Министерство образования и науки Пермского края
государственное бюджетное профессиональное образовательное учреждение
«Пермский техникум промышленных и информационных технологий им. Б.Г. Изгагина»

«СОГЛАСОВАНО»
Генеральный директор ЗАО «Бионт»
_____/Н.А.Григоров/
«02» марта 2020 г
МП

«УТВЕРЖДАЮ»
Директор ГБПОУ «ПТПИТ»
_____/В.В.Аспидов/
«02» марта 2020 г
МП

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения регионального этапа
Всероссийской олимпиады профессионального мастерства обучающихся
по УГС 10.00.00 «Информационная безопасность» в Пермском крае
для специальностей
10.02.01 Организация и технология защиты информации
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Дата проведения - 18.03.2020г.

Пермь 2020

«Рекомендовано к утверждению»
на заседании рабочей группы по организации и проведению регионального этапа Всероссийской олимпиады профессионального мастерства обучающихся по УГС 10.00.00 «Информационная безопасность» в Пермском крае
протокол № 1 от «02» марта 2020 г

Разработчики:

Лекомцев Дмитрий Владимирович, преподаватель ГБПОУ «Пермский техникум промышленных и информационных технологий им. Б.Г. Изгагина», председатель регионального учебно-методического объединения по УГС 10.00.00 Информационная безопасность
Белый Валерий Валерьевич, начальник отделения информационных технологий КГАПОУ «Пермский техникум промышленных и информационных технологий
Бабушкина Нина Геннадьевна, преподаватель КГАПОУ «Пермский техникум промышленных и информационных технологий»

СОДЕРЖАНИЕ

1. ТЕСТОВОЕ ЗАДАНИЕ I УРОВНЯ

1.1. Вопросы тестового задания

1. ИТ в профессиональной деятельности

1.1.В текстовом редакторе набран текст:

«В НЕМ ПРОСТО НАХОДЯТСЯ ПРОЦЕДУРЫ ОБРОБОТКИ ДАТЫ И ВРЕМЕНИ ДНЯ, АНАЛИЗА СОСТОЯНИЯ МАГНИТНЫХ ДИСКОВ, СРЕДСТВА РОБОТЫ СО СПРАВОЧНИКАМИ И ОТДЕЛЬНЫМИ ФАЙЛАМИ».

а. Найти Р, заменить на РА
б. Найти РО, заменить на РА
в. Найти РОБ, заменить на РАБ
г. Найти БРОБ, заменить на БРАБ

1.2. Сеть, которая объединяет компьютеры, установленные в одном помещении или одном здании, называется _____.

1.3.Определите соответствие между расширением файла и его содержанием:

1	.exe	А	Изображение
2	.jpg	Б	Текст
3	.doc	В	Музыка
4	.mp3	Г	Программа

Запишите ответ:

1	2	3	4

1.4.Укажите в порядке возрастания объемы памяти:

а. 20 бит
б. 10 бит
в. 2 байта
г. 1010 байт
д. 1 Кбайт

2. Системы качества, стандартизации и сертификации

2.1.Название международной организации, занимающейся выпуском стандартов

а. ISO

б. IEC

в. EAC

г. CEN

2.2.Добровольное подтверждение соответствия осуществляется по инициативе _____.

2.3.Установите соответствие между термином и методом стандартизации:

1	Органолептический метод	А	Метод определения показателей качества продукции, осуществляемый на основе наблюдения и подсчёта числа определённых событий, предметов или затрат
2	Регистрационный метод	Б	Метод, осуществляемый на основе анализа восприятий органов чувств
3	Расчётный метод	В	Метод, основанный на информации, получаемой с использованием технических измерительных средств и контроля
4	Измерительный метод	Г	Метод, отражающий использование теоретических или эмпирических зависимостей показателей качества продукции от её параметров.

Запишите ответ:

1	2	3	4

2.4.Укажите правильный порядок обозначения ГОСТа из системы ЕСКД:

а. Номер группы

б. Порядковый номер в группе

в. Класс

г. Год утверждения стандарта

3. Охрана труда, безопасность жизнедеятельности, безопасность окружающей среды (охрана окружающей среды, «зеленые технологии»)

3.1.Основной задачей охраны труда является:

а. Созидание и постоянное поддержание здоровых и безопасных условий труда

б. Обеспечение безопасности на производстве

в. Ликвидация несчастных случаев на производстве

г. Обеспечение выполнения законов об охране труда

3.2.Согласно ГОСТ 12.0.004-15 предусмотрено проведение следующих видов инструктажа: вводный, первичный и повторный на рабочем месте, _____, целевой.

3.3.Установите соответствие между факторами и названиями классов факторов:

1	Недостаточная освещенность рабочей зоны	А	Физический фактор
2	Токсическое воздействие на	Б	Биологический фактор

	организм человека		
3	Воздействие на организм патогенных микроорганизмов и продуктов их деятельности	В	Химический фактор
4	Физические и нервные перегрузки	Г	Психофизиологический фактор

Запишите ответ:

1	2	3	4

3.4. Укажите последовательность действий по оказанию первой помощи пострадавшему при поражении электрическим током:

а. Убедиться в отсутствии пульса на сонной артерии и реакции зрачков на свет
б. Оттащить пострадавшего на безопасное расстояние
в. Приступить к реанимационным мероприятиям
г. Обесточить пострадавшего

4. Экономика и правовое обеспечение профессиональной деятельности

4.1. За нарушения трудовой дисциплины работодатель имеет право применить следующие дисциплинарные взыскания:

а. Предупреждение, лишение премии, исправительные работы, выговор
б. Замечание, выговор, увольнение
в. Предупреждение, замечание, отстранение от работы
г. Замечание, предупреждение, штраф, выговор

4.2._____ - это процесс переноса стоимости основных фондов на стоимость произведённой продукции.

4.3. Установите соответствие вида цены и её характеристики:

1	Договорная цена	А	Искусственно завышенная цена, ограничивающая ее снижение
2	Регулируемая цена	Б	Искусственно заниженная цена, отграничивающая рост цены
3	Цена «пола»	В	Цена товара, которая устанавливается по соглашению сторон
4	Цена «потолка»	Г	Цена, которая может отклоняться от базового уровня

Запишите ответ:

1	2	3	4

4.4. Установите последовательность этапов регистрации юридического лица:

а. Представление документов на регистрацию в ИФНС
б. Заключение между учредителями договора об учреждении общества
в. Принятие участниками решения об открытии фирмы
г. Открытие расчетного счета фирмы
д. Изготовление печати

5. Основы информационной безопасности

5.1.Что понимают под термином «политика безопасности»?

а) совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов

б) совокупность управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов

в) специфические потребности организации

г) деятельность в компьютерной информационной системе организации

5.2.Под угрозой удаленного администрирования в компьютерной сети понимается угроза …

5.3.Установите соответствие между терминами

	Термин		Определение
1.	Целостность	А	Свойство информации сохранять свою структуру и содержание в процессе передачи и хранения
2.	Конфиденциальность	Б	Возможность субъекта ознакомления с информацией
3.	Доступность	В	Статус, предоставленный данным и определяющий требуемую степень защиты
4.	Достоверность	Г	Свойство информации, выражающееся в строгой принадлежности субъекту, являющемуся источником информации

Запишите ответ:

1	2	3	4

5.4.Определите порядок действий при проведении атаки:

а. сканирование портов
б. подбор пароля пользователя
в. взлом системы защиты
г. ожидание события в системе

5.5. Для чего используется пароль?

а) аутентификация
б) идентификация
в) регистрация
г) авторизация

5.6. Формой правовой защиты литературных, художественных и научных произведений является_____ право

5.7. Установите соответствие между терминами

	Наименование вируса		Действия
1.	червь	А	размножающий себя на данном компьютере

2.	троян	Б	приводящий к временному изменению ссылок на программы
3.	программа-шутка	В	выдающий себя за какую-либо полезную программу
4.	Программа-закладка	Г	активирующийся при нажатии сочетания клавиш

Запишите ответ:

1	2	3	4

5.8. Указать верную последовательность стадии жизненного цикла компьютерного вируса

а) открытие исполняемого файла

б) анализ заголовков на корректность

в) формирование виртуального адресного пространства исполняемого файла на основе информации заголовков данного файла

г) настройка адресов импортируемых функций библиотек операционной системы на основе информации секции импорта

д) инициализация стека и формирование начального заполнения регистров процессора

е) формирование служебных структур (блок описания процесса (PEB), блок описания первичного потока (TEB) процесса), структур, определяющих обработчики структурных исключений (SEH)

ж) передача управления по адресу первой инструкции исполняемого файла

6. Организация и сопровождение электронного документооборота/ Криптографическая защита информации/ Криптографические средства и методы защиты информации

6.1.При изменении документа его хеш-сумма
а) остается неизменной до обновления хеш-суммы
б) изменяется
в) изменение документа не связано с хеш-суммой
г) зависит от пользователя

