МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт кибернетики и информационных технологий

Кафедра Кибербезопасность, обработка и хранение информации

Еркебай Абылай Ғалымжанұлы

Организация и обеспечение безопасности сети предприятия

ДИПЛОМНЫЙ ПРОЕКТ

Специальность 5В100200 – Системы информационной безопасности

Алматы 2021

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И. Сатпаева
Институт кибернетики и информационных технологий
Кафедра кибербезопасность, обработка и хранение информации

«Допущен к защите»
Заведующий кафедрой КОиХИ
_____ Н.А.Сеилова
26.05.2021

ДИПЛОМНЫЙ ПРОЕКТ

на тему: «Организация и обеспечение безопасности сети предприятия»

по образовательной программе 5В100200 – Системы информационной безопасности

Выполнил Еркебай.А.Ғ

Научный руководитель м.т.н., лектор Юбузова.Х.И

Алматы 2021

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт кибернетики и информационных технологий

Кафедра Кибербезопасность, обработка и хранение информации

5В100200 - Системы информационной безопасности

УТВЕРЖДАЮ
Заведующий кафедрой КОиХИ
канд. техн. наук, доцент
_____ Н.А.Сейлова
«26» 05 2021 г.

ЗАДАНИЕ
на выполнение дипломного проекта

Обучающемуся *Еркебай Абылай Ғалымжанұлы*
Тема: *Организация и обеспечение безопасности сети предприятия*
Утверждена *приказом Ректора Университета № 2131-б* от «*24*» *11 2020 г.*
Срок сдачи законченной работы «*15*» *05 2021г.*
Исходные данные к дипломному проекту:
Инфраструктура предприятия, КС, исходные данные по предприятию
Перечень подлежащих разработке в дипломном проекте вопросов:
а) обзор инфраструктуры предприятия;
б) организация защиты и безопасности сети;
в) способы модернизации сети;
г) проектирование сети на GNS3.
Перечень графического материала (с точным указанием обязательных чертежей):

Рекомендуемая основная литература: *из 10 наименований*

ГРАФИК

подготовки дипломного проекта

Наименования разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Анализ инфраструктуры предприятия	03.03.2021 г.	
Обеспечение безопасности сети предприятия	05.04.2021 г.	
Проектирование сети на ПО GNS3	28.04.2021 г.	

Подписи

консультантов и нормоконтролера на законченный дипломный проект с указанием относящихся к ним разделов проекта

Наименования разделов	Консультанты, И.О.Ф. (уч. степень, звание)	Дата подписания	подпись
Нормоконтроль	магистр техн.наук, ассистент Кабдуллин М.А.	19.05.2021	

Научный руководитель _____ Юбузова.Х.И.

Задание принял к исполнению обучающийся _____ Еркебай.А. Ғ.

Дата «24» 11. 2020г.

АҢДАТПА

Бұл дипломдық жоба компанияның компьютерлік желілеріндегі ақпаратты қорғаныс жүйесін бағдарламалық жасақтама мен бағдарламалық жасақтаманы қолдана отырып, рұқсатсыз қол жетімділіктен жаңартуға арналған.

Бұл мәселені шешу үшін кәсіпорынның ақпараттық инфрақұрылымына талдау жүргізіліп, қорғанысты қамтамасыз етудің қолданыстағы және қолданылатын тетіктері мен құралдары зерттелді. Алынған деректерді талдау нәтижесінде желідегі сегменттер, хосттар, серверлер және олардың арасындағы байланыстар анықталды. Әрі қарай, желілік жабдықты басқару және конфигурациялау жүзеге асырылды. Іс жүзінде іске асыру ретінде кәсіпорын желісі GNS3 платформасында жобаланған және Visio бағдарламалық жасақтамасы кәсіпорын диаграммасын құру үшін қолданылған.

АННОТАЦИЯ

Данный дипломный проект предназначен для модернизации системы защиты информации в компьютерных сетях предприятия от несанкционированного доступа с помощью технических и программных средств.

Для решения поставленной задачи проведен анализ информационной инфраструктуры предприятия, изучены имеющиеся и используемые механизмы и средства обеспечения защиты. В результате анализа полученных данных определены сегменты, хосты, сервера в сети и связи между ними. Далее проведено администрирование и конфигурирование сетевого оборудования. В качестве практической реализации сеть предприятия спроектирована на платформе GNS3, а ПО Visio использовано для построения схемы предприятии.

ANNOTATION

This diploma project is intended for the modernization of the information protection system in the company's computer networks from unauthorized access using hardware and software.

To solve this problem, the analysis of the information infrastructure of the enterprise was carried out, the existing and used mechanisms and means of ensuring protection were studied. As a result of the analysis of the data obtained, segments, hosts, servers in the network and connections between them are identified. Further, administration and configuration of network equipment was carried out. As a practical implementation, the enterprise network was designed on the GNS3 platform, and Visio software was used to build the enterprise diagram.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В эпоху, когда кража данных и нарушения безопасности происходят ежедневно, безопасное хранение данных является ключевым компонентом инфраструктуры безопасности. Ни для кого не секрет, что вакансии в сфере кибербезопасности пользуются большим спросом, а в 2020 году информационная безопасность была в первую очередь в списке желаний каждого ИТ-директора при приеме на работу.

Вопрос защиты информации всегда находятся в центре внимания у специалистов по информационной безопасности. Предприятия для организации защиты информации, циркулирующей в корпоративной сети и предотвращения утечки информации применяют различные специальные методы и средства. Развитие современных технологий, программного обеспечения и использование различных вычислительных устройств в компьютерных сетях оказывает огромное влияние на уязвимость информации: обрабатываемой, хранимой так и накопительной.

Сегодня проблема обеспечения безопасности корпоративной сети является очень важной и должна решаться, начиная с этапа проектирования топологии сети. Таким образом, в последние годы область информационной безопасности значительно выросла и эволюционировала. Она предлагает множество областей для специализации, включая обеспечение безопасности сетей и смежной инфраструктуры, защиту приложений и баз данных, тестирование безопасности, аудит информационных систем, планирование непрерывности бизнеса и т.д.

Обычно проектирование топологии сети выполняются с помощью Cisco Packet Tracer или GNS3. Я же буду использовать GNS3. Это практически полноценный лабораторный стенд, где вы можете макетировать нужные схемы или решения, проверить конфигурацию перед применением на реальном железе.

1. Анализ инфраструктуры предприятия

1.1 Схема офиса предприятия ТОО «ТрастФинАудит»

Компания «ТрастФинАудит» казахстанская аудиторская компания, зарекомендовавшая себя как компания с высококвалифицированными специалистами, имеющая отличную профессиональную репутацию независимого аудитора. «ТрастФинАудит» сотрудничает с компаниями различных видов деятельности, как с предприятиями государственного сектора, так и коммерческими организациями, например, строительные компании, различные холдинги, филиалы.

На предприятии работают 94 сотрудника, в их число входят:

- директор: 1 человек;
- заместители директора: 2 человека;
- отдел кадров: 4 человек;
- бухгалтерия: 4 человек;
- IT специалист: 4 человек;
- отдел по работе с клиентами: 15 человек;
- налоговый сектор: 20 человек;
- аудиторы: 20 человек;
- сектор бухгалтерских услуг: 15 человек;
- кассир: 2 человека;
- служба безопасности: 4 человека (посменно);

Здание предприятия состоит из трех этажей. Ниже на рисунках представлена внутренняя инфраструктура предприятия.

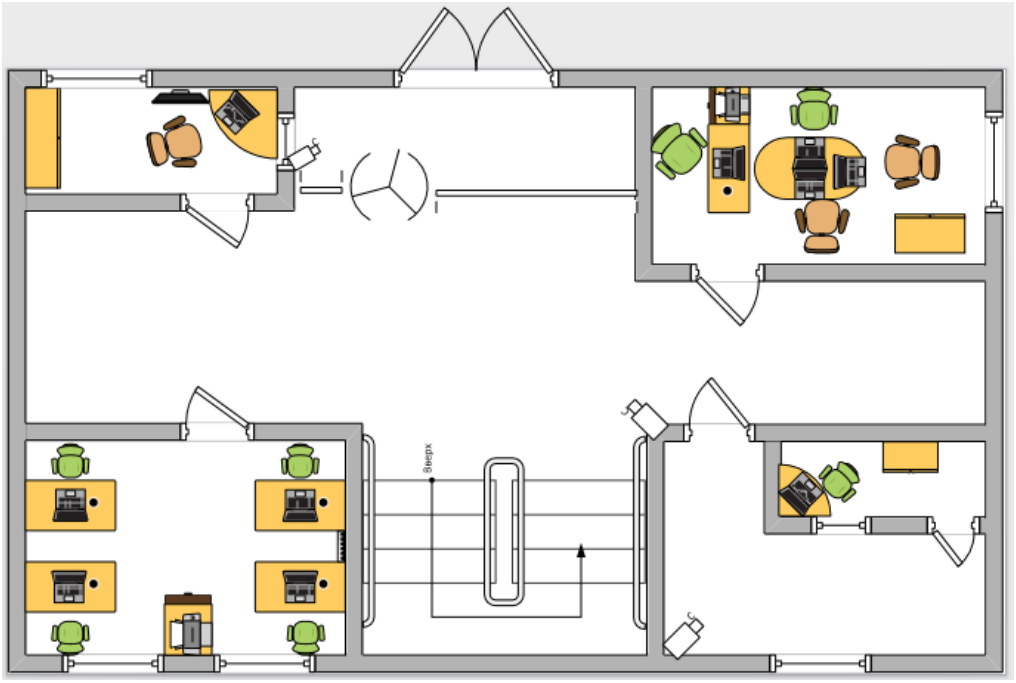


Рисунок 1 - План 1 этажа

На первом этаже находятся кабинеты: службы безопасности, бухгалетерии, кассы и HR менеджеров. На втором этаже находятся кабинеты: руководителя и его заместителей, IT специалистов, сектора бухгалтерских услуг. На третьем этаже находятся кабинеты: отдела по работе с клиентами, налогового сектора и аудиторов.

