient;
using Microsoft.Office.Interop.Excel;

namespace test
{
   public partial class main : Form
   {
      MySqlCommand sCommand;
      MySqlDataAdapter sAdapter;
      MySqlCommandBuilder sBuilder;
      DataSet sDs;
      System.Data.DataTable sTable;
      public static string date;
      public main()
      {
         InitializeComponent();
         day.Enabled = false;
         month.Enabled = false;
         year.Enabled = false;
         comboBox1.Enabled = false;
         comboBox2.Enabled = false;
         comboBox3.Enabled = false;
         string sql = "SELECT * from data";
```

```
        string connectionString =
"server=localhost;user=root;database=netflow;password=1234;";

        MySqlConnection connection = new MySqlConnection(connectionString);
        connection.Open();
        sCommand = new MySqlCommand(sql, connection);
        sAdapter = new MySqlDataAdapter(sCommand);
```

Продолжение Приложения В

```
        sBuilder = new MySqlCommandBuilder(sAdapter);
        sDs = new DataSet();
        sAdapter.Fill(sDs, "data");
        sTable = sDs.Tables["data"];
        connection.Close();
        dataGridView1.DataSource = sDs.Tables["data"];
        dataGridView1.ReadOnly = true;
        dataGridView1.SelectionMode =
DataGridViewSelectionMode.FullRowSelect;
    }

    private void button1_Click(object sender, EventArgs e)
    {
        string sql = "SELECT * from data where host1 !="" ;
        if (comboBox1.Text != "")
        {
            sql += " AND server LIKE '%" + comboBox1.Text + "%'";
        }
        if (comboBox2.Text != "")
        {
            sql += " AND host1 LIKE '%" + comboBox2.Text + "%'";
        }
        if (comboBox3.Text != "")
        {
            sql += " AND check1 LIKE '%" + comboBox3.Text + "%'";
        }


        if (checkBox1.Checked)
        {
            int cs = 0;

            if (day.Text != "День" && month.Text != "Месяц")
            {
```

```
            cs = 1;
        }

        if (day.Text != "День" && month.Text == "Месяц")
        {
            cs = 2;             }
```

Продолжение Приложения В

```
        if (day.Text == "День" && month.Text != "Месяц")
        {
            cs = 3;
        }

        if (day.Text == "День" && month.Text == "Месяц")
        {
            cs = 4;
        }
        switch (cs)
        {
            case 1:
                date = " AND date1 = '" + Convert.ToString(year.Value) + "-" +
month.Text + "-" + day.Text + "'";
                break;

            case 2:
                date = " AND DAY(date1) =" + day.Text + " AND YEAR(date1) = "
+ Convert.ToString(year.Value);
                break;

            case 3:
                date = " AND MONTH(date1) = " + month.Text + " AND
YEAR(date1) = " + Convert.ToString(year.Value);
                break;
                }
            sql = sql + date;
        }

        string connectionString =
"server=localhost;user=root;database=netflow;password=1234;";

        MySqlConnection connection = new
MySqlConnection(connectionString);
        connection.Open();
        sCommand = new MySqlCommand(sql, connection);
```

```
            sAdapter = new MySqlDataAdapter(sCommand);
            sBuilder = new MySqlCommandBuilder(sAdapter);
            sDs = new DataSet();
            sAdapter.Fill(sDs, "data");
            sTable = sDs.Tables["data"];
            connection.Close();
```

Продолжение Приложения В

```
            dataGridView1.DataSource = sDs.Tables["data"];
            dataGridView1.ReadOnly = true;
            dataGridView1.SelectionMode =
DataGridViewSelectionMode.FullRowSelect;
        }


    private void checkBox1_CheckedChanged(object sender, EventArgs e)
    {
        if (checkBox1.Checked)
        {
            day.Enabled = true;
            month.Enabled = true;
            year.Enabled = true;
        }
        else
        {
            day.Enabled = false;
            month.Enabled = false;
            year.Enabled = false;
        }
    }

    private void checkBox2_CheckedChanged(object sender, EventArgs e)
    {
        if (checkBox2.Checked)
        {
            comboBox1.Enabled = true;
        }
        else
        {
            comboBox1.Enabled = false;
        }
```

```
    }

    private void checkBox3_CheckedChanged(object sender, EventArgs e)
    {
        if (checkBox3.Checked)
        {
            comboBox2.Enabled = true;
        }
        else
```

Продолжение Приложения В

```
        {
            comboBox2.Enabled = false;
        }
    }

    private void checkBox4_CheckedChanged(object sender, EventArgs e)
    {
        if (checkBox4.Checked)
        {
            comboBox3.Enabled = true;
        }
        else
        {
            comboBox3.Enabled = false;
        }
    }

    private void exit_Click(object sender, EventArgs e)
    {
        this.Hide();
        Enter Form = new Enter();
        Form.FormClosed += (s, args) => this.Close();
        Form.Show();
    }

    private void reload_Click(object sender, EventArgs e)
    {
        string sql = "SELECT * from data";

        string connectionString =
"server=localhost;user=root;database=netflow;password=1234;";

        MySqlConnection connection = new MySqlConnection(connectionString);
```

```
            connection.Open();
            sCommand = new MySqlCommand(sql, connection);
            sAdapter = new MySqlDataAdapter(sCommand);
            sBuilder = new MySqlCommandBuilder(sAdapter);
            sDs = new DataSet();
            sAdapter.Fill(sDs, "data");
            sTable = sDs.Tables["data"];
            connection.Close();
            dataGridView1.DataSource = sDs.Tables["data"];
```

Продолжение Приложения В

```
            dataGridView1.ReadOnly = true;
            dataGridView1.SelectionMode =
DataGridViewSelectionMode.FullRowSelect;
        }

        private void button2_Click(object sender, EventArgs e)
        {
            Microsoft.Office.Interop.Excel.Application ExcelApp = new
Microsoft.Office.Interop.Excel.Application();
            Workbook wb = ExcelApp.Workbooks.Add(XlSheetType.xlWorksheet);
            Worksheet ws = (Worksheet)ExcelApp.ActiveSheet;
            object misValue = System.Reflection.Missing.Value;
            ws.Cells[2, 1] = "Дата";
            ws.Cells[2, 2] = "Сервер";
            ws.Cells[2, 3] = "Хост";
            ws.Cells[2, 4] = "Протокол";
            ws.Cells[2, 5] = "Адрес";
            ws.Cells[2, 6] = "Сообщение";
            for (int i = 0; i < dataGridView1.Rows.Count; i++)
            {
                for (int j = 0; j < dataGridView1.ColumnCount; j++)
                {
                    ExcelApp.Cells[i + 3, j + 1] =
Convert.ToString(dataGridView1.Rows[i].Cells[j].Value);
                }
            }
            ws.Columns.AutoFit();
            ws.Cells.VerticalAlignment =
Microsoft.Office.Interop.Excel.XlVAlign.xlVAlignTop;
            ws.Cells.HorizontalAlignment =
Microsoft.Office.Interop.Excel.XlHAlign.xlHAlignLeft;
            ExcelApp.Visible = true;
        }
```

```
}
    }
```