6.2.Процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст, это…

6.3.Установите соответствие между терминами

	Термин		Определение
1.	Ключ	А	Конфиденциальная информация аутентификации, обычно состоящая из строки знаков
2.	Пароль	Б	однотипный набор команд выполняемый в процессе блочного шифрования символов несколько раз
3.	раунд	В	персональный идентификационный номер
4.	Пин-Код	Г	Изменяемый элемент (параметр), каждому значению которого однозначно соответствует одно из отображений, реализуемых криптосистемой

Запишите ответ:

1	2	3	4

6.4.Установите правильный порядок выполнения преобразований в шифре AES:
а. Формирование раундового ключа
б. Сдвиг строчки
в. Замена байтов
г. Перемешивание столбцов

7 Технические методы и средства, технологии защиты информации/ Инженерно-техническая защита информации/ Применение инженерно-технических средств обеспечения информационной безопасности

7.1. Оптико-электронный извещатель предназначен для:
а) обнаружения проникновения через двери и окна
б) обнаружения разбития окон
в) обнаружения источника ИК излучения
г) обнаружения возникновения задымления
7.2. Токи и напряжения в токопроводящих элементах, вызванные электромагнитным излучением, емкостными и индуктивными связями, это…

7.3. Установите соответствие между терминами

	Термин		Определение
1.	Перехват	А	Недостаток или слабое место в автоматизированной информационной системе, которые могут быть условием реализации угрозы безопасности, обрабатываемой в ней информации
2.	Утечка (информации) по техническому каналу	Б	Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов
3.	Угроза (безопасности информации)	В	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации
4.	Уязвимость (автоматизированной информационной системы)	Г	Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

Запишите ответ:

1	2	3	4

7.4. Установите последовательность принципа классификации факторов, воздействующих на защищаемую информацию:

а. Вид
б. Группа
в. Подвид
г. Подгруппа
д. Подкласс

8. Программно-аппаратные средства защиты информации/ Программно-аппаратные средства защищенных телекоммуникационных систем/ Программно-аппаратные средства обеспечения информационной безопасности

8.1. Система обнаружения атак (СОА) на основе сигнатурного поиска выполняет поиск
а) признаков сетевых атак в сетевом потоке
б) аномальной активности
в) признаков сетевых атак в сетевом потоке и аномальной активности
г) вирусного заражения компонентов системы

8.2. Перехват сетевых пакетов, передаваемых по линиям передачи данных в сети – это…

8.3. Установите соответствие между терминами

	Термин		Определение
1.	Вирус-фильтр (сторож)	А	специальные программы, предназначенные для просмотра всех возможных мест нахождения вирусов (файлы, операционная система, внутренняя память и т. д.) и сигнализирующие об их наличии
2.	Детектор (сканер)	Б	программа, осуществляющая удаление вируса из программного файла или памяти ПК. Если это возможно, то дезинфектор восстанавливает нормальное функционирование ПК
3.	Дезинфектор (доктор)	В	модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает их уже зараженными и не внедряется в них.
4.	Программы-вакцины	Г	резидентная программа, обнаруживающая свойственные для вирусов действия и требующая от пользователя подтверждения на их выполнение

Запишите ответ:

1	2	3	4

8.4. Установите порядок действий в соответствии с организацией комплексной защиты информации
а. Классификация информационной системы в зависимости от обрабатываемой информации
б. Аудит информационной системы
в. Назначение ответственного лица
г. Разработка организационно - распорядительной документации

9. Обеспечение организации системы безопасности организации/Правовая защита информации/Организационное и правовое обеспечение информационной безопасности/Организационно-правовое обеспечение информационной безопасности

9.1. К верхнему уровню политики безопасности относится
а) формулировка целей, которые преследует организация в области информационной безопасности
б) позиция организации в отношении к доступу в Интернет
в) вопросы прав доступа к объектам поддерживаемые сервисом
г) условия чтения и модификации данных

9.2. Основным ответственным лицом за определение уровня классификации информации является _____.

9.3. Установите соответствие между основными направлениями обеспечения информационной безопасности и областью их действия в соответствии с Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. N 646 113

	Область действия		Направление обеспечения ИБ
1	Область обороны	А	Содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере
2	Область государственной и общественной безопасности	Б	Ликвидация зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет создания, развития и широкого внедрения отечественных разработок
3	Экономическая сфера	В	Противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности
4	Область науки, технологий и образования	Г	Развитие национальной системы управления российским сегментом сети «Интернет»
5	Область стратегической стабильности и равноправного стратегического партнерства	Д	Создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия

Запишите ответ:

1	2	3	4	5

9.4. Установите последовательность разработки модели угроз ИСПДн:

а. Описать ИСПДн
б. Определить пользователей ИСПДн
в. Определить тип ИСПДн
г. Определить вероятность реализации угроз в ИСПДн
д. Определить возможность реализации угроз в ИСПДн
е. Определить исходный уровень защищенности ИСПДн
ж. Оценить опасность угроз
з. Определить актуальность угроз в ИСПДн

1.2. Ответы на вопросы тестового задания

1.1. В

1.2. Локальной (LAN)

1.3. 1 – Г; 2 – А; 3 – Б; 4 – В.

1.4. Б В А Г Д

2.1. А

2.2. заявителя

2.3. 1 – Б; 2 – А; 3 – Г; 4 – В.

2.4. В А Б Г

3.1 А

3.2. внеплановый

3.3. 1 – А; 2 – В; 3 –В; 4 –Г.

3.4. Г Б А В

4.1. Б

4.2. Амортизация

4.3. 1 – В; 2 – Г; 3 –Б; 4 – А.

4.4. В Б А Г Д

5.1. А

5.2. удаленной работы на ПК (усройстве)

5.3. 1 – А; 2 -В – 4; 3 – Б; 4 – Г.

5.4. А Г Б В

5.5. Б

5.6. авторское

5.7. 1 –А; 2 – В; 3 – Б; 4 – Г.

5.8. АВЕГБЖД

6.1.Б

6.2. шифрование

6.3. 1 – Г; 2 – А; 3 – Б; 4 – В.

6.4. ВБГА

7.1. В

7.2. наводки

7.3. 1 – Б; 2 – Г; 3 - В; 4 – А.

7.4. АВ БГД

8.1. В

8.2. сниффинг

8.4. В Б А Г

9.1. А

9.2. руководитель организации

9.3. 1 – А; 2 – В; 3 – Б; 4 – Д; 5 – Г.

9.4. АЖБВГДЗ

1.3. Структура оценки тестового задания

Задание «Тестирование» состоит из теоретических вопросов, сформированных по разделам и темам.

Предлагаемое для выполнения участнику тестовое задание включает 2 части - инвариантную и вариативную, всего 40 вопросов.

2. ПРАКТИЧЕСКИЕ ЗАДАНИЯ I УРОВНЯ

2.1. Перевод профессионального текста

Задание на перевод текста:

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security; and

d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

e) be available as documented information;

f) be communicated within the organization; and

g) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this International Standard; and

b) reporting on the performance of the information security management system to top management.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects; and

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities; and

e) how to

1) integrate and implement the actions into its information security management system processes; and

2) evaluate the effectiveness of these actions.

Вопросы по тексту:

1.Define the place and the kind of information security policy of a company.

2.Define the requirements to security policy changes a company

3.What the aim of segregation of responsibilities and authorities?

4.What measures can guarantee that SMIS achieves expected result?

Deutsch

5.2. Politik

Das Top-Management sollte eine Informationssicherheitsrichtlinie festlegen, die:

a) entspricht dem Zweck der Organisation;

b) enthält Ziele (Aufgaben) im Bereich der Informationssicherheit (siehe Abschnitt 6.2) oder dient als Grundlage für die Festlegung solcher Ziele (Aufgaben);

c) beinhaltet eine Verpflichtung der geltenden Sicherheitsanforderungen entsprechen, die mit der Informationssicherheit verbunden ist; und

d) beinhaltet die Verpflichtung zur kontinuierlichen Verbesserung des Managementsystems der Informationssicherheit.

Eine Informationssicherheitspolitik sollte:

e) als dokumentierte Information eingerahmt sein;

f) den Mitarbeitern der Organisation mitgeteilt werden; und

g) den interessierten Seiten in der vorgeschriebenen Weise zur Verfügung stehen.

5.3. Organisatorische Funktionen, Verantwortung und Vollmacht

Das Top-Management sollte sicherstellen, dass für Funktionen, die für die Informationssicherheit wesentlich sind, werden die Verantwortung und Vollmacht hingewiesen und bestimmt.

Das Top-Management sollte Verantwortung und Vollmacht für Folgendes schaffen:

a) Adäquanzsicherung des Managementsystems der Informationssicherheit den Anforderungen der vorliegenden Internationalen Standardordnung und

b) einen Bericht über die Funktionsweise des Managementsystems der Informationssicherheit an das obere Management.