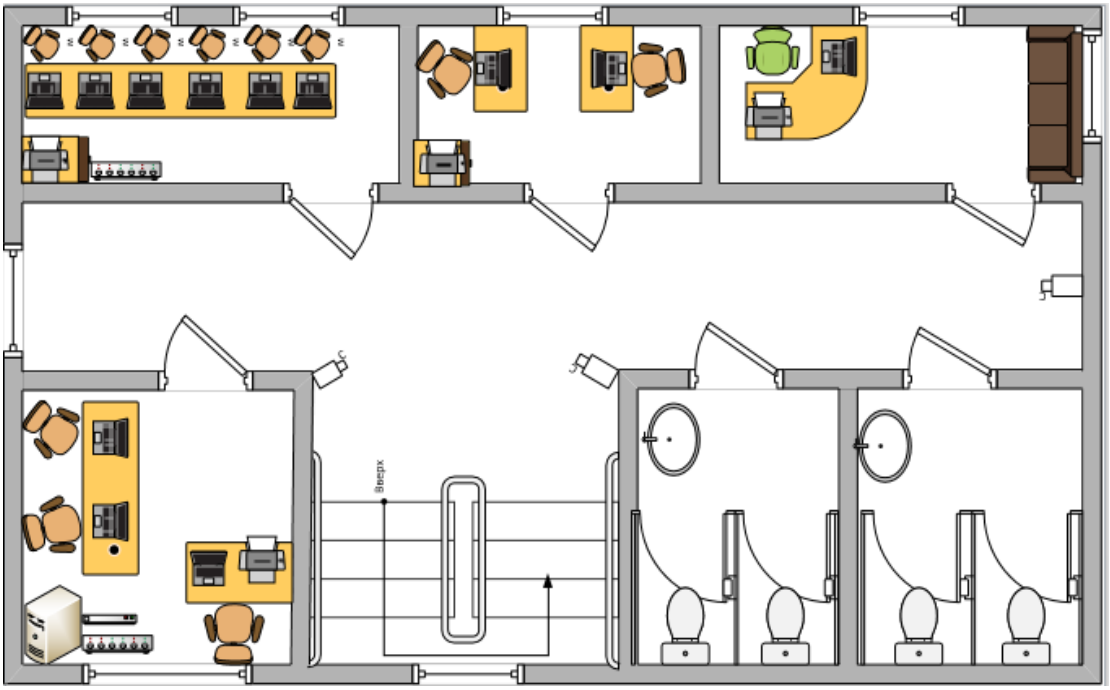


Рисунок 2 - План 2 этажа

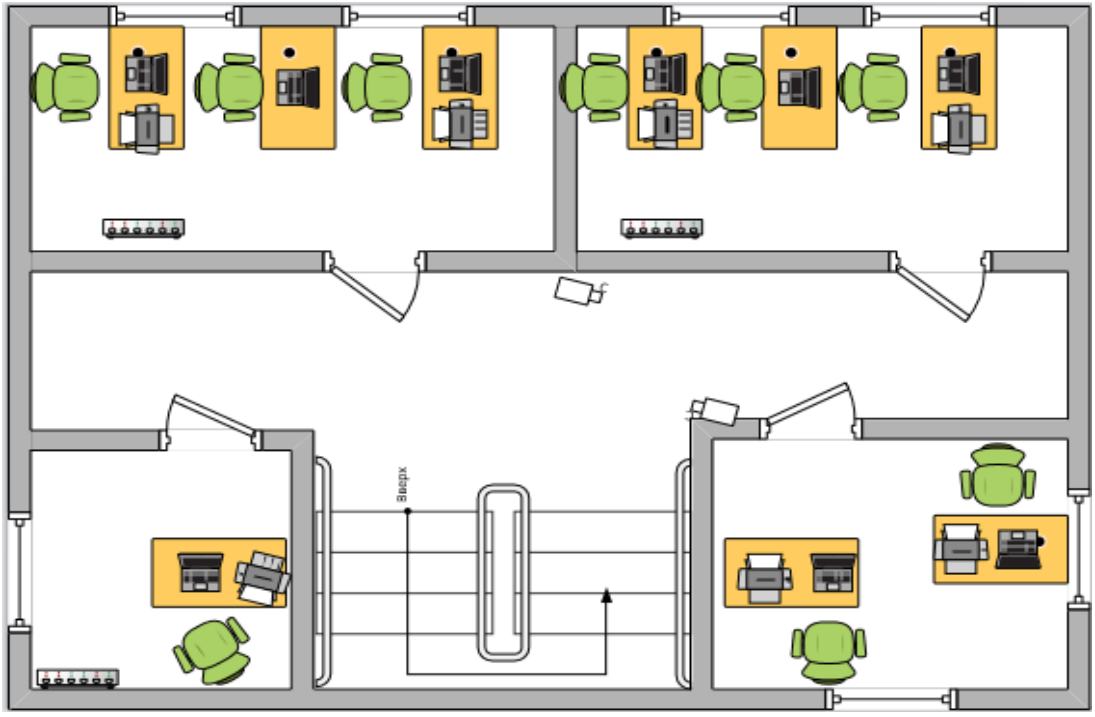


Рисунок 3 - План 3 этажа

1.2 Контроль и управление доступом

Многие компании акцентируют внимание на информационной безопасности, но часто пренебрегают обеспечением необходимого уровня физической безопасности. Информационная безопасность это и есть понятие комплексное, и эффективную информационную безопасность почти невозможно реализовать без надежной физической защиты. Физическая безопасность - это меры, которые входят в состав обеспечения комплексной безопасности и направленные на создание системы защиты организации, активов и персонала от внешних угроз и злонамеренных действий физических лиц. Это технические средства охраны предприятия, сотрудники, обеспечивающие безопасность организации, действующая режимная (пропускная) система охраны организации.

Обычно предприятия используют системы для контроля и управления доступом для организации физической защиты. Эта технология может быть реализована с помощью различных способов. Часто применяемый способ - бесконтактные карты (смарт-карты). При использовании бесконтактных карт сотрудник, для получения доступа на территорию или в какое-либо помещение на предприятии использует ее для идентификации, и на основании сверки идентификатора, вшитого в нее, система проводит сравнение с эталоном, хранящимся в ее базе идентификаторов. На основе анализа выдает разрешение или запрещение на доступ. Системы СКУД имеют недостатки. Например, идентификационная карта может быть потеряна сотрудниками или они могут быть переданы другим людям. При утере смарт карт специалисты службы безопасности должны заблокировать ее и перевыпустить новую в замену ее, но в случае если она передана в чужие руки, то здесь возникают осложнения. Так как идентифицировать владельца карты может только человек. На пропускном пункте в системе должна отобразиться фотография владельца смарт-карты, когда тот проходит через систему контроля.

СКУД повышает уровень физической безопасности имущества охраняемого объекта. Программное обеспечение для управления доступом к дверям является неотъемлемой частью нашей системы контроля доступа. Это позволяет нам управлять дверными считывателями в нашей организации, а затем вводить и управлять всеми людьми, которые будут использовать двери.

Большая часть доступного программного обеспечения для управления доступом обеспечивает простое управление дверным считывателем. Мы можем контролировать, кто, когда и куда могут входить, либо выходить. Дополнительные функции позволяют определить, кто находится в здании, управлять системой с помощью мобильного устройства, заблокировать здание в чрезвычайной ситуации и многие другие функции [1].

Кто может войти в дверь, устанавливается, когда человеку присваиваются учетные данные и вводятся в систему управления. Учетный номер вводится вручную или путем считывания карты. В это время вводится имя человека, его уровень привилегий, возможно, его фотография и другая информация.

В ТОО «ТрастФинАудит» службы безопасности находится на первом этаже следит за камерами видео наблюдения и фиксирует кто, когда заходил и выходил. Это не обеспечивает надежную безопасность информации внутри организации.

Сотрудники организации, чтобы войти в свой кабинет берут ключи от дверей у службы безопасности, то есть это также не обеспечивает достаточный уровень безопасности.

1.3 Средства защиты и администрирование

Существуют основные три аспекта информационной безопасности:

- конфиденциальность;
- целостность;
- доступность.

Обеспечение защиты данных от несанкционированного доступа начинается с момента попытки входа в систему. Операционная система должна проверить пользователя, входящего в систему, в том, что он имеет разрешение главного системного администратора инфраструктуры для входа в нее. Важным средством защиты данных являются функции аудита операционной системы, фиксирующего все происходящие события в системе, влияющие на ее безопасность. При этом администратор операционной системы определяет необходимый перечень событий для отслеживания.

Функции администрирования тесно взаимосвязаны с функциональностью защиты операционной системы, так как системный администратор инфраструктуры раздает права доступа пользователям при их обращении к различным ресурсам системы: либо файлам, либо каталогам, либо другим устройствам и т.д. Также, администратор для ограничения полномочий пользователей локальной сети в совершении каких-либо системных действий применяет функции групповых политик. Например, такие как запрещение смены даты, запрещение завершения работы какого-либо процесса, запрещение изменения прав доступа к различным ресурсам и т.п. Кроме того системный администратор может также ограничить функциональность пользовательского интерфейса, например, удалить из меню операционной системы, отображаемые на мониторе пользователя какие-либо пункты.

Безопасность информационной системы заключается в обеспечении конфиденциальности, целостности и доступности информации, т.е. защиту информации от несакционнированного доступа, модификации, удаления, подмены и т.д.

На предприятии ТОО «ТрастФинАудит», системные администраторы удаленно подключаются используя ПО AnyDesk, чтобы настроить ПК пользователей. Это не совсем удобно и правильно. Для обеспечения определенного уровня защиты необходимо использовать службу каталогов Active Directory. Если внедрить эту систему, то можно предотвратить некоторые

угрозы на информационную инфраструктуру и централизованно управлять всеми компьютерами дистанционно. В Active Directory, чтобы подключиться к контроллеру домена используется протокол Kerberos. Контроллер домена решает разрешить или запретить доступ к активным ресурсам предприятия, авторизуя и аутентифицируя конечных пользователей.

Сервера организации находятся в облаке и на физическом сервере, то есть к серверу есть постоянный доступ. Пароли для входа на удаленный рабочий стол выдает системный администратор. Также ведется корпоративная почта от yandex, в которую системный администратор добавляет пользователей.

Также каждый пользователь может использовать средство шифрования BitLocker, который внедрен в каждую операционную систему. Использую ее можно шифровать жесткие диски, если в нем будут хранится секретные данные.

Средства и методы защиты, используемые в ТОО «ТрастФинАудит»:

- **регулярное резервное копирование –** это процедура постоянного сохранения данных на какой-либо носитель информации либо отдельный резервный сервер, в случае сбоя или повреждения системы для полного ее восстановления.

- **антивирусное ПО.** На предприятии используются антивирусы от компании Kaspersky Internet Security. Они имеют большую актуальную базу вирусных сигнатур и защищают от вредоносных программ на высшем уровне;

- **брандмауэр (МЭ).** На предприятии ТОО «ТрастФинАудит» используется внешняя служба file2ban, но стоит минимальная безопасность, то есть весь пакет разрешен из внутренней сети в сеть интернет и обратно. Нужна конфигурация сети таким образом, чтобы с внешней сети не было возможностей входа в локальную сеть предприятия;

- **резервные ИБП** являются самыми простыми и доступными. На предприятии используются достаточно высокотехнологичные ИБП;

- **камеры видеонаблюдения**. На предприятии используются IP камеры HiWatch. Особенностью таких систем видеонаблюдения является передача видеопотока в цифровом формате по сети Ethernet, использующей межсетевой протокол или IP, отсюда и название. Система видеонаблюдения состоит из сетевых устройств, каждое из которых имеет в сети свой IP-адрес и уникальный MAC-адрес;

- **пропускной пункт**. Именно для оптимизации и повышения эффективности безопасности на предприятии оборудуются пропускные пункты. Основное требование к ПП, она должна обеспечивать необходимую пропускная способность, кроме того эффективность и тщательность проверки документов, досмотра всех видов транспорта;

- **Proxy servers.** Обращения из локальной сети в глобальную сеть осуществляются посредством специальных серверов. Однако этот способ не дает 100% защиты против серьезных угроз.

Обнаруженные уязвимости в защите предприятия:

- многие продукты содержат настройки по умолчанию;

- при входе в систему используются пароли по умолчанию;
- плохо защищенный сервер АТС;
- не используется службы каталогов Active Directory;
- нет физической безопасности к рабочим станциям;
- пользователи используют windows 7 (не поддерживается с 2020 г.).

2 Обеспечение безопасности сети предприятия

2.1 Обеспечение защиты КС и разграничение доступа к ней

Система управления доступом может использоваться для управления и мониторинга разрешений доступа пользователей и прав доступа к файлам, системам и службам, чтобы помочь защитить организации от потери данных и нарушений безопасности.

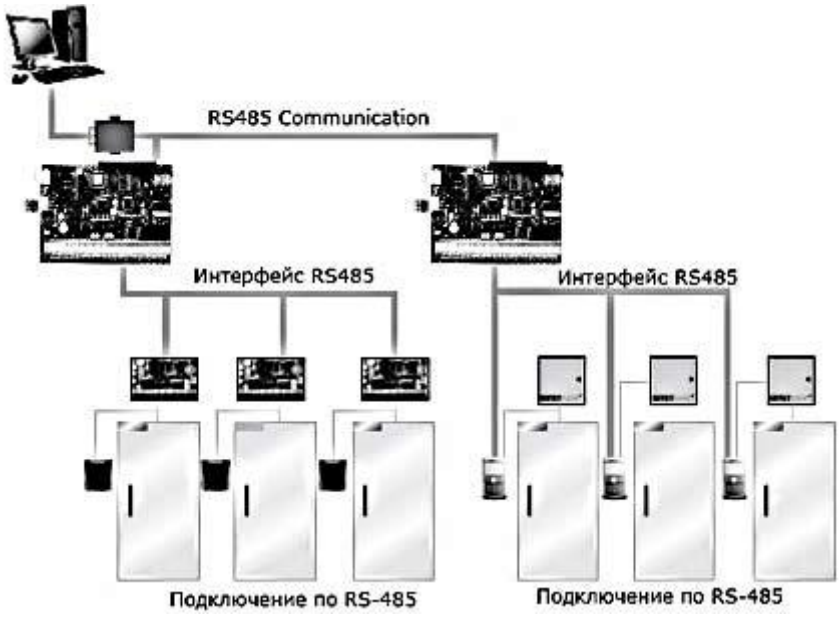


Рисунок 4 - Системы контроля доступа и учета рабочего времени

Системы управления доступом имеют решающее значение, поскольку они помогают повысить безопасность данных организации. Автоматизированное программное обеспечение помогает обеспечить пользователям правильные уровни разрешений и доступ только к тем ресурсам, которые им нужны.

Чтобы потенциальные злоумышленники не могли проникнуть в сеть, необходимо наличие комплексных политик контроля доступа как для пользователей, так и для устройств. Контроль доступа к сети (NAC) может быть установлен на самом детальном уровне. Например, можем предоставить администраторам полный доступ к сети, но запретить доступ к определенным конфиденциальным папкам или запретить их личным устройствам подключаться к сети.

