Технический департамент WSR

Москва, 16 декабря 2015

Конкурсное задание

Компетенция

«Сетевое и системное администрирование»

Конкурсное задание включает в себя следующие разделы:

1. Введение
2. Формы участия в конкурсе
3. Модули задания и необходимое время
4. Критерии оценки
5. Конкурсное задание
6. Приложения (1-9)

Количество часов на выполнение задания: 15 ч.

Разработано экспертами WSR :
Фер С.В.
Лотош Е.В.
Фучко М.М.
Горбачев А.П.
Щербинин А.А.
Овсянников С.В.

Введение

Название профессиональной компетенции: Сетевое и системное администрирование.

Описание профессиональной компетенции.

Сетевое и системное администрирование требует широких познаний в области информационных технологий. В связи с быстрым развитием этой области, требования к администраторам постоянно возрастают.

Системный и сетевой администратор (инженер) должен уметь:

- Разрабатывать и развертывать комплексную информационную инфраструктуру предприятий, включающую рабочие станции, серверы и сетевое оборудование, сетевое оборудование
- Развертывать основные сервисы, включая службы каталогов, резервного копирования, почтовые и другие прикладные сервисы.
- Использовать широкий набор операционных систем и серверного ПО
- Эффективно организовывать защищенные соединения сетей предприятий, доступ в Интернет и иные сети
- Устанавливать и настраивать устройства беспроводной сети, коммутаторы, маршрутизаторы и средства защиты информации
- Организовывать защиту информации от несанкционированного доступа
- Разрабатывать документацию информационной структуры предприятия
- Устанавливать, настраивать и отлаживать программные и аппаратные средства VoIP
- Устанавливать и настраивать сетевые сервисы на базе протоколов IPv4 и IPv6
- Устанавливать, настраивать и поддерживать виртуальные среды
- Осуществлять поиск и устранение неисправностей в работе информационных систем и сетей

Область применения задания

Каждый Эксперт и Участник обязан ознакомиться с данным Конкурсным заданием.

Данное задание рекомендовано для подготовки региональных чемпионатов, финалов чемпионатов по федеральным округам, а также для подготовки участников к Национальному чемпионату WSR 2016г.

Сопроводительная документация

Поскольку данное Конкурсное задание содержит лишь информацию, относящуюся к соответствующей профессиональной компетенции, его необходимо использовать совместно со следующими документами:

- «WorldSkills Russia», Техническое описание по компетенции Сетевое и системное администрирование;
- «WorldSkills Russia», Правила проведения чемпионата
- Принимающая сторона – Правила техники безопасности и санитарные нормы.

Форма участия в конкурсе

Индивидуальный конкурс.

Модули задания и необходимое время

Модули и время сведены в таблице 1

Таблица 1.

№ п/п	Наименование модуля	Рабочее время	Время на задание
1	Модуль 1: День 1. Сетевые технологии	С1 09.00-12.00 С1 13.00-15.00	3 часа 2 часа
2	Модуль 2: День 2. Работа с ОС Microsoft Windows	С1 09.00-12.00 С1 13.00-15.00	3 часа 2 часа
3	Модуль 3: День 3. Работа с ОС Linux CentOS	С1 09.00-12.00 С1 13.00-15.00	3 часа 2 часа

Критерии оценки

В данном разделе определены критерии оценки и количество начисляемых баллов (субъективные и объективные) таблица 2. Общее количество баллов задания/модуля по всем критериям оценки составляет 100.

Таблица 2.

Раздел	Критерий	Оценки		
		Субъективная (в режиме судейства)	Объективная	Общая
A	Модуль 1: День 1. Сетевые технологии	3	31	34
B	Модуль 2: День 2. Работа с ОС Microsoft Windows	0	33	33

C	Модуль 3: День 3. Работа с ОС Linux CentOS	0	33	33
Итого =		0	100	100

Субъективная оценка относится к выполнению участником задания, связанного с ведением технической документации и планированием работ. Субъективная оценка выполняется в режиме судейства (Judgment), где судьи выставляют свои оценки исходя из следующих соображений:

0 - нечего оценивать. Документ отсутствует или не является реализуемой (содержит грубые ошибки).

1 - Документ не конкретен, может трактоваться различными способами, допускает разные варианты реализации.

2 - Документ однозначен и реализуем, но содержит недочеты.

3 - Все выполнено идеально.

Конкурсное задание

Общая информация

Позвольте представиться, мой новый коллега: я начальник ИТ-департамента успешной финансовой корпорации «ЦИС и Ко Финанс», куда вы только что устроились на должность главного системного администратора. Благодаря соблюдению правил регуляторов и собственным строгим внутренним правилам, в кризисное время наша компания сохраняет стабильность, о чем свидетельствует ваша немалая зарплата. К сожалению, ваш коллега, создававший ИТ-инфраструктуру, находится в длительной командировке и еще не успел ввести вас в курс всех дел. Однако благодаря вашей высокой квалификации вам должно хватить и тех обрывков информации, что он успел передать.

У меня для вас отличная новость: два конкурирующих банка получили крупные неприятности, поскольку вели непродуманную и рискованную финансовую политику. Если точнее, решение насчет них Центробанк уже принял: банки передаются нам на санацию и в ближайшем будущем станут интегральной частью нашей финансовой структуры. Эти банки – «Микрошот Бэнк» и «ПинВин Файненшл» – уже давно являлись стратегической целью нашей компании, и сейчас «ЦИС и Ко Финанс» имеет уникальную возможность получить контроль над активами и клиентами этих банков.

Для успешной санации обоих банков необходимо как минимум обеспечить слияние ИТ-инфраструктур и взаимодействие на уровне базовых сервисов. К сожалению, оба банка проводили политику тотальной экономии и мало вкладывались в развитие и поддержание ИТ, поэтому рассчитывать на готовность их инфраструктур к таким изменениям не приходится.

Сейчас каждый час на счету, а потому наше руководство требует, чтобы через три дня все задачи по объединению ИТ-систем банков были выполнены. Общая ситуация такова:

1. Вы должны строго следовать действующим правилам и регламентам своей компании, зафиксированным в Политике корпорации в области информационных технологий и защиты информации (Приложение 1), далее по тексту просто «Политике».
2. Тотальная экономия на оборудовании в подключаемых банках и сжатые сроки привели к тому, что у вас нет большого запаса оборудования для проведения работ. Все, что у вас есть в резерве, это:
   - Один межсетевой экран Cisco ASA 5505
   - Один коммутатор Cisco Catalyst 2960
   - Один ноутбук
   - Один IP-телефон Cisco 7900

   Прочее оборудование вы, конечно, также можете использовать, но имейте в виду, что оно входит в состав действующей инфраструктуры корпорации, и у вас нет права менять ее логику работы. В каждом банке необходимо настроить VPN-шлюз и подключение к сети IP-телефонии. Маршрутизатор ***R2*** уже подключен к сети корпорации, но пока еще не настроен, переносить его куда-либо еще нельзя, решение об этом принято довольно давно.
3. Наши партнеры из компании-оператора «Босс-телеком» выполнили предварительную настройку своей сети и готовы предоставить каналы связи между офисами банков. Технические условия на подключение приведены в Приложении 8.
4. К сожалению, вынужденная спешка в подготовке к работам привела к тому, что некоторые сетевые настройки были выполнены некорректно. Обнаруженные ошибки исправлены, но сложно сказать, какие еще неточности остались незамеченными. Обращайте на это внимание. Возможно, что-то в существующих конфигурациях придется исправлять.

5. Имейте в виду, что все три банка являются действующими, перерывы в обслуживании клиентов должны быть минимизированы. Вам известно, что сервисы «ЦИС и Ко» должны быть доступны постоянно, «Микрошот Бэнк» может по согласованию быстро переключиться на резервную площадку, а в банке «ПинВин Файненшл» работы, связанные с простоем сетевых сервисов, могут проводиться только по окончании рабочего дня (т.е. по завершении всех остальных работ, которые вы запланировали на этот день). Если вы предполагаете выполнение работ, связанных с отключением каких-либо сервисов, вам необходимо согласовывать время и длительность проведения этих работ и обязательно включать их в план.

Мы с вашим коллегой уже нарисовали эскизную схему будущей сети (Приложение 7), но в нее еще нужно внести ряд деталей и решить, какое оборудование и как будет использоваться.

День 1. Сетевые технологии

Сегодня вам предстоит много работы. Сначала необходимо внести некоторые изменения в инфраструктуру собственной сети, затем – обследовать сети присоединяемых банков и принять окончательное решение о будущем дизайне единой сети и использовании имеющегося в вашем распоряжении резервного оборудования. В конце – выполнить работы в офисах банков «Микрошот Бэнк» и «ПинВин Файненшл».

