|  |  |  |
| --- | --- | --- |
|  | | logo_kmpo  **КОЛЛЕДЖ**  **МНОГОУРОВНЕВОГО**  **ПРОФЕССИОНАЛЬНОГО**  **ОБРАЗОВАНИЯ** |
|  |  |  |

|  |  |
| --- | --- |
|  |  |

**КУРСОВОЙ ПРОЕКТ**

**Тема:** **Программное обеспечение локальной вычислительной сети отдела ИТ налоговой инспекции**

**Специальность: 09.02.02 «Компьютерные сети»**

**Выполнил студент группы 31КС-18 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Д.А. Фиранский**

**Руководитель курсового проекта \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н. А. Бабаева**

**Москва 2021**

**РЕФЕРАТ**

Расчетно-пояснительная записка 39 с., 2 ч., 18 рис., 14 табл., 10 источников.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, АНАЛИЗ, АВТОМАТИЗАЦИЯ, ОРГАНИЗАЦИЯ.

Объектом автоматизации является отдел ИТ налоговой инспекции.

Цель работы – грамотный подбор ПО для компьютерной сети отдела ИТ налоговой инспекции.

В процессе работы проводился анализ программного обеспечения, обследование деятельности предприятия и сотрудников.

В результате проведённой работы были проведены следующие модификации:

Установлены операционные системы – Windows 10 Professional для рабочих станций, Windows Server 2016 для сервера. Установлено специальное программное обеспечение: Windows server 2016, Kaspersky Security for Windows Servers. Также выбран антивирус Kaspersky Administration Kit рабочих станций и антивирус Kaspersky Security for Windows Servers для сервера, снабженные широким функционалом и надежной защитой.

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 5](#_Toc69083376)

[1 Аналитический раздел 6](#_Toc69083377)

[1.1 Предпроектное обследование налоговой инспекции 6](#_Toc69083378)

[1.1.1 Анализ существующей ЛВС 8](#_Toc69083379)

[1.1.3 Характеристика аппаратных средств предприятия 10](#_Toc69083380)

[1.1.4 Анализ активного периферийного оборудования. 14](#_Toc69083381)

[1.1.5 Анализ информационных потоков ЛВС 14](#_Toc69083382)

[1.2 Анализ методов безопасности 15](#_Toc69083383)

[1.3 Уточнение технического задания 16](#_Toc69083384)

[2.1 Выбор операционной системы 18](#_Toc69083385)

[2.1.1 Выбор операционной системы для рабочих станций 18](#_Toc69083386)

[2.1.2 Выбор операционной системы для сервера 18](#_Toc69083387)

[2.2 Выбор специального программного обеспечения 21](#_Toc69083388)

[2.3 Выбор средств безопасности ЛВС 23](#_Toc69083389)

[2.4 Установка и настройка службы динамической адресации. 25](#_Toc69083390)

[2.5 Конфигурация DHCP 31](#_Toc69083391)

[2.6 Логическое проектирование 32](#_Toc69083392)

[ЗАКЛЮЧЕНИЕ 35](#_Toc69083393)

[СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 36](#_Toc69083394)

[ПРИЛОЖЕНИЕ 1 37](#_Toc69083395)

[ПРИЛОЖЕНИЕ 2 38](#_Toc69083396)

[ПРИЛОЖЕНИЕ 3 39](#_Toc69083397)

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

**ЛВС** – локально-вычислительная сеть

**ПО** – программное обеспечение

**ПК** – персональный компьютер

**АО** – аппаратное обеспечение

**МФУ** – многофункциональное устройство

**Exe-файл** – Файл с расширением .exe (Исполняемый файл)

**ОЗУ** – оперативная память

**AD** – Active Directory

**DHCP** — сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры

**DNS** — компьютерная распределённая система для получения информации о доменах

# ВВЕДЕНИЕ

Телекоммуникация и сетевые технологии являются в настоящее время той движущей силой, которая обеспечивает развитие мировой цивилизации.

Практически нет области производственных и общественных отношений, которая не использовала бы возможности современных информационных технологий на базе телекоммуникаций.

Большое количество организаций за продолжительный промежуток времени эксплуатации локальной вычислительной сети сталкиваются с вопросом расширения и усовершенствования (модернизации) ЛВС. Основной причиной потребности модернизации программного обеспечения (ПО) является использование устаревших утилит и служб.

Актуальность выбранной темы несомненна, так как Федеральная налоговая служба (ФНС России) – сложный механизм, выполняющий большой массив функций, взаимодействующий с множеством предприятий, организаций и граждан, получающий и обрабатывающий информацию из различных источников. Использование ЛВС позволяет избавиться от бумажного документооборота, увеличивает производительность труда, уменьшает время на обработку информации, а вследствие, уменьшается риск к потерям бюджета.

На стадии анализа программного обеспечения (ПО) налоговой инспекции не были учтены темпы роста информационных потребностей заказчика, поэтому нагрузка на существующую сеть увеличивается, а производительность падает. Побочными причинами модернизации программного обеспечения являются: нарушение безопасности данных и устаревшее программное обеспечение. С переходом на более скоростные технологии возникает потребность внесения большого количества изменений. Упор делается на повышение производительности сети.

# 1 Аналитический раздел

Основной целью проведения обследования является получение информации о: топологии ЛВС отдела ИТ налоговой инспекции.

1.1 Предпроектное обследование налоговой инспекции

Инспекция Федеральной налоговой службы (ИФНС) – это федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соблюдением законодательства о налогах и сборах, за верностью их исчисления. Полнотой и своевременностью внесения в бюджет налогов и сборов, в случаях, предусмотренных законодательством РФ, за правильностью исчисления, полнотой и своевременностью внесения в соответствующий бюджет иных обязательных платежей, за производством и оборотом этилового спирта, спиртосодержащей, алкогольной и табачной продукции, а также функции агента валютного контроля в пределах компетенции налоговых органов.

Основной структурной единицей районной инспекции ФНС, является отдел. Отдел – самостоятельное структурное подразделение инспекции, которое возглавляется начальником отдела, подчиняется руководителю или заместителю руководителя инспекции в соответствии с распределением обязанностей между ними.

В организации задействовано большое количество отделов:

* отдел общего и хозяйственного обеспечения (канцелярия);
* юридический отдел;
* отдел досудебного аудита;
* отдел ввода и обработки данных;
* отдел регистрации и учета налогоплательщиков;
* отдел работы с налогоплательщиками;
* отдел камеральных проверок №1;
* отдел камеральных проверок №2;
* отдел камеральных проверок №3;
* отдел кадров;
* отдел информационных технологий;
* отдел предпроверочного анализа;
* отдел выездных проверок №1;
* отдел выездных проверок №2;
* отдел выездных проверок №3;
* отдел оперативного контроля (контрольно-кассовая техника);
* отдел урегулирования задолженности;
* отдел обеспечения процедуры банкротства.

Организационная структура Инспекции Федеральной налоговой службы представлена на (Рисунок 1).

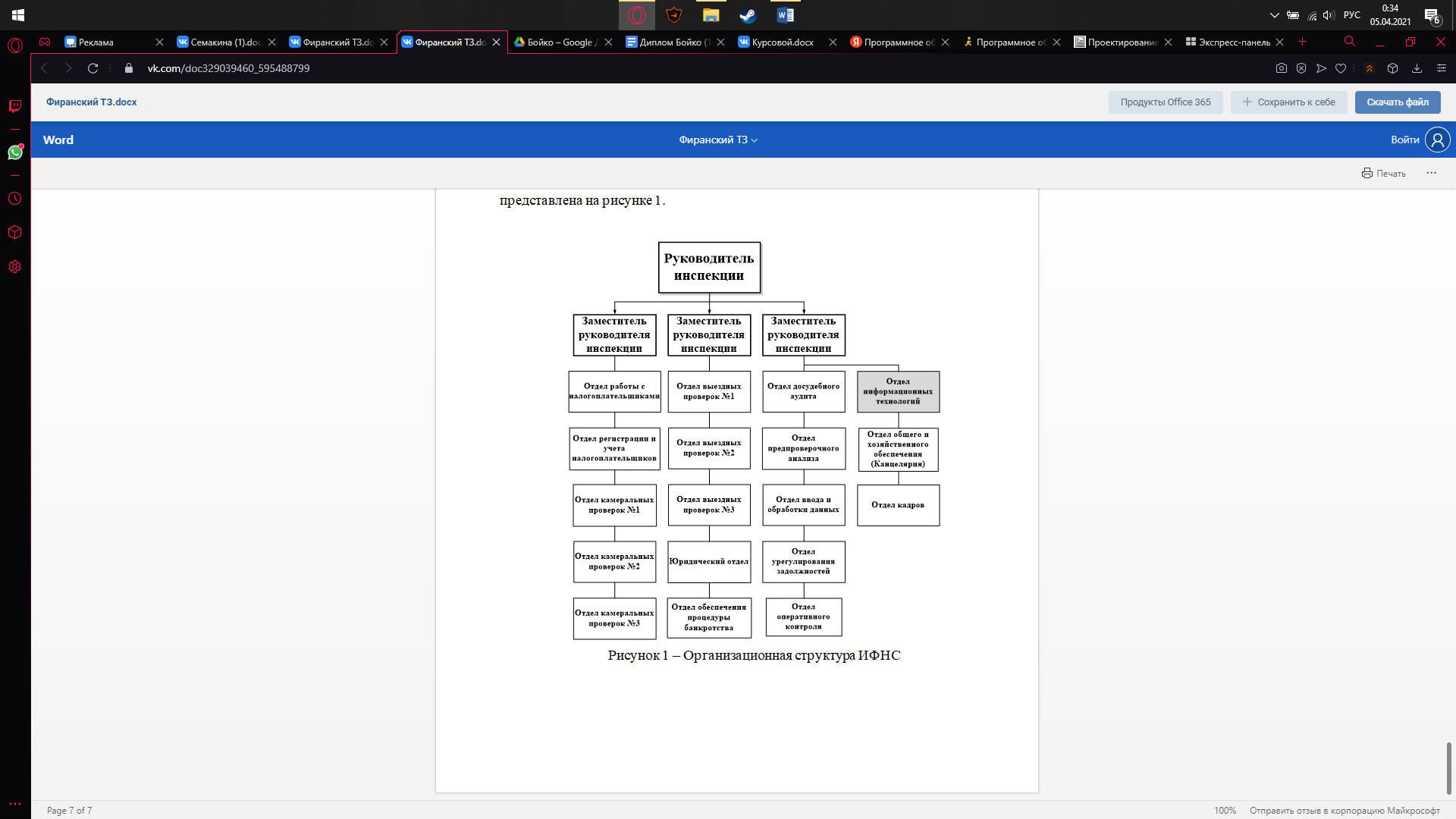


Рисунок 1 – Организационная структура налоговой инспекции

1.1.1 Анализ существующей ЛВС

В рамках предпроектного обследования была составлена и проанализирована структурная схема существующей ЛВС налоговой инспекции, которая представлена на (Рисунок 2).