На самом базовом уровне контроля доступа - это средство контроля затем кто, как и когда входит на территорию организации. Мы склонны называть это физическим контролем доступа, чтобы отличать его от контроля доступа, который не позволяет людям входить в виртуальные пространства - например, при входе в компьютерную сеть. И хотя одно из ее основных применений -

повышение безопасности, система контроля физического доступа имеет достоинства. Например, рост результативности бизнес-процессов, управление сайтом, зданием.

Системы обеспечивающие физический контроль доступа, это часто электронные системы безопасности. Они применяют идентификатор, например, карту доступа, для разрешения входа на территорию организации. Так как системы физического контроля фиксируют всех, кто и в какое время обращался, они сохраняют все важную информацию, позволяющую отслеживать, участки к непосредственно к которым имеют доступ сотрудники [1].

Самая доступная форма физического контроля доступа, используемая небольшими организациями - механические ключи. Такой метод контроля доступа используется в ТОО «ТрастФинАудит». По мере укрупнения организации применение механических ключей имеет ряд недостатков. Например, проблемы, возникающие при использовании ключей:

- утеря ключа**.** Если сотрудник теряет свой ключ, то необходимо сменить замок, чтобы удостовериться, что утерянный ключ не может быть использован злоумышленником. Далее нужно передать новые ключи всем сотрудникам, кому нужен доступ к двери;

- механические ключи не оставляют следа. Нет никакой вероятности увидеть, когда кто-то использовал механический ключ, поэтому нельзя узнать, кто и в какое время вошел в дверь;

- ключами непросто распоряжаться. При потребности входа в разные помещения и кабинеты, нужно огромное количество механических ключей, которые не совсем удобно носить с собой и использовать. Может быть такой случай, что трудно запомнить, какой ключ от какой двери, но и пометить их - очень большая угроза безопасности.

Использование KeePass. Нужен пароль для многих веб-сайтов, учетная запись электронной почты, веб-сервер, вход в сеть и т.д. Список бесконечен и кроме того, должны использоваться разные пароли для каждой учетной записи, потому что, если будет использоваться только один пароль везде, и кто-то получит этот пароль, то возникнет проблема: пользователь будет иметь доступ ко всем учетным записям. Менеджер паролей с открытым исходным кодом, KeePass обеспечивает возможность безопасного управления паролями, хранящиеся на компьютере. Все пароли можно хранить в одной базе данных, которая заблокирована одним паролем. Таким образом, нужно запомнить только один главный ключ, чтобы разблокировать всю базу данных. Файлы базы данных шифруются с использованием лучших и наиболее безопасных алгоритмов шифрования, известных в настоящее время (AES-256, ChaCha20 и Twofish).

Усиленный контроль и безопасность. Применяя электронную систему контроля доступа, можно предотвратить многие угрозы.

Данный метод позволяет контролировать:

- **имеющих доступ.** Можно, например, разрешить автоматический доступ только сотрудникам компании. Доступ посетителям разрешен только после регистрации у службы безопасности.

- **имеющих доступ к определенным дверям.** Можно разрешить только определенным сотрудникам входить в определенные зоны. Например, в кабинет IT специалиста могут иметь доступ только технические специалисты или только IT специалист;

- **определенное время, доступа.** Подрядчикам и непривилегированным сотрудникам разрешен доступ только во время их рабочей смены, а привилегированные сотрудники имеют постоянный доступ в здание;

- **условия предоставления доступа.** Например, настройка системы разрешающий доступ подрядчикам только в случае, предоставления ими сертификатов.

Рассмотренный метод обеспечивает строгий контроль, и система, позволяющая устанавливать такие параметры для каждого пользователя считается эффективной системой контроля доступа. Кроме того, она позволяет системе оперативно и свободно обновлять параметры, когда ей потребуется.

Предоставит полную информацию обо всех, получивших доступ, место и время, и в случае инцидента позволяет оперативно определять, все возникшие нарушения.

2.2 Организационно-техническая защита информации

Технические средства защиты информации применяются для разработки физических барьеров на пути к защищаемой информации:

- механические;
- электронно-механические;
- электромеханические;
- оптические;
- акустические;
- радиолокационные;
- другие устройства;
- системы.

Технические средства защиты информации применяются как самостоятельно, так ив комплексе с другими средствами защиты информации [2].

Система охранно-тревожной сигнализации (ОТС) имеет такие функциональные возможности как:

- регистрация помещений для наблюдения и защиты;
- снятие с наблюдения;
- реагирование на несанкционированный доступ или попыток осуществления взлома и проникновение в защищаемые и охраняемые помещения;

- подача звукового сигнала в случае нарушения защитного механизма;

- организация видеонаблюдения за состоянием защищаемых помещений с помощью автоматизированных рабочих мест интегрированной системы безопасности, отражением графически на плане здания, подача сигналов тревоги, либо изображение дефектов на плане здания, либо в формате сообщения, либо в формате голосового сообщения;

- журналирование всех происходящих инцидентов в системе ОТС, сбор информации в базе данных, с возможностью дальнейшего просмотра и анализа событий;

- фиксирование всех действий операторов в различных ситуациях.

Для обеспечения информационной безопасности предприятия руководству организации ТОО «ТрастФинАудит» необходимо разработать концепцию по ИБ, внедрить ее в бизнес-процесс и донести до всех сотрудников компании. Такой документ является базовым, служит для формулирования внутренних правил обеспечения безопасности и системы защитных мер. Политика безопасности разрабатывается совместно с квалицированными экспертами по защите информации, выполняющие аудит как информационной системы, так и всей организационной структуры компании, различных бизнес-процессов, выработать рекомендации по проектированию эффективного комплекса мер по обеспечению защиты информации. Для внедрения DLP-системы, а также других программных средств, решающих задачи по защите инфраструктуры организации, конфиденциальных данных может стать базой концепция безопасности.

Руководство компаний само решает какую информацию следует обеспечить защитой. Такой информацией может быть какие-то базы клиентов, патенты и другая конфиденциальная информация. Кроме этого каждая организация имеет объекты защиты, требующие обеспечения безопасности, гарантирующее защищенность данных от разглашения. В первую очередь сюда относятся автоматизированные информационные системы организации. Целью злоумышленников является обнаружение и организация утечки информации, поэтому объектами наблюдения и атак становятся персональные компьютеры, серверы, каналы коммуникаций, периферийные устройства (принтеры, сканеры и т.п.). Злоумышленники для достижения своих целей разрабатывают алгоритмы, программы, закладки для хищения информации через сеть, либо копирования информации, либо прослушивания. Поэтому все организационные и технические меры в первую очередь нацелены на обеспечение физической защиты системы, а также внедрение программных средств, устраняющие вмешательство в сеть из вне [2].

Вся конфиденциальная информация, которая обрабатывается в ТОО «ТрастФинАудит» может быть классифицирована следующим образом:

- персональные данные, подлежащие защите на основании законодательства РК;

- программные продукты, содержащие в себе как финансовую, так и стратегическую информацию;

- базы документооборота;

- данные внутренней переписки организации, в том числе архивы корпоративной почты;

- конфиденциальная информация производстве и его документы;

- финансовая и аналитическая информация, подготавливаемая по указанию руководства предприятия.

Организационные меры. Эти меры включают:

- тщательный подбор сотрудников на ответственные должности;

- проведение аудита по защите информации от различных атак (соц. инженерия, фишинг и т.д.);

- определение уровня доступа к содержащей коммерческую тайну информации;

- установку пропускной системы для сотрудников и выдать им электронные средства идентификации;

- техническая защита помещений и оборудования, сертификация классов защиты, проверка соответствия нормативно-правовым требованиям.

Технические меры. Эти меры включают:

- использование только лицензированного ПО;

- фиксирование всех действий пользователей в системах, работающих с файлами, содержащих конфиденциальную информацию, а также случаев с НСД;

- использование эшелонированной обороны, в которой для каждого возможного канала утечки предусмотрено несколько барьеров системы защиты, осложняющий хакеру выполнения несанкционированного действия.

Для реализации таких принципов обеспечения ИБ решаются задачи по привлечению дополнительных средств защиты информации, к которым можно отнести:

- криптографические средства защиты (VPN), обеспечивающих шифрование передаваемой по каналам связи информации как на рабочих станциях, так и на серверах;

- антивирусы;

- DLP - системы, гарантирующие защиту от утечки информации, а также перехвата исходящего трафика по возможным каналам утечки;

- SIEM - системы собирают данные из нескольких систем и анализируют эти данные, чтобы выявить аномальное поведение или потенциальные кибератаки.

- IDS - это система мониторинга, которая обнаруживает подозрительные действия и генерирует предупреждения при их обнаружении.

- IPS - системы контролируют вашу сеть, выявляя возможные вредоносные инциденты и собирая информацию о них.

Уязвимости и слабые стороны. При осмотре инфраструктуры организации выявлены**:**

- окна не обеспечены защитой от визуального наблюдения (жалюзи, шторы и т.д.);

- отсутствуют датчики и охранная сигнализация;

- слабо подготовленные сотрудники по вопросам обеспечения защиты от атак (на случай хакерской атаки);

- нет контроля наружной части здания.

DLP. Данные могут попасть в чужие руки, независимо от того, отправлены ли они по электронной почте или в мгновенных сообщениях, через формы веб-сайтов, при передаче файлов или другими способами. Стратегии DLP должны включать решения, которые отслеживают, обнаруживают и блокируют несанкционированный поток информации. [3]

Организации используют DLP для защиты своих данных и соблюдения нормативных требований.

Организации обычно используют DLP для:

- защиты личной информации и соблюдение соответствующих правил;

- защиты интеллектуальной собственности, критически важной для организации;

- обеспечение прозрачности данных в крупных организациях;

- обеспечение безопасности в средах с собственным устройством (BYOD);

- защиты данных в удаленных облачных системах.

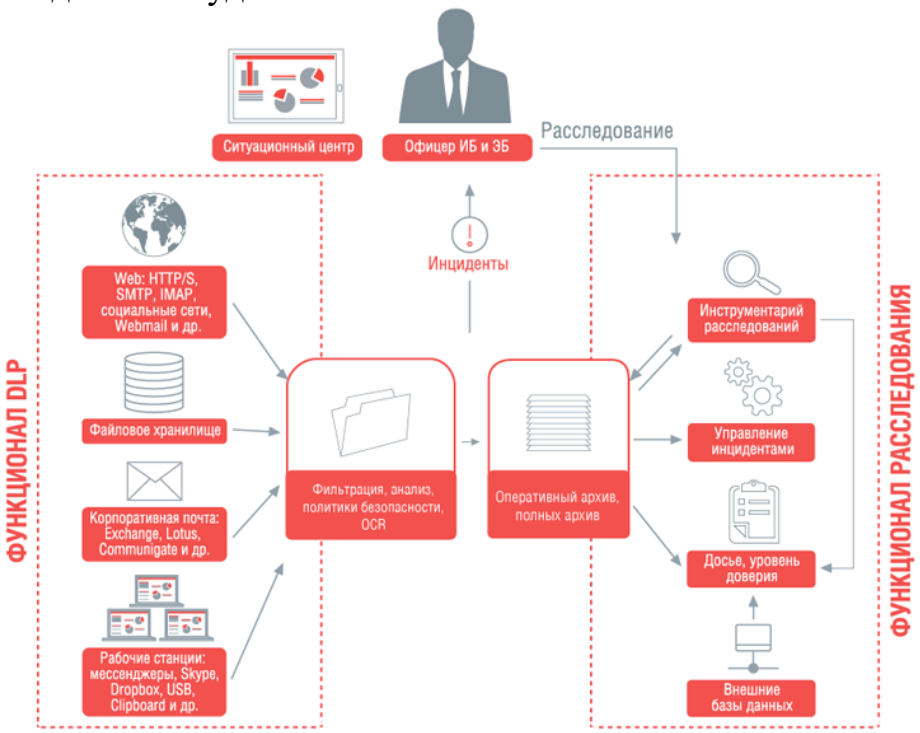


Рисунок 5 - Функционал DLP систем

Системы предотвращения вторжений. Технологии IPS могут обнаруживать или предотвращать атаки сетевой безопасности, такие как атаки методом грубой силы, атаки типа «отказ в обслуживании» (DoS) и эксплойты уязвимостей. Уязвимость - это слабое место в программной системе, а эксплойт - это атака, которая использует эту уязвимость для получения контроля над системой. Когда объявляется эксплойт, у злоумышленников

часто появляется возможность воспользоваться этой уязвимостью до того, как будет применено исправление безопасности. В этих случаях можно использовать систему предотвращения вторжений, чтобы быстро заблокировать эти атаки.

