Министерство науки и высшего образования Российской Федерации
Лысьвенский филиал
федерального государственного автономного образовательного учреждения
высшего образования
**«Пермский национальный исследовательский
политехнический университет»**

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации обучающихся по дисциплине
«Администрирование информационно-вычислительных систем»
Приложение к рабочей программе дисциплины

Направление подготовки:	**09.03.01 Информатика и вычислительная техника**
Направленность (профиль) образовательной программы:	Компьютерные системы
Квалификация выпускника:	«Бакалавр»
Выпускающая кафедра:	Технических дисциплин
Форма обучения:	Очная, очно-заочная, заочная

Курс: 3 (4, 3) **Семестр**: 5 (7, 5)

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч.

Форма промежуточной аттестации:
Экзамен: 5 (7, 5) семестр

Лысьва 2024

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД освоение учебного материала дисциплины запланировано в течение одного семестра (5-го семестра учебного плана очной и заочной форм обучения; 7-го семестра учебного плана очно-заочной формы обучения). Предусмотрены аудиторные лекционные, лабораторные работы, практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам, практическим занятиям и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**			**Итоговый**
	С	**ТО**	**ОЛР**	**ОПЗ**	**Т/КР**	**Экзамен**
Усвоенные знания						
З.1 Знать требования к современным информационным системам, возможности платформ, средств и систем администрирования, методы администрирования и контроля;	С1	ТО1			Т	ТВ
З.2 Знать функции, принципы действия и алгоритмы работы сетевого оборудования, критерии оценки эффективности и надежности средств защиты информационных систем; критерии и методы оценивания механизмов функционирования информационных систем	С2	ТО2			Т	ТВ
Освоенные умения						
У.1 Уметь администрировать компьютерные сети, читать структурные и функциональные схемы систем и сетей связи;			ЛР1-5	ОПЗ	Т	ПЗ
У.2 Уметь анализировать состояние информационной системы; пользоваться средствами технического аудита информационной системы.			ЛР 1-5	ОПЗ	Т	ПЗ
Приобретенные владения						
В.1 Владеть навыками терминологией			ЛР 1-	ОПЗ	Т	КЗ

информационных систем, навыками администрирования компьютерных сетей, современными сетевыми информационными технологиями;			5			
В.2 Владеть навыками работы с сетевым оборудованием и сетевым программным обеспечением, методикой формирования комплекса мер по повышению защищенности информационных систем.			ЛР 1-5	ОПЗ	Т	КЗ

С – собеседование по теме; ТО – теоретический опрос; ОЛР – отчет по лабораторной работе; ОПЗ – отчет по практическому занятию; Т/КР – рубежное тестирование; ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в форме экзамена, проводимая с учётом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;

- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;

- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;

- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме защиты лабораторных работ, практических занятий и рубежного тестирования (после изучения каждого модуля учебной дисциплины).

2.2.1. Защита лабораторных работ

Всего запланировано 5 лабораторных работ. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом или группой студентов. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.2.2. Защита практических занятий

Всего запланировано 5 практических занятий. Типовые темы практических занятий приведены в РПД.

Защита практического занятия проводится индивидуально каждым студентом или группой студентов. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.2.3. Рубежное тестирование

Запланировано рубежное тестирование (Т) после освоения студентами учебных разделов.

Типовые шкала и критерии оценки результатов рубежного тестирования приведены в общей части ФОС образовательной программы.

Типовые задания теста:

1. **Какие протоколы относятся к транспортному уровню четырехуровневой модели стека протоколов TCP/IP?**

a. ARP
b. TCP
c. UDP
d. IP
e. ICMP
f. Выберите все правильные ответы

2. **Что протокол IPSec добавляет к пакетам для аутентификации данных?**

a. Заголовок аутентификации (заголовок AH)
b. Заголовок подписи (заголовок SH)
c. Заголовок авторизации (заголовок AvH)
d. Заголовок цифровой подписи (заголовок DSH)

3. Что из предложенного входит в процедуру согласования IPSec?

a. Только соглашение безопасности ISAKMP
b. Соглашение безопасности ISAKMP и одно соглашение безопасности IPSec
c. Соглашение безопасности ISAKMP и два соглашения безопасности IPSec
d. Только два соглашения безопасности IPSec

4. Протокол ESP из IPSec:

a. Обеспечивает только конфиденциальность сообщения
b. Обеспечивает только аутентификацию данных
c. Обеспечивает конфиденциальность и аутентификацию сообщения
d. Не обеспечивает ни конфиденциальность, ни аутентификацию

