

Министерство образования и науки Самарской области
ГБПОУ «ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ КОЛЛЕДЖ»

Дипломный проект по теме:
«Проектирование компьютерной сети ПАО Сбербанк»

Специальность: 09.02.02 Компьютерные сети

Группа: КС-414

Выполнил: Балашов Алексей Николаевич

Руководитель дипломного проекта: Рогов Роман Романович



Актуальность темы. Цели и задачи дипломного проекта.

Актуальность исследования. В связи с расширением отделов предприятия ПАО «Сбербанк» появляется необходимость в создании новой компьютерной сети отдела автоматизации.

Цель дипломного проекта: Разработка компьютерной сети отдела автоматизации ПАО «Сбербанк».

Задачи исследования:

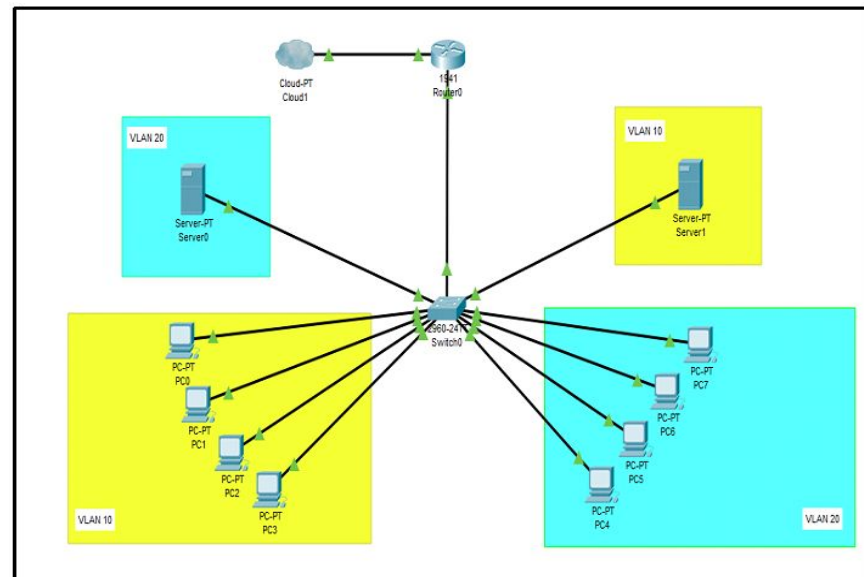
- ✓ Разработать проект работоспособной сети;
- ✓ Выполнить администрирование спроектированной сети;
- ✓ Настроить механизмы безопасности в спроектированной сети;
- ✓ Составить смету проекта;





Логическая топология сети

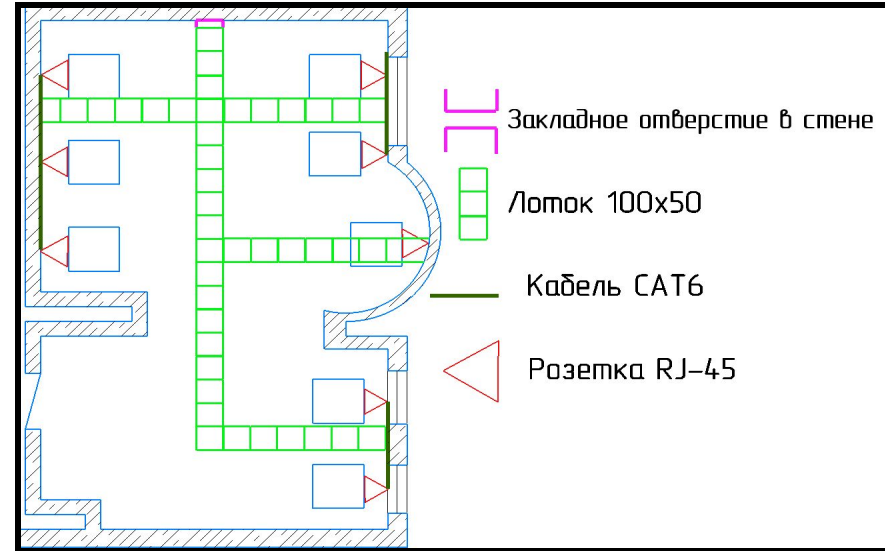
- Нами была выбрана топология типа «Звезда». В ней присутствуют коммутатор, маршрутизатор, сервер для обеспечения безопасности и мониторинга сети, сервер для хранения и организации объектов сети в иерархическую защищенную логическую структуру, сервис аутентификации. А также восемь рабочих станций.
- Наша сеть будет логически разделена на два сегмента сети, сегментирование осуществляется путем использования тегированного трафика. Четыре компьютера и один сервер будут работать в 10 Vlane, а остальные четыре компьютера и сервер в 20 Vlane.