6. Planung

6.1 Maßnahmen zum Risikoumgang und zur Möglichkeitsrealisierung

6.1.1 Allgemeine Vorschriften

Bei der Planung eines Managementsystems der Informationssicherheit soll eine Organisation die in Abschnitt 4.1 genannten Probleme und die in Abschnitt 4.2 genannten Anforderungen berücksichtigen und die Risiken und Potenziale identifizieren, die berücksichtigt werden müssen, damit:

a) sicherstellen, dass das Managementsystem der Informationssicherheit die erwarteten Ergebnisse erzielen kann;

b) unerwünschte Wirkungen verhindern oder reduzieren; und

c) kontinuierliche Verbesserung erreichen.

Die Organisation sollte Folgendes planen:

d) Maßnahmen zum Umgang mit diesen Risiken und Chancen; und

e) auf welche Weise

1) diese Aktionen in die Prozesse des Managementsystems der Informationssicherheit einbetten und implementieren; und

2) die Wirksamkeit dieser Maßnahmen bewerten.

Вопросы по тексту:

1. Bestimmen Sie den Ort und den Typ der Informationssicherheitsrichtlinie des Unternehmens.
2. Bestimmen Sie die Anforderungen zur Änderung der Sicherheitsrichtlinie im Unternehmen.
3. Warum sollte das Management die Verantwortung und Vollmacht verteilen?
4. Wie kann man sicherstellen, dass das Managementsystem der Informationssicherheit die erwarteten Ergebnisse erzielt?

2.2. Ответы по тексту.

Перевод.

5.2 Политика

Высшее руководство должно установить политику информационной безопасности, которая:

a) соответствует назначению организации;

b) включает цели (задачи) в области информационной безопасности, (см. раздел 6.2) или служит основой для задания таких целей (задач);

c) включает обязательство соответствовать действующим требованиям, связанным с информационной безопасностью; и

d) включает обязательство непрерывного улучшения системы менеджмента информационной безопасности.

Политика информационной безопасности должна:

e) быть оформлена как документированная информация;

f) быть доведена до сведения сотрудников в организации; и

g) быть доступной в установленном порядке для заинтересованных сторон.

5.3 Организационные функции, ответственность и полномочия

Высшее руководство должно гарантировать, что для функций, существенных с точки зрения информационной безопасности, ответственность и полномочия назначены и доведены до сведения.

Высшее руководство должно установить ответственность и полномочия для:

a) обеспечения соответствия системы менеджмента информационной безопасности требованиям Настоящего Международного Стандарта; и

b) отчета о функционировании системы менеджмента информационной безопасности высшему руководству.

6 Планирование

6.1 Действия по обработке рисков и реализации возможностей

6.1.1 Общие положения

Планируя систему менеджмента информационной безопасности, организация должна принять во внимание проблемы, упомянутые в разделе 4.1 и требования, установленные в разделе 4.2, а также определить риски и потенциальные возможности, которые необходимо принять во внимание, чтобы:

a) гарантировать, что система менеджмента информационной безопасности может достигать ожидаемых результатов;

b) предотвратить или уменьшить нежелательные эффекты; и

c) достичь непрерывного совершенствования.

Организация должна планировать:

d) действия по обработке этих рисков и реализации возможностей; и

e) каким образом

1) встраивать эти действия в процессы системы менеджмента информационной безопасности и выполнять их; и

2) оценивать результативность этих действий.

Вопросы по тексту:

1. Определите место и вид нахождения политики информационной безопасности компании. (5.2)

Ответ: в документированном виде и в доступном виде.

2. Определите требования к изменению политики безопасности в компании (5.2)

Ответ: При изменении структуры организации, законодательства и непрерывного улучшения менеджмента безопасности.

3. Для чего руководство должно распределить ответственность и полномочия? (5.3)

Ответ: Чтобы обеспечить соответствие СМИБ международным стандартам и отчетности о функционировании СМИБ

4. Какими мерами можно гарантировать, что СМИБ достигнет ожидаемых результатов? (6.1.1.)

Ответ: оценкой рисков

2.3. Критерии оценивания.

Перевод и ответы на вопросы выполняются на компьютере и сохраняются в файл с наименованием шифра участника на «Рабочем столе».

Задание по переводу текста с иностранного языка на русский включает 2 задачи:

- перевод текста, содержание которого включает профессиональную лексику (возможен вариант аудирования);
- ответы на вопросы по тексту (аудирование, выполнение действия).

Задание по переводу иностранного текста разработано на языках, которые изучают участники Олимпиады.

В качестве контрольного текста выбран международный стандарт INTERNATIONAL STANDARD ISO/IEC 27001 Second edition 2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Объем контрольного участка текста на иностранном языке (до 1500) знаков и контрольные вопросы будут предоставлены участнику перед выполнением задания.

Во время выполнения задания разрешено пользоваться словарем http://www.lingoes.net.

Оценивание конкурсного задания «Перевод профессионального текста» осуществляется следующим образом:

1 задача - перевод текста - 5 баллов;

2 задача – ответы на вопросы, выполнение действия, инструкция на выполнение которого задана в тексте – 5 баллов;

Критерии оценки 1 задачи письменного перевода текста

№	Критерии оценки	Количество баллов
1.	Качество письменной речи	0-3
2.	Грамотность	0-2

По критерию «Качество письменной речи» ставится:

3 балла – текст перевода полностью соответствует содержанию оригинального текста; полностью соответствует профессиональной стилистике и направленности текста; удовлетворяет общепринятым нормам русского языка, не имеет синтаксических конструкций языка оригинала и несвойственных русскому языку выражений и оборотов. Все профессиональные термины переведены правильно. Сохранена структура оригинального текста. Перевод не требует редактирования.

2 балла - текст перевода практически полностью (более 90% от общего объема текста) – понятна направленность текста и его общее содержание соответствует содержанию оригинального текста; в переводе присутствуют 1-4 лексические ошибки; искажен перевод сложных слов, некоторых сложных устойчивых сочетаний, соответствует профессиональной стилистике и направленности текста; удовлетворяет общепринятым нормам русского языка, не имеет синтаксических конструкций языка оригинала и несвойственных русскому языку выражений и оборотов. Присутствуют 1-2 ошибки в переводе профессиональных терминов. Сохранена структура оригинального текста. Перевод не требует редактирования.

1 балл – текст перевода лишь на 50% соответствует его основному содержанию: понятна направленность текста и общее его содержание; имеет пропуски; в переводе присутствуют более 5 лексических ошибок; имеет недостатки в стиле изложения, но передает основное содержание оригинала, перевод требует восполнения всех пропусков оригинала, устранения смысловых искажений, стилистической правки.

0 баллов – текст перевода не соответствует общепринятым нормам русского языка, имеет пропуски, грубые смысловые искажения, перевод требует восполнения всех пропусков оригинала и стилистической правки.

По критерию «Грамотность» ставится

2 балла – в тексте перевода отсутствуют грамматические ошибки (орфографические, пунктуационные и др.);

1 балл – в тексте перевода допущены 1-4 лексические, грамматические, стилистические ошибки (в совокупности);

0 баллов – в тексте перевода допущено более 4 лексических, грамматических, стилистических ошибок (в совокупности).

Критерии оценки 2 задачи
«Перевод профессионального текста (сообщения)»
(ответы на вопросы)

№	Критерии оценки	Количество баллов
1.	Глубина понимания текста	0-4
2.	Независимость выполнения задания	0-1

По критерию «Глубина понимания текста» (в содержание индикаторов выполнения добавляется информация, касающаяся особенностей профиля, УГС) ставится:

4 балла – участник полностью понимает основное содержание текста, умеет выделить отдельную, значимую для себя информацию, догадывается о значении незнакомых слов по контексту;

3 балла – участник не полностью понимает основное содержание текста, умеет выделить отдельную, значимую для себя информацию, догадывается о значении более 80% незнакомых слов по контексту;

2 балла – участник не полностью понимает основное содержание текста, умеет выделить отдельную, значимую для себя информацию, догадывается о значении более 50% незнакомых слов по контексту;

1 балл - участник не полностью понимает основное содержание текста, с трудом выделяет отдельные факты из текста, догадывается о значении менее 50% незнакомых слов по контексту

0 баллов - участник не может выполнить поставленную задачу.

По критерию «Независимость выполнения задания» (в содержание индикаторов выполнения добавляется информация, касающаяся особенностей профиля, УГС 10.00.00 «Информационная безопасность») ставится:

1 балл – участник умеет использовать информацию для решения поставленной задачи самостоятельно без посторонней помощи;

0 баллов - полученную информацию для решения поставленной задачи участник может использовать только при посторонней помощи.

2.4. Практическое задание по организации работы коллектива

Задание

1. Определить продолжительность проекта (в рабочих днях). (Ответ занести в файл)

При определении продолжительности проекта учесть производственный календарь, действующий на территории Пермского края.