Ваши решения должны быть отражены в документации в виде схем, таблиц и планов и одобрены мной. Я все еще не имел возможность убедиться в вашей реальной квалификации (да-да, ваше резюме очень красивое, но резюме и жизнь – несколько разные вещи), а потому стану очень внимательно следить за всем ходом работ. Изменить принятые и утвержденные решения позднее будет невозможно, поэтому перед началом работы **ПРОЧИТАЙТЕ ВСЕ ЗАДАНИЯ, ИЗУЧИТЕ ТЕКУЩИЕ НАСТРОЙКИ ОБОРУДОВАНИЯ, НЕ ИЗМЕНЯЯ ИХ,** и подготовьте необходимые документы.

1. Используя предоставленные документы, формы и схемы, подготовьте следующие материалы в том виде, в котором они представляются вам по окончании всех работ
   - Таблицу соединений и подключений портов оборудования (Приложение 3)
   - Схему сетевого уровня в объединенной сети (Приложение 7)
2. Вы должны представить мне на утверждение План работ, которые предполагаете выполнить в течение сегодняшнего дня (форма плана находится в Приложении 2).
3. По правилам нашей корпорации я должен поставить резолюцию на вашем плане работ, прежде чем вы приступите к выполнению настроек. С этого момента все ваши действия регулируются планами, схемами, политиками, регламентами и техническими условиями. Ни в коем случае не нарушайте их, или вам предстоит очень неприятный разговор со мной. Вам запрещается:
   - Удалять существующие и добавлять новые VLAN, если этого явно не требует план работ
   - Удалять и добавлять новые статические маршруты, если это явно не разрешено
   - Изменять режимы работы протоколов STP и VTP
   - Удалять или снимать с интерфейсов списки контроля доступа. Однако вы можете их редактировать

После получения одобрения вам необходимо выполнить ряд подготовительных операций и настроить связь между сетями банков в соответствии с собственной политикой нашей корпорации и техническими условиями оператора связи. Кроме того, прошу провести ряд работ по оптимизации внутренней сети корпорации, используя выделенные вам временн***ы***е окна для проведения работ.

4. На сервере NMS запущено прикладное ПО, выполняющее функции TFTP-сервера и syslog-сервера. Выполните резервное копирование конфигураций сетевого оборудования и баз данных VLAN коммутаторов корпоративной сети на TFTP-сервер, запущенный на сервере ***NMS***. Используйте имена файлов в формате *<ИМЯ УСТРОЙСТВА>-<ТЕКУЩЕЕ ВРЕМЯ>.cfg* (например, ***R1-10.05.cfg***) и *<ИМЯ УСТРОЙСТВА>-VLAN.dat* (например, ***SW2-VLAN.dat***). По завершении работ всего дня не забудьте повторить процедуру для всех сетевых устройств. В конце дня у вас должны быть сохранены конфигурации всех сетевых устройств, подключенных к сети, и базы VLAN коммутаторов SW1 и SW2. Сохранять копии конфигураций оборудования, не подключенного к сети, не требуется. Сохраняйте файлы в папку ***C:\TFTP***. При совпадении имен файлы должны перезаписываться.
5. В соответствии с Политикой, все сетевые устройства Cisco в вашей сети должны отсылать журнальные сообщения с критичностью большей или равной 5 (Informational) на syslog-сервер. Локально на

устройствах хранятся сообщения с критичностью 3 (Error) и выше. Убедитесь, что эти политики соблюдены на всех устройствах, включая те, что вы планируете подключать к сети.

6. Сетевое оборудование (коммутаторы, маршрутизаторы и межсетевые экраны) Cisco, подключенное к сети, должно синхронизировать свои часы по времени контроллера домена ***New-DC*** и находиться в правильной временной зоне (GMT+3). Убедитесь, что это так, особенно, по окончании работ сегодняшнего дня.

Между коммутаторами ***SW1*** и ***SW2*** в текущей конфигурации присутствует три параллельных канала связи, которые используются не очень эффективно. Ваша задача – изменить конфигурации коммутаторов, чтобы добиться описанных ниже результатов.

К счастью, ***SW2***, как и весь ***VLAN 10***, обслуживает только ваше собственное подключение, поэтому вы можете проводить работы в любое время, но все равно – будьте осторожны. Сервисы банка пострадать не должны! При выполнении работ не изменяйте настройки порта F0/22 коммутатора SW2.

7. Порты ***F0/23*** и ***F0/24*** коммутаторов должны быть объединены в агрегированный канал с номером ***Port-Channel 1***. Используйте динамический протокол согласования, соответствующий стандарту IEEE 802.3ad.
8. Все каналы связи ***F0/22-24*** должны быть переведены в транковый режим работы, соответствующий стандарту IEEE 802.1Q.
9. Трафик всех VLAN, существующих в сети, при передаче между коммутаторами ***SW1*** и ***SW2*** должен передаваться через ***Port-Channel 1***, за исключением трафика ***VLAN 10***, который должен передаваться через порт ***F0/22***. В случае обрыва связи на порту ***F0/22*** трафик ***Admin PC*** должен быть переключен на ***Port-Channel 1*** не более, чем за 5 секунд.

Маршрутизатор ***R2*** предполагалось использовать как IP-телефонную станцию и резервный маршрутизатор для подключения внутренних сегментов сети. Прежде чем использовать ***R2*** в качестве шлюза для связи с офисами банков, необходимо настроить все запланированные ранее функции.

10. Маршрутизатор ***R2*** подключен к коммутатору ***SW1*** двумя портами, как и ***R1***. В сторону маршрутизаторов должен передаваться трафик только тех VLAN, которые терминируются на его интерфейсах и подинтерфейсах. Используйте интерфейсы ***F0/0*** маршрутизаторов исключительно для связи их между собой, в частности, для обмена анонсами по протоколу OSPF. На коммутаторе ***SW1*** для этого должен быть создан ***VLAN 12***.
11. Настройте на ***R1*** и ***R2*** IP-адресацию в соответствии с утвержденной схемой сетевого уровня.
12. Маршрутизаторы ***R1*** и ***R2*** должны обеспечивать взаимное резервирование при подключении серверов в ***VLAN 20***. Все необходимые настройки на ***R1*** уже выполнены. Проведите настройки на ***R2*** так, чтобы в штатной ситуации в паре ***R1***-***R2*** на все ARP-запросы отвечал ***R2***.
13. Маршрутизаторы ***R1*** и ***R2*** должны обеспечивать взаимное резервирование при подключении пользователей в ***VLAN 10***. ***R1*** должен являться основным шлюзом по умолчанию, ***R2*** – резервным, который берет на себя функции шлюза по умолчанию только в случае, когда ***R1*** недоступен. Используйте протокол HSRP версии ***2***, номер группы – ***12*** и ключ аутентификации ***CISCO***.
    Убедитесь, что после выполнения работ рабочие станции в ***VLAN 10*** сохраняют связь с серверами сети даже в случае, когда маршрутизатор ***R1*** недоступен. Изменять настройки шлюза по умолчанию на рабочих станциях не разрешается.
14. Между маршрутизаторами ***R1*** и ***R2*** в ***VLAN 12*** настройте обмен маршрутными анонсами по протоколу OSPF в соответствии с Политикой в области ИТ. ***R1*** и ***R2*** должны обмениваться префиксами сетей

своих интерфейсов ***Loopback 0***. На интерфейсах, соответствующих VLAN 10, 20 и 101 протокол OSPF должен быть выключен .

15. Запустите на ***R2*** сервис IP-телефонии. В качестве тестового аппарата подключите к телефонной сети софтфон Cisco IP Communicator, дистрибутив которого есть в вашем комплекте ПО. Софтфон должен зарегистрироваться и получить номер ***10001***.

После того как закончите с нашей сетью, переходите к сети банка «Микрошот Бэнк», где вас ожидает много сюрпризов. Банк предпочитал не иметь собственной ИТ-инфраструктуры, а арендовать у оператора «Босс-Телеком» вычислительные мощности и каналы связи. Поэтому в офисе банка расположены почти исключительно рабочие места сотрудников, а все сервисы размещены на площадке оператора. Оператор несет полную ответственность за настройку и корректную работу сетевой инфраструктуры банка. Поэтому у вас нет доступа к граничному маршрутизатору сети «Микрошот Бэнк», но вам известны его настройки и схема подключения.

Чтобы вы могли спокойно выполнять свои работы, сегодня банковские процессы в «Микрошот Бэнк» переведены на резервную площадку. Однако в конце дня будет произведено обратное переключение. К этому моменту вы должны закончить свою часть работ. Также я ожидаю, что в конце дня вашими силами будет установлена внутренняя телефонная связь по защищенному каналу с банком «Микрошот Бэнк».

Граничный маршрутизатор офиса «Микрошот Бэнк» уже настроен вашими партнерами из «Босс-телекома» под те задачи, которые вам предстоит решить. Его конфигурация у вас есть (Приложение 9), но вносить в нее изменения вы не можете, поскольку это требует длительного согласования и времени, которого у вас нет.