Описание физической топологии компьютерной сети

Проведя анализ зоны проектирования мы построили и описали физическую топологию сети (Подробнее в главе 2.3.).





Выбор оборудования и материалов для построения компьютерной сети

На данном этапе проектирования мы произвели подбор необходимых материалов и оборудования, для обеспечения максимально эффективного и надежного функционирования ЛВС.

Таблица необходимых материалов для построения компьютерной сети

№	Название	Единица измерения	Количество
1	Кабель Cavel LAN 641	1м	90000 мм
2	Кабель-канал 25x25 белый Электропласт.	2м/шт.	28000 мм
3	CABEUS WS-8P8C-CAT.6-1 Розетка компьютерная RJ-45, категория 6, одинарная, внешняя, Dual IDC	штука	8 штук
4	Патч-корд Gembird PP6-1.5m	штука	18 штук
5	Лоток 100x50 L3000 ДКС	3м/шт.	18000 мм
6	С-подвес потолочный 100 мм СППУ-100	штука	36 штук
7	Анкер-клин Stinger 6x40 мм	упаковка (200шт)	200 штук
8	Дюбель-гвоздь с бортом 6x40	упаковка (200шт)	200 штук

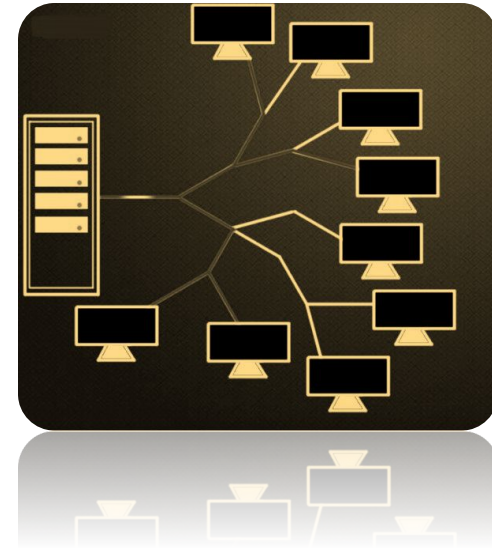
Таблица необходимого оборудования для построения компьютерной сети

№	Название	Количество, шт.
1	Патч-панель CABEUS PL-24-CAT.6-SH-DUAL IDC	1
2	Cabeus JB07-1U-GY Кабельный органайзер	1
3	Коммутатор Allied Telesis AT-GS950/24	1
4	Сервер аутентификации HPE ProLiant MicroServer Gen10	1
5	Сервер мониторинга HP ProLiant DL380 G7	1