Дата начала проекта – 10.01.2019 г. Продолжительность рабочего дня – 8 часов, продолжительность рабочей недели – 40 часов, количество рабочих дне в месяц – 20 (установлено по умолчанию). Рабочее время с 8:00 до 17:00 с перерывом на обед с 12:00 до 13:00. В предпраздничные дни рабочее время сокращается на 1 час.

Продолжительность работ в рабочих днях и порядок их следования приведены в таблице. Тип зависимостей для всех работ– FS (Финиш-Старт).

№ п/п	Название задачи	Длительность, дн.	Предшественник
1	РАЗРАБОТКА СОИБ		
2	Предпроектное обследование	10	
3	Формирование требований к системе	5	
4	ПРОЕКТИРОВАНИЕ СИСТЕМЫ		
5	обсуждение и согласование технических решений	10	2; 3
6	разработка эскизного проекта	8	5
7	разработка технического проекта	20	6
8	разработка комплекта рабочей документации	10	6; 7
9	разработка комплекта эксплуатационной документации	9	7
10	разработка комплекта сметной документации	6	8; 9
11	разработка программы и методики испытаний	6	10
12	ВНЕДРЕНИЕ СИСТЕМЫ		
13	поставка необходимых программных и технических средств	30	11
14	проведение монтажных работ	20	11; 13
15	проведение пусконаладочных работ	20	14
16	КОМПЛЕКС ИСПЫТАНИЙ		
17	предварительные испытания	7	15
18	опытная эксплуатация	3	17
19	приемочные испытания	3	18

2. Перечислить задачи, лежащие на критическом пути проекта. (Ответ занести в файл)

3. Распределить ресурсы по задачам проекта согласно таблице и определить стоимость проекта. (Ответ занести в файл)

Тип ресурса – работа, доступность ресурса – 100 %.

№ п/п	Название задачи	Название ресурса
1	Разработка СОИБ	
2	Предпроектное обследование	гл. инженер специалист по ИБ 1
3	Формирование требований к системе	гл. инженер специалист по ИБ 1 специалист по ИБ 2
4	Проектирование системы	
5	обсуждение и согласование технических решений	гл. инженер проекта (ГИП) гл. инженер специалист по ИБ 1 специалист по ИБ 2
6	разработка эскизного проекта	ГИП проектировщик 1 программист 1
7	разработка технического проекта	ГИП проектировщик 1 проектировщик 2 программист 1 программист 2 программист 3
8	разработка комплекта рабочей документации	ГИП оформитель
9	разработка комплекта эксплуатационной документации	ГИП
10	разработка комплекта сметной документации	ГИП инженер-сметчик
11	разработка программы и методики испытаний	ГИП
12	Внедрение системы	
13	поставка необходимых программных и технических средств	специалист службы снабжения
14	проведение монтажных работ	прораб монтажник 1 монтажник 2 монтажник 3 техник 1 техник 2
15	проведение пусконаладочных работ	прораб техник 1 техник 2 наладчик 1 наладчик 2 наладчик 3
16	комплекс испытаний	

17	предварительные испытания	прораб наладчик 1 техник 1 техник 2 специалист по ИБ 1
18	опытная эксплуатация	прораб представитель эксплуатационной организации
19	приемочные испытания	прораб представитель эксплуатационной организации

Стоимость единицы ресурсов приведена в таблице (стандартная ставка). Способ начисления – пропорционально.

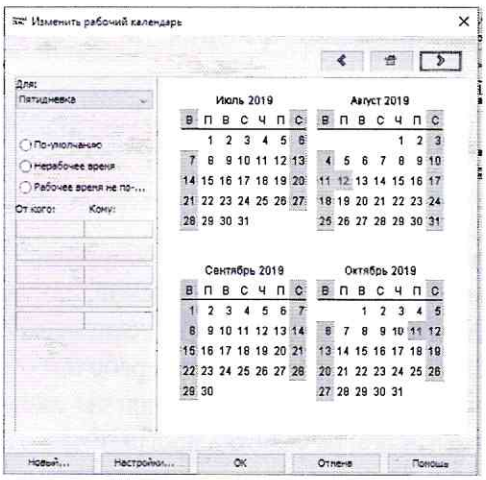
Название ресурса	Стоимость, руб./мес.
гл. инженер	80 000
специалист по ИБ 1	40 000
специалист по ИБ 2	40 000
прораб	50 000
монтажник 1	30 000
монтажник 2	25 000
монтажник 3	24 000
техник 1	20 000
техник 2	15 000
наладчик 1	22 000
наладчик 2	17 000
наладчик 3	15 000
ГИП	90 000
проектировщик 1	40 000
проектировщик 2	44 000
программист 1	25 000
программист 2	30 000
программист 3	35 000
оформитель	25 000
инженер-сметчик	37 000
специалист службы снабжения	26 000
представитель эксплуатационной организации	50 000

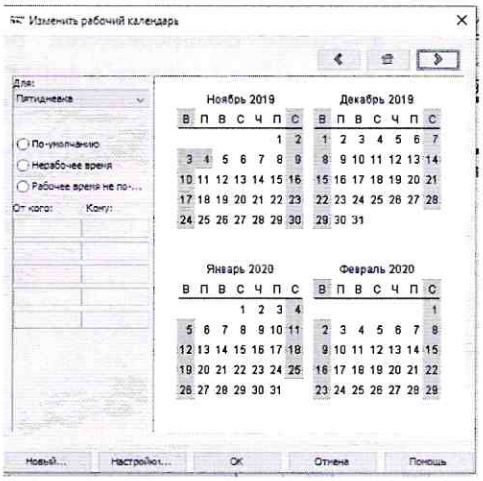
4. После распределения ресурсов определить, какие ресурсы и в какое время перегружены. (Ответ занести в файл)

Форма представления результатов выполнения задания

<table>
<tr><td>1</td><td>Продолжительность проекта, раб. дни</td><td colspan="3">117</td></tr>
<tr><td>2</td><td>Критический путь</td><td colspan="3">Предпроектное обследование, обсуждение и согласование технических решений, разработка эскизного проекта, разработка технического проекта, разработка комплекта рабочей документации, разработка комплекта сметной документации, разработка программы и методики испытаний, поставка необходимых программных и технических средств, проведение монтажных работ, проведение пусконаладочных работ, предварительные испытания, опытная эксплуатация, приемочные испытания</td></tr>
<tr><td>3</td><td>Стоимость проекта, руб.</td><td colspan="3">929 850</td></tr>
<tr><td rowspan="4">4</td><td rowspan="4">Перегруженные ресурсы</td><td rowspan="2">Наименование ресурса</td><td colspan="2">Календарные даты перегрузки ресурса</td></tr>
<tr><td>с</td><td>по</td></tr>
<tr><td>Гл. инженер</td><td>10.01.2019
14.01.2019</td><td>11.01.2019
15.01.2019</td></tr>
<tr><td>Специалист по ИБ 1</td><td>10.01.2019
14.01.2019</td><td>11.01.2019
15.01.2019</td></tr>
<tr><td>ГИП</td><td>25.02.2019
04.03.2019</td><td>01.03.2019
04.03.2019</td></tr>
</table>

Календарь проекта





Разработка системы обеспечения информационной безопасности (СОИБ) для предприятия

Задание выполняется на компьютере, в ПО (opensource) – ProjectLibre, результаты задания заполняются в файле Office Word с наименованием шифра участника и сохраненного файла проекта ProjectLibre на «Рабочем столе».

2.5. Критерии оценки практического задания по организации работы коллектива

1. Определение продолжительности проекта.

Ответ: /количество рабочих дней/ - Оценка за правильный результат - 3балла

несущественные погрешности в расчетах – минус 1 балл;

частичное правильное решение задачи – минус 2 балла

2. Перечислить задачи, лежащие на критическом пути проекта.

Ответ:/перечислить все этапы, лежащие на критическом пути проекта/Оценка за правильный результат - 2 балла.

частичное правильное решение задачи – минус 1 балл

3. Распределить ресурсы по задачам проекта согласно таблице и определить стоимость проекта.

Ответ:/ рублей/ - Оценка за правильный результат - 3 балла

несущественные погрешности в расчетах – минус 1 балл;

частичное правильное решение задачи – минус 2 балла

4. После распределения ресурсов определить, какие ресурсы и в какое время перегружены.

Ответ:/наименование перегруженного ресурса по датам/Оценка за правильный результат - 2 балла

частичное правильное решение задачи – минус 1 балл

3. ПРАКТИЧЕСКИЕ ЗАДАНИЯ II УРОВНЯ

3.1. Задание инвариантной части «Организация защищенной локально-вычислительной сети»

Описание ПО и оборудования для моделирования сети

Задание выполняется на компьютере в ПО Cisco Packet Tracer v.7.2.1.,

Результат выполнения сохраняется под шифром участника на Рабочем столе.