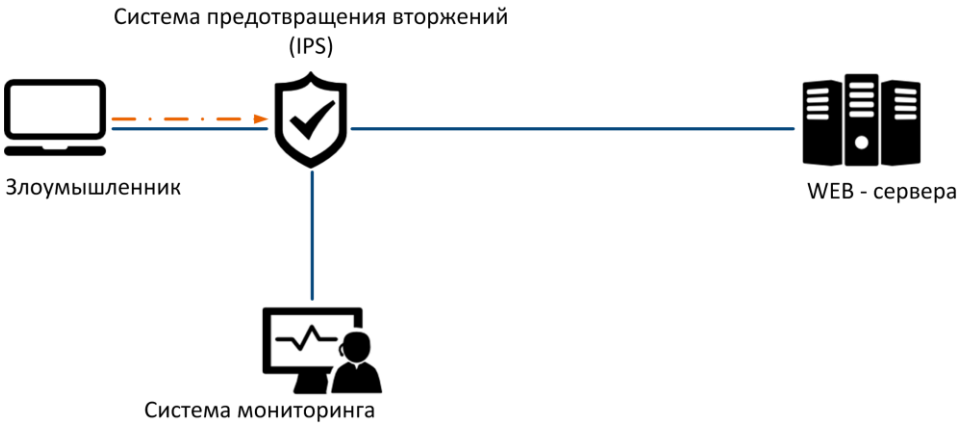


Рисунок 6 - Как располагается система IPS

Управление событиями и данными об информационной безопасности. Управление информацией и событиями безопасности (SIEM) - это программное решение, которое объединяет и анализирует активность множества различных ресурсов по всей вашей ИТ-инфраструктуре.

SIEM собирает данные о безопасности с сетевых устройств, серверов, контроллеров домена и т.д. SIEM хранит, нормализует, агрегирует и применяет аналитику к этим данным, чтобы обнаруживать тенденции, обнаруживать угрозы и позволять организациям исследовать любые предупреждения. [4]

Рисунок 7 - Сбор информации

SIEM предоставляет две основные возможности группе реагирования на инциденты:

- отчетность и криминалистическая экспертиза инцидентов безопасности;

- оповещения на основе аналитики, соответствующие определенному набору правил, указывающие на проблему безопасности.

2.3 Разработка VLSM для сети

Технология VLSM применяется с целью экономии IP адресов. VLSM позволяет администраторам сети разделить пространство IP-адресов на подсети разного размера, в отличие от простого разделения подсетей одинакового размера. VLSM в некотором смысле означает разбиение подсети на несколько подсетей. Для упрощения, VLSM - это разбиение IP-адресов на подсети и их распределение в соответствии с индивидуальными потребностями в сети. Это также можно назвать бесклассовой IP-адресацией. Классовая адресация следует общему правилу, которое, как было доказано, приводит к потере IP-адреса. [5]

Для эффективного использования технологии VLSM необходимо планировать адреса.

В предприятии ТОО «ТрастФинАудит» используется сетевой адрес 192.168.100.0/24.

Таблица 1 – VLSM для сети

Название подсети	Необходимое количество узлов	Сетевой адрес	Маск	Адрес перво узла	Широковещательный адрес
Налоговый сектор	22	192.168.100.0	/27	192.168.100.1	192.168.100.31
Аудиторы	22	192.168.100.32	/27	192.168.100.33	192.168.100.63
Отдел по рабо с клиентами	17	192.168.100.64	/27	192.168.100.65	192.168.100.95
Сектор бух уче	17	192.168.100.96	/27	192.168.100.97	192.168.100.127
Бухгалтерия	6	192.168.100.128	/29	192.168.100.12	192.168.100.135
IT специалисть	6	192.168.100.136	/29	192.168.100.13	192.168.100.143
Отдел кадров	6	192.168.100.144	/29	192.168.100.14	192.168.100.151
Дирекция	5	192.168.100.152	/29	192.168.100.15	192.168.100.159
Касса и служ безопасности	5	192.168.100.160	/29	192.168.100.16	192.168.100.167

С помощью программного обеспечения GNS3 спроектирован план прокладки кабелей и расположение всех промежуточных и оконечных устройств сети предприятия (рис. 5).

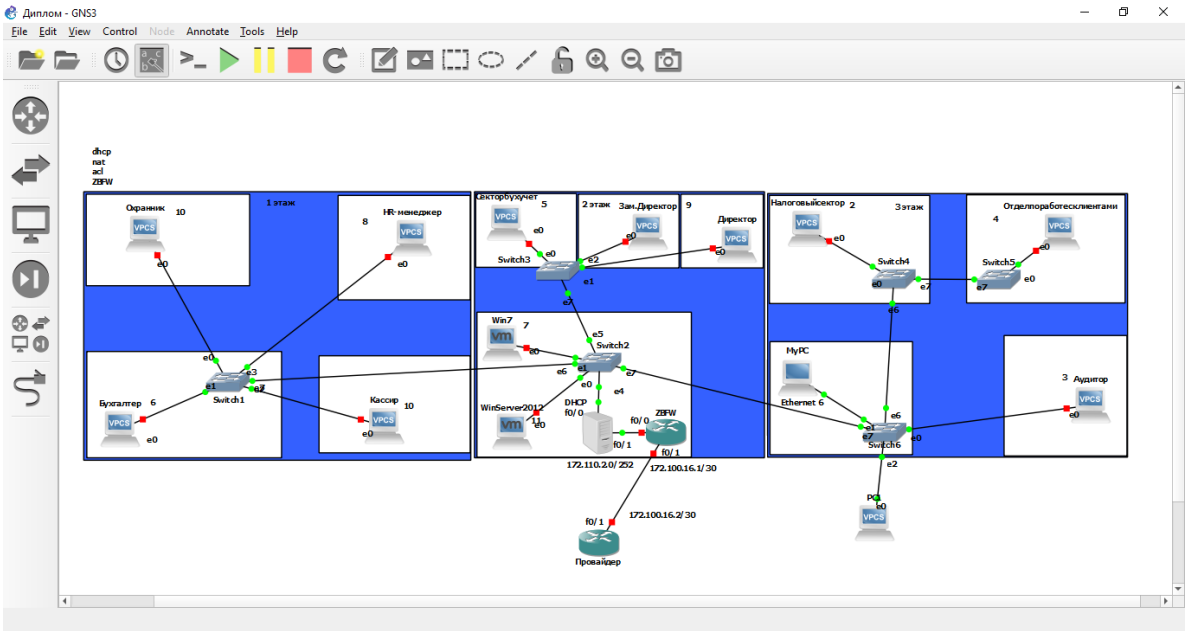


Рисунок 8 - План расположение устройств

Топология и VLSM обеспечивает решение задач:
- эффективное использование адресного пространства;
- централизованное управление;
- защищенность сети;
- простота модификации сети;
- использование SPAN/RSPAN;
- фильтрация по MAC адресам;

2.4 Внедрение Zone-Based FireWall и использование Access Control List

Межсетевые экраны позволяют предотвращать множество атак злоумышленников. Компания Forrester, одна из крупнейших аналитических компаний мира, в своем последнем отчете «Forrester Wave: Enterprise Firewalls, Q3 2020» назвала Cisco лидером на рынке корпоративных межсетевых экранов, обойдя такие бренды, как Check Point, Fortinet и ряд других. Межсетевые экраны Cisco обеспечивают средствами управления безопасностью мирового класса повсюду с постоянной прозрачностью, гармонизацией политик и унифицированным управлением. Защита сетей в настоящее время от изощренных угроз требует применение лучших в отрасли аналитических данных и последовательной защиты повсюду. По мере того, как сети становятся все более взаимосвязанными, становится трудно добиться полной видимости угроз и последовательного управления политиками. Добиться управления безопасностью и получения прозрачности в распределенных и гибридных сетях можно с помощью межсетевого экрана, разработанного компанией Cisco.

В том случае если организация, не имеет возможность применения аппаратного брандмауэра, используют альтернативный вариант, то есть

брандмауэр на роутере Cisco IOS с функцией CBAC или брандмауэра на основе зон. CBAC является предшественником брандмауэра на основе зон.

Zone-Based FW - эффективный брандмауэр на маршрутизаторах Cisco с отслеживанием состояния. Межсетевой экран поддерживает базу данных с отслеживанием состояния, содержащей полную информацию как IP-адрес источника, IP-адрес назначения, номера портов источника и назначения. Если трафик генерируется изнутри сети, то разрешены только ответы внутреннего трафика сети.

Существует два варианта реализации межсетевой экран из маршрутизатора Cisco IOS:

- используя CBAC. При этом создается список доступа, применяемый в дальнейшем к интерфейсам роутера. Необходимо также сохранить в настройках разрешенный или запрещенный трафики и их направление. Это может привести к дополнительным расходам для администратора;

- применение брандмауэра на основе зон.

Зона – область, охватывающая все сетевые устройства с одним и тем же уровнем доверия. Каждой зоне назначается интерфейс. По умолчанию трафики между зонами запрещены [6].

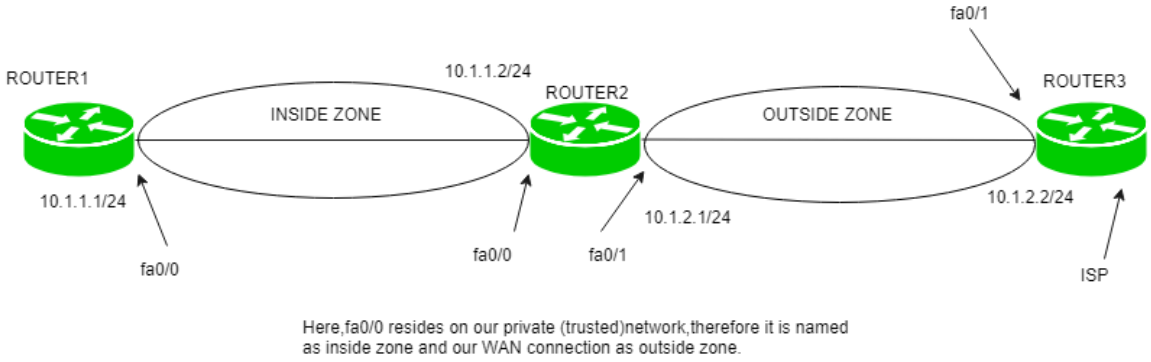


Рисунок 9 - Внутренние и внешние зоны

По мере того как угрозы и сети становятся все более сложными, крайне важно иметь правильные инструменты для защиты данных, приложений и сетей. Устройства Cisco ASA серии 5585-X обладают мощностью и гибкостью, которые необходимы, чтобы быть на шаг впереди угроз. Они предлагают резкое трехкратное повышение производительности по сравнению с устройствами предыдущего поколения в дополнение к уникальным аппаратным возможностям для проверки зашифрованного трафика в масштабе. [7]

Межсетевые экраны Cisco могут быть интегрированы с другими защитными технологиями – предотвращением вторжением, контролем сетевого доступа, многофакторной аутентификацией, анализом сетевых аномалий, мониторингом DNS, анализом уязвимостей, реагированием на инциденты и т.п. Именно эта бесшовная интеграция защитных технологий, которая поддерживается сквозной политикой безопасности, позволяет заказчикам эффективно интегрироваться в существующую инфраструктуру, обеспечить полную видимость всех приложений и сервисов, реализовать различные виды

сегментации и микро-сегментации, что повышает защищенность активов от широкого спектра угроз и нарушений информационной безопасности. [8]

Межсетевые экраны Cisco ASA серии 5585-X – динамический межсетевой экран, оснащенный набором сервисов межсетевого экранирования. Такой экран хорошо подходит для разного размера сети – как для организаций малого и среднего бизнеса, которые могут физически размещаться на одном или нескольких объектах, так для больших предприятий, операторов связи и в особо крупных важных ЦОД. Cisco ASA 5585-X обеспечивают хорошую производительность и функциональные возможности гибкости сервисов, масштабируемостью, расширенным функционалом, с небольшими затратами на развертывание и эксплуатацию [7].

Cisco ASA 5585-X - межсетевые экраны, разработанные для использования в маленьких организациях. Такие экраны защищают клиентские устройства:

- прозрачность действий в сети, их контролируемость, безопасное использование новых приложений и устройств;
- обеспечение контроля поведения микро-приложений посредством Cisco AVC;
- в зависимости от репутации сайтов, ограничивают работу веб-приложений, с помощью Cisco Web Security Essentials (WSE);
- с помощью комплекса облачных и программных услуг гарантируют многоуровневую сетевую безопасность с помощью Cisco Security Intelligence Operations (SIO);
- с помощью Cisco Global Correlation реализуется высокоэффективная система предотвращения вторжений (IPS);
- высокая производительность VPN и постоянный удаленный защищенный доступ;
- дополнительные виды услуг безопасности.

