Согласовано
Директор
ФГУП филиал РТРС
«Белгородский ОРТПЦ
_____ С.П. Моисеев
от «20» января 2020 г.

Рассмотрено
Председателем Регионального
учебно-методического
объединения
_____ Е.Н. Масловская
от «20» января 2020 г.

Утверждаю
Директор ОГАПОУ
«Белгородский
индустриальный колледж»
_____ О.А. Шаталов
от «20» января 2020 г.

Фонд оценочных средств
Всероссийской олимпиады профессионального мастерства
по укрупненной группе специальностей СПО
10.00.00 Информационная безопасность
код и наименование

Белгород, 2020

ФОС разработан в ОГАПОУ «Белгородский индустриальный колледж»

– Внукова Наталья Владимировна – преподаватель ОГАПОУ «Белгородский индустриальный колледж»;

– Солдатенко Мария Николаевна – преподаватель ОГАПОУ «Белгородский индустриальный колледж»;

– Третьяк Ирина Юрьевна – преподаватель ОГАПОУ «Белгородский индустриальный колледж»;

– Александров Виталий Витальевич – доцент, к.т.н. АНО ВО «Белгородский университет кооперации, экономики и права».

(указываются авторы разработки)

Рецензенты

1. Утенин Алексей Петрович – заместитель технического директора Белгородского филиала ПАО «Ростелеком»

Ф.И.О., должность, место работы (указывается полностью в соответствии с правоустанавливающими документами), ученая степень, ученое звание (при наличии).

СОДЕРЖАНИЕ

I. СПЕЦИФИКАЦИЯ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1. Назначение Фонда оценочных средств

1.1. Фонд оценочных средств (далее – ФОС) - комплекс методических и оценочных средств, предназначенных для определения уровня сформированности компетенций участников Всероссийской олимпиады профессионального мастерства обучающихся по специальностям среднего профессионального образования (далее – Олимпиада).

ФОС является неотъемлемой частью методического обеспечения процедуры проведения Олимпиады, входит в состав комплекта документов организационно-методического обеспечения проведения Олимпиады.

Оценочные средства – это контрольные задания, а также описания форм и процедур, предназначенных для определения уровня сформированности компетенций участников олимпиады.

1.2. На основе результатов оценки конкурсных заданий проводятся следующие основные процедуры в рамках Всероссийской олимпиады профессионального мастерства:

процедура определения результатов участников, выявления победителя олимпиады (первое место) и призеров (второе и третье места);

процедура определения победителей в дополнительных номинациях.

2. Документы, определяющие содержание Фонда оценочных средств

2.1. Содержание Фонда оценочных средств определяется на основе и с учетом следующих документов:

Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

приказа Министерства образования и науки Российской Федерации от 14 июня 2013 г. № 464 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования» (в ред. приказа Минобрнауки России от 15 декабря 2014 г. № 1580);

приказа Министерства образования и науки Российской Федерации от 29 октября 2013 г. № 1199 «Об утверждении перечня специальностей среднего профессионального образования» (в ред. Приказов Минобрнауки России от 14.05.2014 N 518, от 18.11.2015 N 1350, от 25.11.2016 N 1477);

регламента организации и проведения Всероссийской олимпиады профессионального мастерства обучающихся по специальностям среднего профессионального образования, утвержденного директором Департамента государственной политики в сфере профессионального

образования и опережающей подготовки кадров Министерства просвещения Российской Федерации И.А. Черноскутовой 06.02.2019 № 05-99;

приказа Министерства образования и науки Российской Федерации от 28.07.2014 г. № 805 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.01 Организация и технология защиты информации»;

приказа Министерства образования и науки Российской Федерации от 21.08.2014 г. 806 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.03 Информационная безопасность автоматизированных систем»;

приказа Министерства образования и науки Российской Федерации от 13.08.2014 г. № 1000 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.02 Информационная безопасность телекоммуникационных систем»;

приказа Министерства труда и социальной защиты РФ от 3 ноября 2016 г. № 608н «Об утверждении профессионального стандарта Специалист по защите информации в телекоммуникационных системах и сетях»;

приказа Министерства труда и социальной защиты РФ от 15.09.2016 № 522н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах»; Регламента Финала национального чемпионата «Молодые профессионалы» (WORLDSKILLS RUSSIA)

3. Подходы к отбору содержания, разработке структуры оценочных средств и процедуре применения

3.1. Программа конкурсных испытаний Олимпиады предусматривает для участников выполнение заданий двух уровней.