Оборудование

Маршрутизаторы R1, R2, R3 – платформа Cisco 2911 (в R3 в слот eHWIC0 вставлена плата HWIC-2T), маршрутизатор DHCP – платформа Cisco 2811, маршрутизатор RB – платформа Cisco 1841. Коммутаторы S1, S2, SB – платформа Cisco WS-C2960-24TT. Оконечное оборудование: ПК – устройство PC-PT, IP-телефоны типа 7960, сервер – Server-PT

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
R3	Se0/0/0	209.165.24.33	255.255.255.240
	Gi0/0	192.168.0.1	255.255.255.240
	Gi0/1	10.0.0.1	255.255.255.252
	G0/2	10.0.0.5	255.255.255.252
R2	Gi0/0		
	Gi0/0.15	10.0.15.2	255.255.255.0
	Gi0/0.30 Gi0/0.45	10.0.30.2 10.0.45.2	255.255.255.0 255.255.255.0
	Gi0/0.60	10.0.60.2	255.255.255.0
	Gi0/0.75	10.0.75.2	255.255.255.0
	G0/2	10.0.0.6	255.255.255.252
R1	Gi0/0		
	Gi0/0.15	10.0.15.1	255.255.255.0
	Gi0/0.30	10.0.30.1	255.255.255.0
	Gi0/0.45	10.0.45.1	255.255.255.0
	Gi0/0.60	10.0.60.1	255.255.255.0
	Gi0/0.75	10.0.75.1	255.255.255.0
	Gi0/1	10.0.0.2	255.255.255.252
DHCP	Fa0/1		
	Fa0/1.15	10.0.15.3	255.255.255.0
	Fa0/1.30	10.0.30.3	255.255.255.0
	Fa0/1.45	10.0.45.3	255.255.255.0
	Fa0/1.60	10.0.60.3	255.255.255.0
	Fa0/1.75	10.0.75.3	255.255.255.0
S1	VLAN Manage	10.0.30.4	255.255.255.0
S2	VLAN Manage	10.0.30.5	255.255.255.0
RB	Fa0/0	192.168.1.254	255.255.255.0
	Fa0/1	209.165.24.49	255.255.255.240
SB	Vlan1	192.168.1.250	255.255.255.0

ПК-7	Fa0	192.168.1.151	255.255.255.0
ПК-8	Fa0	192.168.1.152	255.255.255.0
ПК-9	Fa0	192.168.1.153	255.255.255.0
Датчик влажности	Fa0	192.168.1.1	255.255.255.0
Датчик температуры	Fa0	192.168.1.2	255.255.255.0
Сервер	Gi1	192.168.0.2	255.255.255.240

Таблица сетей VLAN

Номер сети VLAN — имя	Сеть
15 – Teachers	10.0.15.0/24
30 – Management	10.0.30.0/24
45 – Students	10.0.45.0/24
60 – Guests	10.0.60.0/24
75 – IP-Phones	10.0.75.0/24

Реализация

Все устройства в облаке (топология Интернет – рис.1) полностью настроены, Вы не имеете доступа к устройствам. Вы можете получить доступ ко всем сетевым устройствам основной сети (рис. 2) и устройствам сети филиала (рис.3) для выполнения настройки и проверки.

Используя документацию, реализуйте приведённые ниже требования:

На всех устройствах согласно таблице адресации настройте статические IP-адреса узла, маски подсети, шлюзы по умолчанию (при необходимости).

Маршрутизаторы R1, R2, R3, DHCP, RB, коммутаторы S1, S2, SB:

- Настройте доступ к удалённому управлению устройством, в том числе IP-адресацию и SSH:
  - домен – olimp-spo.ru;
  - пользователь – Admin, секретный пароль – P@55w0rd;
  - длина ключа шифрования составляет 1024 бит;
  - протокол SSH версии 2 с ограничением на две попытки аутентификации и временем ожидания 60 секунд;
  - безопасный вход (там, где это возможно – по протоколу SSH) с локальной проверкой паролей на линиях VTY, консольном входе, линиях AUX сетевых устройств (при их наличии);
  - при бездействии пользователя в течении 5-ти минут произойдёт отключение пользователя;
  - запретить вывод каких-либо консольных сообщений, которые в свою очередь могут прервать ввод команд в консольном режиме;
  - незашифрованные пароли необходимо зашифровать;
  - установить баннер MOTD This is a secure system. Authorized Access Only!;
  - минимальная длина паролей – 8 символов;
  - настроить противодействие атакам типа «подбор пароля»: ограничение количества попыток входа на устройство (если было предпринято 5 неуспешных попыток входа

в течении 60 секунд, то запретить дальнейшие попытки входа на 300 секунд), а также сохранение в журнале успешных и неудачных попыток подключения.

Маршрутизаторы R1, R2, R3, DHCP, RB:

- настроить NTP:
  - NTP-сервер 192.168.0.2;
  - ключ №1;
  - аутентификация по алгоритму MD5 с паролем Ufa2018.

Маршрутизаторы R1, R2, R3, DHCP:

- настройте маршрутизацию между VLAN по стандарту IEEE 802.1Q;
- организуйте маршрутизацию:
  - в качестве протокола маршрутизации используйте OSPF;
  - все интерфейсы (подинтерфейсы) вышеуказанных маршрутизаторов должны принадлежать магистральной области (зоне);
  - отключите интерфейсы, которые не должны посылать сообщения OSPF;
  - организуйте распространение статического маршрута в Интернет по умолчанию;
  - настройте парольную защиту для работы протоколов динамической маршрутизации:
    - алгоритм аутентификации – MD5;
    - пароль OSPF_GUARD;

На маршрутизаторах R3 (в качестве шлюза указать соответствующий интерфейс), RB (в качестве шлюза указать IP-адрес соответствующего соседнего устройства) настройте статические маршруты в Интернет по умолчанию.

Маршрутизатор DHCP:

- настройте службы DHCP для VLAN 15, 30, 45, 60, 75:
  - используйте слово VLAN_X в качестве имени пула (с учетом регистра), где X – номер VLAN;
  - исключите из диапазона адреса A.B.C.1–A.B.C.5, A.B.C.10 для каждой VLAN;
  - для VLAN, используемой для IP-телефонии назначить адрес TFTP-сервера (option 150);
- настройте IP-телефонию:
  - максимальное количество телефонов – 4;
  - максимальное количество линий (номеров) – 4;
  - зарезервировать номера вручную по MAC-адресам IP-телефонов;
  - тип IP-телефона – 7960.

Маршрутизаторы R3, RB, R1, R2:

- настройте преобразование NAT:
  - на R3 настройте именованный список контроля доступа с именем NAT, содержащий восемь записей:
    - пять записей должны запрещать преобразования NAT для IP-трафика сетей VLAN Teachers, Managements, Students, 10.0.0.0/30, 10.0.0.4/30, если из вышеуказанных сетей идёт пересылка данных в сеть филиала;
    - для узла Сервер, если к нему производится доступ с ПК-8;
    - две записи должны разрешать преобразования NAT всего остального IP-трафика для сети, в которой находится сервер Сервер, а также для сети 10.0.0.0/16;
  - на R3 только для протоколов HTTP и HTTPS настройте статический NAT для сервера Сервер, заменяя его внутренний адрес на адрес 209.165.24.40;
  - настройте динамическую трансляцию NAT с использованием PAT, указав выбранное имя пула R3POOL, маску /30 и следующие два общедоступных адреса для R3: 209.165.24.37 и 209.165.24.38;

- на RB настройте именованный список контроля доступа с именем NAT, содержащий семь записей:
  - пять записей должны запрещать преобразования NAT для IP-трафика сети филиала, если из неё идёт пересылка данных в сети VLAN Teachers, Managements, Students, 10.0.0.0/30, 10.0.0.4/30;
  - одна запись должна запрещать преобразования NAT для IP-трафика узла сервер Сервер к ПК-8;
  - одна запись должны разрешать преобразования NAT для всего остального IP-трафика сети филиала;
- настройте динамическую трансляцию NAT с использованием PAT, указав выбранное имя пула RBPOOL, маску /30 и следующие два общедоступных адреса для RB: 209.165.24.53 и 209.165.24.54;