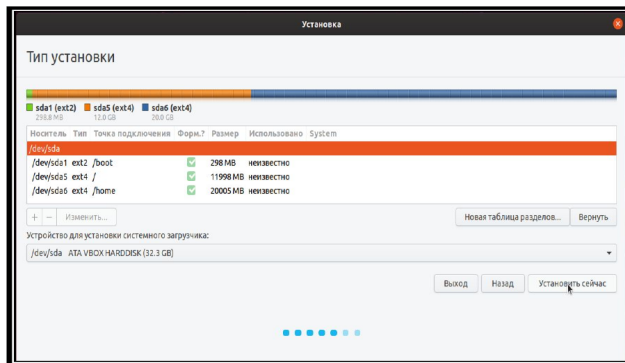
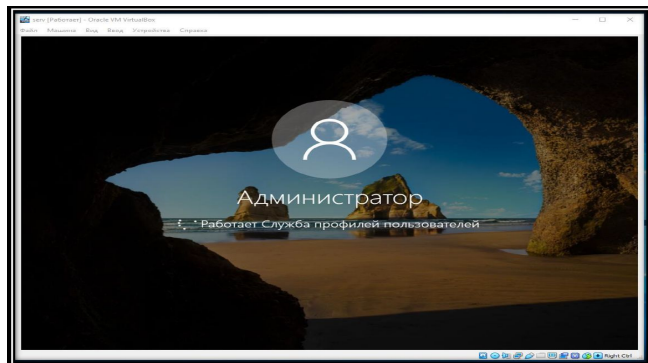
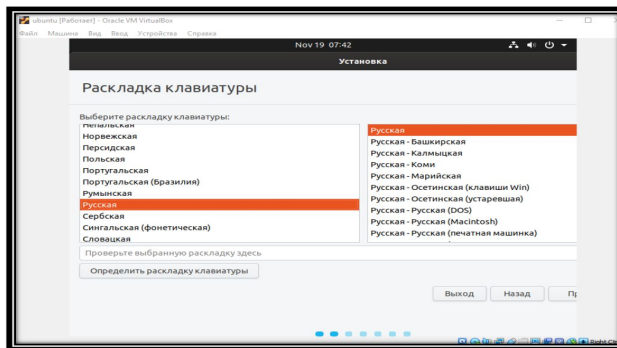
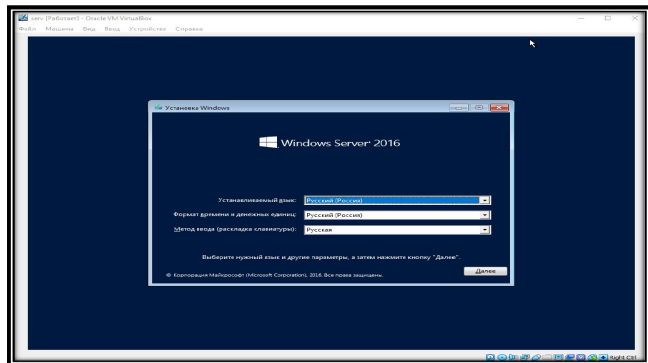
Анализ и обоснование выбора программного обеспечения

- Произведя анализ рынка операционных систем, мы выбрали Ubuntu 19.10. для наших пользователей, основываясь на её бесплатном использовании.
- И Windows Server 2016 для серверных машин, руководствуясь его преимуществами в эффективной службе поддержки и малой стоимостью.





Установка и первичная настройка программного обеспечения



В данной главе мы осуществим установку операционных систем клиентских и серверных компьютеров предприятия.

установка ОС Windows Server 2016

установка ОС Ubuntu



Администрирование компьютерной сети

- В начале администрирования будет произведена установка ролей, создан корневой домен предприятия, созданы учётные записи пользователей и настроены их политики.
- Далее будут настроены DHCP и DNS зоны.
- В завершение мы осуществим подключение к глобальным сетям и настройку локальной маршрутизации посредством сегментирования с использованием тегированного трафика. (подробнее в главах 3.5-3.7)

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.5

Pinging 192.168.10.5 with 32 bytes of data:

Ping statistics for 192.168.10.5:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\>ping 192.168.10.5

Pinging 192.168.10.5 with 32 bytes of data:

Reply from 192.168.10.5: bytes=32 time<lms TTL=127
Reply from 192.168.10.5: bytes=32 time<lms TTL=127
Reply from 192.168.10.5: bytes=32 time<lms TTL=127
Reply from 192.168.10.5: bytes=32 time<lms TTL=127