16. Обеспечьте подключение сети корпорации «ЦИС и Ко Финанс» к VPN-сегменту оператора «Босс-телеком» с учетом Технических условий. Терминируйте выданный оператором PVC на роутере ***R2***, используя настройки, соответствующие параметрам ТУ.
17. Установите в сети «Микрошот Бэнк» оборудование, которое вы запланировали использовать, и подключите его в соответствии с утвержденной таблицей соединений.
18. Настройте параметры IP на ***VPN-шлюзе*** в соответствии с выданными техническими условиями оператора и утвержденной схемой сетевого уровня. Настраивать какие-либо функции сетевой безопасности на ***VPN-шлюзе*** не требуется (хотя, конечно, не возбраняется), он будет использоваться как обычный маршрутизатор.

Предварительное обследование выявило еще одну проблему. В сети банка «Микрошот Бэнк» используются адреса из диапазона ***10.0.0.0/16***, который зарезервирован для сети нашей корпорации. Сервер ***WWW*** имеет адрес, который, к счастью, не используется в нашей сети, но все равно – Политика требует, чтобы префикс ***10.0.0.0/16*** анонсировался только из сети «ЦИС & Ко Финанс», а изменять адресацию в «Микрошот Бэнк» мы сейчас не можем – никакого времени не хватит.

19. Между сетями «Микрошот Бэнк» и головным офисом корпорации должна быть настроена маршрутизация по протоколу OSPF, соответствующая техническим условиям оператора. Маршрутизатор ***R2*** должен передавать в сеть «Микрошот Бэнк» только анонсы агрегированного префикса ***10.0.0.0/16***. Граничный маршрутизатор сети «Микрошот Бэнк» уже настроен партнерами из «Босс-телекома» и готов к подключению в OSPF-домен через VLAN 100.
20. Настройте на ***VPN-шлюзе*** NAT-трансляцию так, чтобы сервер ***WWW*** банка «Микрошот Бэнк» был доступен из сети нашей корпорации по адресу ***10.1.0.100***. Менять настройки на сервере запрещено, но можно использовать статическую маршрутизацию на ***VPN-шлюзе***.
21. Между маршрутизатором ***R2*** и ***VPN-шлюзом*** банка «Микрошот Бэнк» должен быть настроен статический IPSec-туннель. Параметры защиты данных описаны в Политике информационной

безопасности корпорации. Этот туннель должен защищать весь трафик системы IP-телефонии. Прочий трафик защищать не обязательно.

Последний шаг: нужно обеспечить работу IP-телефонии. Необходимое оборудование у вас имеется, но его нужно включить и настроить.

22. Обеспечьте подключение нового оборудования в соответствии с утвержденной таблицей соединений и подключений. Настройте ***VPN-шлюз*** так, чтобы все необходимые параметры для работы телефонии выдавались устройству динамически по протоколу DHCP.
23. Настройте маршрутизатор ***R2*** так, чтобы новое устройство могло зарегистрироваться в системе телефонии с номером ***10101***. Убедитесь, что звонок на номер ***10001*** проходит в обе стороны и обе стороны слышат друг друга.
24. Настройте кнопку второй линии телефона так, чтобы при нажатии на нее происходил автоматический вызов номера ***10001***.

С руководством «ПинВин Файненшл» согласовано кратковременное отключение сети банка от Интернета в конце рабочего дня. О начале работ (т.е. об отключении) вы должны уведомить меня. У вас будет только двадцать минут, чтобы выполнить переключение и проверить результат, поэтому все действия вы должны спланировать заранее. Имейте в виду, что скоро в этот офис переедет несколько сотрудников вашей корпорации, так что им понадобится телефонная связь.

25. Изучите конфигурацию сервера, который выполняет функцию маршрутизатора в офисе «ПинВин Файненшл». Выполните все необходимые настройки для того, чтобы подключить его к VPN-сегменту, предоставляемому «БОСС-Телекомом», в соответствии с Техническими Условиями. Маршрутизатор должен установить соединение по протоколу OSPF и проанонсировать в сеть оператора используемые префиксы из диапазона 10.2.0.0/16. Настраивать IPSec-туннель с центральным офисом сейчас не требуется, это вы выполните в другой раз. Зато надо добиться, чтобы в будущем при подключении дополнительных телефонных аппаратов в сеть офиса от нее не потребовалось отключать какое-либо оборудование.

День 2. Работа с ОС Microsoft Windows

Доброе утро, коллега. Судя по всему, первый день на боевом дежурстве выдался нелегким. Хотя настройка сетевого оборудования уже позади, радости мало: работы впереди все еще непочатый край. Сеть служит лишь базой для предоставления сервисов пользователям, и с этими сервисами вам предстоит повозиться.

Ключевыми задачами, решаемыми любой инфраструктурой, является контролируемый доступ пользователей к данным. Я уже успел немного проанализировать инфраструктуру двух новых компаний, а заодно заново взглянуть на свою собственную. Даже беглый взгляд обнаруживает множество проблем, требующих срочного решения.

Вот что мне известно о всех трех инфраструктурах:

1) Центральный офис компании «ЦИС и Ко Финанс»

В офисе функционирует домен Active Directory (AD) под названием ***kiska.ru.*** Операционная система на единственном контроллере домена (КД) с именем ***New-DC*** – Windows Server 2012 R2. Когда-то в домене присутствовал и второй контроллер домена ***Cool-DC***, но в один прекрасный день этот КД полностью вышел из строя из-за внезапного сбоя жесткого диска с утратой как пользовательских файлов, так и локальной копии баз AD. Выводы были сделаны, и теперь пользовательские файлы, хранящиеся на контроллере домена, регулярно сохраняются с помощью системы резервного копирования (до которой вам пока дела нет – и без того проблем хватает).

2) Компания «Микрошот Бэнк»

В офисе отсутствует домен AD. Пользователи хранят файлы на сервере с именем ***FS*** под управлением Windows Server 2012 R2 (папка ***d:\files*** с сетевым именем ***\\FS\files***), но доступ к нему осуществляется с помощью одной локально заведенной на сервере учетной записи пользователя с именем ***ServUsr*** и паролем ***12345***, используемой всеми пользователями. Индивидуальный контроль доступа пользователей к данным и сервисам отсутствует в принципе. DNS-имена на станциях разрешаются через DNS-серверы в Интернете. Соответствие имени сервера ***FS*** его IP-адресу прописано в файле *hosts* на каждом ПК. Резервные копии данных на сервере не делаются. Всего в офисе работает 50 пользователей, каждый входит на свой персональный компьютер без пароля с реквизитами учетной записи ***User*** с административными правами. На всех компьютерах используется статическая адресация. Один из компьютеров под управлением Windows 8.1 сейчас не используется и доступен вам для экспериментов.

3) Компания «ПинВин Файненшл»

Здесь все не так плохо, как в «Микрошот Бэнк». В офисе функционирует домен Active Directory под названием ***pinwin.ru.*** Операционная система на единственном КД с именем ***Server01*** установлена устаревшая – Windows Server 2008 R2. Данные защищаются нормально работающей системой резервного копирования. В домене обнаружился еще один сервер ***GoodSRV*** на базе Windows Server 2012 R2, ранее предназначавшийся на роль нового КД, но системный администратор банка так и не довел дело до конца. Сейчас на ***GoodSRV*** не поднято ни одной роли, и сейчас он не занимается обслуживанием пользователей. В целом состояние ИТ-инфраструктуры – средней тяжести. Главная проблем в том, что здесь работает очень много устаревших компьютеров, с трудом справляющихся или не справляющихся вообще с запуском современных приложений.

Внимательно посмотрев на серверную инфраструктуру всех трех офисов, я понял, что обмен данными и доступ к ним при нынешних настройках крайне затруднен. С учетом большого количества пользователей в каждом офисе перед вами, коллега, встает большая задача: необходимо модифицировать существующие домены Active Directory, обеспечить резервное копирование файлов в офисе «Микрошот Бэнк», а также каким-то образом справиться с нехваткой производительности рабочих станций.

Сегодня у меня большое совещание с директором нашего банка, которое затянется на весь день, а потому я не могу заранее оценивать ваши планы. Однако я намерен проконтролировать ваши действия постфактум, а потому **вы обязаны фиксировать ВСЕ** свои действия: изменение системных настроек и конфигурационных файлов, тексты скриптов, выполненные процедуры (кратко, если выполняется стандартный мастер со стандартными настройками) и так далее в журнале выполненных работ. Форму журнала для серверной инфраструктуры вы найдете в приложении 2. По окончании работ журнал должен быть передан мне. Если какое-то ваше действие не описано в журнале, будет сложно понять, какие изменения произошли в системе, и все ли сделано верно, так что постарайтесь вести детальный учет своих работ.