Рисунок 2 – Логическая схема ЛВС

При построении сети использовалось следующее сетевое оборудование:

* сервер (1 ед.);
* коммутатор для соединения сервера и компьютеров (1 ед.);
* маршрутизатор для соединения сервера и интернет-провайдера (1 ед.);
* сетевой кабель типа витая пара категории 5е, соединяющий компьютеры пользователей с сетевым оборудованием и сервером;
* информационные розетки для подключения компьютеров сотрудников к сети

ЛВС налоговой инспекции построена по топологии «звезда» и включает в себя 9 рабочих станций. В результате подсчёта количества рабочих станций в отделах организации выявлено:

* кабинет директора (1 рабочая станция);
* кабинеты заместителей (3 рабочих станций);
* кабинет системного администратора (1 рабочая станция);
* кабинет руководителя инспекции (1 рабочая станция);
* кабинеты отделов

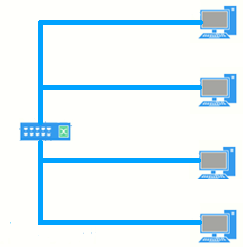


Рисунок 3 – Логическая схема сегмента ЛВС налоговой инспекции

Звезда – это топология ЛВС, где каждая рабочая станция присоединена к центральному устройству (коммутатору). Центральное устройство занимается управляет движением пакетов в сети. Каждый компьютер подключается к коммутатору отдельным кабелем через сетевую карту.

На предприятии имеет смысл строить сеть с использованием нескольких коммутаторов, иерархически соединенных к одному маршрутизатору связями типа «звезда». В настоящее время, иерархическая звезда является самой распространенной топологией как в локальных, так и глобальных сетях.

К преимуществам такой топологии относятся:

* выход из строя одной рабочей станции или повреждение ее кабеля не отражается на работе всей сети в целом;
* отличная масштабируемость: для подключения новой рабочей станции достаточно проложить от коммутатора отдельный кабель;
* легкий поиск и устранение неисправностей и обрывов в сети;
* высокая производительность;
* простота настройки и администрирования;
* в сеть легко встраивается дополнительное оборудование.

1.1.3 Характеристика аппаратных средств предприятия

Аппаратное обеспечение представляет собой совокупность технических средств. Обычно это электронные и механические устройства. Такие устройства позволяют обеспечить как нормальное функционирование каких-либо систем – компьютеров, сетей и систем передачи данных, так и расширяющих их основные функции.

На сегодняшний день отдел ИТ имеет в своем составе 9 компьютеров, которые имеют следующие характеристики (Таблица 1):

Таблица 1 – Характеристики аппаратных средств

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Должность** | **CPU** | **Материнская плата** | **ОЗУ** | **HDD** |
| Системный администратор | Intel Core i3-3220 | Asus P10S-I | 16 Гб | 4 ТБ |
| Заместитель руководителя | Intel Pentium G4560 | ASUS SABERTOOTH Z77 LGA 1155 ATX RTL | 8 Гб | 500Гб |
| Директор | Intel Pentium G4560 | ASUS SABERTOOTH Z77 LGA 1155 ATX RTL | 8 Гб | 500Гб |
| Отделы | Intel Pentium G4560 | ASUS SABERTOOTH Z77 LGA 1155 ATX RTL | 8 Гб | 500Гб |
| Руководитель инспекции | Intel Pentium G4560 | ASUS SABERTOOTH Z77 LGA 1155 ATX RTL | 8 Гб | 500Гб |

Коммутатор является областью концентрации сети и позволяет значительно увеличивать сеть в случае необходимости.

На данном предприятии используется коммутатор фирмы D-link модель DGS-1024C/A1A. Характеристики данного коммутатора представлены (Таблица 2).

Таблица 2 - Характеристики коммутатора D-link DGS-1024C/A1A

|  |  |
| --- | --- |
| **Характеристика** | **Значение** |
| Объем оперативной памяти | 512 КБ |
| Внутренняя пропускная способность | 48 Гбит/сек |
| Количество портов коммутатора | 24 |
| Базовая скорость передачи данных | 10/100/1000 Мбит/сек |
| Потребляемая мощность | 13,5 Вт |

(Рисунок 3) Представлен внешний вид коммутатора:



Рисунок 4 – Внешний вид коммутатора D-link DGS-1024C/A1A

Сервером называется компьютер, выделенный из группы персональных компьютеров (или рабочих станций) для выполнения какой-либо сервисной задачи без непосредственного участия человека.

Большую часть времени работы сервера обязательного участия человека в ней не нужно. Исключениями являются такие ситуации, как: первичная настройка сервера и аппаратно-техническое обслуживание. В таблице ниже представлены технические характеристики сервера предприятия (Таблица 3):

Таблица 3 – Технические характеристики сервера

|  |  |
| --- | --- |
| характеристика | описание |
| Модель | HP ProLiant ML370 G4 |
| поддерживаемые операционные системы | Microsoft® Windows® 2016 Server  Windows® Server 2019 Server |
| процессоры | Intel Xeon Bronze 3204 1,9 GHz |
| кэш-память | 3 МБ кэш-памяти третьего уровня |
| количество процессоров | до 2-х |
| набор микросхем | Intel® E7520 с шиной 800 МГц FSB |
| оперативная память | 32 ГБ PC2-3200R 1600 МГц |
| расширенная защита памяти | Advanced ECC и Online Spare |
| сетевой контроллер | интегрированный NC7781 PCI-X Gigabit NIC |
| слоты ввода / вывода | 4×64-bit/100MHz PCI-X  PCI Express x4  PCI Express x4 |
| дисковый контроллер / RAID-контроллер | интегрированный двухканальный Ultra320 SCSI адаптер  Smart Array 6402 (стандартно только на моделях с массивом) |
| флоппи-дисковод | 1,44 МБ |
| оптический привод | 48x CD-ROM |
| максимальное количество стандартных внутренних дисковых отсеков | 8×1″ Ultra3/Ultra320 (с установленной опциональной корзиной для двух дисков с горячей заменой)  2 отсека для сменных накопителей |
| максимальная емкость внутренних накопителей (с возможностью «горячей» замены, если не указано иное) | 2,4 ТБ SCSI (6×300 ГБ + 2×300 ГБ) с опциональной корзиной для двух дисков с горячей заменой |
| интерфейсы | 3×USB (2 сзади и 1 впереди)   2×последовательный  параллельный  указательное устройство (мышь)  графический  клавиатура  разъем RJ-45  iLO порт удаленного доступа |
| графический адаптер | интегрированный видеоконтроллер ATI RAGE XL с 8 МБ видеопамяти SDRAM |

Продолжение таблицы 3

|  |  |
| --- | --- |
| резервные источники питания | опционально с горячей заменой (1+1) |
| резервные вентиляторы | опционально с горячей заменой |
| интегрированное управление | iLO |
| поддержка proliant essentials value pack | RDP WMP RSO PMP iLO |
| форм-фактор | башня (трансформируется для монтажа в стойку, высота 5U) |
| соответствие отраслевым стандартам | ACPI 1.0b Compliant  PCI 2.2 Compliant  WOL Support  Microsoft® Logo certifications  PXE Support |
| габариты (В×Ш×Г) | 46,88×22,07×71,12 см |
| Вес | 31,75 кг (без жестких дисков и RPS) |
| требования к питанию | напряжение от 100 до 120 В или от 200 до 240 В, частота тока от 50 до 60 Гц |
| максимальная выходная мощность (одного источника питания) | 735 Вт |
| температура | рабочая от 5 до 35 ºC, хранения от -40 до 85 ºС |
| влажность (без конденсации) | рабочая от 5 до 95%, хранения от 5 до 95% |
| гарантия (части / работы / выезд) | 3/3/3 |
| Цена, У.Е. | 6176 |

Дополнительные характеристики сервера:

* твердотельный накопитель (HDD): 960 Гб SATA 62b/s 2.5";
* оптический привод DVD-RW;
* сетевая карта Ethernet 100 Мбит/с;
* блок питания 600 Вт ATX;
* корпус Midi-Tower.

На рисунке 4 представлен корпус сервера:



Рисунок 5 – Корпус сервера

1.1.4 Анализ активного периферийного оборудования.

Также имеется периферийное оборудование, установленного на всех рабочих станциях, список которого представлен в таблице 4.

Таблица 4 – Периферийные устройства

|  |  |
| --- | --- |
| Тип | Название |
| Мышь | Мышь A4Tech N-70FX Black USB |
| Клавиатура | Клавиатура Logitech Keyboard K120 EER Black USB |
| Принтер | Принтер Canon PIXMA iP7240 |
| Монитор | Монитор AOC 24V2Q |
| МФУ | МФУ Canon MAXIFY MB2140 |

Таким образом можно сделать вывод, что в налоговой инспекции используется устаревшее аппаратное обеспечение, а именно это касается комплектующих сервера. Но в отличие от сервера, комплектующие рабочих станций являются достаточно современным решением.