– настройте VPN-туннель между маршрутизаторами R3 и RB:
- на маршрутизаторе RB создать расширенный список контроля доступа, состоящий из 6 записей и имеющий номер 110:
  - 5 записей для пар подсетей, 192.168.1.0/24–10.0.15.0/24, 192.168.1.0/24–10.0.30.0/24, 192.168.1.0/24–10.0.45.0/24, 192.168.1.0/24–10.0.0.0/30, 192.168.1.0/24–10.0.0.4/30;
  - шестая запись для доступа к серверу Сервер с ПК-8;
- на маршрутизаторе R3 для пар подсетей 192.168.1.0/24–10.0.15.0/24, 192.168.1.0/24–10.0.30.0/24, 192.168.1.0/24–10.0.45.0/24, 192.168.1.0/24–10.0.0.0/30, 192.168.1.0/24–10.0.0.4/30 создать расширенный список контроля доступа, состоящий из 5 записей и имеющий номер 110;
- первая фаза:
  - политика (приоритет) – 10;
  - тип алгоритма шифрования – AES;
  - тип алгоритма обеспечения целостного данных – SHA;
  - обмен ключами: группа – 2;
  - тип аутентификации – с заранее заданным ключом (pre-share);
  - пароль – VPN_P@55w0rd;
  - время жизни туннеля – 1 час;
- вторая фаза:
  - название VPN_SET;
  - тип алгоритма шифрования – AES;
  - тип алгоритма обеспечения целостного данных – SHA-HMAC;
  - тэг (криптографическая карта) для дальнейшего использования на интерфейсе – VPN_MAP;

– на R1 и R2 настройте именованные списки контроля доступа VLAN15, VLAN30, VLAN45, VLAN60, VLAN75 для ограничения трафика доступа между группами пользователей:
- ACL VLAN15 должен состоять из 7 записей:
  - первые четыре записи должны запрещать по протоколу IP доступ из сети 10.0.15.0/24 в сети 10.0.30.0/24, 10.0.45.0/24, 10.0.60.0/24, 10.0.75.0/24;
  - следующие две записи должны запрещать по протоколу IP доступ из сети 10.0.15.0/24 к узлам 192.168.1.152 и 192.168.1.153;
  - седьмая запись должна разрешать любой трафик по протоколу IP;
  - применить этот ACL на входящем направлении подинтерфейса GigabitEthernet0/0.15;
- ACL VLAN30 должен состоять из 7 записей:
  - первые четыре записи должны запрещать по протоколу IP доступ из сети 10.0.30.0/24 в сети 10.0.15.0/24, 10.0.45.0/24, 10.0.60.0/24, 10.0.75.0/24;

        - следующие две записи должны запрещать по протоколу IP доступ из сети 10.0.30.0/24 к узлам 192.168.1.151 и 192.168.1.153;
        - седьмая запись должна разрешать любой трафик по протоколу IP;
        - применить этот ACL на входящем направлении подинтерфейса GigabitEthernet0/0.30;
    - ACL VLAN45 должен состоять из 7 записей:
        - первые четыре записи должны запрещать по протоколу IP доступ из сети 10.0.45.0/24 в сети 10.0.15.0/24, 10.0.30.0/24, 10.0.60.0/24, 10.0.75.0/24;
        - следующие две записи должны запрещать по протоколу IP доступ из сети 10.0.45.0/24 к узлам 192.168.1.151 и 192.168.1.152;
        - седьмая запись должна разрешать любой трафик по протоколу IP;
        - применить этот ACL на входящем направлении подинтерфейса GigabitEthernet0/0.45;
    - ACL VLAN60 должен состоять из 8 записей:
        - первые четыре записи должны запрещать по протоколу IP доступ из сети 10.0.60.0/24 в сети 10.0.15.0/24, 10.0.30.0/24, 10.0.45.0/24, 10.0.75.0/24;
        - следующие три записи должны запрещать по протоколу IP доступ из сети 10.0.60.0/24 к узлам 192.168.1.151, 192.168.1.152 и 192.168.1.153;
        - восьмая запись должна разрешать любой трафик по протоколу IP;
        - применить этот ACL на входящем направлении подинтерфейса GigabitEthernet0/0.60;
    - ACL VLAN75 должен состоять из 8 записей:
        - первые четыре записи должны запрещать по протоколу IP доступ из сети 10.0.75.0/24 в сети 10.0.15.0/24, 10.0.30.0/24, 10.0.45.0/24, 10.0.60.0/24;
        - следующие три записи должны запрещать по протоколу IP доступ из сети 10.0.75.0/24 к узлам 192.168.1.151, 192.168.1.152 и 192.168.1.153;
        - восьмая запись должна разрешать любой трафик по протоколу IP;
        - применить этот ACL на входящем направлении подинтерфейса GigabitEthernet0/0.75.

Маршрутизаторы R1, R2:

- настроить протокола резервирования шлюза HSRP на R1:
    - для VLAN 15, 30 назначить группу резервирования 1, приоритет 110, отслеживание интерфейса Gi0/1;
    - для VLAN 45, 60, 75 назначить группу резервирования 2, приоритет 90, отслеживание интерфейса Gi0/1;
- настроить протокола резервирования шлюза HSRP на R2:
    - для VLAN 15, 30 назначить группу резервирования 1, приоритет 90, отслеживание интерфейса Gi0/2;
    - для VLAN 45, 60, 75 назначить группу резервирования 2, приоритет 110, отслеживание интерфейса Gi0/2.

Коммутаторы S1, S2:

- настройте сети VLAN, присвойте им имена и выполните назначение портов доступа с учётом голосовой VLAN;
- включите функцию PortFast для портов доступа;
- включите функцию BPDU guard;
- создайте между S1 и S2 агрегированный канал по технологии Etherchannel:
    - интерфейсы, используемые для создания канала – Fa0/15– Fa0/20;
    - название канала – Port-channel 1;
    - группа каналов – 1;
    - режим и протокол работы – активный/LACP;
    - переведите его в режим транка (магистрального канала);

- настройте транки (магистральные каналы);
- выключите неиспользуемые порты коммутаторов;
- создайте стандартный список контроля доступа из двух строк с номером 20 в котором разрешите доступ узлу ПК-8, а также из VLAN Management и примените его для линий VTY;
- настройте защиту протоколов связующего дерева на S1:
  - для VLAN 1, 15, 30 назначить его основным корневым мостом;
  - для VLAN 35, 60, 75 назначить его вспомогательным корневым мостом;
- настройте защиту протоколов связующего дерева на S2:
  - для VLAN 1, 15, 30 назначить его вспомогательным корневым мостом;
  - для VLAN 45, 60, 75 назначить его основным корневым мостом;
- настройте функцию Port Security для интерфейсов Fa0/1, Fa0/2:
  - разрешите доступ для трёх MAC-адресов, которые автоматически добавляются в файл конфигурации после обнаружения;
  - в случае нарушения безопасности порт не должен выключаться, но должно быть зафиксировано сообщение системного журнала;
- настройте функцию Port Security для интерфейса Fa0/3:
  - разрешите доступ для одного MAC-адреса, которые автоматически добавляются в файл конфигурации после обнаружения;
  - в случае нарушения безопасности порт не должен выключаться, но должно быть зафиксировано сообщение системного журнала;
- настройте функцию Port Security для интерфейса Fa0/24 коммутатора S1:
  - разрешите доступ для одного MAC-адреса, которые автоматически добавляются в файл конфигурации после обнаружения;
  - в случае нарушения безопасности порт не должен выключаться, но должно быть зафиксировано сообщение системного журнала;
- настройте защиту от атак, связанных с протоколами ARP(DAI) и DHCP (DHCP Snooping):
  - для VLAN 15, 30, 45, 60, 75;
  - примените её на интерфейсе Fa0/24 коммутатора S2;
- настройте ограничение протокола DHCP на активных не доверенных портах доступа на 10 запросов;
- настройте шлюз по умолчанию для VLAN Management.

Коммутатор SB:

- включите функцию PortFast для портов доступа;
- включите функцию BPDU guard;
- выключите неиспользуемые порты коммутаторов;
- создайте стандартный список контроля доступа из двух строк с номером 20 в котором разрешите доступ узлу ПК-8 а также из VLAN Management и примените его для линий VTY;
- настройте функцию Port Security для интерфейсов Fa0/1, Fa0/2, Fa0/15, Fa0/16:
  - разрешите доступ для одного MAC-адреса, которые автоматически добавляются в файл конфигурации после обнаружения;
  - в случае нарушения безопасности порт не должен выключаться, но должно быть зафиксировано сообщение системного журнала;
- настройте шлюз по умолчанию.
-

Проверка

В рамках задания необходимо:

1. Успешно отправить эхо-запросы между узлами:
   - ПК-1 – ПК-4;
   - ПК-2 – ПК-5;

- ПК-3 – ПК-6;
- ПК-1 – ПК-7;
- ПК-2 – ПК-8;
- ПК-3 – ПК-9.

2. Получить доступ с узлов ПК-1, ПК-2, ПК-3, ПК-7 к серверу Сервер по протоколу HTTP.