Итак, первая большая задача, стоящая перед вами – справиться с проблемами аутентификации в офисе «Микрошот Бэнк». Полагаю, для этого вам следует сделать локальный файл-сервер вторым контроллером домена ***kiska.local***. Вам необходимо выполнить следующие предварительные действия:

1. Запустив программу диагностики на ***New-DC***, я обнаружил множественные ошибки, связанные с репликацией AD на сервер ***Cool-DC***. Ваша первая задача – ликвидировать их и добиться полного здоровья домена ***kiska.ru***. Вы также должны убрать все следы ***Cool-DC*** из зоны DNS. Программа диагностики не должна выдавать сообщений об ошибках и важных предупреждений. Сохраните в журнале работ выдачу диагностической программы в отремонтированном домене.
2. Я обнаружил, что при существующей настройке прямой зоны ***kiska.ru*** ее функционирование в распределенной сети не будет оптимальным. Вам необходимо оптимизировать настройки зоны таким образом, чтобы избавиться от разделения DNS-серверов на первичные и вторичные и позволить рабочим станциям регистрировать свои адреса на любом DNS-сервере в лесу AD.
3. Вам также необходимо добиться, чтобы DNS-сервер мог разрешать в имена IP-адреса компьютеров как в главном офисе, так и в офисе «Микрошот Бэнк». Как и на предыдущем шаге, модификация связей между именами и адресами должна осуществляться на любом DNS-сервере в лесу.

Завершив подготовку домена ***kiska.ru***, вы должны создать новый контроллер домена.

4. Введите сервер ***FS*** в офисе «Микрошот Бэнк» в домен ***kiska.ru***.
5. Повысьте роль этого сервера до контроллера домена.
6. Настройте инфраструктуру AD таким образом, чтобы рабочие станции в каждом офисе в первую очередь обращались к контроллеру домена в своем офисе и только при его недоступности – к контроллеру в другом офисе.
7. Дополнительно настройте новый КД ***FS*** таким образом, чтобы минимизировать служебный трафик AD между офисами при поиске информации, относящейся к пользователям.
8. Протестируйте работоспособность AD с помощью стандартной утилиты и поместите в журнал выполненных работ ее вывод в качестве доказательства, что серьезных проблем не имеется.

9. Для отработки процедуры перед ее применением ко всем станциям в офисе «Микрошот Бэнк» введите в домен рабочую станцию в его офисе. Ликвидируйте на ней разрешение имени сервера ***FS*** через файл *hosts* и настройте отказоустойчивое разрешение имен на станциях (с учетом пункта 6).

После завершения создания нового контроллера вам необходимо упростить администрирование рабочих станций.

10. Разверните на КД ***FS*** службу DHCP и настройте ее для выдачи адресов из подсети рабочих станций. Требуемая настройка роутера уже выполнена, вам ее делать не требуется.
11. Переведите тестовую рабочую станцию в режим получения IP-адреса по протоколу DHCP и выполните на DHCP-сервере настройки, позволяющие ей в дальнейшем всегда получать тот же самый адрес.

Все пользователи работают на своих ПК с административными правами, из-за чего у службы техподдержки постоянно возникают проблемы с вирусами и несанкционированными приложениями (торренты, игры, мессенджеры и т.п.) Кроме того, превращение файл-сервера в контроллер домена приведет к тому, что все локальные учетные записи на нем пропадут, и у пользователей больше не будет доступа к данным на нем. Вам необходимо завести для них доменные учетные записи, а заодно и отобрать у них административные права на ПК. К счастью, системный администратор бывшего «Микрошот Бэнк» когда-то думал о том же и успел подготовить CSV-файл, содержащий новые логины и пароли пользователей. Также меня беспокоит отсутствие резервных копий файлов на сервере ***FS***.

Вам необходимо:

12. Сегодня же завести все учетные записи пользователей. Учтите, что у вас нет времени вводить данные вручную, по-отдельности для каждого пользователя, поэтому вы должны завести их с помощью скрипта. Все учетные записи должны быть размещены в контейнере ***MicroOU*** домена ***Kiska.ru*** и быть активными. Каждая учетная запись должна иметь пароль, указанный в CSV-файле. Скопируйте в журнал текст скрипта.
13. Создать группу ***MicroUsers*** и предоставить ее членам права на запись в директорию ***\\fs\files***. Внести все созданные учетные записи в эту группу. При этом доступ в директорию ***d:\files\admins*** (но не в другие поддиректории ***d:\files***) должны иметь полный доступ только члены группы *Domain Admins* и локальная операционная система, всем остальным она не должна быть доступна даже на просмотр.
14. Создать в AD группу ***MicroAdmins***, пользователи в которой автоматически получали бы административные права на все компьютеры в офисе «Микрошот Бэнк» за исключением контроллеров домена.
15. Обеспечить автоматическую двустороннюю репликацию файлов между директорией ***d:\files*** на сервере ***FS*** и директорией ***d:\files\microshot*** на сервере ***New-DC***.
16. Обеспечить автоматическое подключение сетевого диска ***K:*** к файловой директории ***\\fs\fles*** на всех ПК в офисе «Микрошот Бэнк», причем таким способом, чтобы пользователи автоматически переключались на директорию ***d:\files\microshot*** на сервере ***New-DC*** при недоступности сервера ***FS***. Если сервер ***FS*** доступен, пользователи всегда должны подключаться именно к нему.

После завершения работ в «Микрошот Бэнк» займитесь офисом компании «ПинВин Файненшл». Из-за имеющего место цейтнота пока что оставьте существующий там домен ***pinwin.ru*** в неизменном состоянии. Однако задачи совместной работы пользователей всех офисов по-прежнему актуальны, и вы не можете позволить себе заводить лишние учетные записи в обоих доменах. Кроме того, руководство бывшей компании сообщило, что у них возникали проблемы с утечкой конфиденциальной информации к конкурирующей фирме «Злоботрясов и партнеры». Однако так и не удалось установить, явилось ли она следствием взлома учетных записей пользователей посторонними злоумышленниками или же добровольной передачи сведений подкупленными сотрудниками «ПинВин».

Поэтому вам необходимо:

17. Создать в домене ***Pinwin.ru*** группу ***Enhanced Security*** и добиться, чтобы к ее членам применялись гранулярная политика усиленной безопасности, в частности опция повышенной сложности паролей. Эта политика не должна применяться к пользователям, не входящим в данную группу.
18. Блокировать доступ ко всем веб-сайтам компании «Злоботрясов и партнеры» в домене ***zlobny.yh***, за исключением сайта ***www.zlobny.yh***, где сотрудники бывшей «ПинВин Файненшл» сами подсматривают информацию о конкуренте. К сожалению, «Злоботрясов» все время меняет IP-адреса сайтов (кроме сайта **www**, имеющего постоянный IP-адрес ***20.10.0.100***), так что блокировка может быть выполнена только по имени. Блокировка должна быть выполнена централизованно на DNS-сервере, индивидуальные настройки ПК выполняться не должны.
19. Настроить двусторонние доверительные отношения между доменами ***Kiska.ru*** и ***Pinwin.ru***. При этом количество ручных модификаций на DNS-серверах в обоих доменах должно быть минимизировано, новые серверы DNS, если таковые появятся, должны получать соответствующие настройки автоматически.
20. Создать в домене ***Pinwin.ru*** группу ***PinwinMicroAccess*** и предоставить ей права на чтение и запись в директории ***d:\files\pinwin*** на сервере ***FS*** в офисе «Микрошот Бэнк». Настроить на всех ПК в офисе «ПинВин Файненшл» автоматическое подключение этой директории как диска ***T:***

Ну и под занавес еще одна плохая новость: отдохнуть не удастся. Руководство нашей корпорации настаивает, что для всех сотрудников, в том числе в бывшей компании «Пинвин Файненшл», обязательно использование программного обеспечения ***Wordpad*** для обработки документов. К сожалению, у некоторых сотрудников «ПинВин» настолько слабые ПК, что на них толком не работает даже эта простая программа. Поскольку затраты на санацию конкурентов и без того очень высоки, закупка новых ПК в ближайшее время не планируется, но указание начальства должно быть выполнено. Сервер ***GoodSRV*** в офисе «ПинВина» развернут, но не используется, и при этом обладает неплохими аппаратными характеристиками. Однако при его работе наблюдаются странные проблемы, подробно исследовать которые у меня не было времени.