5. Виртуальные частные сети:

a. Передают частные данные по выделенным сетям
b. Инкапсулируют частные сообщения и передают их по общественной сети
c. Не используются клиентами Windows
d. Могут использоваться с протоколами L2TP или PPTP

6. Основные отличия протоколов L2TP и PPTP состоят в следующем (выберите все возможные варианты):

a. Протокол L2TP обеспечивает не конфиденциальность, а только туннелирование
b. Протокол PPTP используется только для туннелирования TCP/IP
c. Протокол L2TP может использоваться со службами IPSec, а протокол PPTP используется самостоятельно
d. Протокол PPTP поддерживается крупнейшими производителями, а протокол L2TP является стандартом корпорации Microsoft

7. Служба, осуществляющая присвоение реальных IP-адресов узлам закрытой приватной сети, называется:

a. NAT
b. PAT
c. Proxy
d. DHCP
e. DNS

8. Правила, применяемые в брандмауэрах, позволяют:

a. Сначала запретить все действия, потом разрешать некоторые
b. Сначала разрешить все действия, потом запрещать некоторые
c. Передавать сообщения на обработку другим приложениям
d. Передавать копии сообщений на обработку другим приложениям
e. a, c
f. b, c, d
g. a, b, c, d

9. На каком из четырех уровней модели стека протоколов TCP/IP к передаваемой информации добавляется заголовок, содержащий поле TTL (time-to-live)?

a. На уровне приложений (application layer)
b. На транспортном уровне (transport layer)
c. На сетевом уровне (internet layer)
d. На канальном уровне (link layer)

10. На каком уровне четырехуровневой модели стека протоколов TCP/IP работает служба DNS?

a. На Уровне приложений (application layer)
b. На Транспортном уровне (transport layer)
c. На Межсетевом уровне (internet layer)
d. На Канальном уровне (link layer)

11. Какой транспортный протокол используется протоколом Simple Mail Transfer Protocol (SMTP)?

a. TCP
b. UDP
c. ICMP
d. Ни один из перечисленных

12. Назовите отличия концентраторов (hub) от коммутаторов 2-го уровня (switch).

a. Коммутаторы работают на более высоком уровне модели OSI, чем концентраторы
b. Коммутаторы не могут усиливать сигнал, в отличие от концентраторов
c. Коммутаторы избирательно ретранслируют широковещательные кадры, концентраторы передают широковещательные кадры на все свои порты
d. Коммутаторы анализируют IP-адреса во входящем пакете, а концентраторы анализируют MAC-адреса

13. В описании правил для межсетевого экрана FreeBSD действие fwd означает:

a. Установление вероятности совершения действия
b. Имитацию задержки пакетов
c. Перенаправление пакетов на обработку другой программе
d. Перенаправление пакетов на другой узел

14. Выберите верное утверждение:

a. Протокол L2TP не имеет встроенных механизмов защиты информации
b. Протокол L2TP не применяется при создании VPN
c. Протокол PPTP более функциональный и гибкий чем L2TP, но требует более сложных настроек

15. Служба IPSec может быть использована:

a. Только для шифрования
b. Только для аутентификации
c. Для аутентификации и шифрования
d. Не может быть использования ни для шифрования, ни для аутентификации

16. Бастион – это:

a. Группа серверов корпоративной сети, предоставляющая сервисы узлам внешних сетей
b. Любой пограничный маршрутизатор, связывающий локальную сеть с внешними сетями
c. комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами

17. «Злоумышленник генерирует широковещательные ICMP-запросы от имени атакуемого узла». Это описание метода:

a. Маскарадинг
b. Смерфинг
c. Активная имитация
d. Пассивная имитация

18. В межсетевом экране FreeBSD действие reject соответствует действию

a. unreach net
b. unreach host
c. unreach port

19. Протокол RIP:

a. Не имеет механизма предотвращения зацикливания
b. Имеет простой и не эффективный механизм предотвращения зацикливания
c. Имеет высокоэффективный механизм предотвращения зацикливания

20. Какой протокол служит, в основном, для передачи мультимедийных данных, где важнее своевременность, а не надежность доставки.

a. TCP
b. UDP
c. TCP, UDP

21. Протокол передачи команд и сообщений об ошибках.