1.1.5 Анализ информационных потоков ЛВС

Информационные потоки между сотрудниками налоговой инспекции представлены (Рисунок 5):

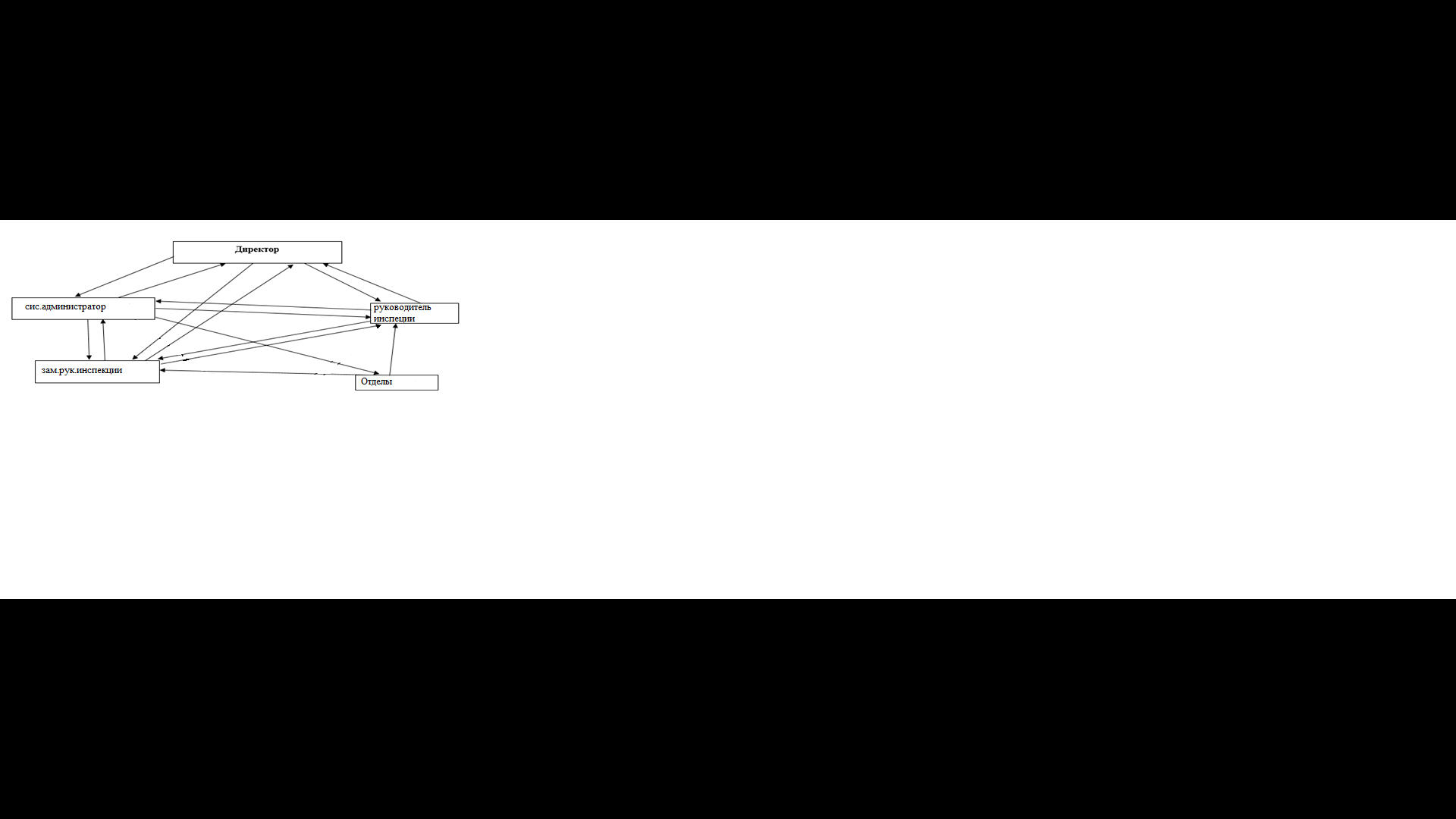


Рисунок 6 – Схема информационных потоков ЛВС

На схеме видно, что сетевой администратор взаимодействует с каждым сотрудником налоговой инспекции, например, задает необходимые групповые политики. Директор, руководитель инспекции и заместитель руководителя инспекции могут общаться между собой по Microsoft Outlook. Данные с отделов доступны заместителю руководителя инспекции и системному администратору, которые в свою очередь могут передать эти данные директору и руководителю инспекции, а при необходимости дать доступ к этим данным.

1.2 Анализ методов безопасности

Защитные методы подразделяются на 4 группы:

1. организационные;
2. технические и аппаратные;
3. программные;
4. аппаратно-программные.
5. Организационные:

К организационным методам относят внутренние нормативные акты, содержащие порядок работы с информацией. Это положение о порядке доступа к документам, коммерческой тайне, а также порядке работы с информационными ресурсами.

1. Технические:

Технические средства защиты информации популярны, т.к. позволяют надежно защитить данные. Им характерна устойчивость к внешнему воздействию, защита от вмешательства вторых лиц в конструкцию, гарантия ограничения несанкционированного доступа в 100%-ом объеме.

Технические средства делятся на две группы:

1. Аппаратные, они встраиваются в компьютеры или совместимы с ними через определенный интерфейс (канал передачи данных – USB, Wi-Fi);
2. Физические, представляющие собой оборудование или архитектуру помещений, защищающих от несанкционированного доступа локально-вычислительную сеть и её элементы.
3. Программные:

По мере усовершенствования вирусов улучшаются и методы борьбы с ними, которое к сегодняшнему дню может продолжительное время скрываться в сетях и не распознаваться антивирусами.

1. Аппаратно-программные средства:

Отдельную группу методов защиты данных в ЛВС составляют аппаратно-программные средства, включающие в себя аппаратно-техническую часть и программный код, позволяющий ею управлять.

В отличие от программных средств защиты информации, аппаратно-программный комплекс сложнее и дороже поменять на новое, усовершенствованное.

Обеспечение безопасности информации также требует выделения всех необходимых ресурсов на подготовку и обучение персонала.

1.3 Уточнение технического задания

В ходе проведенного предпроектного анализа было выявлено:

* проанализирована существующая структура ЛВС;
* проанализированы существующая аппаратно-техническая база;
* изучены всеобщие и существующие методы безопасности ЛВС.

На основе полученных данных сформулированы следующие задачи для решения проблем безопасности ЛВС предприятия:

* логическое проектирование;
* выбор программных средств;
* выбор вариантов решения с учетом имеющихся ограничений в материальной и временной областях;

Целью курсового проекта является модернизация и автоматизация протекающих процессов в налоговой инспекции, путем внедрения программных средств, а также организационных нормативных актов и непосредственно физической составляющей.

**2 Проектный раздел**

По результатам предпроектного обследования налоговой инспекции в данном разделе производится выбор необходимого программного обеспечения в соответствии с данным функционалом.

2.1 Выбор операционной системы

2.1.1 Выбор операционной системы для рабочих станций

Linux — это семейство Unix-подобных ОС, на прямую использующие ядро Linux. Операционные системы, использующие ядро Linux, называются дистрибутивами Linux. Само ядро Linux было создано в 1991 году Линусом Торвальдсом, желающий написать свободное ядро ОС, которым сможет пользоваться каждый. К сегодняшнему дню, ядро Linux содержит около 25 млн. строк исходного кода, распространяющегося, начиная с 1993 года, под лицензией бесплатного ПО GNU General Public License.

Windows 10 - операционная система для ПК и рабочих станций, разработанная Microsoft в рамках семейства Windows NT. Была выпущена 28 июля 2015 года. Согласно статистическим данным сайта WSchools, Windows 10 занимает лидирующее место во всём мире среди ОС, используемых для доступа к сети Интернет, опередив в 2017 году Windows 7. Минимальные системные представлены (Таблица 8). Достоинства и недостатки (Таблица 9).

Таблица 5 – Минимальные системные требования Linux Debian

|  |  |
| --- | --- |
| **Характеристики** | **Значение** |
| Разрядность: x86 (32-bit) | Разрядность: x86 (32-bit) |
| ЦП [CPU]: Pentium 4 1 GHz | ЦП [CPU]: Pentium 4 1 GHz |
| Видеоадаптер [GPU]: любой | Видеоадаптер [GPU]: любой |
| Винчестер [HDD]:2 Gb | Винчестер [HDD]:2 Gb |
|  | |

Таблица 6 – Достоинства и недостатки Linux Debian

|  |  |
| --- | --- |
| **Достоинства** | **Недостатки** |
| Поддержка от менеджера. | Трудная настройка |
| Надёжность | Поддержка не всего аппаратного обеспечения |

Продолжение таблицы 6

|  |  |
| --- | --- |
| Конфигурация очень логична и упорядочена | Находится в неактуальном состоянии |
| Нет проблем с обновлениями | Плохая адаптация |

Таблица 7 – Минимальные системные требования Windows 10

|  |  |
| --- | --- |
| **Характеристики** | **Значение** |
| ОЗУ | 1 ГБ (для 32-разрядных систем) или 2 ГБ для (64-разрядных систем) |
| Место на жестком диске | 16 ГБ для 32-разрядных систем или 32 ГБ для 64-разрядных систем |
| Процессор | Частота процессор 1 ГГц или быстрее, или система на кристалле SoC |
| Графическое устройство | DirectX 9 или более поздней версии с драйвером WDDM 1.0 |
| Интернет-соединение | Обязательно |

Таблица 8 – Достоинства и недостатки Windows 10

|  |  |
| --- | --- |
| **Достоинства** | **Недостатки** |
| Автоматическое обновление системы | Может установится с 2-3 раза |
| Низкие системные требования | Отсутствие DVD драйвера |
| Возможность работы с несколькими рабочими столами |
| Улучшилась производительность системы |
| Меню «Пуск» стало более функциональным и совмещает в себе удобство плиточного интерфейса |
| Универсальность |

Минимальные системные требования для Windows 10 и Debian практически одинаковые. Нельзя утверждать, что одна ОС будет лучше другой. Каждая предназначена для определенных целей. Однако, если выбирать, то предпочтительней ОС Windows 10, так как большинство людей уже знакомы с управлением и привычным интерфейсом.