Вам необходимо:

21. Выяснить и ликвидировать причину, по которой сервер ***GoodSrv*** хаотично и непредсказуемо теряет доступ к домену ***Pinwin.ru***.
22. Превратить сервер ***GoodSRV*** в терминальный сервер с доступом всех пользователей домена к опубликованному приложению ***Wordpad***. Закупка терминальных лицензий будет выполнена позже, до тех пор сервер должен функционировать в пробном режиме.
23. Пользователи должны получать доступ к приложениям, опубликованным на сервере, через веб-интерфейс. Правильный адрес для доступа к веб-интерфейсу – ***https://goodsrv.pinwinm.ru/RDWeb***, но у большинства пользователей возникают проблемы с его запоминанием. Вы должны изменить

настройки IIS так, чтобы при доступе пользователей к ***http://goodsrv.pinwin.ru*** и ***https://goodsrv.pinwin.ru*** они автоматически перенаправлялись на правильный адрес.

24. Также пользователи должны получать доступ к приложению ***Wordpad*** через RDP-файл, размещенный в файловой директории ***\\GoodSRV\Apps***, связанной с локальной директорией сервера ***c:\apps***. RDP-файл должен быть сгенерирован автоматически, хотя при необходимости вы можете вручную перемещать его между компьютерами и директориями. Пользователи, не обладающие административными правами, не должны иметь возможности модифицировать или удалять файлы в этой директории ни по сети, ни локально при работе на терминальном сервере, но должны иметь возможность читать ее содержимое.

Прежде чем вы начнете переводить пользователей на терминальный режим работы, хочу напомнить об одной типичной проблеме. При небрежной настройке пользователям постоянно приходится подтверждать, что терминальный сервер, с которым они работают, является доверенным. Это смущает некоторых людей настолько, что они не в состоянии нажать вполне очевидную нужную кнопку и начинают звонить в техподдержку. Проблема связана с тем, что терминальный сервер по умолчанию использует самосгенерированный и самоподписанный SSL-сертификат для подписи коммуникаций с клиентом. Покупка сертификата у стороннего центра сертификации (ЦС) нам сейчас не по карману, так что придется использовать свой собственный. При этом я планирую в обозримом будущем полностью вывести домен ***pinwin.ru*** из эксплуатации и не хочу развертывать центр сертификации в нем.

Вам следует:

25. Развернуть доменный центр сертификации на контроллере домена ***New-DC*** в главном офисе. Название центра сертификации должно быть следующим: ***Kiska-Main-CA***.
26. Создать и опубликовать на нем необходимый шаблон SSL-сертификата, назвав его ***TermServSSL***. Срок действия сертификата должен составлять 5 лет.
27. Сгенерировать по этому шаблону SSL-сертификат для сервера ***goodsrv.pinwin.ru*** и экспортировать его в защищенный паролем файл (файл вместе с паролем должен быть передан мне в дополнение к обычной записи в журнале операций).
28. Установить этот сертификат на сервере ***goodsrv.pinwin.ru*** и привязать его как к веб-сайту IIS, так и ко всем необходимым компонентам терминальной инфраструктуры (не менее трех компонентов).
29. Удостовериться, что данный сертификат воспринимается как доверенный на всех компьютерах в домене ***pinwin.ru***. Необходимые модификации должны быть выполнены централизованно. Модификация индивидуальных настроек рабочих станций проводиться не должна – у вас на это нет времени.

После завершения работ убедитесь, что в результате ваших действий вход на веб-интерфейс терминального сервера через веб-браузер, а также запуск RDP-файла не приводят к появлению вопросов, связанных с недоверенным SSL-сертификатом, иначе получится, что вы зря тратили время.

На этом все. В конце дня убедитесь еще раз, что вы задокументировали все свои действия и оставьте на своем рабочем месте журнал выполненных работ и все вспомогательные файлы.

День 3. Работа с ОС Linux CentOS

И снова доброе утро, коллега. Мне искренне вас жаль, но вынужден сообщить, что самое интересное еще впереди. Сегодня вам предстоит сделать завершающий шаг в слиянии трех офисов. Для этого необходимо разобраться с оставшейся информационной инфраструктурой компании «ПинВин Файнэншл».

Вчера после совещания я успел съездить в «ПинВин» и выяснил, что администратор «ПинВин Файненшл» часто использовал свободно распространяемое программное обеспечение, что, безусловно, было следствием политики банка. Настроенные вами контроллер домена и терминальный сервер – единственные windows-серверы в инфраструктуре «ПинВин». Однако кроме них там нашлись еще маршрутизатор, который вы пару дней назад настраивали, и два виртуальных сервера под управлением Linux – настраивать их также предстоит вам. Ну, и IP-телефония тоже за вами (я ведь упоминал на собеседовании, что нам нужен не простой системный администратор, а многорукий Шива, не так ли?)

По обрывочной информации известно, что один из Линукс-серверов является веб-сервером, а другой использовался как тестовая машина с типовой пользовательской конфигурацией. Так же известно, что к консолям серверов обычно можно получить доступ с правами суперпользователя используя пароль “***toor***”.

Первый шаг в вашей работе – чисто косметический:

1. На схемах сети «ПинВин Файненшл», которые имеются в вашем распоряжении, исправьте имена так, чтобы они соответствовали реальным именам серверов.

Так как большое количество сервисов теперь предоставляется из центрального офиса нашей компании, вам в первую очередь необходимо наладить внутреннюю связь между ИТ-инфраструктурами:

2. Организуйте отдельную ВЛВС с номером 10 для трафика IP-телефонии и поместите в него устройство, которое вам согласовали для использования в качестве IP-телефона. Данное устройство должно зарегистрироваться в системе телефонии корпорации с номером ***10201***.
3. Не забывайте о том, что при работе с голосовым трафиком вам необходимо соответствовать требованиям Политики вашей корпорации в области информационных технологий и защиты информации.

Во время моего краткого визита один из сотрудников «ПинВин Файненшл» спросил: «Когда снова будет доступен удаленный доступ в офис?» Ну, по крайней мере, теперь мы знаем, что такой сервис был там реализован. Тем более, что сотрудникам «ЦИС и Ко Финанс» возможность удаленно работать с документами на файловом сервере будет крайне полезной при проведении процедуры санации. В кабинете бывшего системного администратора я обнаружили распечатки статьи с сайта Хабрахабр с примером конфигурации сервиса OpenVPN. Скорее всего, именно этот пакет использовался для предоставления удаленного доступа.

Сделайте следующее:

4. На сервере, выполняющем функцию маршрутизатора, изучите существующую конфигурацию OpenVPN. Устраните неисправности в работе данного сервиса.
5. Для вашего же удобства и удобства ваших сотрудников при удаленном подключении пользователи должны получать доступ к локальным сетям всех трех офисов.
6. Проверьте работу OpenVPN с веб-сервера в офисе «Микрошот».

Тот же самый сотрудник «ПинВин» оказался весьма назойливым. Он привязался ко мне со следующим вопросом: «Я обычно хожу на работу со своим ноутбуком. Тут я купил новый, принес его, подключил сетевой кабель, а Интернета нет. Подключаю старый – Интернет работает». Я уделил несколько минут, чтобы понять проблему поближе, и обнаружил, что на старом ноутбуке настроен статический IP-адрес. Я настроил статический адрес на новом ноутбуке, и все заработало нормально. Однако попытка автоматического получения IP-адреса не сработала.

Нужно разобраться с этой проблемой немедленно.

7. Настройте автоматическую выдачу IP-адресов в локальной подсети офиса. Исключите из диапазона раздачи адреса, присвоенные серверам и маршрутизатору.

Далее вам следует разобраться с веб-сервером. После разговора с местными сотрудниками мне стало известно, что на нем работает Интернет-банкинг. Изучив поверхностно его конфигурацию, я заметил, что данный сервер имеет прямой выход в Интернет, минуя маршрутизатор. С одной стороны, это правильно, поскольку веб-сервер в основном и посещается через Интернет. Однако это обстоятельство и могло стать главной причиной утечки конфиденциальной информации к конкурирующей фирме «Злоботрясов и партнеры».

Поэтому в целях повышения безопасности вам необходимо:

8. Оставить на веб-сервере в рабочем состоянии единственный сетевой интерфейс, подключенный в VLAN20, но сохранить доступ к нему из Интернета по прежнему IP-адресу.
9. Убедиться, что из Интернета к данному серверу можно обращаться только с использованием протоколов HTTP и HTTPS.
10. Настроить аутентификацию пользователей на веб-сервере таким образом, чтобы она требовалась только при доступе из Интернета, но не при входе на сайт из локальных сетей остальных офисов.

После завершения работ необходимо убедиться, что пользователи могут получить к серверу доступ с использованием доменного имени. Кстати, я забыл записать, какое имя имел веб-сервер и какой DNS сервер отвечал за его разрешение. Разберитесь с конфигурацией DNS в данном офисе и, раз уж вы занялись этим вопросом, следует реализовать правильную схему доступа ко всем ключевым серверам по имени.