Ping statistics for 192.168.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```
C:/>
```



Выбор и обоснование программно-аппаратных средств защиты информации в сети

- По результатам анализа, для защиты серверных машин был выбран Avast Business Antivirus, т.к. он имеет функциональные системы защиты, а также недорогую лицензию.
- В результате исследования, для защиты пользовательских машин был выбран Sophos т.к. он сочетает в себе лучшие методы защиты от вирусного ПО и наличие бесплатной лицензии.
- В качестве программного обеспечения для организации мониторинга сети был выбран Zabbix, по причине его надёжности и бесплатности.





Настройка оборудования

В данной главе мы выполнили настройку нашего активного сетевого оборудования. И сделали это посредством изменения имён устройств, присвоения доменного имени, добавлением баннера, установки паролей и настройки Port Security.

```
Switch1
Switch#conf t
Switch(config)#no
Switch(config)#hostname S1
S1(config)#ip d
S1(config)#ip do
S1(config)#ip dom
S1(config)#ip doma
S1(config)#ip domain
S1(config)#ip domain?
domain domain-lookup domain-name
S1(config)#ip domain-name Sberbank.ru
S1(config)# banner motd "This is a secure system. Authorized Access Only!"
S1(config)#line c
S1(config)#line console 0
S1(config-line)#pass
S1(config-line)#password Fktrctq2999
S1(config-line)#login
S1(config-line)#ex
% Ambiguous command: "ex"
S1(config-line)#exit
S1(config-line)#line vty 0 4
S1(config-line)#password Fktrctq2999
S1(config-line)#login
S1(config-line)#exit
S1(config)#enable secret Fktrctq2999
S1(config)#service password-encryption
S1(config)#exit
S1#
Ctrl+F6 to exit CLI focus
```

```
Switch1
Switch#conf t
Switch(config)#
Switch(config)#int Fa0/9
Switch(config-if)#sw
Switch(config-if)#switchport port-security
Switch(config-if)#sw
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#sw
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address s
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#sw
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security vi
Switch(config-if)#switchport port-security violation sw
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#
Ctrl+F6 to exit CLI focus
```

```
Router2
Router#conf t
Router(config)#hostname R1
R1(config)#ip domain-name Sberbank.ru
R1(config)#banner motd "This is a secure system. Authorized Access Only!"
R1(config-line)#line console 0
R1(config-line)#password Fktrctq2999
R1(config-line)#login
R1(config-line)#ex
R1(config-line)#line vty 0 4
R1(config-line)#password Fktrctq2999
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret Fktrctq2999
R1(config)#service password-encryption
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
Ctrl+F6 to exit CLI focus
```



Установка и первичная настройка межсетевого экрана на серверных машинах.

С помощью правил iptables мы разграничим доступ клиентов до подсетей друг друга

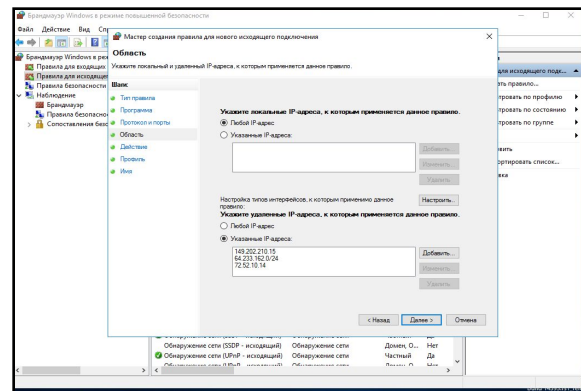
Далее мы ограничим доступ к сайтам с помощью iptables и Firewall.