**2.1.2 Выбор операционной системы для сервера**

Среди наиболее актуальных и популярных серверных операционных систем широко используются Windows Server 2016 и Linux.

Дистрибутивы Linux, в качестве серверных ОС, пользуются спросом среди широких категорий пользователей. Основным отличие Linux server от Windows server — это доступное для всех бесплатное пользование ОС на базе Линукс и потребление ресурсов, склоняющееся к минимуму. Однако, имеются особенности, которые останавливают неопытных пользователей от выбора Линукс. Это необходимость проведения работ через командную строку и настройка конфигурационных файлов, что, безусловно, требует от пользователей специализированных навыков и опыта работы в данном направлении. Также отметить можно то, что под Линукс создано намного меньше вредоносных программ, чем под Windows, что делает ее уязвимой в плане информационной безопасности.

Windows Server 2016 - операционная система для серверов, созданная Microsoft. Система является частью семейства Windows NT и разрабатывалась параллельно с Windows 10. Релиз состоялся 15 октября 2016 года. Минимальные системные требования представлены (Таблица 9). Достоинства и недостатки (Таблица 10).

CentOS разрабатывалась на базе RedHat Linux. В сравнении с последней ОС, она является абсолютно бесплатной. В основном, CentOS не пользуется спросом на домашние компьютеры. Она предназначена для решения бизнес-задач.

Таблица 9 – Минимальные системные требования Windows Server 2016

|  |  |
| --- | --- |
| **Характеристики** | **Значение** |
| ОЗУ | 2 ГБ |
| Место на жестком диске | 32 ГБ |
| Процессор | 64 разрядный с частотой 1.4 ГГц |
| Видеопамять | 32 МБ |
| Интернет-соединение | Обязательно |

Таблица 10 – Достоинства и недостатки Windows Server 2016

|  |  |
| --- | --- |
| **Достоинства** | **Недостатки** |
| Усовершенствованная многоуровневая безопасность | Не обеспечивает безопасность на высшем уровне |

Продолжение таблицы 10

|  |  |
| --- | --- |
| Обеспечивает более гибкую и экономичную операционную систему для любого центра обработки данных | Поддерживает малое количество программ на базе Linux |
| Повышенная точность работы времени благодаря усовершенствованиям в Win32 Time и Hyper-V Time Synchronization Service. |  |
| Использование базы Azure SQL для подключения к удаленному рабочему столу в режиме высокой доступности. |  |
| Динамический контроль доступа |  |

Таблица 11 -Минимальные системные требования Linux CentOS

|  |  |
| --- | --- |
| **Характеристики** | **Значение** |
| Разрядность: x86 (32-bit) или x64 (64-bit) | Разрядность: x86 (32-bit) или x64 (64-bit) |
| ЦП [CPU]: Intel или AMD | ЦП [CPU]: Intel или AMD |
| Видеоадаптер [GPU]: интегрированный | Видеоадаптер [GPU]: интегрированный |
| Винчестер [HDD]:10 Gb | Винчестер [HDD]:10 Gb |
| Оперативная память [RAM]:1 Gb | Оперативная память [RAM]:1 Gb |
| Аудиокарта [AUDIO]: любая | Аудиокарта [AUDIO]: любая |

Таблица 12 – Достоинства и недостатки Linux CentOS

|  |  |
| --- | --- |
| **Достоинства** | **Недостатки** |
| Низкое потребление ресурсов | Нерегулярное обновление приложений в репозиториях |
| Удобный и быстрый менеджер пакетов yum | Система обновлений только через yum и RPM-пакеты |
| Нацеленность на решение именно корпоративных задач | Сообщество пользователей CentOS не такое многочисленное |

Минимальные системные требования рассматриваемых серверных операционных систем схожи почти по всем параметрам и характеристикам. Для сети, рассматриваемой в данном проекте, больше подойдет 16 сервер, так он (Windows Server 2016) оптимален для администрирования небольшой группы компьютеров, а также привычен для системных администраторов своим интерфейсом.

2.2 Выбор специального программного обеспечения

**Выбор антивирусного программного обеспечения**

Антивирусная программа – это утилита, распознающая и удаляющая код вредоносных, «заражённых» файлов. Основной деятельностью этих программ является использование множества принципов для опознания и анализа зараженных файлов. Если антивирусное ПО распознает вирус в файле, то оно удаляет из него, непосредственно, сам код вирусной программы и обеспечивает тем самым полное сохранение данных. Если, так называемое, «лечение» файла невозможно, то зараженный файл полностью удаляется и его восстановление становится невозможным.

Известны несколько типажей антивирусных программ – полифаги, ревизоры, блокировщики, сторожа, вакцины:

**Антивирусные сканеры** – после запуска компьютерной техники начинается сканирование файлов и оперативной памяти. Это гарантируют, что найденный вирус нейтрализован (код вирусной программы удален).

**Антивирусные сторожа** – всегда располагаются в ОП и контролируют процесс проверки файлов во время загрузки в ОП.

**Полифаги** – одни из самых универсальных и эффективных видов антивирусных программ. Направленность их деятельности базируется на проверки файлов, загрузочных секторов дисков и ОП на наличие новых и неизвестных вирусных кодов. Являются требовательны к памяти устройства и их работоспособность характеризуется низкой скоростью.

**Ревизоры** – проверяют на наличие изменений длины файла. Не могут обнаружить вирус в новых файлах (на дискетах, при распаковке), т.к. в базе данных нет абсолютно никакой информации об этих файлах.

**Блокировщики** – предназначены для обнаружения и остановки вирусной программы на самой ранней стадии её развития (при записи в загрузочные сектора дисков). Антивирусные блокировщики, как правило, могут входить в BIOS Setup.

Антивирус – необходимое ПО, которое поможет обеспечить информационную безопасность на компьютерах. Функции антивируса:

* защита от вирусов в реальном времени;
* обнаружение угроз;
* автоматические обновления;
* оповещения об угрозах;
* межсетевой экран;
* поиск уязвимостей в ПО;
* сканирование компьютера по расписанию;
* блокировка доступа к опасным сайтам.

Для выявления наиболее подходящей антивирусной утилиты составлены сравнительные характеристики антивирусов (таблица 13).

Исходя из анализа характеристик антивирусов, сделан вывод, что наиболее подходящим антивирусом для организации информационной безопасности ПК является антивирус Kaspersky Total Security, являясь единственным антивирусом поддерживаемый возможности: «Безопасный веб-сёрфинг», «Родительский контроль», «Фильтрация содержимого по типу данных», «Защита от сетевых вторжений», которые необходимы для безопасной работы компьютеров.

Таблица 13 - Сравнительная характеристика антивирусов

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование** | **Kaspersky Total Security** | **Avast** | **McAfee** |
| 1 | 2 | 3 | 4 |
| Файловый антивирус | + | + | + |
| Мониторинг и ограничение активности программ | + | + | + |
| Почтовый фильтр | + | + | - |
| Фильтрация содержимого по типу данных | + | - | - |
| Гибкое управление правами доступа к устройствам на чтение/запись с возможностью настройки расписания | + | - | + |
| Защита от сетевых вторжений | + | + | + |
| Безопапасный веб-сёрфинг | + | - | - |
| Родительский контроль | + | - | + |
|  |  |  |  |

# 2.3 Выбор средств безопасности ЛВС

Основная проблема, встречающейся во время разработки системы безопасности информационных данных в локальных распределённых сетях является обязанность размещения в одну систему множество компьютеров, серверов, сетей и узлов. Выбор подходящей топологии сети минимизирует средства, выделенные на защиту данных.

Топология должна обеспечивать затрату минимум ресурсов на обработку информационных данных. Основной проблемой является то, что во время непосредственной разработки системы безопасности не используются средства криптографической защиты, в связи с их критичным замедлением процесс обработки данных. Время обработки бизнес-процессов возносится на передний план, нежели надежная защита данных. Однако на вопросах безопасности экономить не стоит.

Первыми шагами на пути к повышению как внутренней, так внешней безопасности ЛВС будет внедрено:

1. физическое препятствие, функцией которого является - исключить возможность соприкосновения 3-го лица с элементами сети, путем доступа к серверной комнате через кабинет системного администратора;
2. физическая изоляция коммутационных шкафов от внешнего воздействия на сеть;
3. создание для каждого сотрудника сети отдельного индивидуального пользователя с уникальным логином и паролем (см. приложение 2);
4. дополнительная настройка групповых политик, путем регламентирования разрешенных работ в сети для каждой категории пользователей (см. рисунок 5);
5. запрет на посещение отдельных сайтов (социальные сети, YouTube);
6. запрет на установление скачанных пользователем новых ПО;
7. определённые реакции системы при выявлении НСД.