Удостоверьтесь, что выполняются следующие условия:

11. Доменные имена маршрутизатора и веб-сервера должны разрешаться во внешний адрес для доступа из Интернета.
12. Доменные имена для всех серверов в данном офисе (включая маршрутизатор и веб-сервер) должны разрешаться во внутренний адрес при обращении из внутренней сети.
13. Сайт на веб-сервере должен быть доступен по инмени pinwin.ru.
14. Используя наш шаблон плана производства работ, составьте план, отражающий, каким серверам какие имена будут присвоены, на каком сервере будет располагаться DNS-сервис и какие ресурсы окажутся недоступными в период проведения работ.
15. Приступить к выполнению этой части работ вы можете только после получения от меня одобрения вашего плана.

Движемся дальше. Простите меня за трюизм, но безопасность должна быть безопасной. Так как у нас в центральном офисе теперь функционирует центр сертификации, следует воспользоваться этим.

16. На доменном центре сертификации ***Kiska-Main-CA*** сгенерируйте сертификат для веб-сервера «ПинВин Файненшл» и используйте его для доступа к сайту Интернет-банкинга по протоколу HTTPS.
17. Убедитесь в том, что при обращении к сайту Интернет-банкинга по протоколу HTTP происходит автоматическое перенаправление веб-броузера на тот же адрес, но с использованием протокола HTTPS.
18. Убедитесь, что парольные политики на веб-серверах соответствуют Политике корпорации, и, кстати, проверьте веб-сервер в «Микрошот Бэнк» – а вдруг и там надо ужесточить политику?

Ну вот и все… Спасибо за работу, теперь можете отдохнуть! Хотя… наверняка ведь завтра будет куча звонков от пользователей, у которых чего-то не работает. Готовьтесь – кто как не вы будет им помогать!

Приложение 1. Политика корпорации «ЦИС и Ко Финанс» в области информационных технологий и защиты информации

1. Вся информация, хранимая, передаваемая и обрабатываемая с использованием вычислительных средств корпорации «ЦИС и Ко Финанс», является собственностью корпорации. Руководство компании имеет неограниченный доступ к информации. Доступ прочих сотрудников к информации определяется действующими регламентами и распоряжениями руководства.
2. В корпоративной сети используется диапазон адресов 10.0.0.0/16. Все устройства в сети, если это не указано явно, должны иметь адреса из указанного диапазона. Каждое подразделение должно иметь собственный диапазон адресов с маской 255.255.255.0. Транзитные сети (предназначенные для обеспечения связи между маршрутизаторами) должны иметь адреса из диапазона 10.0.255.128/25 и максимальную длину маски, достаточную для обеспечения связи. Использование маски /31 категорически запрещено, использование маски /32 допускается только для адресации Loopback-интерфейсов.
3. Все маршрутизаторы должны иметь интерфейс Loopback 0 с адресом в формате 10.0.255.z/32 из диапазона 10.0.255.0/25. Выделение адресов производится по возрастанию.
4. Все сетевые устройства должны синхронизировать свои часы с часами контроллера домена. Журнальная информация с сетевых устройств должна передаваться на специализированный syslog-сервер. Перед проведением работ, связанных с изменением конфигураций, критическая информация должна быть сохранена на TFTP-сервер. По окончании работ финальные конфигурации также должны сохраняться.
5. Для подключения к сети Интернет используется диапазон адресов 20.15.0.0/24, выделенный корпорации европейским регистром RIPE и закрепленный за номером автономной системы AS 2015.
6. Граничные маршрутизаторы AS 2015 должны принимать из сети Интернет только и исключительно маршрут по умолчанию (префикс 0.0.0.0/0), прочие префиксы должны фильтроваться.
7. Для организации связи между подразделениями корпорации используются выделенные каналы связи и сервисы L2/L3 VPN. Использование Интернета и иных публичных сетей для организации связи между подразделениями категорически запрещено.
8. Телефонная связь внутри корпорации осуществляется по технологиям IP-телефонии. Звонки между филиалами и центральным офисом в обязательном порядке должны шифроваться.
9. Шифрование телефонных звонков между филиалами, а также шифрование всего прочего трафика не обязательно, но допускается.
10. При использовании шифрования трафика применяются IPSec-туннели со следующими характеристиками:
    - Аутентификация – по общему ключу
    - Шифрование – 3DES или более стойкое
    - Контроль целостности – SHA1 или более стойкий
11. Функции криптошлюза в головном офисе корпорации должны быть вынесены на отдельный маршрутизатор. Совмещение функций граничного маршрутизатора сети Интернет и криптошлюза категорически запрещено.
12. Допускается совмещение функций IP-телефонного шлюза и криптошлюза на одном устройстве.
13. Внутри сети корпорации используется протокол динамической маршрутизации OSPF. Сеть головного офиса включается в Backbone Area (Area 0).
14. Удаленный доступ к интерфейсам управления разрешается только в случае использования защищенных протоколов передачи данных, поддерживающих как аутентификацию, так и шифрование данных.
15. Доступ к корпоративным ресурсам разрешен только с использованием рабочих станций, где предварительно выполнена авторизация с использованием централизованной службы каталогов.

16. Для всех используемых веб-серверов на платформе ОС Linux должна соблюдаться следующая парольная политика:
    - пароль должен состоять из символов принадлежащих как минимум трем множествам (например, верхний и нижний регистр, цифры);
    - длина пароля не должна быть меньше 8 символов;
    - рядовой пользователь не может создать пароль, противоречащий заданным правилам; администратор может, но должен получать предупреждение;
    - пользователи не должны входить в системную консоль как администраторы, но должны иметь возможность переключаться в контекст суперпользователя, используя команду su;

Приложение 2. Типовые формы заявок и журналов

Утверждаю:

Зам. директора по ИТ

_____ Цискин С.С.

«____»_____ 2015г.

Заявка на модернизацию сетевой инфраструктуры

№ п.п.	Наименование работы	Длительность работ	Недоступные сервисы
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

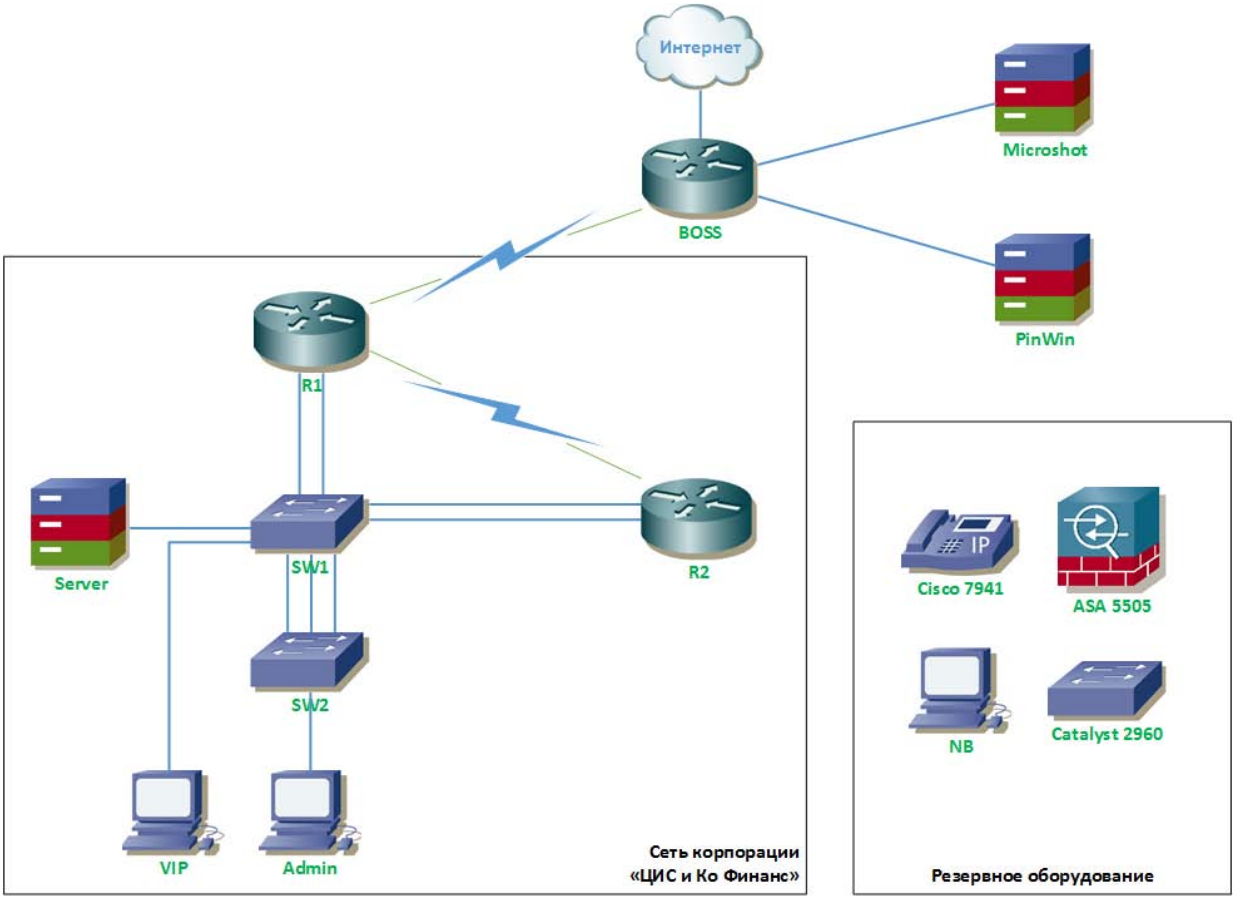
* Количество пунктов может быть увеличено при необходимости