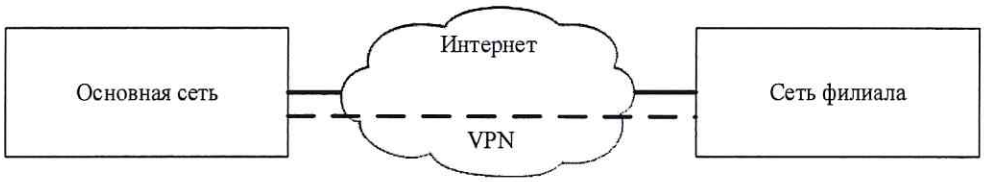


Рисунок 1 – Общая топология сети

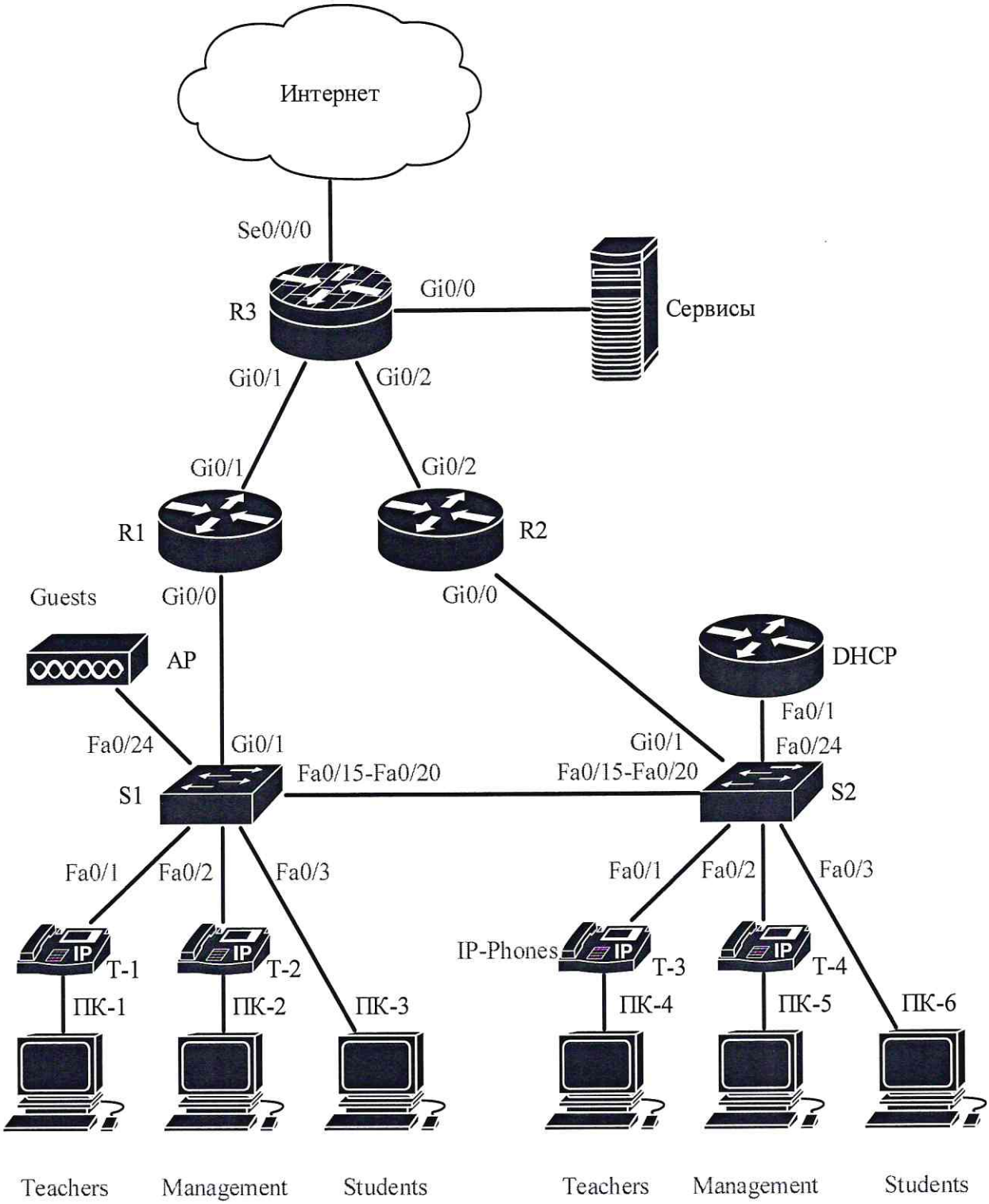


Рисунок 2 – Топология основной сети
(синим цветом указана принадлежность портов к VLAN)

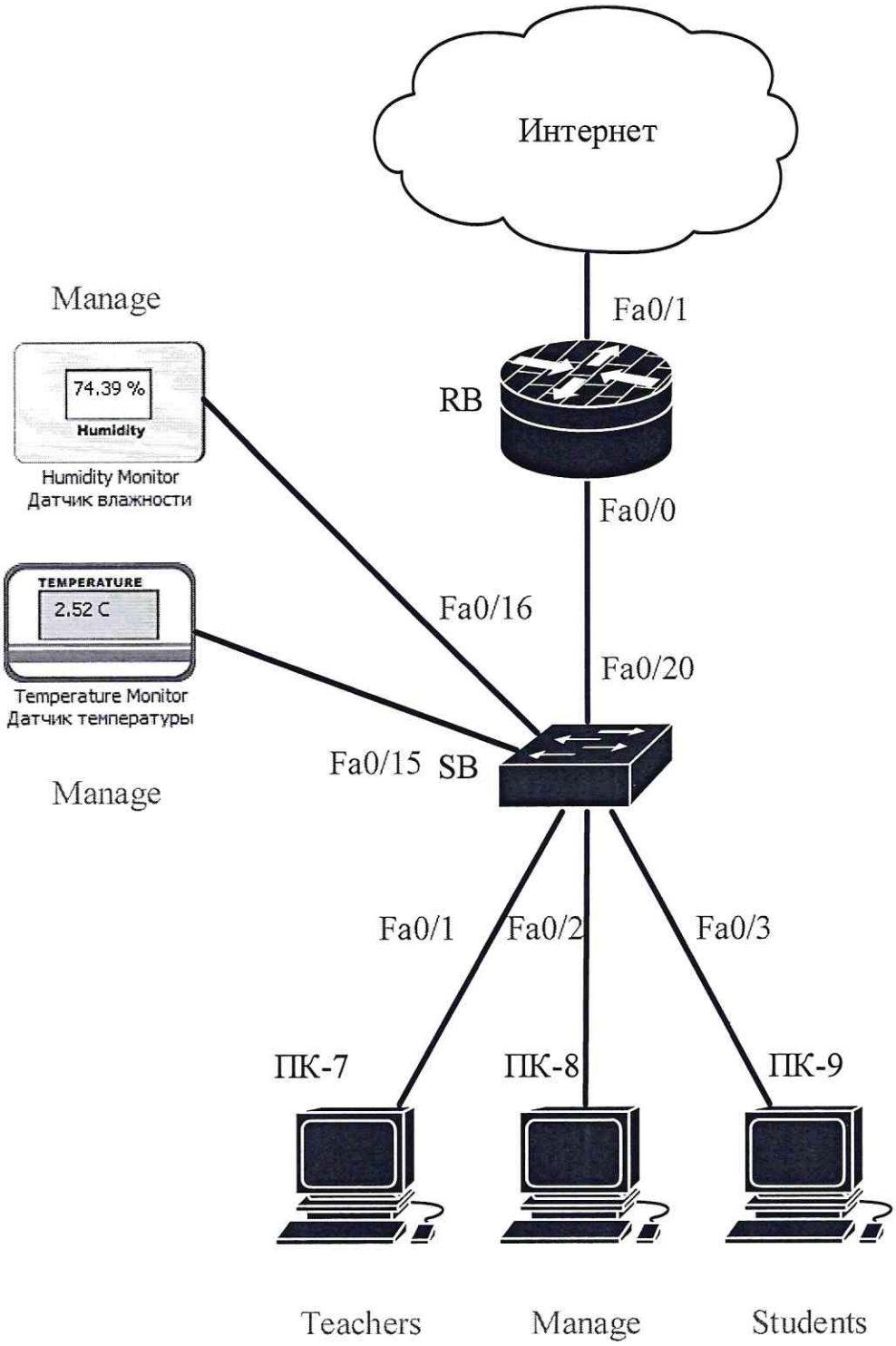


Рисунок 3 – Топология сети филиала

3.2. Критерии оценки «Организация защищенной локально-вычислительной сети»

Общая оценка программы: 350. Для оценивания результат данного этапа олимпиады предлагается поделить оценку программы, заработанных участником на 10 для того, чтобы не превысить лимит в 35 очков.