Задания I уровня формируются в соответствии с общими и профессиональными компетенциями специальностей среднего профессионального образования.

Задания II уровня формируются в соответствии с общими и профессиональными компетенциями специальностей укрупненной группы специальностей СПО.

Для лиц с ограниченными возможностями здоровья формирование заданий осуществляется с учетом типа нарушения здоровья.

3.2. Содержание и уровень сложности предлагаемых участникам заданий соответствуют федеральным государственным образовательным стандартам СПО, учитывают основные положения соответствующих профессиональных стандартов, требования работодателей к специалистам среднего звена.

3.3. Задания 1 уровня состоят из тестового задания и практических задач.

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

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

Инвариантная часть задания «Тестирование» содержит 16 вопросов по четырем тематическим направлениям, из них 4 – закрытой формы с выбором ответа, 4 – открытой формы с кратким ответом, 4 - на установление соответствия, 4 - на установление правильной последовательности.

Вариативная часть задания «Тестирование» содержит 24 вопроса не менее, чем по трем тематическим направлениям. Тематика, количество и формат вопросов по темам вариативной части тестового задания формируются на основе знаний, общих для специальностей, входящих в УГС, по которой проводится Олимпиада.

Алгоритм формирования инвариантной части задания «Тестирование» для участника Олимпиады единый для всех специальностей СПО.

Таблица 1. Алгоритм формирования содержания задания «Тестирование»

№ п\п	**Наименование темы вопросов**	**Кол-во вопросов**	**Формат вопросов**				
			Выбор ответа	**Открытая форма**	**Вопрос на соответствие**	**Вопрос на установление послед.**	**Макс. балл**
	Инвариантная часть тестового задания						
1	Информационные технологии в профессиональной деятельности	4	1	1	1	1	1
2	Системы качества, стандартизации и сертификации	4	1	1	1	1	1
3	Охрана труда, безопасность жизнедеятельности, безопасность окружающей среды	4	1	1	1	1	1

4	Экономика и правовое обеспечение профессиональной деятельности	4	1	1	1	1	1
	ИТОГО:	**16**	4	4	4	4	**4**
	Вариативный раздел тестового задания УГС10.00.00 Информационная безопасность						
5	Основы информационной безопасности	8	2	2	2	2	2
6	Организация и сопровождение электронного документооборота/ Криптографическая защита информации/ Криптографические средства и методы защиты информации	4	1	1	1	1	1
7	Технические методы и средства, технологии защиты информации/ Инженерно-техническая защита информации/ Применение инженерно-технических средств обеспечения информационной безопасности	4	1	1	1	1	1
8	Программно-аппаратные средства защиты информации/ Программно-аппаратные средства защищенных телекоммуникационных систем/ Программно-аппаратные средства обеспечения информационной безопасности	4	1	1	1	1	2
9	Обеспечение организации системы безопасности организации/Правовая защита информации/	4	1	1	1	1	1
	ИТОГО:	**24**	6	6	6	6	**6**
	ИТОГО:	**40**	10	10	10	10	**10**

Вопрос закрытой формы с выбором одного варианта ответа состоит из неполного тестового утверждения с одним ключевым элементом и множеством допустимых заключений, одно из которых являются правильным.

Вопрос открытой формы имеет вид неполного утверждения, в котором отсутствует один или несколько ключевых элементов, в качестве которых могут быть: число, слово или словосочетание. На месте ключевого элемента в тексте задания ставится многоточие или знак подчеркивания.

Вопрос на установление правильной последовательности состоит из однородных элементов некоторой группы и четкой формулировки критерия упорядочения этих элементов.

Вопрос на установление соответствия. Состоит из двух групп элементов и четкой формулировки критерия выбора соответствия между ними. Соответствие устанавливается по принципу 1:1 (одному элементу первой группы соответствует только один элемент второй группы). Внутри каждой группы элементы должны быть однородными. Количество элементов во второй группе должно соответствовать количеству элементов первой группы. Количество элементов как в первой, так и во второй группе должно быть не менее четырех.