a. ICMP
b. SMTP
c. TCP

22. С помощью какой команды можно просмотреть таблицу маршрутизации

a. Route
b. Ping

c. Tracert

23. Что означает MAC-адрес

a. IP-адрес компьютера
b. Физический адрес
c. Адрес компьютера во внешней сети

24. Какой порт может использоваться клиентом (со своей стороны) при подключении к Web-серверу

a. 80
b. 1030
c. 28

Ключ к тесту

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
bc	a	c	c	b	acb	a	g
9	**10**	**11**	**12**	**13**	**14**	**15**	**16**
c	a	a	a	d	a	c	a
17	**18**	**19**	**20**	**21**	**22**	**23**	**24**
b	b	b	b	a	a	b	b

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Администрирование информационно-вычислительных систем на базе операционных систем семейства Linux
2. Операционные системы на базе систем семейства Linux
3. Установка ОС Linux
4. Настройка ОС Linux.
5. Управление пользователями базе систем семейства Linux
6. Управление устройствами базе систем семейства Linux.
7. Работа с файлами.
8. Системные процессы.
9. Установка программного обеспечения.

10. Разработка системного программного обеспечения.
11. Администрирование элементов сетевой инфраструктуры информационно-вычислительных систем
12. Сетевое администрирование.
13. Удаленный доступ.
14. Установка FTP-сервера
15. Настройка FTP-сервера.
16. Установка Web-сервера
17. Настройка Web-сервера.
18. Принципы обеспечения безопасности.

Типовые вопросы и практические задания для контроля освоенных умений:

Настройка сети центрального офиса

1) Для выдачи адресов в сети WINA и WINB настройте DHCPv6-сервер на DC1 и обеспечьте его отказоустойчивость с помощью DC2. Вместе с тем отказоустойчивость должна быть обеспечена и для всех областей DHCPv4.

2) DC2 должен быть резервным контроллером домена skill39.wsr. Роль RID pool manager должна быть передана на этот сервер. Реплику глобального каталога должен нести только DC1.

3) На DC2 должны быть переданы все DNS-зоны с DC1.

4) На DC1 и DC2 с SRV2 должна быть передана DNS-зона ext.skill39.wsr

5) В сети LINA должен работать SLAAC.

6) В качестве DNS-серверов все клиенты сетей WINA, WINB и LINA должны использовать DC1 и DC2.

7) На всех виртуальных машинах и сетевых устройствах в сети центрального офиса должен быть включен мониторинг.

a) Опрос всех устройств будет производиться с машины SRV1.

b) Достаточно использовать SNMPv2c.

c) Используйте строку сообщества notpublic в режиме “только чтение”

8) Должна быть обеспечена связь между внутренними сетями центрального офиса и филиалами 1 и 2 через интернет с помощью GRE-туннелей.

a) В центральном офисе на маршрутизаторе R1 должны быть созданы два туннельных интерфейса с номерами 0 и 1.

b) Туннель с номером 0 должен использоваться для связи с R2.

c) Туннель с номером 1 должен использоваться для соединения по GRE с виртуальной машиной LINRTR

d) GRE-туннель на LINRTR должен устанавливаться при загрузке операционной системы.

e) Прямое последовательное соединение между центральным офисом и филиалом будет демонтировано в конце дня.

f) Для обеспечения маршрутизации IPv4 между центральным офисом и филиалами поверх туннелей необходимо использовать протокол OSPFv2

g) Дополнительно настройте OSPFv3 между R1 и R2 для обмена маршрутами IPv6.

h) Весь трафик между центральным офисом и филиалами должен передаваться

через GRE-туннели.

9) Протоколы динамической маршрутизации на компьютерах под управлением ОС Linux должны использовать пакет quagga

10)Выход в интернет должен обеспечиваться бесперебойно.

a) В случае сбоя у провайдера должно происходить автоматическое переключение на резервный канал.

b) В случае сбоя одного из провайдеров у пользователей должен работать интернет хотя бы по протоколу IPv4.

c) В случае сбоя одного из провайдеров серверы LINDMZ и WINDMZ должны быть доступны из интернета хотя бы по протоколу IPv4.

11) Интерфейсы F0/4 и F0/5, соединяющие коммутаторы, необходимо объединить в Etherchannel.

a) Канал должен согласовываться с помощью LACP. S2 должен ждать согласования, а S1 его инициировать.

b) Трафик сетей WINA, WINB, LINA должен ходить через этот канал. Трафик сети DMZ должен ходить через интерфейс F0/3, не входящий в Etherchannel

12) Необходимо обеспечить отказоустойчивость локальной сети:

a) Корнем STP во всех настроенных VLAN должен быть коммутатор S1.

b) В случае сбоя или изменения в коммутации пересчёт STP должен происходить в течение 10 секунд.

c) В случае сбоя соединения между коммутаторами трафик всех сетей должен ходить по оставшимся каналам.

d) Сервер LINDMZ должен получать маршрут по умолчанию динамически по протоколу BGP от R1 и ASA.

e) R1 и ASA должны анонсировать в сторону LINDMZ только маршрут по умолчанию и фильтровать другие префиксы.

f) Входящий трафик из интернета до сервера LINDMZ должен приходить через R1 и переключаться на ASA только в случае сбоя у провайдера.