Список управления доступом (ACL) содержит правила, которые разрешают или запрещают доступ к определенным цифровым средам. Есть два типа ACL:

- списки управления доступом к файловой системе − фильтруют доступ к файлам и/или каталогам. Списки управления доступом к файловой системе сообщают операционным системам, какие пользователи могут получить доступ к системе и какие привилегии им предоставлены;
- сетевые списки ACL − фильтруют доступ к сети. Сетевые ACL сообщают маршрутизаторам и коммутаторам, какой тип трафика может получить доступ к сети и какая активность разрешена.

Причины использования ACL:

- управление транспортным потоком;
- ограниченный сетевой трафик для повышения производительности сети;
- уровень безопасности для доступа к сети, определяющий, какие области сервера/сети/службы могут быть доступны пользователю, а какие – нет;
- детальный мониторинг трафика, уходящего и входящего в систему.

Основная цель использования ACL - обеспечить безопасность сети. Без него любому трафику разрешено входить или выходить, что делает его более уязвимым для нежелательного и опасного трафика.

ACL файловой системы - это таблица, информирующая компьютерную операционную систему о правах доступа пользователя к системному объекту, включая отдельный файл или файловый каталог. Каждый объект имеет свойство безопасности, которое связывает его со списком управления доступом. В списке есть запись для каждого пользователя с правами доступа к системе.

Типичные привилегии включают право читать один файл (или все файлы) в каталоге, выполнять файл или записывать в файл или файлы.

Когда пользователь запрашивает объект в модели безопасности на основе ACL, операционная система изучает ACL для соответствующей записи и определяет, допустима ли запрошенная операция.

Сетевые ACL устанавливаются в маршрутизаторы или коммутаторы, где они действуют как фильтры трафика. Каждый сетевой ACL содержит предопределенные правила, определяющие, каким пакетам или обновлениям маршрутизации разрешен или запрещен доступ к сети.

Маршрутизаторы и коммутаторы с ACL работают как фильтры пакетов, которые передают или отклоняют пакеты на основе критериев фильтрации. Как устройство уровня 3, маршрутизатор с фильтрацией пакетов использует правила, чтобы определить, следует ли разрешить или запретить доступ для трафика. Он решает это на основе IP адресов источника и назначения, порта назначения и порта источника

Списки контроля доступа можно рассматривать в отношении двух основных категорий:

- стандартный ACL;
- расширенный ACL.

Стандартный ACL. Список доступа, который создается исключительно с использованием исходного IP адреса. Эти списки контроля доступа разрешают или блокируют весь набор протоколов. Они не различают IP трафик, такой как UDP, TCP и HTTPS.

Расширенный ACL. Список доступа, который широко используется, поскольку он может различать IP трафик. Он использует как исходный, так и целевые IP адреса и номера портов, чтобы понять IP трафик. Можно указать, какой IP трафик должен быть разрешен или запрещен.

2.5 Сеть VPN

Виртуальная частная сеть или VPN - это зашифрованное соединение через Интернет от устройства к сети. Зашифрованное соединение помогает обеспечить безопасную передачу конфиденциальных данных. Это предотвращает перехват трафика посторонними лицами и позволяет

пользователю выполнять работу удаленно. Технология VPN широко используется в корпоративных средах. Работа в Интернете или операции в незащищенной сети Wi-Fi означает, что может быть раскрыта личная информация и привычки просмотра. Вот почему виртуальная частная сеть, более известная как VPN, должна быть обязательной для всех, кто обеспокоен своей онлайн-безопасностью и конфиденциальностью.

VPN, предоставляющие функции шифрования информации и анонимности, позволяют защищать любую активность в глобальной сети: электронная переписка, осуществление бесконтактных покупок в интернет-магазинах, оплата счетов через мобильные приложения. VPN обеспечивают скрытность пользователя в сетях интернета при просмотре различных сайтов.

По сути, виртуальные частные сети создают туннель данных между локальной сетью и выходным узлом в другом месте, которое может находиться за тысячи миль, создавая впечатление, что вы находитесь в другом месте. Это преимущество дает свободу в Интернете или возможность доступа к любимым приложениям и веб-сайтам в пути.

Вот более подробный взгляд на то, как работает виртуальная частная сеть. VPN используют криптографию для шифрования данных, когда они отправляются по сети интернет. Шифрование делает данные нечитаемыми. Безопасность данных особенно важна при использовании общедоступной сети Wi-Fi, поскольку она предотвращает перехват вашей активности в Интернете кем-либо еще в сети.

Существует два основных типов VPN:

- Remote Access VPN;
- Site to site.

Remote Access VPN: VPN с удаленным доступом надежно подключает устройства за пределами корпоративного офиса. Эти устройства называются конечными точками и могут быть ноутбуками, планшетами или смартфонами.

Site to site: VPN типа «сеть-сеть» соединяет корпоративный офис с филиалами через Интернет. VPN типа «сеть-сеть» используются, когда расстояние делает непрактичным прямое сетевое соединение между этими офисами. Выделенное оборудование используется для установления и поддержания соединения.

NordVPN ведущий мировой поставщик услуг VPN, развертывает NordLynx, новую технологию, основанную на протоколе WireGuard, который считается отраслевым стандартом будущего. NordLynx - это наиболее значительное технологическое усовершенствование. Это быстродействующий протокол VPN нового поколения. По результатам ряда тестов NordLynx стабильно превосходит в комбинациях, в которых тесты были убедительными. Когда пользователь подключается к ближайшему VPN-серверу и загружает контент, который обслуживается из сети доставки контента (CDN) в пределах нескольких тысяч миль, он может рассчитывать на увеличение скорости в два раза. NordLynx основан на протоколе WireGuard, который использует современную криптографию. Это быстродействующий протокол VPN, по

сравнению с такими протоколами как OpenVPN и IPSec. Основной целью усовершенствования NordVPN и разработки новой технологии NordLynx является частые критики в его адрес. NordLynx высокскоростной WireGuard с настраиваемой системой преобразования сетевых адресов (NAT) NordVPN обеспечивает защиту конфиденциальности пользователей. Система двойного NAT NordVPN позволяет обеспечить безопасное VPN-соединение без афиширования каких-либо идентификационных данных на сервере. Только на время активного сеанса динамические локальные IP-адреса остаются предопределенными. А сама аутентификация пользователя реализуется посредством внешней хорошо защищенной базы данных.

3 Проектирование сети на ПО GNS3

Настройка DHCP. На рисунке можно увидеть, процесс создания DHCP пулов, которые будут раздавать IP адреса (рис. 7) [10].

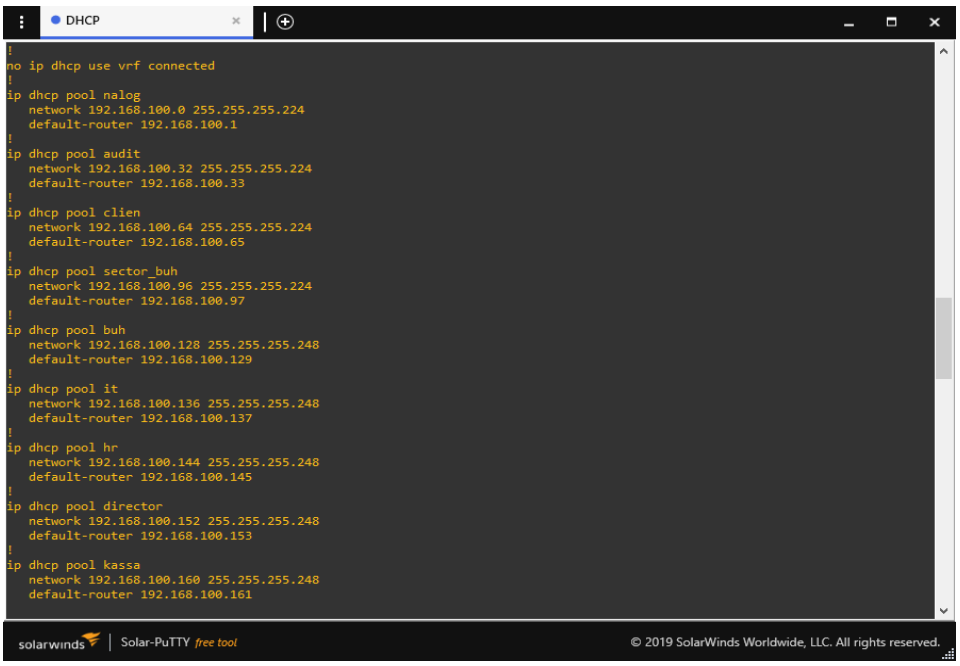


Рисунок 10 - Dhcp пул

Создание sub интерфейсов и перенаправление на DHCP сервер, чтобы получить IP адреса. Также прописанные на каждом sub интерфейсе NAT (рис.8).

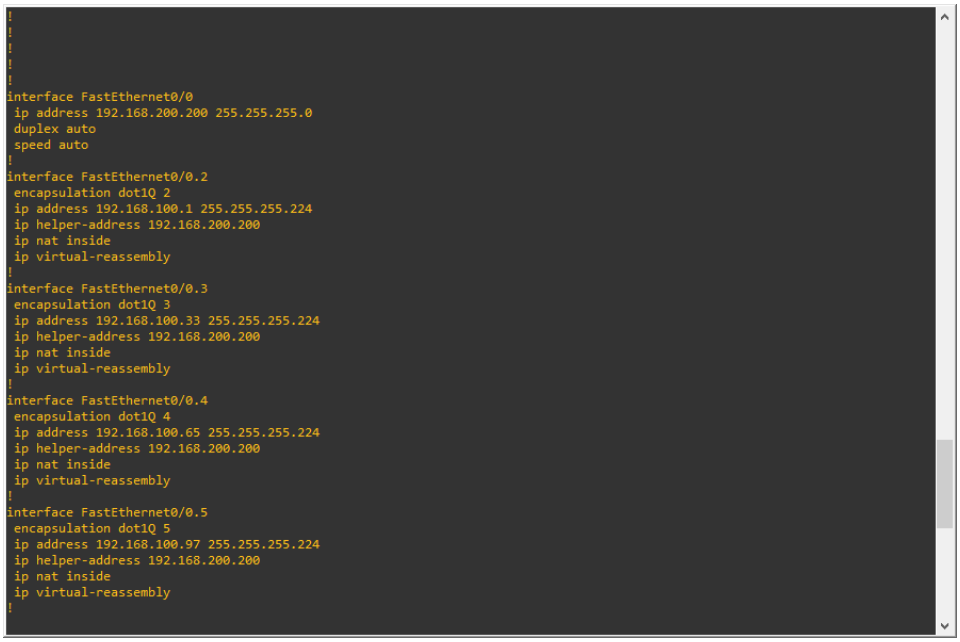


Рисунок 11 - Настройка sub интерфейсов и использование NAT

Определение inside nat и outside nat на интерфейсах и создание ACL, чтобы серые IP адреса могли выходить во внешнюю сеть используя белый IP адрес (рис. 9).

Рисунок 12 - Использование ACL

Настройка Zone-Based FireWall. Определение в class-map какие протоколы инспектировать. Создание policy-map, чтобы маркировать пакеты в соответствии с тем классом обслуживания, к которому принадлежит пакет. Определение внешней и внутренней зон.

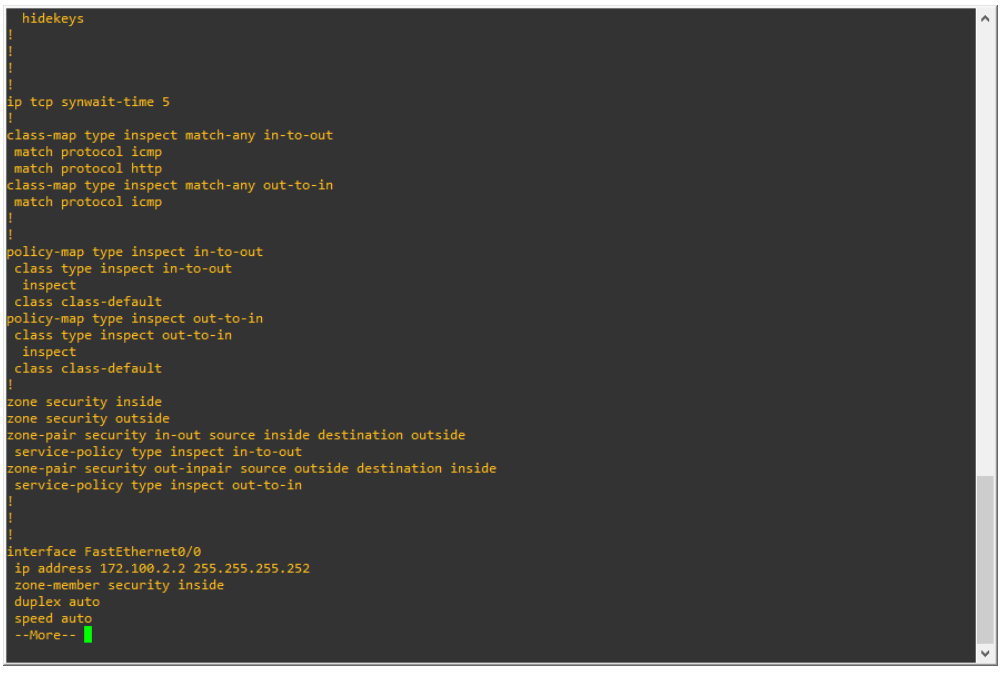


Рисунок 13 - Настройка ZBFW

Рисунок 14 - Определение внешних и внутренних зон

Прописывание на роутере провайдера маршрута по умолчанию в локальную сеть предприятия и проверка связи. Как видно на рисунке 12 связи нет, потому что стоит защита на уровне ZBFW и ACL который блокирует любой трафик из внешней сети.