Выполнение задания «Тестирование» реализуется посредством применения прикладных компьютерных программ, что обеспечивает возможность генерировать для каждого участника уникальную последовательность заданий, содержащую требуемое количество вопросов из каждого раздела и исключающую возможность повторения заданий. Для лиц с ограниченными возможностями здоровья предусматриваются особые условия проведения конкурсного испытания.

При выполнении задания «Тестирование» участнику Олимпиады предоставляется возможность в течение всего времени, отведенного на выполнение задания, вносить изменения в свои ответы, пропускать ряд вопросов с возможностью последующего возврата к пропущенным заданиям.

3.5. Практические задания I уровня включают два вида заданий: задание «Перевод профессионального текста (сообщения)» и «Задание по организации работы коллектива».

3.6. Задание «Перевод профессионального текста (сообщения)» позволяет оценить уровень сформированности:

умений применять лексику и грамматику иностранного языка для перевода текста на профессиональную тему;

умений общаться (устно и письменно) на иностранном языке на профессиональные темы;

способность использования информационно-коммуникационных технологий в профессиональной деятельности.

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

перевод текста, содержание которого включает профессиональную лексику (возможен вариант аудирования);

ответы на вопросы по тексту (аудирование, выполнение действия).

Объем текста на иностранном языке составляет не менее 1500 знаков.

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

В качестве текста для перевода используется международный стандарт по профилю УГС 10.00.00 Информационная безопасность.

3.7. «Задание по организации работы коллектива» позволяет оценить уровень сформированности:

умений организации производственной деятельности подразделения;

умения ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий;

способности работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями;

способность использования информационно-коммуникационных технологий в профессиональной деятельности.

Задание по организации работы коллектива включает две задачи:

1. Определение продолжительности проекта с перечислением задач, лежащих на критическом пути проекта.

2. Распределение ресурсов по задачам проекта согласно таблице и определение стоимости проекта и выявления перегруженных ресурсов.

3.8. Задания II уровня - это работа, которую необходимо выполнить участнику для демонстрации определённого вида профессиональной деятельности в соответствии с требованиями ФГОС и профессиональных стандартов с применением практических навыков.

Количество заданий II уровня, составляющих общую или вариативную часть, одинаковое для специальностей или УГС профильного направления Олимпиады.

3.9. Задания II уровня подразделяются на инвариантную и вариативную части.

3.10. Инвариантная часть заданий II уровня формируется в соответствии с общими и профессиональными компетенциями специальностей УГС10.00.00 Информационная безопасность, умениями и практическим опытом, которые являются общими для всех специальностей, входящих в УГС10.00.00 Информационная безопасность.

Инвариантная часть заданий II уровня представляет собой практическое задание, которые содержит 1- 3 задачи.

Количество оцениваемых задач, составляющих то или иное практическое задание, одинаковое для всех специальностей СПО, входящих в УГС10.00.00 Информационная безопасность, по которой проводится Олимпиада.

3.11. Вариативная часть задания II уровня формируется в соответствии с общими компетенциями и со специфическими для каждой специальности, входящей в УГС10.00.00 Информационная безопасность, профессиональными компетенциями, умениями и практическим опытом с учетом трудовых функций профессиональных стандартов.

Практические задания разработаны в соответствии с объектами и видами профессиональной деятельности обучающихся по конкретным специальностям, или подгруппам специальностей, входящим в УГС10.00.00 Информационная безопасность.

Вариативная часть задания II уровня представляет собой практическое задание, которые содержит 1- 4 задачи.

3.12. Для лиц с ограниченными возможностями здоровья определение структуры и отбор содержания оценочных средств осуществляется с учетом типа нарушения здоровья.