```
aleksey@PC2:~$ sudo apt-get install iptables
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
E: Пакет sav-llnux:1386 нуждается в переустановке, но найти архив для него не удалось.
aleksey@PC2:~$ sudo iptables -L | grep policy
chain INPUT (policy ACCEPT)
chain FORWARD (policy ACCEPT)
chain OUTPUT (policy ACCEPT)
aleksey@PC2:~$ sudo iptables -A INPUT -s 192.168.20.0/24 -j DROP
aleksey@PC2:~$
```

Настройка межсетевого экрана на Linux клиенте

```
aleksey@PC2:~$ sudo /sbin/iptables-save
# Generated by iptables-save v1.6.1 on Sun Mar 15 12:12:33 2020
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
- A INPUT -m string --string "lgrl-2012.ru" --algo kmp --to 65535 -j DROP
- A INPUT -m string --string "getcar.org" --algo kmp --to 65535 -j DROP
- A INPUT -m string --string "furry.reactor.cc" --algo kmp --to 65535 -j DROP
- A INPUT -s 192.168.20.0/24 -j DROP
COMMIT
# Completed on Sun Mar 15 12:12:33 2020
aleksey@PC2:~$
```

Настройка межсетевого экрана на Linux клиенте



Настройка межсетевого экрана на Windows server



Установка и настройка антивирусного ПО.

В главе 4.5

описаны работы по установке и настройке антивирусного ПО.

```
aleksey@PC2: ~/Загрузки/sav-linux-free-9/sophos-av
Файл Правка Вид Поиск Терминал Справка
It can update either from Sophos directly (requiring username/password details)
or from your own server (directory or website (possibly requiring
username/password)).

Which type of auto-updating do you want? From Sophos(s)/From own server(o)/None
(n) [s]
> s

Updating directly from Sophos.
Do you wish to install the Free (f) or Supported (s) version of SAV for Linux?
[s]
> f

The Free version of Sophos Anti-Virus for Linux comes with no support.
Forums are available for our free tools at http://openforum.sophos.com/
Do you need a proxy to access Sophos updates? Yes(Y)/No(N) [N]
> n

Fetching free update credentials.
Installing Sophos Anti-Virus...
Selecting appropriate kernel support...
When Sophos Anti-Virus starts, it updates itself to try to find a Sophos kernel
interface module update. This might cause a significant delay.
Sophos Anti-Virus starts after installation.