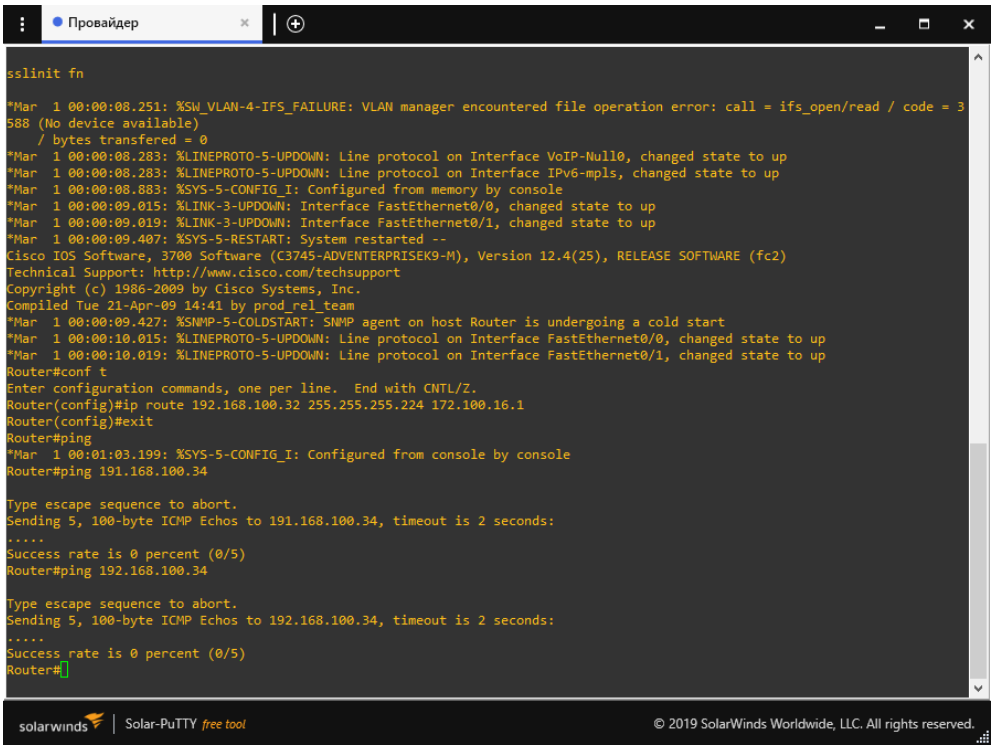


Рисунок 15 - Попытка ping запроса в локальную сеть прописывая маршрут по умолчанию

На рисунке 13 можно проверить, что ПК пользователя получил IP адрес от DHCP сервера.

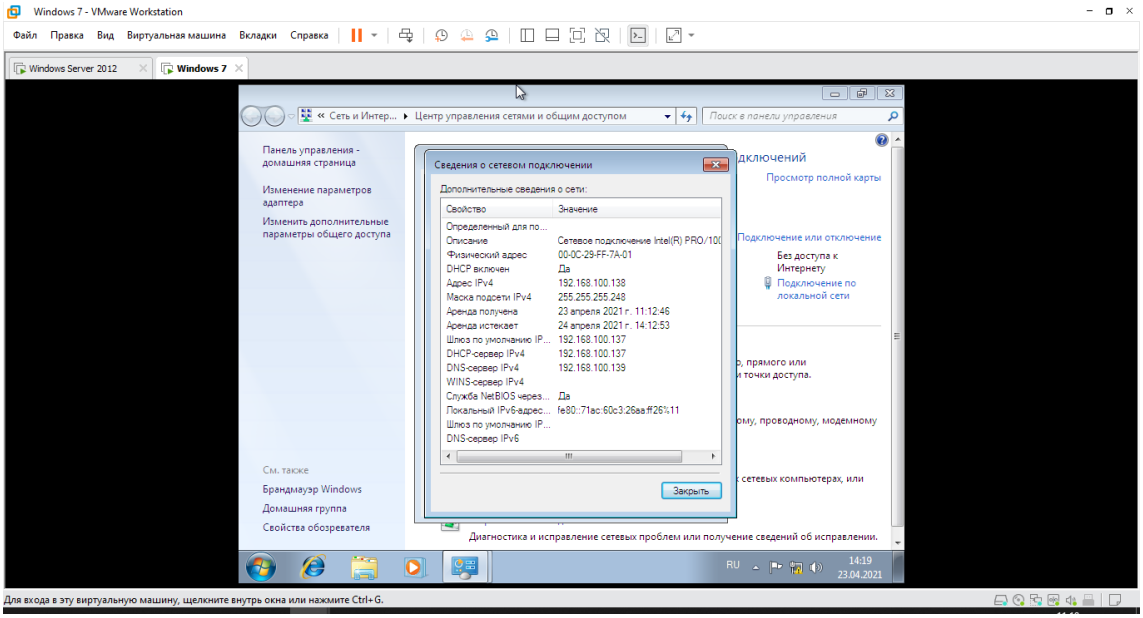


Рисунок 16 - Сведение сетевого интерфейса win 7

Далее введение Windows 7 в домен, который был создан на Windows Server 2012 R2. Пользователь был создан на сервере и вход был выполнен из учетной записи abylai. Результат ниже на рисунке 14.

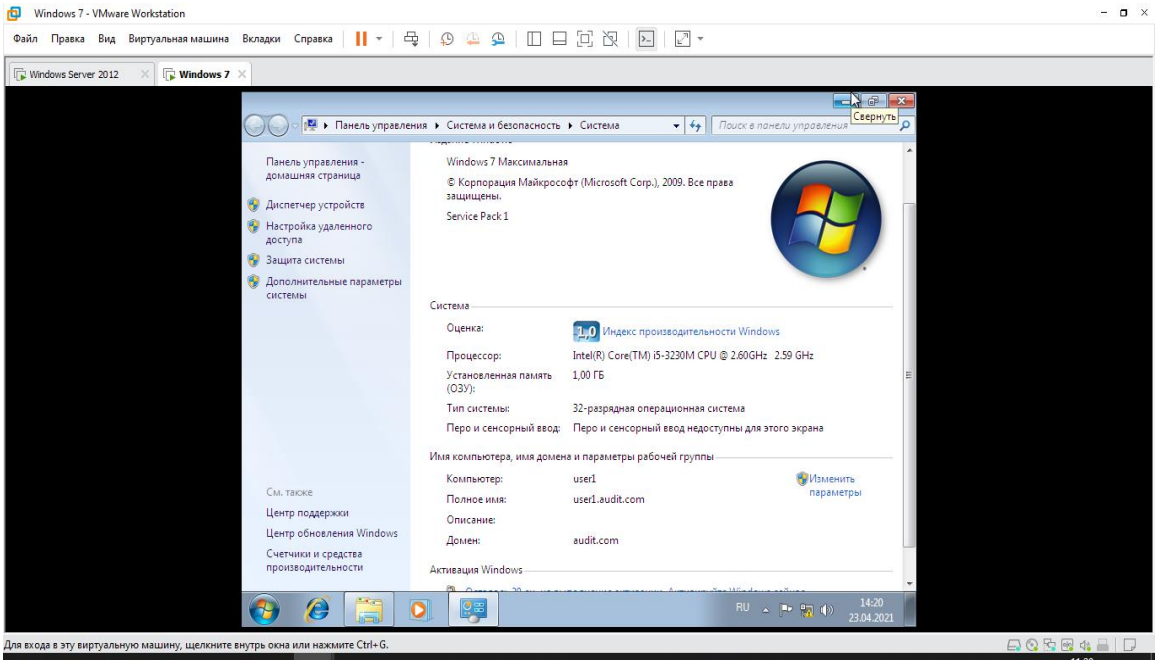


Рисунок 17 - Введение хоста в домен

Так как был вход хоста в домен, появились записи DNS на сервере.

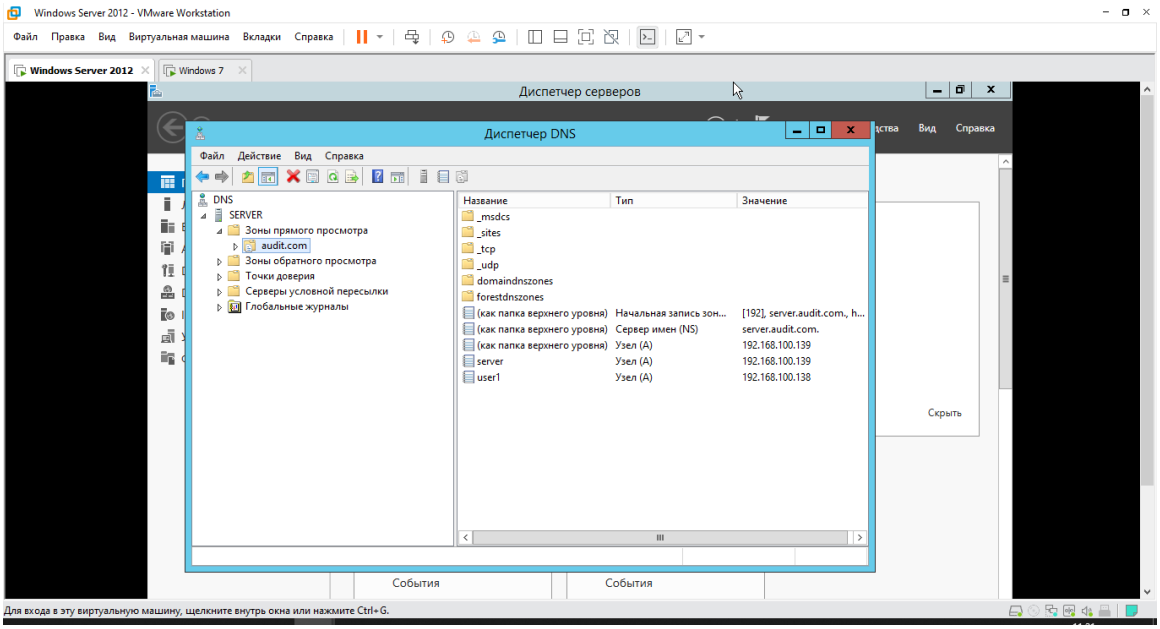


Рисунок 18 - DNS записи сервера

Создание сетевого loopback интерфейса и добавление в виртуальную сеть предприятия. В результате получен IP адрес от DHCP сервера, который был настроен виртуально.