4. Система оценивания выполнения заданий

4.1. Оценивание выполнения конкурсных заданий осуществляется на основе следующих принципов:

соответствия содержания конкурсных заданий ФГОС СПО по специальностям, входящим в укрупненную группу специальностей, учёта требований профессиональных стандартов и работодателей;

достоверности оценки – оценка выполнения конкурсных заданий должна базироваться на общих и профессиональных компетенциях участников Олимпиады, реально продемонстрированных в моделируемых профессиональных ситуациях в ходе выполнения профессионального комплексного задания;

адекватности оценки – оценка выполнения конкурсных заданий должна проводиться в отношении тех компетенций, которые необходимы для эффективного выполнения задания;

надежности оценки – система оценивания выполнения конкурсных заданий должна обладать высокой степенью устойчивости при неоднократных (в рамках различных этапов Олимпиады) оценках компетенций участников Олимпиады;

комплексности оценки – система оценивания выполнения конкурсных заданий должна позволять интегративно оценивать общие и профессиональные компетенции участников Олимпиады;

объективности оценки – оценка выполнения конкурсных заданий должна быть независимой от особенностей профессиональной ориентации или предпочтений членов жюри.

4.2. При выполнении процедур оценки конкурсных заданий используются следующие основные методы:

метод экспертной оценки;

метод расчета первичных баллов;

метод расчета сводных баллов;

метод агрегирования результатов участников Олимпиады;

метод ранжирования результатов участников Олимпиады.

4.3. Результаты выполнения практических конкурсных заданий оцениваются с использованием следующих групп целевых индикаторов: основных и штрафных.

4.2. При оценке конкурсных заданий используются следующие основные процедуры:

процедура начисления основных баллов за выполнение заданий;

процедура начисления штрафных баллов за выполнение заданий;

процедура формирования сводных результатов участников Олимпиады;

процедура ранжирования результатов участников Олимпиады.

4.4. Результаты выполнения конкурсных заданий оцениваются по 100-балльной шкале:

за выполнение заданий I уровня максимальная оценка - 30 баллов: тестирование -10 баллов, практические задачи – 20 баллов (перевод текста – 10 баллов, задание по организации работы коллектива – 10 баллов);

за выполнение заданий II уровня максимальная оценка - 70 баллов (инвариантная часть задания – 35 баллов, вариативная часть задания – 35 баллов).

4.5. Оценка за задание «Тестирование» определяется простым суммированием баллов за правильные ответы на вопросы.

В зависимости от типа вопроса ответ считается правильным, если:

при ответе на вопрос закрытой формы с выбором ответа выбран правильный ответ;

при ответе на вопрос открытой формы дан правильный ответ;

при ответе на вопрос на установление правильной последовательности установлена правильная последовательность;

при ответе на вопрос на установление соответствия, если сопоставление произведено верно для всех пар.

Таблица 2. Структура оценки за тестовое задание

Инвариантная часть					
Специальность	Наименование темы вопросов	Вопрос с выбором ответа - 0,1 балл;	Вопрос с открытой формой ответа - 0,2 балла;	Вопрос на установление соответствия - 0,3 балла;	Вопрос на установление правильной последовательности - 0,4 балла.
10.02.01(ОП.04) 10.02.02(ОП.06) 10.02.03(ОП.02)	**1. ИТ в профессиональной деятельности**	**0,1**	**0,2**	**0,3**	**0,4**
10.02.01(ОП.01) 10.02.02(ОП.04) 10.02.03(ОП.03)	**2. Системы качества, стандартизации и сертификации**	**0,1**	**0,2**	**0,3**	**0,4**
10.02.01(ОП.10) 10.02.02(ОП.10) 10.02.03(ОП.11)	**3. Охрана труда, безопасность жизнедеятельности, безопасность окружающей среды (охрана окружающей среды, «зеленые технологии»)**	**0,1**	**0,2**	**0,3**	**0,4**
10.02.01(ОП.07) 10.02.02(ОП.08) 10.02.03(ОП.09)	**4. Экономика и правовое обеспечение профессиональной деятельности**	**0,1**	**0,2**	**0,3**	**0,4**
Вариативная часть					
10.02.01 (ОП06) 10.02.02 (ОП05) 10.02.03 (ОП01)	**5. Основы информационной безопасности**	**0,2**	**0,4**	**0,6**	**0,8**
10.02.01 (МДК 02.03) 10.02.02 (МДК02.01) 10.02.03 (МДК02.02)	**6. Организация и сопровождение электронного документооборота/ Криптографическая защита информации/ Криптографические средства и методы защиты информации**	**0,1**	**0,2**	**0,3**	**0,4**
10.02.01 (МДК03.01) 10.02.02 (МДК 02.02) 10.02.03 (МДК 03.01)	**7. Технические методы и средства, технологии защиты информации/ Инженерно-техническая защита информации/ Применение инженерно-технических средств обеспечения информационной безопасности**	**0,1**	**0,2**	**0,3**	**0,4**
10.02.01 (МДК 03.02) 10.02.02 (МДК 02.03) 10.02.03 (МДК 02.01)	**8. Программно-аппаратные средства защиты информации/ Программно-аппаратные средства защищенных телекоммуникационных систем/ Программно-аппаратные средства обеспечения информационной безопасности**	**0,1**	**0,2**	**0,3**	**0,4**
10.02.01 (МДК01.01/ МДК 02.01) 10.02.02 (МДК03.01) 10.02.03 (ОП03)	**9. Обеспечение организации системы безопасности организации/Правовая защита информации/ Организационное и правовое обеспечение информационной безопасности/Организационно-правовое обеспечение информационной безопасности**	**0,1**	**0,2**	**0,3**	**0,4**