13) Виртуальная машина SRV1 должна предоставлять сервис удаленного доступа на основе технологии OpenVPN с учетом следующих требований: a) Устройство TUN. b) Протокол UDP. c) Порт сервера 8081. d) Применяется дополнительная TLS аутентификация.

14) На виртуальной машине LINDMZ должна быть добавлена поддержка протокола IPv6 для веб-сервера NGINX.

a) Веб-сайт web.skill39.wsr должен быть также доступен по доменному имени web.skill39.ru по протоколу IPv4 для клиентов в интернете.

b) Веб-сайт web6.skill39.wsr должен быть доступен по доменному имени только по протоколу IPv6 для всех клиентов в сети центрального офиса и по доменному имени web6.skill39.ru по протоколу IPv6 для клиентов в интернете.

c) Для обеспечения работы доменных имён web.skill39.ru и web6.skill39.ru необходимо зарегистрировать их на сайте nic.moogle.ru, указав актуальные IP-адреса сервера.

d) Файлы веб-сайта web6 должны располагаться в каталоге /var/www/ip6

15) На виртуальной машине WINDMZ используйте только протокол IPv6.

16) На виртуальной машине WINDMZ настройте роль web-сервера и разместите на нем сайт

17)В домене skill39.wsr:

a) на сервере DC2 с использованием двух свободных жестких дисков создайте RAID0-массив. Для доступа к нему используйте букву G:\

b) создайте общую папку g:\shares\users:

c) Все пользователи домена, кроме членов группы Visitors, должны иметь права на запись в эту папку;

d) Члены группы Visitors не должны иметь прав доступа к этой папке;

e) Запретите выполнение любого программного кода из указанной папки (учтите, что пользователи не должны лишиться возможности сохранять исполняемые файлы); ограничьте объем указанной папки до 100 Мб.

Настройка сети филиала 1

1) На виртуальной машине SRV2 должна быть включена поддержка протокола IPv6 для службы DNS с учетом следующих требований:

a) Сервер должен обслуживать зону ext.skill39.wsr.

b) Разрешение имен необходимо организовать в соответствии с Таблицей 1.

c) Запросы, которые выходят за рамки зоны skill39.wsr должны пересылаться DNS серверу MOOGLE. Для проверки используйте адрес ip6.worldskills.ru.

d) Настройте подчиненную зону (Secondary DNS) для зоны skill39.wsr.

e) Реализуйте поддержку разрешения обратной зоны

2) На виртуальной машине SRV2 должен быть настроен веб-сервер Apache2.

a) Используйте стандартный порт протокола HTTP.

b) Файлы веб-сайта должны располагаться в каталоге /var/www/.

c) В качестве страницы по умолчанию создайте файл index.html.

d) Сайт ext.skill39.wsr должен быть доступен по доменному имени по протоколу IPv4 для всех клиентов в сети центрального офиса.

Настройка сети филиала 2

1) Виртуальная машина LINRTR должна обеспечивать автоматическое предоставление настроек IPv6 для клиентов локальной сети.

a) Клиенты сети должны иметь доступ к сайтам, работающим по протоколам IPv4 и IPv6. Для проверки можете использовать адрес moogle.ru и ip6.moogle.ru.

2) Должна выполняться односторонняя синхронизация файлов веб-сайтов с LINDMZ на сервер SRV2.

a) Период синхронизации - 1 минута.

b) Каталог для синхронизации на LINDMZ - /var/www

c) Каталог для синхронизации на SRV2 - /var/www

d) Файлы на SRV2 должны обновляться, но не удаляться при их отсутствии на LINDMZ.

e) Файлы index.html должны быть исключены из синхронизации. Изначальная информация в этих файлах на SRV2 должна быть сохранена.