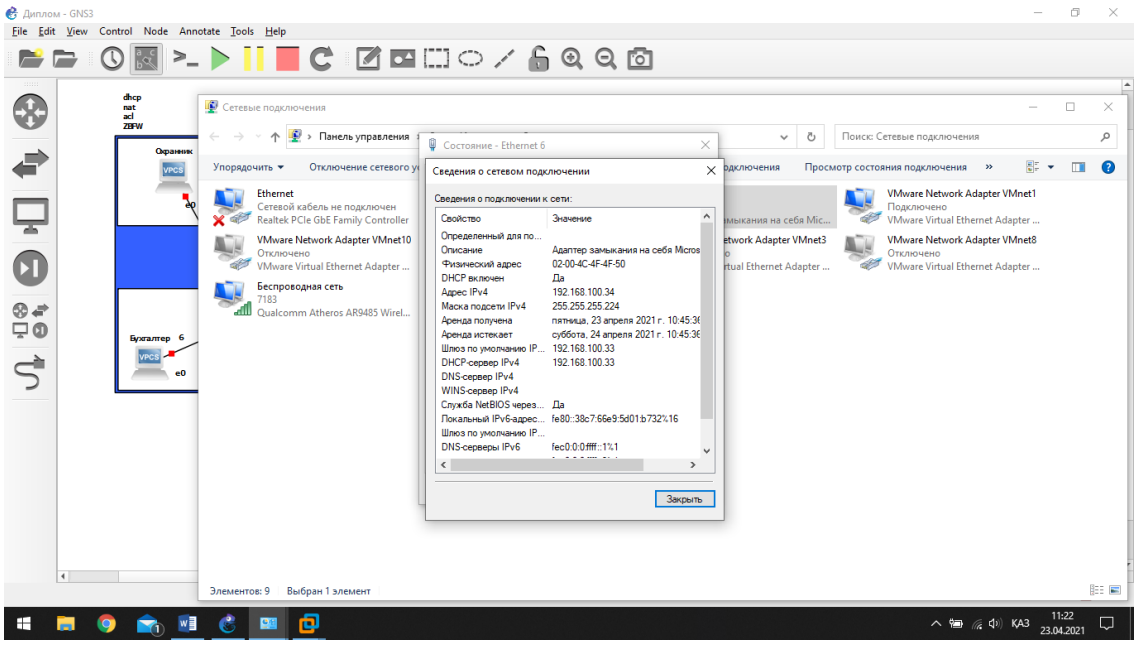


Рисунок 19 - Loopback интерфейс(My PC)

После того как были получены динамические адреса, проверка связи между виртуальным хостом и loopback интерфейсом, который был создан на ноутбуке.

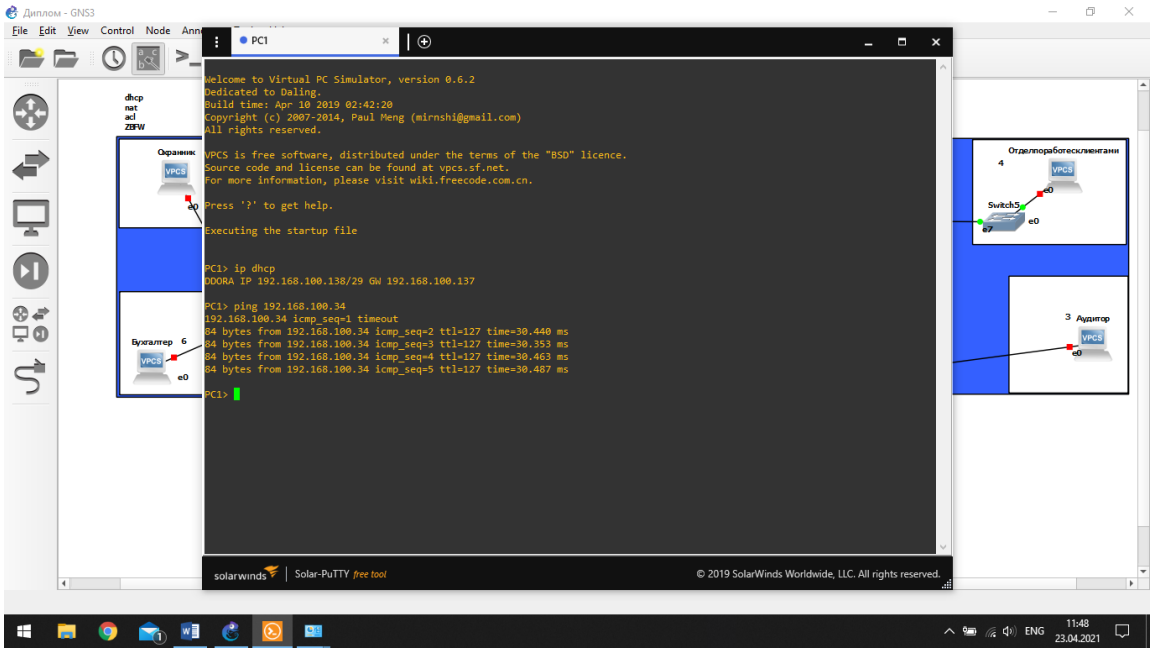


Рисунок 20 - Проверка связи между хостами

Создание сетевого диска для пользователей, для обмена данными по локальной сети.

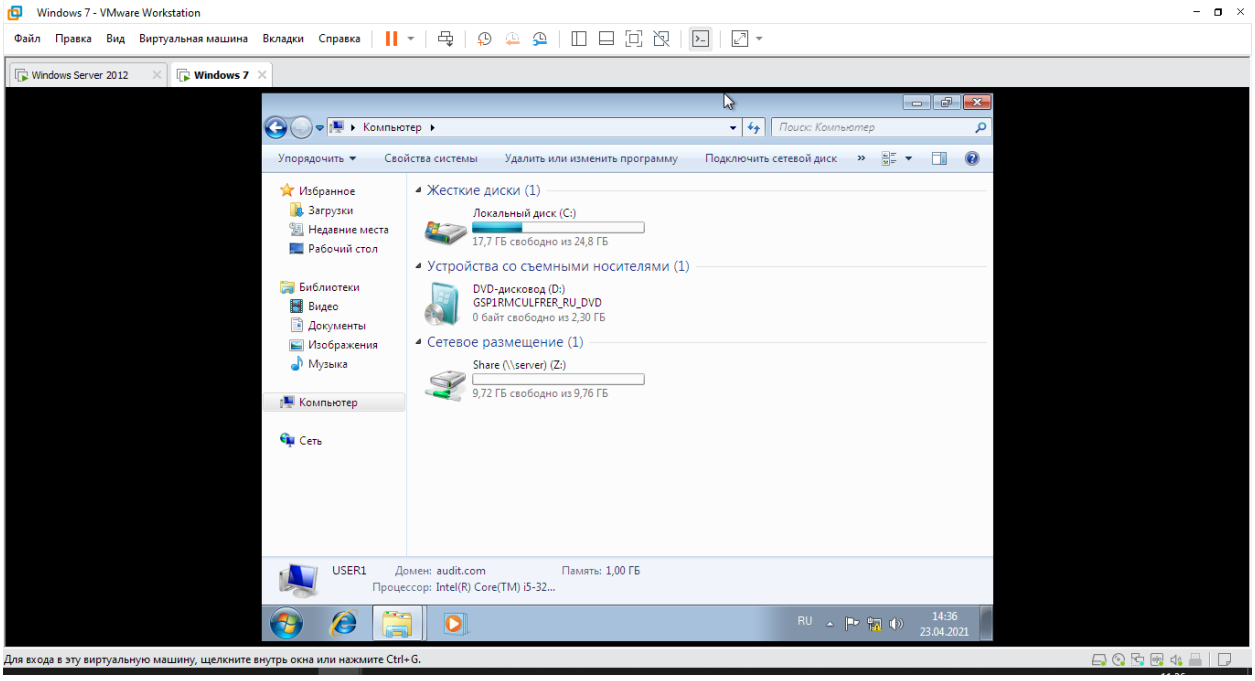


Рисунок 21 - Создание сетевого диска для пользователей

На сетевом диске создание 3 каталогов (Договоры, документы важного характера и общий ресурс). Для папки документы важного характера у пользователя Abylai есть доступ только на чтение. То есть пользователь Abylai не может создавать или удалять данные из этой папки.

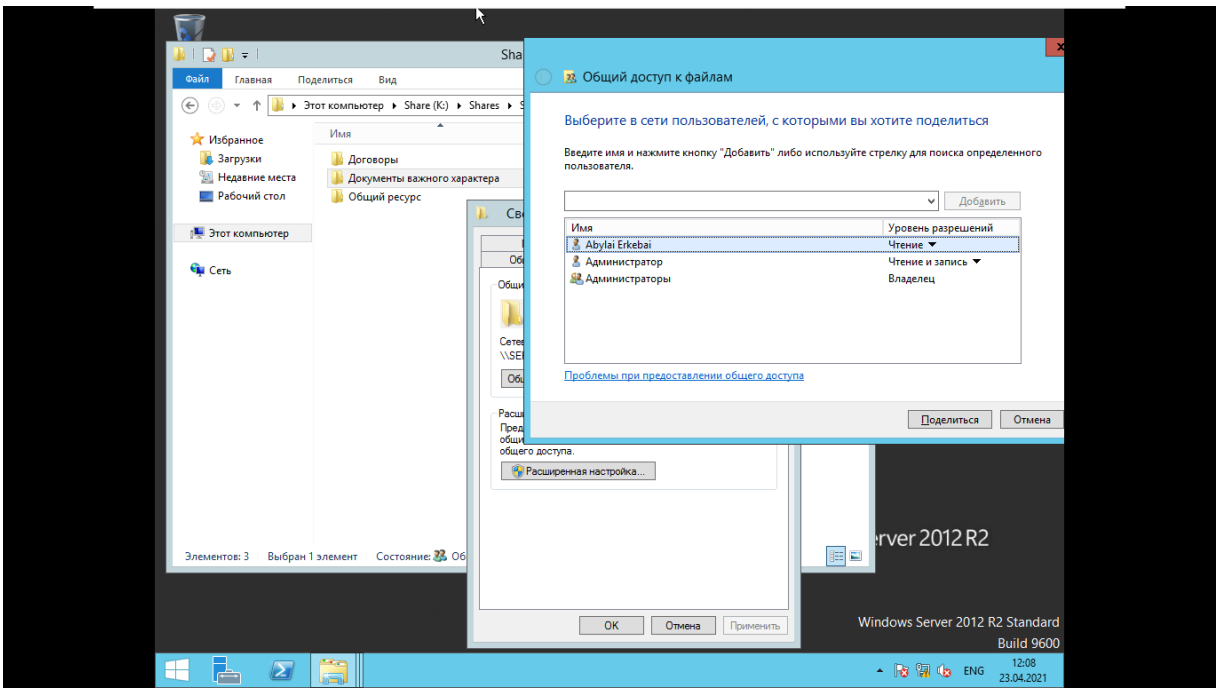


Рисунок 22 - Ограничение доступа к данным (Чтение)

Для папки договоры у пользователя Abylai есть полный доступ. То есть пользователь Abylai может создавать, записывать и удалять данные, которые находятся в этой папке.

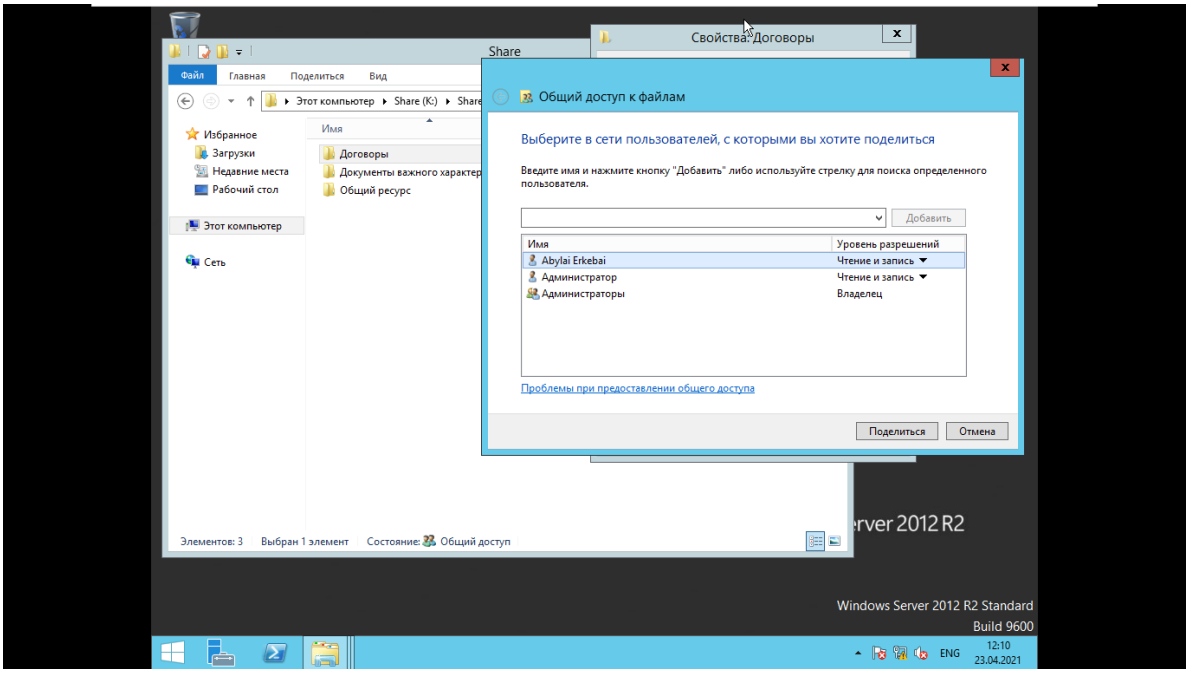


Рисунок 23 - Ограничение доступа к данным (Чтение и запись)

Результат можно увидеть на рисунке 21. Пользователь Abylai пытается удалить документ, который находится в каталоге документы важного характера. Как мы помним для данного пользователя в этом каталога есть доступ только на чтение.