	Сумма баллов по типам вопросов	**1**	**2**	**3**	**4**
	Максимальное количество баллов	**10**			

4.6. Оценивание выполнения практических конкурсных заданий I уровня осуществляется в соответствии со следующими целевыми индикаторами:

а) основные целевые индикаторы:

качество выполнения отдельных задач задания;

качество выполнения задания в целом.

б) штрафные целевые индикаторы, начисление (снятие) которых производится за нарушение условий выполнения задания (в том числе за нарушение правил выполнения работ).

Критерии оценки выполнения практических конкурсных заданий представлены в соответствующих паспортах конкурсного задания.

4.7. Максимальное количество баллов за практическое конкурсное задание I уровня **«Перевод профессионального текста (сообщения)»** составляет 10 баллов.

4.8. Оценивание конкурсного задания «Перевод профессионального текста (сообщения)» осуществляется следующим образом:

1 задача - перевод текста (сообщения) - 5 баллов;

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

Таблица 3

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 пять 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 другие);

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).

При выполнении второй задачи в содержание критериев могут быть внесены дополнения (изменения) касающиеся конкретной УГС, которые не влияют на удельный вес каждого критерия.

Таблица 4. Критерии оценки 2 задачи «Перевод профессионального текста при помощи словаря» (ответы на вопросы по тексту)

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

По критерию «Глубина понимания текста» 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» 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.

4.9. Максимальное количество баллов за выполнение задания «Задание по организации работы коллектива» - 10 баллов.

Оценивание выполнения задания 1 уровня **«Задание по организации работы коллектива»** осуществляется следующим образом:

Критерии оценки:

Таблица 5. Критерии оценки 2 задачи «Задание по организации работы коллектива»

№ задания	Тип задания	Критерии оценки
1.1	Определение продолжительности проекта. Ответ: /количество рабочих дней/	Оценка за правильный результат - 3 балла несущественные погрешности в расчетах – минус 1 балл; частичное правильное решение задачи – минус 2 балла
1.2	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
Итого:		5 баллов
2.1	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
2.2	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
Итого		5 баллов
Максимальный результат		10 баллов

4.10. Оценивание выполнения конкурсных заданий II уровня может осуществляться в соответствии со следующими целевыми индикаторами:

а) основные целевые индикаторы:

качество выполнения отдельных задач задания;

качество выполнения задания в целом;

скорость выполнения задания (в случае необходимости применения),

б) штрафные целевые индикаторы:

нарушение условий выполнения задания;

негрубые нарушения технологии выполнения работ;

негрубые нарушения санитарных норм.

Значение штрафных целевых индикаторов уточнено по каждому конкретному заданию.

Критерии оценки выполнения профессионального задания представлены в соответствующих паспортах конкурсных заданий.

4.11. Максимальное количество баллов за конкурсные задания II уровня 70 баллов.

4.12. Максимальное количество баллов за выполнение инвариантной части практического задания II уровня **Задание 1 «Организация защищенной локально-вычислительной сети»** - 35 баллов.