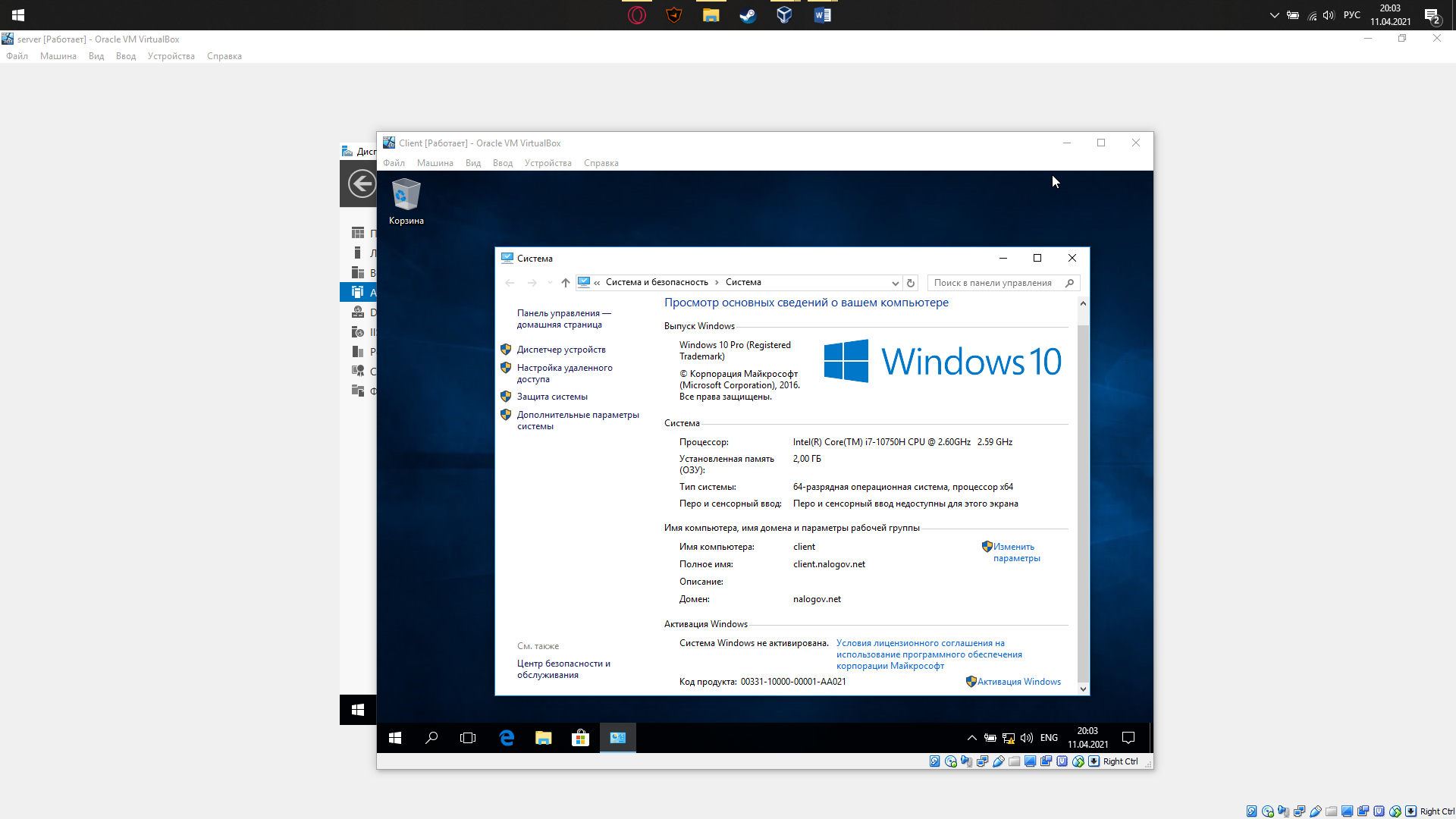
С организационной точки зрения для регламентирования действий пользователей целесообразно:

1. ввести на самом предприятии режим коммерческой тайны, предварительно составив перечень конфиденциальных данных;
2. включить в трудовые договоры пункт об ответственности за разглашение коммерческой тайны организации или персональных данных сотрудников;
3. организация лекций, посвященных способам защиты информации.

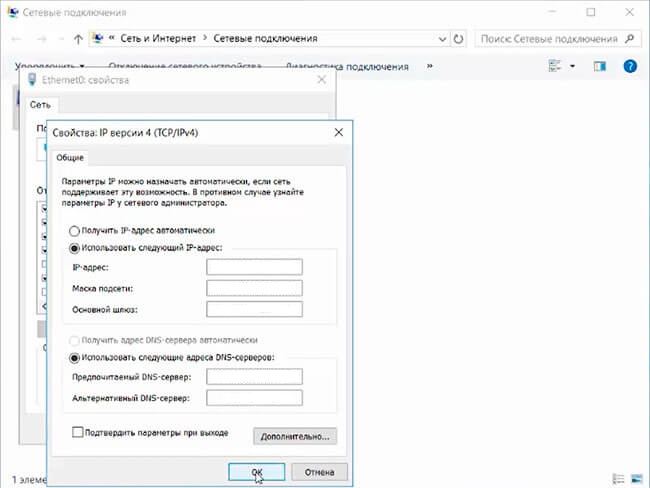
# 2.4 Установка и настройка службы динамической адресации.

До установки ролей сервера рекомендуется задать имя будущему серверу, а также статический IP-адрес для возможности отображения в сети.

Необходимо кликнуть правой клавишей мыши на «Этот компьютер» и выбрать «Свойства». В открывшемся окне – «Изменить параметры» – «Изменить». Задать имя компьютера и нажать «ОК». Для того, чтобы изменения вступили в силу, нужно перезагрузить компьютер (рисунок 8).

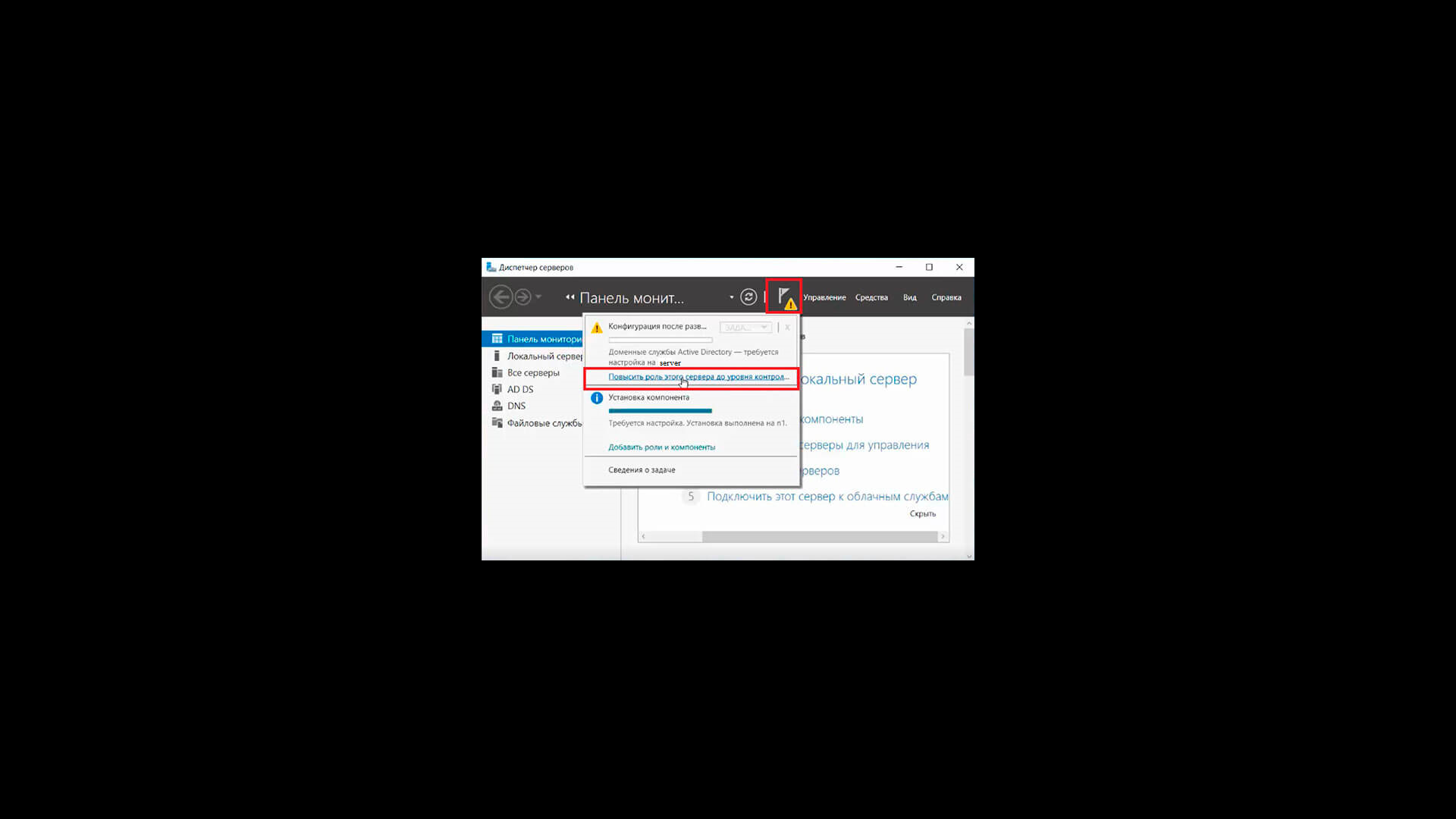
  
Рисунок 7 – Задание новое имя серверу

Для того, чтобы открыть сетевые соединения, в поле «Поиск» команда ncpa.cpl. Выбрать нужный сетевой интерфейс, правой клавишей мыши – «Свойства». Выбирать IP версии (TCP/IPv4).