Журнал проведения работ в серверной инфраструктуре

№ задания	Описание работ и изменений настроек
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	

* Количество пунктов может быть увеличено при необходимости

Приложение 3. Схема соединений и подключений (физический уровень)



Приложение 4. Таблица соединений и подключений

Корпорация "ЦИС и Ко Финанс"

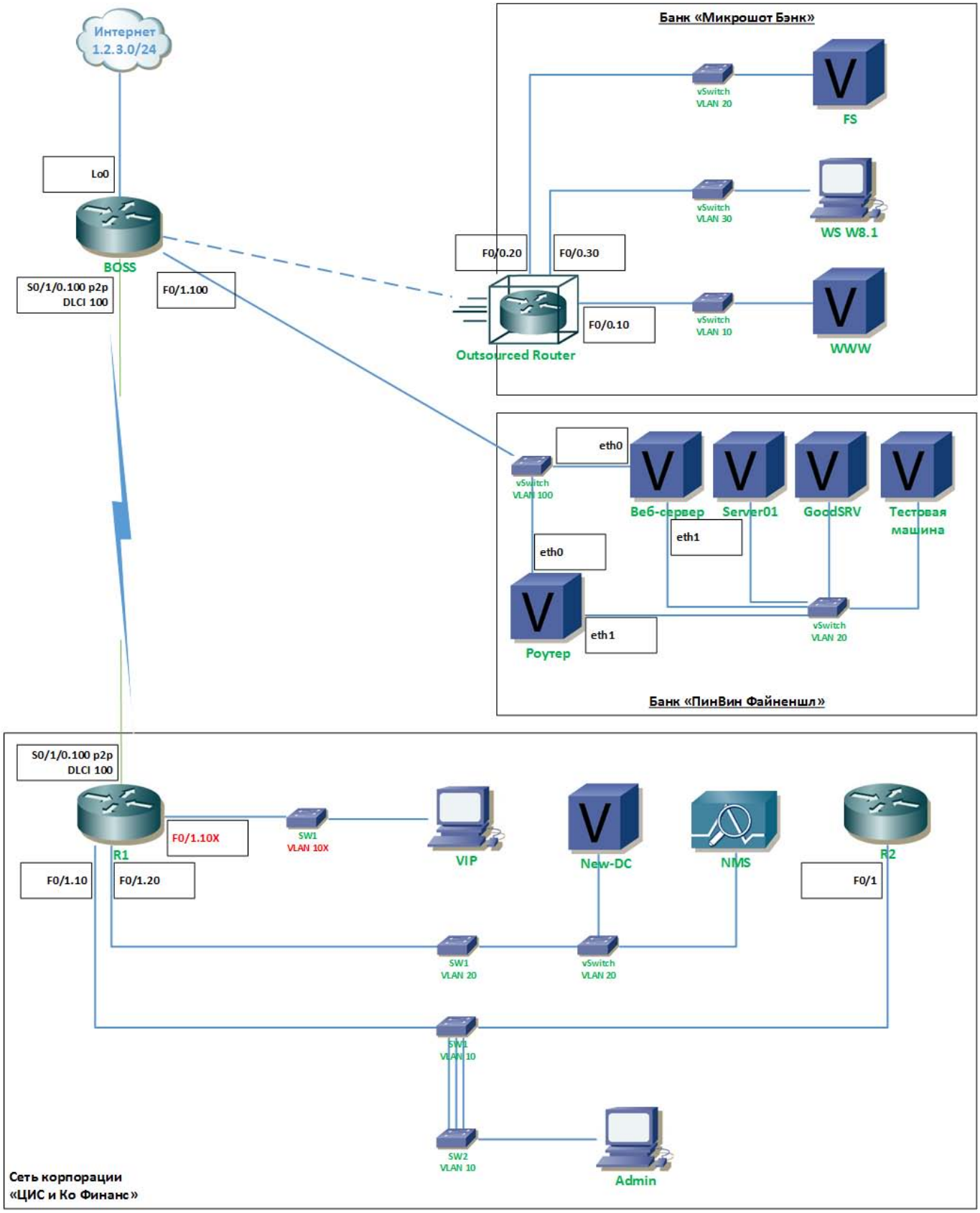
Таблица соединений и подключений

Утверждаю

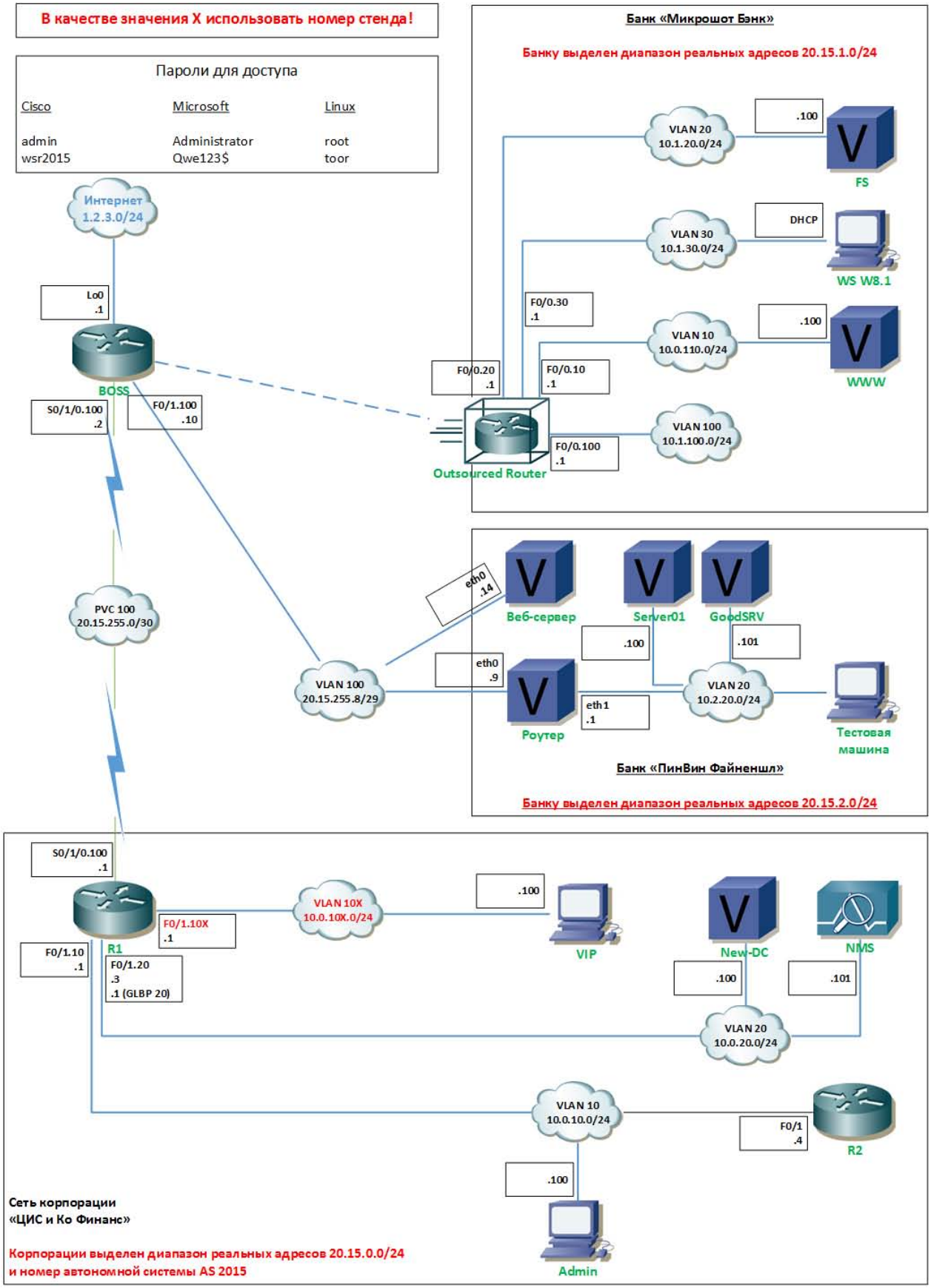
Зам. директора по ИТ _____ Цискин С.С.