Оценивание выполнения данного задания осуществляется следующим образом:

Критерии оценки

№	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
32.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R1	3	0,3
33.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R2	3	0,3
34.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R3	3	0,3
35.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе RB	3	0,3
36.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе S1	3	0,3
37.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе S2	3	0,3
38.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе SB	3	0,3
39.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе DHCP	2	0,2
40.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R1	2	0,2
41.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R2	2	0,2
42.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R3	2	0,2
43.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе RB	2	0,2
44.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе S1	2	0,2

45.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе S2	2	0,2
46.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе SB	2	0,2
47.	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе DHCP	3	0,3
48.	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R1	3	0,3
49.	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R2	2	0,2
50.	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R3	3	0,3
51.	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе RB	3	0,3
52.	Настройка баннера MOTD, шифрование незашифрованных паролей на коммутаторе S1	2	0,2
53.	Настройка баннера, шифрование незашифрованных паролей на коммутаторе S2	2	0,2
54.	Настройка баннера, шифрование незашифрованных паролей на коммутаторе SB	2	0,2
55.	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство DHCP	3	0,3
56.	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R1	3	0,3
57.	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R2	3	0,3
58.	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R3	3	0,3
59.	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство RB	3	0,3
60.	Настройка NTP-клиента на маршрутизаторе DHCP	5	0,5
61.	Настройка NTP-клиента на маршрутизаторе R1	5	0,5
62.	Настройка NTP-клиента на маршрутизаторе R2	5	0,5
63.	Настройка NTP-клиента на маршрутизаторе R3	5	0,5
64.	Настройка NTP-клиента на маршрутизаторе RB	5	0,5
65.	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R1	2	0,2
66.	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R2	2	0,2
67.	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R3	4	0,4
68.	Настройка именованного списка контроля доступа **NAT** на маршрутизаторе R3	1	0,1
69.	Настройка именованного списка контроля доступа **NAT** на маршрутизаторе RB	1	0,1
70.	Настройка пула NAT R3POOL на маршрутизаторе R3	2	0,2
71.	Настройка статического NAT для сервера **Сервер** на маршрутизаторе R3	2	0,2
72.	Настройка пула NAT RBPOOL на маршрутизаторе RB	2	0,2
73.	Настройка VPN-туннеля на маршрутизаторе R3	20	2
74.	Настройка VPN-туннеля на маршрутизаторе RB	20	2
75.	Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45, VLAN60, VLAN75** на маршрутизаторе R1	10	1

76.	Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45, VLAN60, VLAN75** на маршрутизаторе R2	10	1
77.	Настройка протокола резервирования шлюза HSRP на маршрутизаторе R1	20	2
78.	Настройка протокола резервирования шлюза HSRP на маршрутизаторе R2	20	2
79.	Настройка VLAN, присвоение им имён на коммутаторе S1	5	0,5
80.	Настройка VLAN, присвоение им имён на коммутаторе S2	5	0,5
81.	Назначение портов доступа на интерфейсах коммутатора S1, включение функций PortFast и BPDU guard	14	1,4
82.	Назначение портов доступа на интерфейсах коммутатора S2, включение функций PortFast и BPDU guard	11	1,1
83.	Настройка функции Port Security на коммутаторе S1	12	1,2
84.	Настройка функции Port Security на коммутаторе S2	9	0,9
85.	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
86.	Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S1	4	0,4
87.	Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S2	3	0,3
88.	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
89.	Настройка шлюза по умолчанию на коммутаторе SB	1	0,1
Максимальная оценка программы		350	
Максимальное количество баллов			35

4.13. Максимальное количество баллов за выполнение вариативной части практического задания II уровня - 35 баллов.