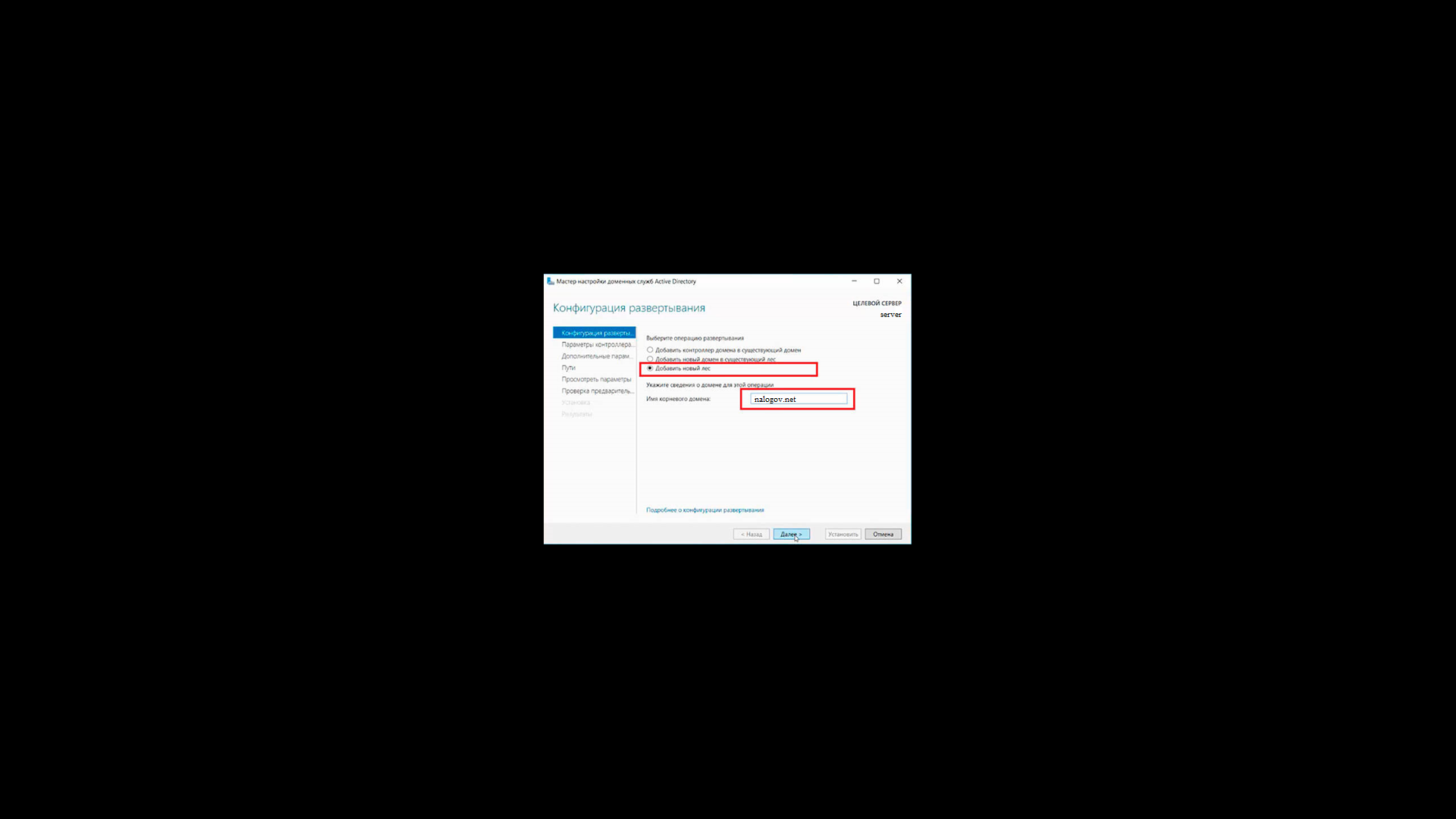
  
Рисунок 8 – Настройка сетевых соединений

Далее необходимо начать установку ролей сервера. Для этого нужно выбрать «Диспетчер серверов». Выбора ролей сервера –галочки напротив «DNS-сервера» и «Доменные службы Active Directory». При появлении запроса о добавлении компонентов – «Добавить компоненты».

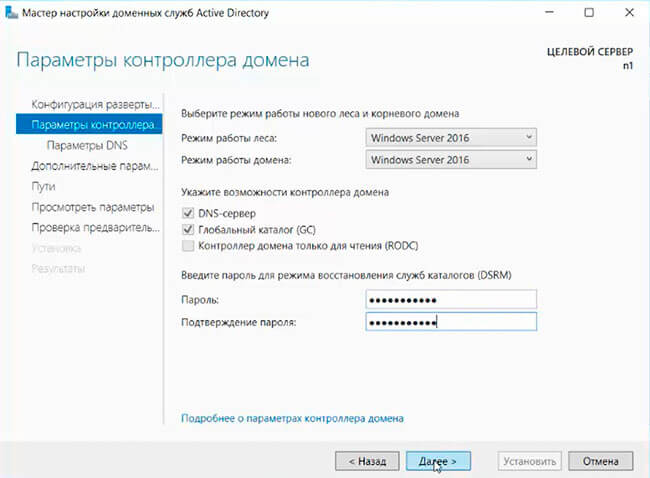
После окончания установки выбранных ролей сервера выбрать «Повысить роль этого сервера до уровня контроллера домена» (рисунок 9).

  
Рисунок 9 – Добавления как контроллер домена

В следующем окне – «Добавить новый лес». Имя корневого домена – уникальное имя домена (рисунок 10).

  
Рисунок 10 – Конфигурирование AD

В «Параметрах контроллера домена» оставить по умолчанию режим работы леса и домена – «Windows Server 2016». Вводим пароль DSRM (Рисунок 11).

  
Рисунок 11 – Конфигурирование AD

Расположение базы данных AD DS, файлов журналов и папок SYSVOL оставить по умолчанию. После того, как сервер проверит соответствие предварительных требований – «Установить».

После настройки контроллера домена, можно перейти к настройке обратной зоны DNS-сервера. Для этого в «Диспетчер серверов» необходимо выбрать «Средства», далее «DNS» (рисунок 12).

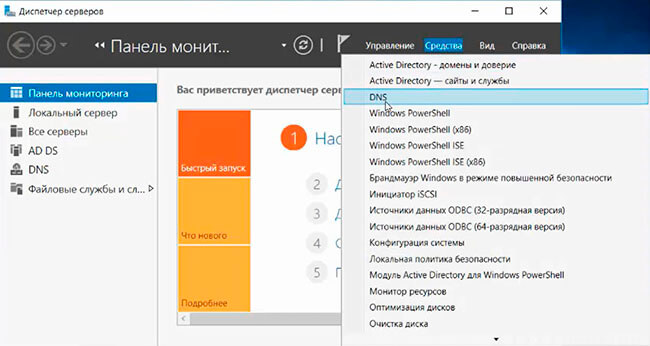


Рисунок 12 – Установка DNS

В открывшемся окне нежно выбрать сервер, затем «Зона обратного просмотра». Правой клавишей мыши – «Создать новую зону». В мастере создания новой зоны установить тип зоны – «Основная зона» (рисунок 13).

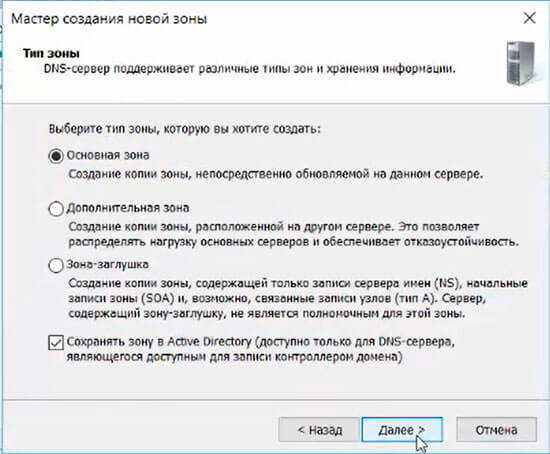


Рисунок 13 – Конфигурация DNS

Установить по умолчанию чекбокс на «Для всех DNS-серверов, работающих на контроллерах домена в этом домене» (рисунок 14).



Рисунок 14 – Конфигурация DNS

В следующем окне – «Зона обратного просмотра IPv4».

Для настройки зоны обратного просмотра задать «Идентификатор сети». После этого появится автоматически зона обратного просмотра. В следующем окне по умолчанию «Разрешить только безопасные динамические обновления»

Появится зона обратного просмотра для домена (рисунок 15).

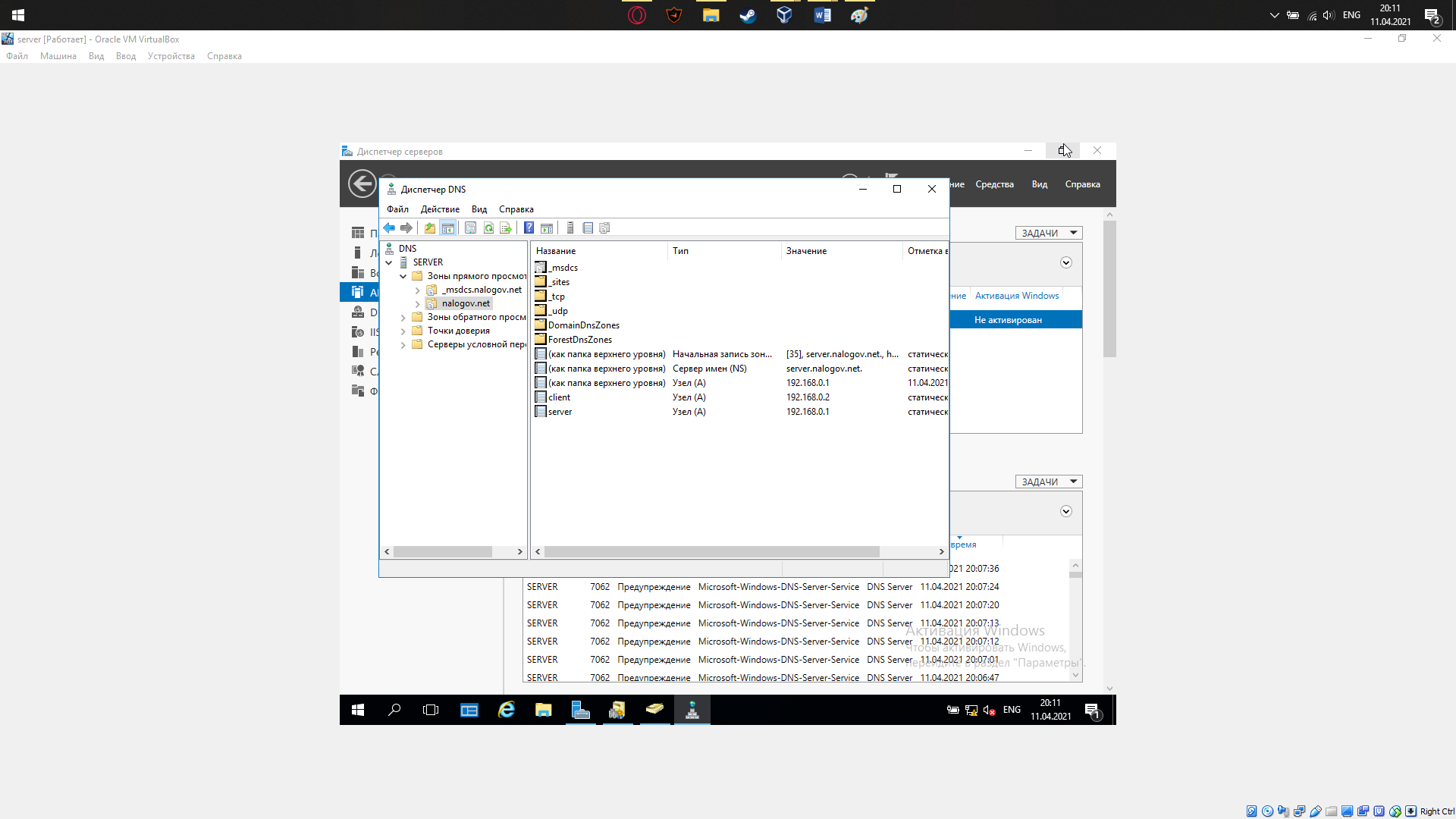


Рисунок 15 – Проверка новой зоны

В «Диспетчере серверов» находим «Пользователи и компьютеры Active Directory» проверить работу Active Directory.