Настройка мобильных клиентов

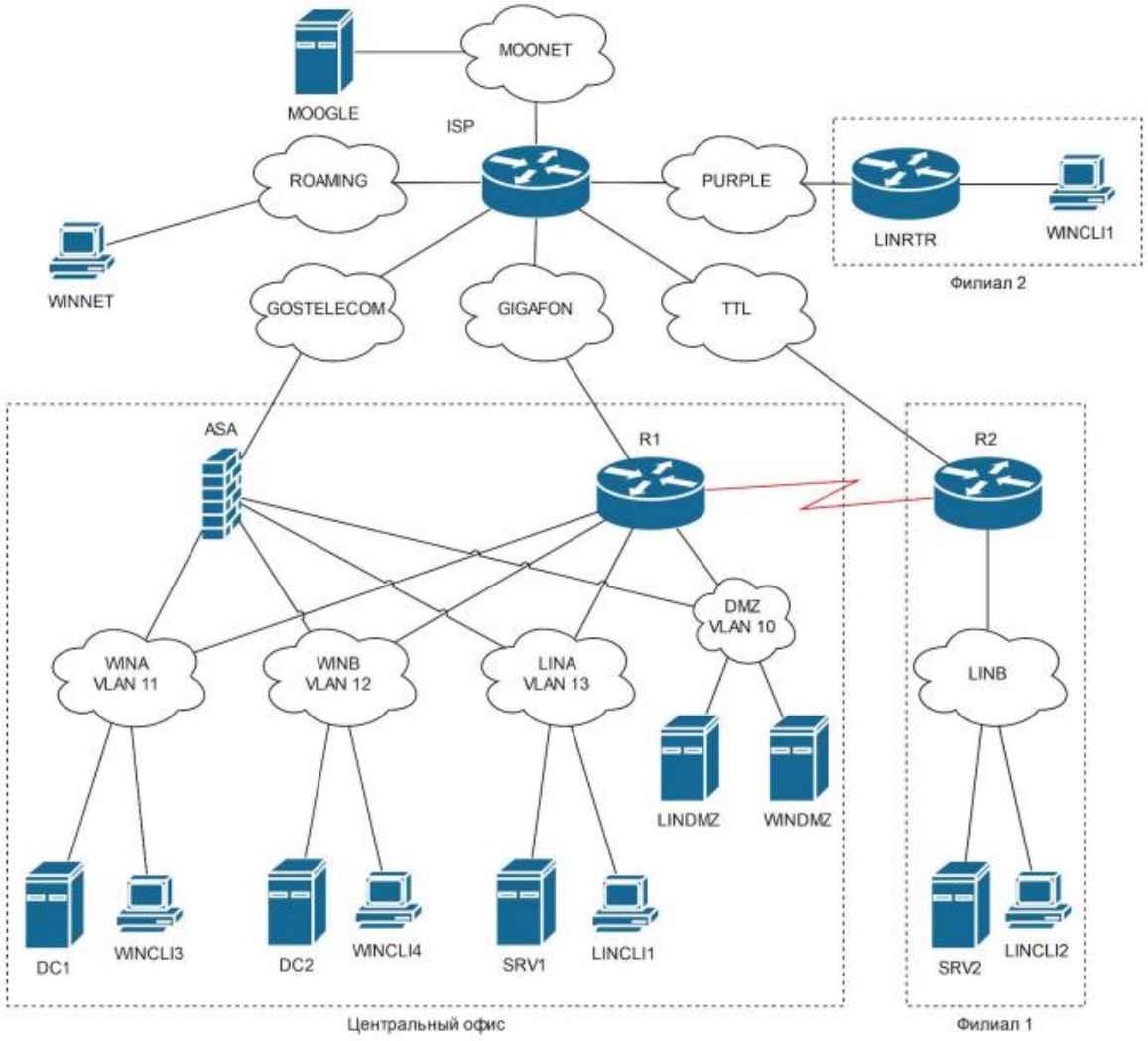
1) На виртуальной машине WINNET:

a) Установите клиент удаленного доступа на основе технологии OpenVPN.

b) Сформируйте конфигурационный файл client.ovpn в каталоге C:\vpn\ для автоматизации установления VPN соединения.

c) При подключении к VPN серверу не должен запрашиваться ввод дополнительных параметров.

d) После установления VPN соединения WINNET должен иметь возможность доступа к локальным ресурсам сети по доменным именам зоны skill39.wsr.



Типовые комплексные задания для контроля приобретенных владений:

Вы – системный администратор компании, находящейся в городе Казань. В главном офисе вы управляете доменом Kazan.wsr. Вам необходимо настроить сервисы в локальной сети головного офиса. Компания, в которой вы работаете, хочет выйти на рынки северной Европы. Для этого она устанавливает партнерские отношения с одной из компаний, находящейся в Санкт-Петербурге. Вам нужно помочь администратору партнерской компании с настройкой своего домена (SPB.wse), а потом настроить между доменами доверие. Также Вам предстоит

настроить канал связи между офисами с помощью статических маршрутов

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в форме экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.