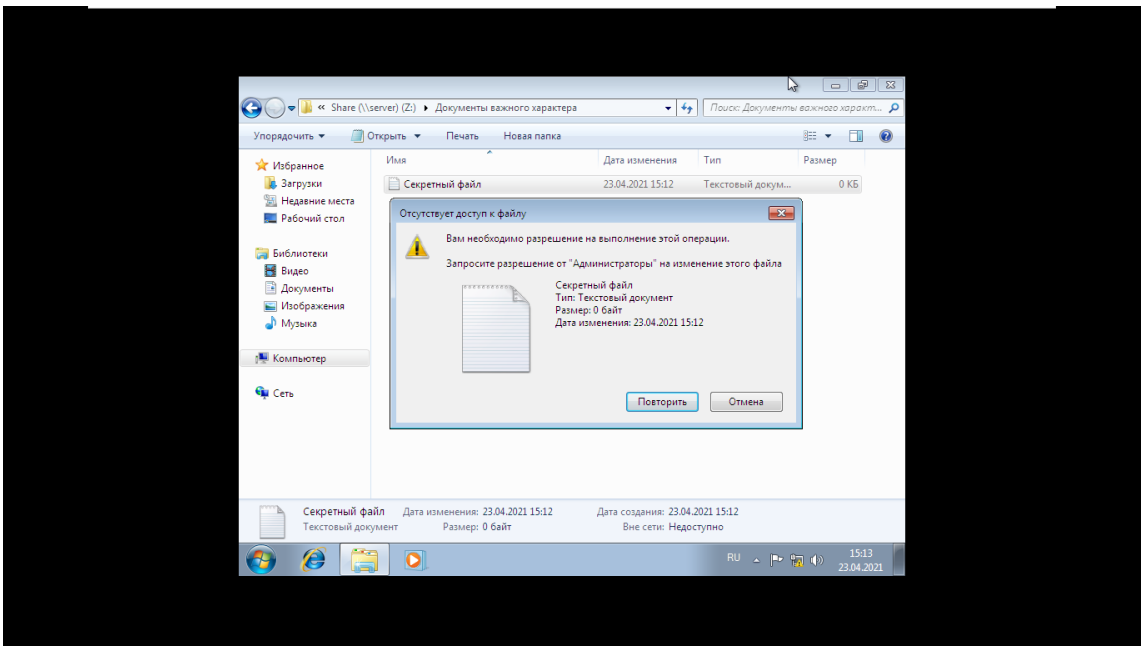


Рисунок 24 - Попытка удалить тех данных, которым доступа нет и результат

В папке договоры у пользователя Abylai есть полный доступ, на рисунке 22 происходит процесс удаления документа и результат рисунок 23.

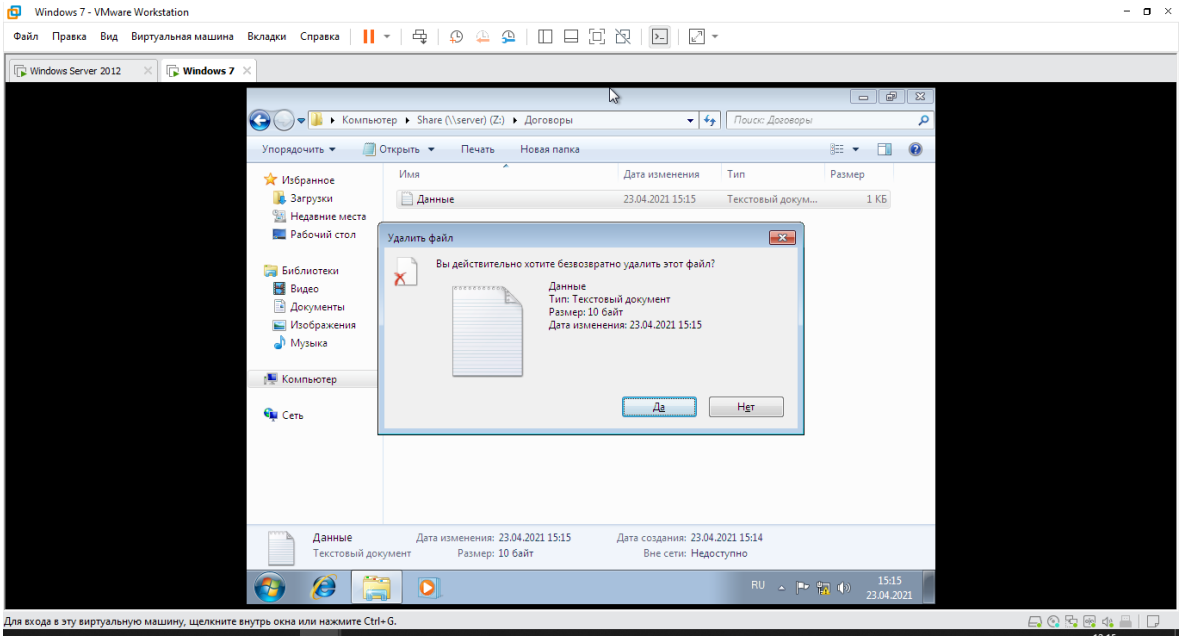


Рисунок 25 - Проверка доступа

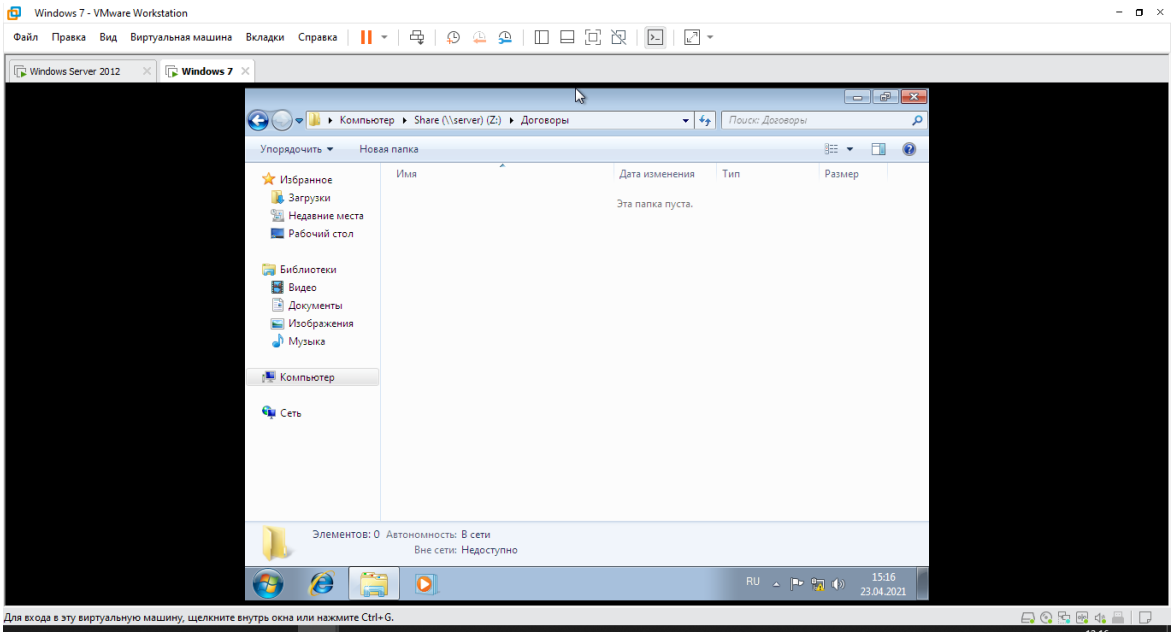


Рисунок 26 - Результат доступа

ЗАКЛЮЧЕНИЕ

В ходе выполнения дипломного проекта была проведена работа с ориентацией на задачи администратора по информационной безопасности для обеспечения защиты и безопасности сети.

Определены основные средства защиты информации в компьютерных сетях. Рассмотрены механизмы администрирования, среди которых были определены методы оптимизация и обслуживания работы системной инфраструктуры, реагирование на инциденты информационной безопасности, и контроль потока информации в пределах локальной сети. Также была рассмотрена реализация политики безопасности и шифрование данных в компьютерных сетях. Для решения задач специалиста по информационной безопасности было рассмотрено сетевое оборудование и средства защиты от компании Cisco, а также других известных компании, которые специализируются в этой отрасли.

Для обеспечения информационной безопасности, а именно целостности и конфиденциальности данных организации, было предложено использовать между филиалами и удаленными сотрудниками сеть VPN.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
2. Организация и обеспечение безопасности информации. Учеб. Пособие: - Харьков, Изд-во, - 200 с.
3. https://falcongaze.com/
4. https://www.ibm.com/
5. Олифер В. Г., Олифер Н. А. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016 – 992 с.
6. Олифер В. Г, Олифер Н. А. Безопасность компьютерных сетей. — М.: Горячая линия-Теле- ком, 2014. – 644 с.
7. Олифер В. Г., Олифер Н. А. Основы компьютерных сетей. — СПб.: Питер, 2009. – 352 с.
8. https://www.cisco.com/
9. https://www.microsoft.com/
10. https://www.gns3.com/

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

ОТЗЫВ

НАУЧНОГО РУКОВОДИТЕЛЯ

на дипломный проект

Еркебай Абылай Ғалымжанұлы

(Ф.И.О. обучающегося)

5В100200 - Системы информационной безопасности

Тема: «Организация и обеспечение безопасности сети предприятия»

Еркебай А. Ғ. при дипломировании получил задание по обеспечению защиты сети предприятия, с которой он успешно справился. Задачами дипломного проекта является организация защиты сети, путем ее модернизации и конфигурации предприятия ТОО «ТрастФинАудит».

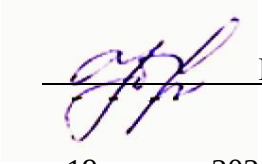
Еркебай А. Ғ. самостоятельно выполнил всю работу по дипломному проекту. Изучил инфраструктуру предприятия, провел анализ работы существующей сети предприятия, изучил требования и характеристики предприятия, провел анализ всех используемых в компании механизмов и средств обеспечения защиты, выбрал соответствующее аппаратное и программное обеспечение. Исследовал все уязвимые и слабые места в обеспечении защиты предприятия. Для решения проблемы модернизации сети Еркебай А. Ғ. привел способы ее решения с применением таких средств разграничение доступа к сети, VLSM, внедрение Zone-Based FireWall, Access Control List, VPN и др. средства защиты.

Рассмотрена платформа GNS3, с помощью которой реализована практическая часть и спроектирована модель сети предприятия ТОО «ТрастФинАудит» с применением механизмов обеспечения защиты.

В процессе дипломирования Еркебай А. Ғ. показал практическое умение и навыки работы с технической литературой, пакетом прикладных программ, хорошие инженерные навыки как в области анализа, так и решения проблем защиты сети.

Дипломный проект на тему «Организация и обеспечение безопасности сети предприятия» выполнен Еркебай А. Ғ. на хорошем уровне и может быть допущен к защите.

Научный руководитель
лектор, м.т.н.



Юбузова Х.И.

« 19 » мая 2021 г.

Протокол анализа Отчета подобия заведующего кафедрой

Заведующий кафедрой заявляет, что ознакомился (-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Еркебай Абылай Ғалымжанұлы
Название: Организация и обеспечение безопасности сети предприятия
Координатор: Юбузова Халича Ибрагимовна
Коэффициент подобия 1: 2,67
Коэффициент подобия 2: 0
Тревога:0,46

После анализа Отчета подобия заведующий кафедрой констатирует следующее:

✓ □ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;

□ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

□ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

После анализа отчета по плагиату и работы дипломника выявлено, что заимствования являются добросовестными и не обладают признаками плагиата, так в основном связаны с применением общеизвестных терминов, а также повторяющееся наименование компании.

« 24» мая 2021 г.
Дата

Сейлова Н.А.., подпись зав. кафедрой

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомилась с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Еркебай Абылай Ғалымжанұлы
Название: Организация и обеспечение безопасности сети предприятия
Координатор: Юбузова Халича Ибрагимовна
Коэффициент подобия 1: 2,67
Коэффициент подобия 2: 0
Тревога:0,46

После анализа Отчета подобия констатирую следующее:

✓ □ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

□ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

□ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

Заимствования в работе являются добросовестными и не обладают признаками плагиата, объясняются использованием общепринятой технической терминологией, а также использованием наименования компании.

«24» мая 2021 г.
Дата

Подпись Научного руководителя