2.5 Конфигурация DHCP

Рекомендуется установить DHCP через диспетчера устройств и добавление ролей. В окне настройки DHCP, нажать правой клавиши мыши на сервер домена, выбирать «Добавить или удалить зону привязки» (рисунок 16).

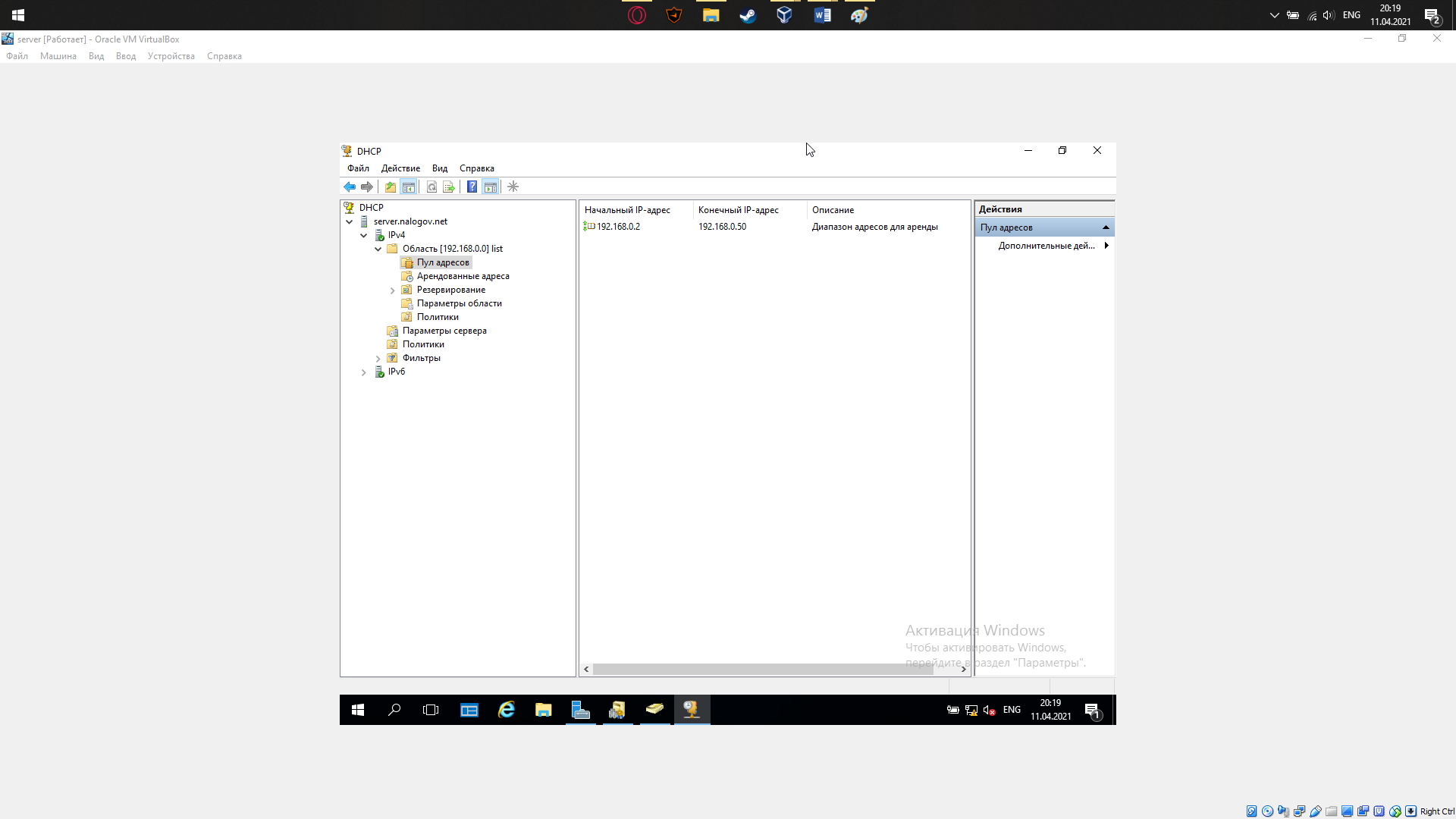


Рисунок 16 – Создание области

На этом настройка DHCP завершена.

* 1. Логическое проектирование

Ограничения, возникающие из-за использования общей разделяемой среды, можно преодолеть, разделив сеть на несколько разделяемых подсетей.

Логическая сегментация сети (VLAN):

* увеличивает гибкость сети – каждая подсеть может быть адаптирована к специфическим потребностям рабочей группы или отдела;
* повышает безопасность данных – устанавливая логические фильтры на коммутаторы можно контролировать доступ пользователей к ресурсам других подсетей;
* упрощает управление сетью – проблемы одной подсети локализуются внутри сегмента.

Однако сегментация проводится в случае, если все компьютеры находятся в одном общем логическом сегменте сети. Определяется логическая структура вычислительной сети на основе расчётов коэффициента загрузки «Проверка на необходимость логической структуризации».

Коэффициент загруженности сети:

где – максимальная пропускная способность базовой технологии сети;

– общая пропускная способность сети ( = );

= (1,1, 1,5) – коэффициент учета протокольной избыточности стека протоколов, измеренного в практикуемой сети; для стека TCP/IP k1≈1,3;

– коэффициент запаса производительности для будущего расширения сети, по техническому заданию = 1,2;

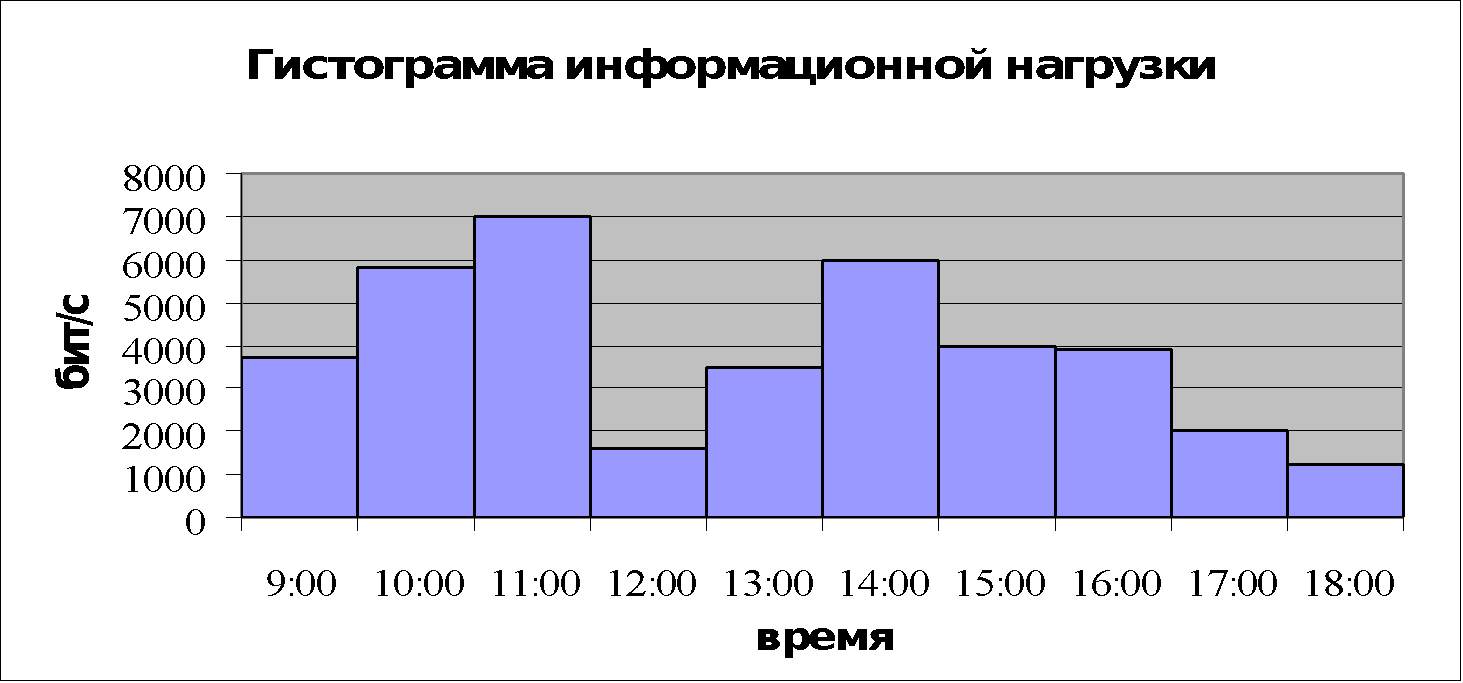


Рисунок 17 – Гистограмма информационной нагрузки

= = 1,3\*1,2\* 7000 = 10920 (бит/с) = 0,0104141 Мбит/с;

= 0.0104141/100 ≈ 0,000104141‬;

Проверка выполнения условия допустимой нагрузки ЛВС (домена коллизий):

= 0,35

где – коэффициент нагрузки неструктурированной сети или домена коллизий – логического сегмента ЛВС.