Installation completed.
Your computer is now protected by Sophos Anti-Virus.
aleksey@PC2:~/Загрузки/sav-linux-free-9/sophos-av$ sudo init 6
```

Рисунок 1 – установка и настройка антивируса Sophos

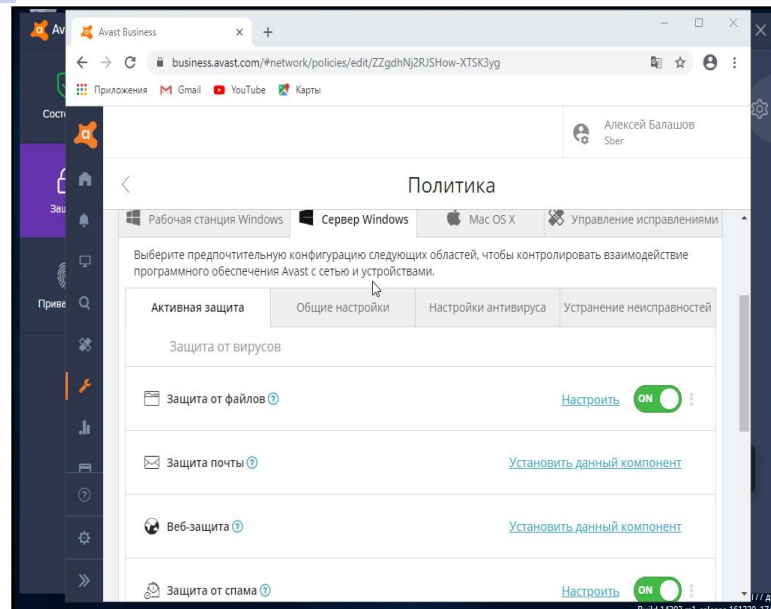
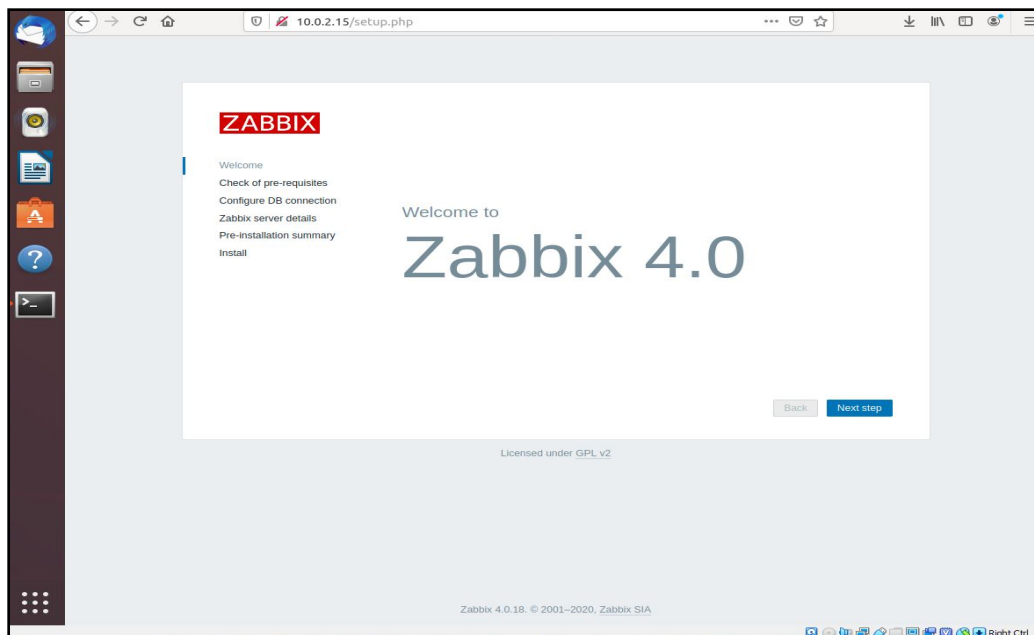


Рисунок 2 – установка и настройка Avast Business Antivirus



Организация мониторинга сетевых устройств и рабочих станций.

В главе 4.6 описаны работы по организации мониторинга сетевых устройств и рабочих станций.

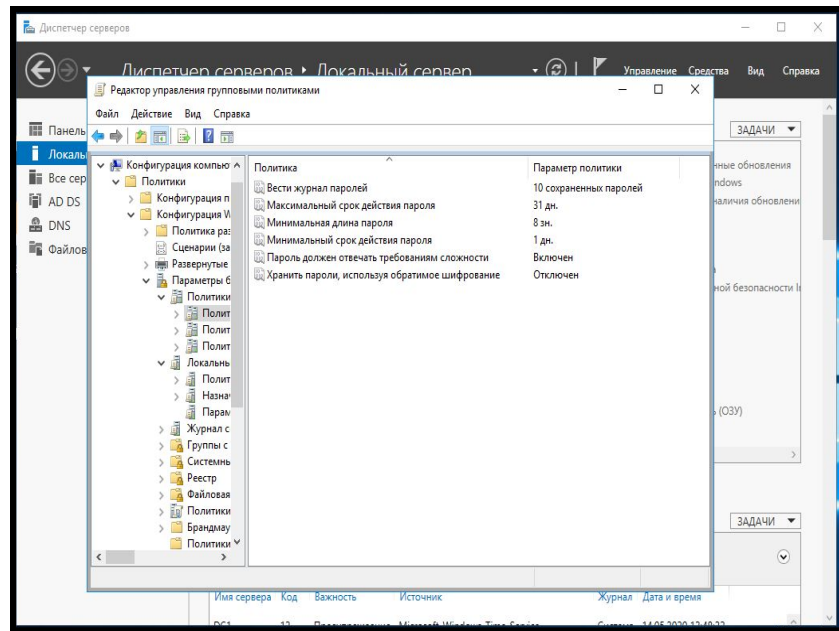




Описание и настройка методов защиты персональных данных пользователей.

Так как каждый сотрудник имеет личные конфиденциальные данные для использования своего аккаунта, мы организовали надёжную защиту, с целью снижения вероятности утечки конфиденциальной информации.

В главе 4.7 подробно описаны и продемонстрированы используемые нами методы защиты.



настройка параметров безопасности



Разработка плана аварийного восстановления сети .

В главе 4.8 описаны

превентивные меры по

предотвращению угроз и меры

послеаварийного восстановления

сети, задействованные на

предприятии ПАО «Сбербанк».

План аварийного восстановления сети и превентивных мер			
№ п/п	Угроза	Превентивные меры по предотвращению угрозы	Меры послеаварийного восстановления сети
1	Потеря соединения с серверными или рабочими станциями.	Организованный мониторинг сети.	Идентифицирование проблемы с помощью сервиса мониторинга сети или вручную, повторное включение в сеть.
2	Отказ рабочей станции в случае технической неисправности.	Проведение профилактического и технического обслуживания.	Обратиться к техническому специалисту для проведения ремонтных работ.
3	Заражение серверных или рабочих станций вредоносным ПО.	<u>Установленное и настроенное антивирусное ПО, включенное автоматическое сканирование.</u>	Выйти из рабочей среды, запустить полное сканирование ПК в антивирусной программе, по необходимости обратиться за помощью к системному администратору.
4	Потеря сотрудником конфиденциальных данных (доменный профиль занят третьим лицом, потеря логина или пароля).	Превентивные меры описаны в главе 2.4 (страница 38).	Обратиться к сетевому администратору для блокировки профиля и последующей смены логина или пароля.