SW1	Устройство	Порт	SW2	Устройство	Порт	R1	Устройство	Порт	R2	Устройство	Порт		Устройство	Порт		Устройство	Порт
F0/1	R1	F0/0	F0/1			F0/0	SW1	F0/1	F0/0	SW1	F0/1						
F0/2	R1	F0/1	F0/2			F0/1	SW1	F0/2	F0/1	SW1	F0/2						
F0/3	R2	F0/0	F0/3			S0/1/0	BOSS	S0/1/0	S0/1/0	R1	S0/1/1						
F0/4	R2	F0/1	F0/4			S0/1/1	R2	S0/1/0	S2/1								
F0/5			F0/5														
F0/6			F0/6														
F0/7			F0/7														
F0/8			F0/8														
F0/9			F0/9														
F0/10	CIS&Ko Serv	NIC0	F0/10														
F0/11			F0/11														
F0/12			F0/12														
F0/13			F0/13														
F0/14			F0/14														
F0/15			F0/15														
F0/16			F0/16														
F0/17			F0/17														
F0/18			F0/18														
F0/19			F0/19														
F0/20	VIP PC*	NIC0	F0/20	Admin PC	NIC0												
F0/21			F0/21														
F0/22	SW2	F0/22	F0/22	SW1	F0/22												
F0/23	SW2	F0/23	F0/23	SW1	F0/23												
F0/24	SW2	F0/24	F0/24	SW1	F0/24												

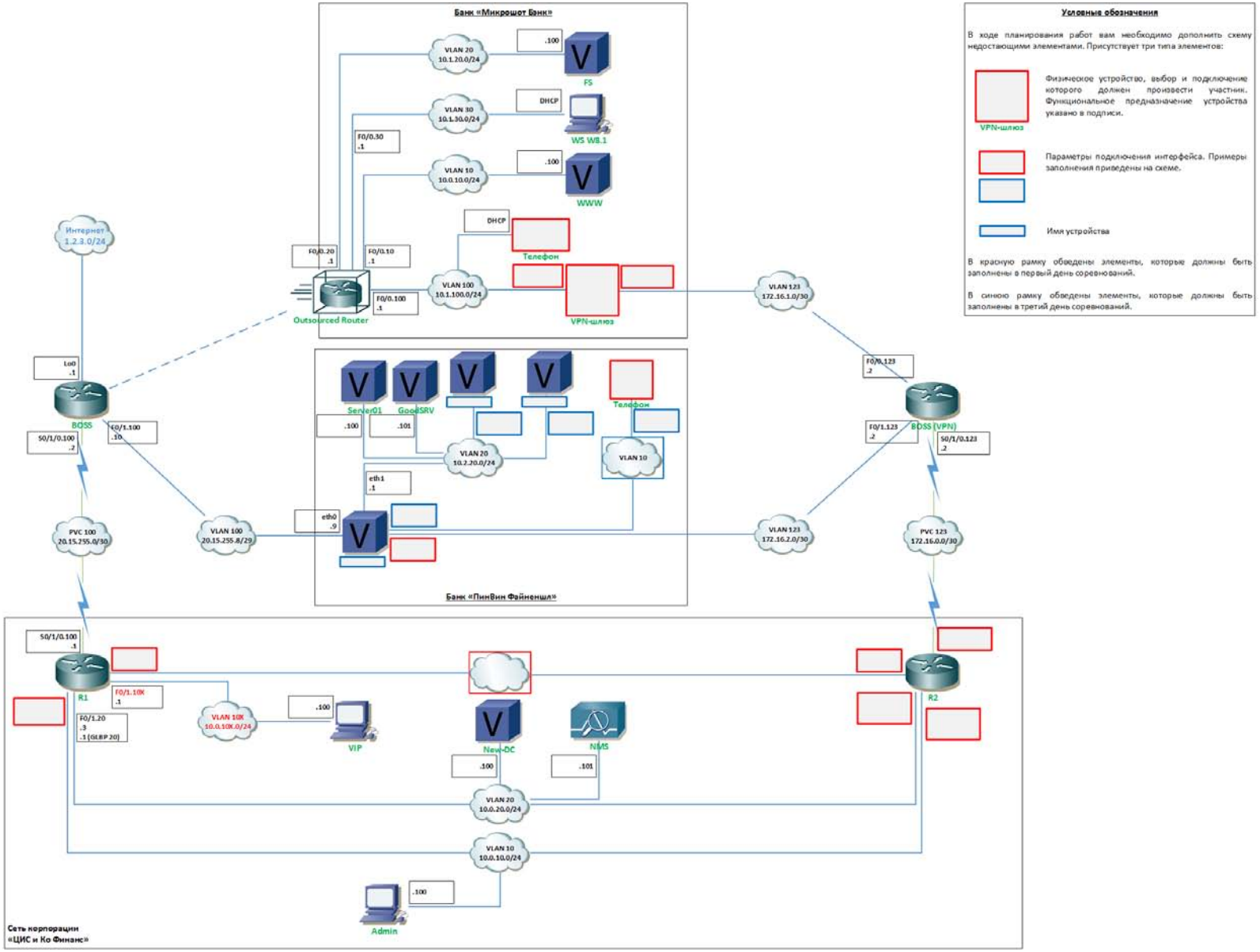
Приложение 5. Схема соединений и подключений (канальный уровень)



Приложение 6. Схема соединений и подключений (сетевой уровень)



Приложение 7. Проект схемы соединений и подключений (сетевой уровень)



Приложение 8. Технические условия на подключение

УТВЕРЖДАЮ

Генеральный директор ОАО «Босс-телеком»

_____ С.Г. Босс

ТЕХНИЧЕСКИЕ УСЛОВИЯ

Технические условия действительны в течение трех календарных дней, начиная с _____.

Условия	Параметры
Присоединение к сети L3 VPN оператора «Босс-телеком»	Адреса: 1. Корпорация «ЦИС и Ко Финанс» 2. Банк «Микрошот Бэнк» 3. Банк «ПинВин Файненшл»
Физическое подключение	1. Корпорация «ЦИС и Ко Финанс» Использовать существующее последовательное соединение к маршрутизатору BOSS, порт Serial 0/1/0 2. Банк «Микрошот Бэнк» Использовать существующее витопарное соединение к маршрутизатору BOSS, порт FastEthernet 0/0 3. Банк «ПинВин Файненшл» Использовать существующее витопарное соединение к маршрутизатору BOSS, порт FastEthernet 0/1
Канальное подключение	1. Корпорация «ЦИС и Ко Финанс» На интерфейсе Serial 2/0 маршрутизатора BOSS выделить дополнительный DLCI с номером 123, терминировать его на подинтерфейсе типа точка-точка Serial 0/1/0.123 2. Банк «Микрошот Бэнк» Выделить дополнительный VLAN с номером 123, использовать подинтерфейс Fa 0/0.123 3. Банк «ПинВин Файненшл» Выделить дополнительный VLAN с номером 123. использовать подинтерфейс Fa 0/1.123 Объединить перечисленные подинтерфейсы в VRF с именем VPN. Использовать RD 65000:123
IP-адресация	1. Корпорация «ЦИС и Ко Финанс» Использовать диапазон 172.16.0.0/30 2. Банк «Микрошот Бэнк» Использовать диапазон 172.16.1.0/30 3. Банк «ПинВин Файненшл» Использовать диапазон 172.16.2.0/30 Адрес .2 из каждого диапазона назначить соответствующему интерфейсу роутера BOSS.
Маршрутизация	Использовать протокол OSPF, Area 123, тип Normal

Приложение 9. Конфигурация граничного маршрутизатора банка «Микрошот Бэнк»

КОНФИДЕНЦИАЛЬНО

ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ

УТВЕРЖДАЮ
Генеральный директор ОАО «Босс-телеком»

_____ С.Г. Босс

```
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname Microshot
!
ip cef
no ip domain lookup
ip domain name microshot.ru
!
username admin privilege 15 secret *****
!
interface Loopback1
 ip address 10.1.0.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 123
!
interface FastEthernet0/0
 description Microshot Bank
 no ip address
!
interface FastEthernet0/0.10
 description WWW
 encapsulation dot1q 10
 ip address 10.0.110.1 255.255.255.0
!
interface FastEthernet0/0.20
 description Servers
 encapsulation dot1q 20
 ip address 10.1.20.1 255.255.255.0
 ip ospf 1 area 123
!
interface FastEthernet0/0.30
 description Users
 encapsulation dot1q 30
 ip address 10.1.30.1 255.255.255.0
 ip helper-address 10.1.20.100
 ip ospf 1 area 123
!
interface FastEthernet0/0.100
 description Reserved for MS BackBone
 encapsulation dot1q 100
 ip address 10.1.100.1 255.255.255.0
 ip ospf 1 area 123
!
router ospf 1
```

```
 passive-interface default
 no passive-interface FastEthernet0/0.100
!
```