Путем изменения конфигурации на имеющемся сетевом оборудовании (коммутатор), подсеть, отведенная для отдела ИТ налоговой инспекции, разделилась на 2 подсети (рисунок 18). Таким образом, мы исключили критическую нагрузку, возлагаемую ранее на отдел ИТ налоговой инспекции.

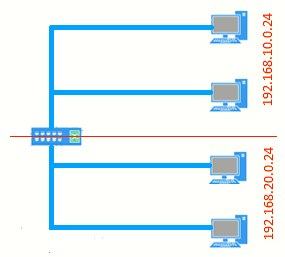


Рисунок 18 – Логическая схема сегмента ЛВС налоговой инспекции

# ЗАКЛЮЧЕНИЕ

В рамках курсового проекта на тему «Программное обеспечение локальной вычислительной сети отдела ИТ налоговой инспекции», в соответствии с техническим заданием, выполнены задачи:

* изучить общий принцип работы ЛВС;
* проанализировать существующую ЛВС;
* проанализировать аппаратное обеспечение;
* подобрать ПО для налоговой инспекции.

Были проведены следующие модификации: установлены операционные системы – Windows 10 для рабочих станций, Windows Server 2016 для сервера, а также установлены и настроены DHCP, DNS, Active Directory. Установлено программное обеспечение, выбран антивирус Kaspersky Total Securiry c широким функционалом и высокой защитой, а также настроена на логическом уровне сегментация сети.

# СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Kali Linux от разработчиков. — СПб. Питер, 2019. — 320 с.: ил. — (Серия «Для профессионалов»).
2. BPF для мониторинга Linux [Калавера Д.](https://amital.ru/Kalavyera-D-m239349.html) – Питер Пресс, 2021. – 208с.
3. ГОСТ 19.201-78 ЕСПД - Техническое задание. Требования к содержанию и оформлению.
4. Научная статья «Лучшие шестнадцатеричные редакторы для Linux», – 2019. – 15с.
5. Внутреннее устройство Windows, 7-е издание, СПБ. Питер, 2019. – 944 с., Марк Руссинович, Дэвид Соломон, Алекс Ионеску.
6. Windows 10. Новейший самоучитель. 4-е издание, - издательство «Эксмо», - 384 с., 2020г.
7. ГОСТ 2.105-98 ЕСКД - Общие требования к текстовым документам.
8. Основы локальных компьютерных сетей – http://www.intuit.ru/studies/courses/57/57/info.

# ПРИЛОЖЕНИЕ 1

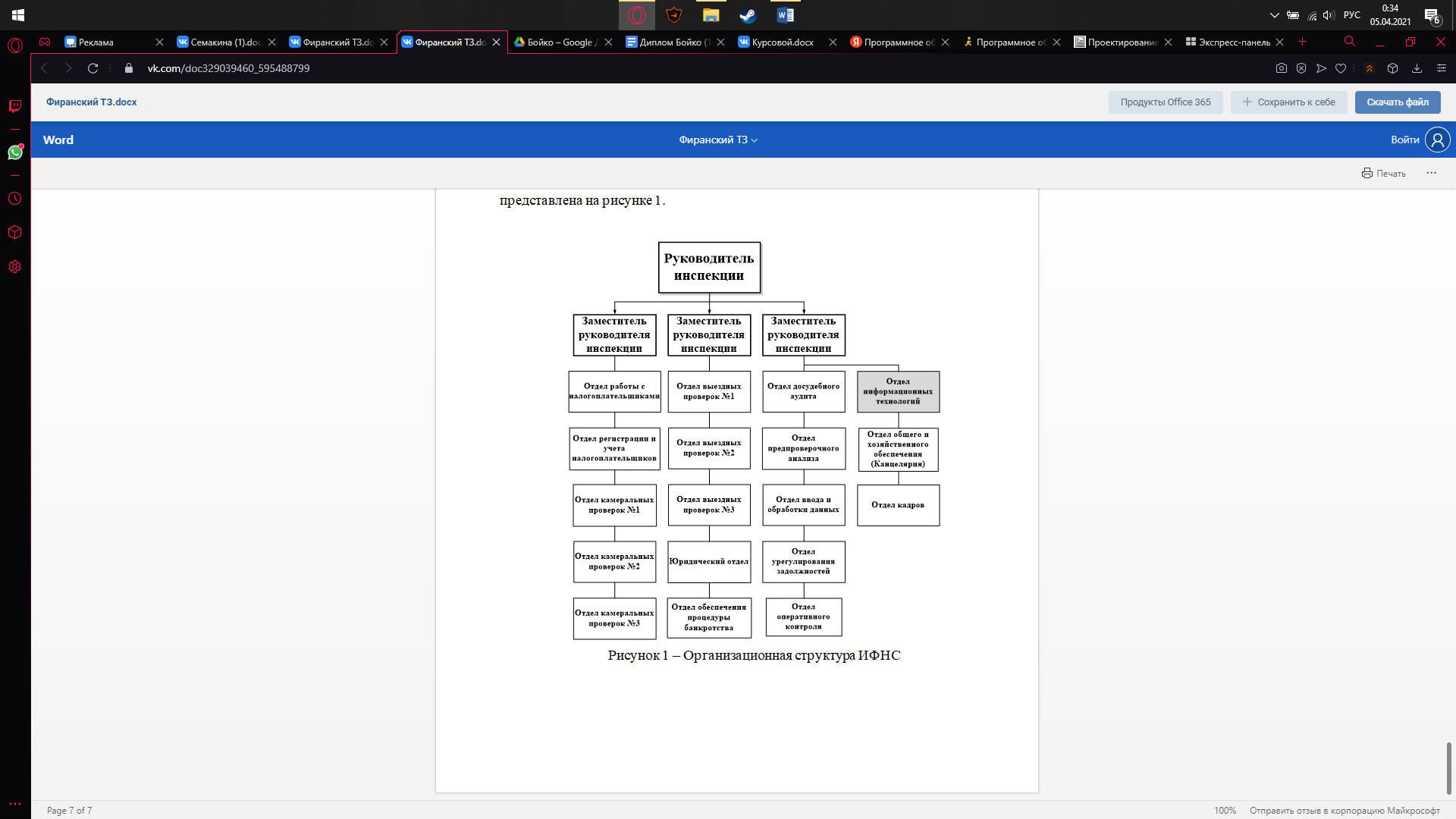


Рисунок 1 – Организационная структура налоговой инспекции

# ПРИЛОЖЕНИЕ 2



Рисунок 2 – Логическая схема ЛВС

# ПРИЛОЖЕНИЕ 3

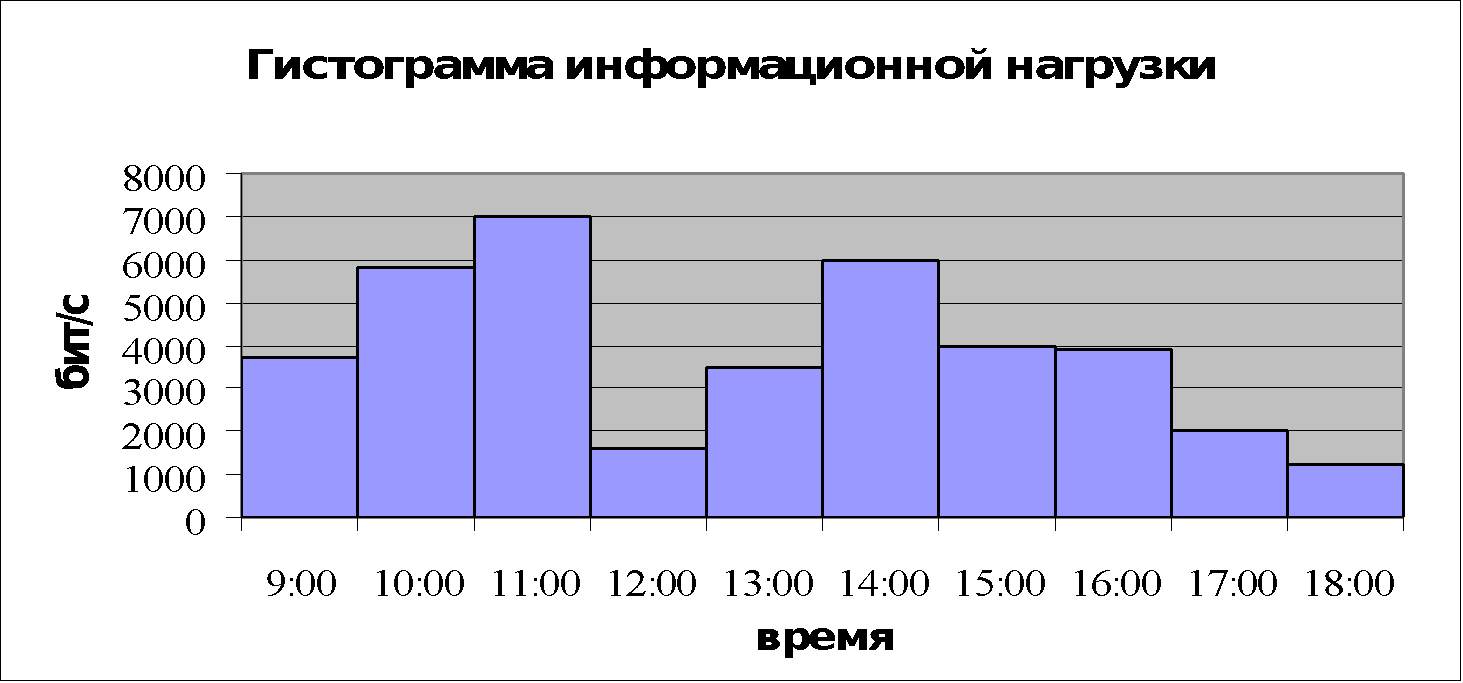


Рисунок 17 – Гистограмма информационной нагрузки