5	Обрыв линий связи, таких как, сетевые кабели.	Агрегирование основных каналов связи, а так же укладывание линий связи в кабельканалы.	Повторное соединение компьютеров сети кабельными линиями.



Разработка плана технического и профилактического обслуживания.

В главе 4.9 мы составили план профилактических работ на предприятии ПАО «Сбербанк».

План проведения профилактических и технических работ				
№ п/п	Машины для проведения работ	Наименование работ	Ответственный за выполнение	Период выполнения работ
1	PC0 – PC7; Server0, Server1.	Очистка корпуса и внутренних компонентов.	Технический специалист отдела автоматизации.	1 раз в месяц.
2	PC0 – PC7; Server0, Server1.	Обновление программной части рабочих станций.	Системный администратор отдела автоматизации.	По мере поступления обновлений.
3	PC0 – PC7; Server0, Server1.	Обновление аппаратной части рабочих станций.	Технический специалист отдела автоматизации.	По необходимости: при недостатке аппаратных мощностей: не чаще 1 раза в год.
4	PC0 – PC7; Server0, Server1; пассивное сетевое оборудование (кабели, розетки и т.д.).	Проверка работоспособности аппаратной части отдела автоматизации.	Технический специалист отдела автоматизации.	1 раз в месяц.
5	PC0 – PC7; Server0, Server1.	Проверка работоспособности программной части рабочих станций.	Системный администратор отдела автоматизации.	1 раз в месяц.



Расчётно-экономическая часть

Расчёт общей сметы стоимости проекта

№ п/п	Наименование	Стоимость руб.
1	Стоимость работ по монтажу КС	17 547
2	Стоимость работ по администрированию КС	11 550
3	Стоимость работ по обеспечению безопасности КС	26 000
Итоговая стоимость работ:		55 097
4	Общая стоимость программного обеспечения	47 937
5	Общая стоимость аппаратных средств	81 040,40
6	Общая стоимость материалов	19968,60
Итоговая стоимость проекта:		204 043



Заключение

В результате проделанной работы, был спроектирован работоспособный проект компьютерной сети, было выполнено сетевое администрирование и была организована безопасность в компьютерной сети на предприятии ПАО “Сбербанк” в отделе автоматизации.

Спасибо за внимание!