№	Оцениваемый параметр	Оценка программы	Количество баллов
1	Успешный эхо-запрос между узлами ПК-1 – ПК-4	1	0,1
2	Успешный эхо-запрос между узлами ПК-2 – ПК-6	1	0,1
3	Успешный эхо-запрос между узлами ПК-3 – ПК-6	1	0,1
4	Успешный эхо-запрос между узлами ПК-1 – ПК-7	1	0,1
5	Успешный эхо-запрос между узлами ПК-2 – ПК-8	1	0,1
6	Успешный эхо-запрос между узлами ПК-3 – ПК-9	1	0,1
7	Настройка пользователя Admin на маршрутизаторе DHCP	1	0,1
8	Настройка пользователя Admin на маршрутизаторе R1	1	0,1
9	Настройка пользователя Admin на маршрутизаторе R2	1	0,1
10	Настройка пользователя Admin на маршрутизаторе R3	1	0,1
11	Настройка пользователя Admin на маршрутизаторе RB	1	0,1
12	Настройка пользователя Admin на коммутаторе S1	1	0,1
13	Настройка пользователя Admin на коммутаторе S2	1	0,1
14	Настройка пользователя Admin на коммутаторе SB	1	0,1
15	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе DHCP	2	0,2
16	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R1	2	0,2
17	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R2	2	0,2
18	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R3	2	0,2
19	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе RB	2	0,2
20	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе S1	2	0,2
21	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе S2	2	0,2
22	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе SB	2	0,2
23	Настройка доступа по протоколу SSH на маршрутизаторе DHCP	3	0,3
24	Настройка доступа по протоколу SSH на маршрутизаторе R1	3	0,3
25	Настройка доступа по протоколу SSH на маршрутизаторе R2	3	0,3
26	Настройка доступа по протоколу SSH на маршрутизаторе R3	3	0,3
27	Настройка доступа по протоколу SSH на маршрутизаторе RB	3	0,3
28	Настройка доступа по протоколу SSH на коммутаторе S1	3	0,3
29	Настройка доступа по протоколу SSH на коммутаторе S2	3	0,3
30	Настройка доступа по протоколу SSH на коммутаторе SB	3	0,3
31	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе DHCP	3	0,3

3	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R1	3	0,3
3	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R2	3	0,3
3	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R3	3	0,3
3	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе RB	3	0,3
3	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе S1	3	0,3
3	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе S2	3	0,3
3	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе SB	3	0,3
3	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе DHCP	2	0,2
4	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R1	2	0,2
4	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R2	2	0,2
4	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R3	2	0,2
4	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе RB	2	0,2
4	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе S1	2	0,2
4	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе S2	2	0,2
4	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе SB	2	0,2
4	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе DHCP	3	0,3
4	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R1	3	0,3
4	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R2	2	0,2
5	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R3	3	0,3
5	Настройка баннера MOTD и минимальной длины паролей,	3	0,3

	шифрование незашифрованных паролей на маршрутизаторе RB		
5	Настройка баннера MOTD, шифрование незашифрованных паролей на коммутаторе S1	2	0,2
5	Настройка баннера, шифрование незашифрованных паролей на коммутаторе S2	2	0,2
5	Настройка баннера, шифрование незашифрованных паролей на коммутаторе SB	2	0,2
5	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство DHCP	3	0,3
5	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R1	3	0,3
5	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R2	3	0,3
5	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R3	3	0,3
5	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство RB	3	0,3
6	Настройка NTP-клиента на маршрутизаторе DHCP	5	0,5
6	Настройка NTP-клиента на маршрутизаторе R1	5	0,5
6	Настройка NTP-клиента на маршрутизаторе R2	5	0,5
6	Настройка NTP-клиента на маршрутизаторе R3	5	0,5
6	Настройка NTP-клиента на маршрутизаторе RB	5	0,5
6	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R1	2	0,2
6	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R2	2	0,2
6	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R3	4	0,4
6	Настройка именованного списка контроля доступа **NAT** на маршрутизаторе R3	1	0,1
6	Настройка именованного списка контроля доступа **NAT** на маршрутизаторе RB	1	0,1
7	Настройка пула NAT R3POOL на маршрутизаторе R3	2	0,2
7	Настройка статического NAT для сервера **Сервер** на маршрутизаторе R3	2	0,2
7	Настройка пула NAT RBPOOL на маршрутизаторе RB	2	0,2
7	Настройка VPN-туннеля на маршрутизаторе R3	20	2
7	Настройка VPN-туннеля на маршрутизаторе RB	20	2
7	Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45, VLAN60, VLAN75** на маршрутизаторе R1	10	1
7	Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45, VLAN60, VLAN75** на маршрутизаторе R2	10	1
7	Настройка протокола резервирования шлюза HSRP на маршрутизаторе R1	20	2
7	Настройка протокола резервирования шлюза HSRP на	20	2

	маршрутизаторе R2		
7	Настройка VLAN, присвоение им имён на коммутаторе S1	5	0,5
8	Настройка VLAN, присвоение им имён на коммутаторе S2	5	0,5
8	Назначение портов доступа на интерфейсах коммутатора S1, включение функций PortFast и BPDU guard	14	1,4
8	Назначение портов доступа на интерфейсах коммутатора S2, включение функций PortFast и BPDU guard	11	1,1
8	Настройка функции Port Security на коммутаторе S1	12	1,2
8	Настройка функции Port Security на коммутаторе S2	9	0,9
8	Настройка защиты от атак, связанных с протоколом DHCP (DHCP Snooping) для VLAN 15, 30, 45, 60, 75 и применение её на интерфейсе Fa0/24 коммутатора S2	6	0,6
8	Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S1	4	0,4
8	Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S2	3	0,3
8	Настройка стандартного списка контроля доступа из двух строк с номером 20 в котором разрешён доступ узлу ПК-8 и VLAN Management и применение его для линий VTY на коммутаторе SB	10	1
8	Настройка шлюза по умолчанию на коммутаторе SB	1	0,1
Максимальная оценка программы		350	
Максимальное количество баллов			35

3.3. Задание вариативной части с применением знаний, умений в области информационно-коммуникационных технологий

Настройка Secret Net Studio

1. Настроить вход в систему:
    - 1.1. Максимальный период неактивности до блокировки экрана: 15 мин.
    - 1.2. Количество неудачных попыток: 10
    - 1.3. Задать парольную политику:
        - 1.1.1. Минимальная длина: 12 символов
        - 1.1.2. Максимальный срок действия паролей: 40 дней
        - 1.1.3. Включить контроль сложности пароля
2. Средствами Secret Net Studio создать группы пользователей Преподаватели и Студенты
3. Средствами Secret Net Studio создать пользователей

Пользователь	Группы
Студент1	Студенты
Студент2	Студенты
Студент3	Студенты
Преподаватель1	Преподаватели
Преподаватель2	Преподаватели

4. Настройка полномочного доступа:
    - 4.1. Создать уровни доступа следующим образом (порядок важен!):
        - 4.1.1. Неконфиденциально
        - 4.1.2. Студенты
        - 4.1.3. Преподаватели
        - 4.1.4. Конфиденциально
        - 4.1.5. Строго конфиденциально

Пользователю **admin** задать пароль, назначить максимальный уровень доступа.
Пользователям групп

3.4. Критерии оценивания вариативной части с применением знаний, умений в области информационно-коммуникационных технологий

3.4.

<table>
<tr><td>№</td><td colspan="5">10.00.00 Информационная безопасность</td></tr>
<tr><td>1</td><td colspan="3">10.02.01 Организация и технология защиты информации,
№ 805 от 28.07.2017 г.</td><td colspan="2">10.02.02 Информационная безопасность телекоммуникационных систем, № 1000 от 13 августа 2014 г.</td></tr>
<tr><td>2</td><td colspan="3">ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.
ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов
ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.
3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов</td><td colspan="2">ПК 2.1. Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем.
ПК 2.2. Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем, их диагностику, обнаружение отказов, формировать предложения по их устранению.
ПК 2.3. Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем.
ПК 2.4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей</td></tr>
<tr><td></td><td colspan="3">10.02.03 Задание 3 «Настройка программного средства безопасности Secret Net Studio»</td><td colspan="2">10.02.02 Задание 3 «Настройка программного средства безопасности Secret Net Studio»</td></tr>
<tr><td></td><td colspan="3"><table>
<tr><td>№</td><td>Оцениваемый параметр</td><td>Количество баллов</td></tr>
<tr><td>1</td><td>- Настройка системы в соответствии с условиями</td><td>1</td></tr>
<tr><td>2</td><td>Создать уровни доступа и права в системе</td><td>1</td></tr>
</table></td><td colspan="2"><table>
<tr><td>№</td><td>Оцениваемый параметр</td><td>1</td></tr>
<tr><td>1</td><td>- Настройка системы в соответствии с условиями</td><td>1</td></tr>
<tr><td>2</td><td>Создать уровни доступа и права в системе</td><td>1</td></tr>
</table></td></tr>
</table>

	3	Создать файлы и настроить доступ	1	3	Создать файлы и настроить доступ	1
	4	- создать файл и настроить ему уровень доступа.	1	4	- создать файл и настроить ему уровень доступа.	1
	5	-Заблокировать доступ к оптическим дискам	1	5	-Заблокировать доступ к оптическим дискам	1
	6	- настройка запуска программ	1	6	- настройка запуска программ	1
	7	- Выполнить аудит системы	1	7	- Выполнить аудит системы	1