Оценивание выполнения данного задания осуществляется следующим образом:

10.02.01 Задание 2 «Настройка АПМДЗ ПАК «Соболь» и программного обеспечения SecretNet Studio8»

№	Оцениваемый параметр	Количество баллов
1	- Произвести Подключение АПМДЗ, блокировки по Reset, управление блокировкой корпуса.	3
2	- Произвести инициализацию устройства, настроить общие параметры. Создать первичного администратора, произвести первичную смену пароля	3
3	Произвести настройку контроля целостности, поставить на контроль файл	3
4	произвести настройку комплекса в режиме Администратора - создать Администратора и пользователей - настроить общие параметры	4
5	- Произвести вход пользователем. Заблокировать пользователя неправильным входом. Разблокировать пользователя. Вывести отчет журнала событий	4
6	- Установить Secret Net Studio	4

7	- Настройка «Политики и Регистрации событий»	3
8	- Настроить доступ к пользователю «adminsns» по идентификатору Рутокен	4
9	- Настроить параметры входа в систему Провести проверочные мероприятия выполненных настроек Произвести экспорт журнала	3
10	- Выполнить аудит системы	4
Максимальное количество баллов		35

5. Продолжительность выполнения конкурсных заданий

Рекомендуемое максимальное время, отводимое на выполнения заданий в день – 8 часов (академических).

Рекомендуемое максимальное время для выполнения 1 уровня:

тестовое задание – 1 час (астрономический);

перевод профессионального текста, сообщения – 1 час (академический);

решение задачи по организации работы коллектива – 1,5 часа (академический).

Рекомендуемое максимальное время для выполнения отдельных заданий 2 уровня:

- 2 уровень Задание 1 Инвариантная часть – 3 часа 30 минут.

- 2 уровень Задание2 Вариативная часть – 3 часа 30 минут.

6. Условия выполнения заданий. Оборудование

6.1. Для выполнения задания «Тестирование» необходимо соблюдение следующих условий:

наличие компьютерного класса (классов) или других помещений, в котором размещаются персональные компьютеры, объединенные в локальную вычислительную сеть –примерная конфигурация компьютера Core i5 6400 2700 МГц ОЗУ 8 ГБ HDD1 ТБ USB 3.0

наличие специализированного программного обеспечения - ОС Microsoft Windows 7, ПО 1С.

Должна быть обеспечена возможность единовременного выполнения задания всеми участниками Олимпиады.

6.2. Для выполнения заданий «Перевод профессионального текста» необходимо соблюдение следующих условий:

наличие компьютерного класса (классов) или других помещений, в котором размещаются персональные компьютеры, объединенные в локальную вычислительную сеть–примерная конфигурация компьютера Core i5 6400 2700 МГц ОЗУ 8 ГБ HDD1 ТБ USB 3.0, используемое

программное обеспечение ОС Microsoft Windows10, Microsoft Office Word, (open source) –ПО Lingoes.

Должна быть обеспечена возможность единовременного выполнения задания всеми участниками Олимпиады.

6.3. Для выполнения заданий «Задание по организации работы коллектива» необходимо соблюдение следующих условий:

наличие компьютерного класса (классов) или других помещений, в котором размещаются персональные компьютеры, объединенные в локальную вычислительную сеть–примерная конфигурация компьютера Core i5 6400 2700 МГц ОЗУ 8 ГБ HDD1 ТБ USB 3.0, используемое программное обеспечение ОС Microsoft Windows10, (open source) – Project Libre.

6.4. Выполнение конкурсных заданий II уровня проводится на разных производственных площадках, используется специфическое оборудование.

Задание 1.

наличие компьютерного класса (классов) или других помещений, в котором размещаются персональные компьютеры, объединенные в локальную вычислительную сеть–примерная конфигурация компьютера Core i5 6400 2700 МГц ОЗУ 16 ГБ HDD1 ТБ USB 3.0;

используемое программное обеспечение ОС Microsoft Windows10, Microsoft Office Word, Cisco Packet Tracer 7.2.1, VirtualBox 5.2.

Задание2

10.02.01 - наличие компьютерного класса (классов) или других помещений, в котором размещаются персональные компьютеры, объединенные в локальную вычислительную сеть–примерная конфигурация компьютера Core i5 6400 2700 МГц ОЗУ 16 ГБ HDD1 ТБ USB 3.0;

используемое программное обеспечение ОС Microsoft Windows7, Microsoft Office Word, SecretNet Studio8, драйвер «Рутокен»

Используемое оборудование: - АПМДЗ ПАК «Соболь3.0»

- ПАК «Рутокен 32S»
- Флеш накопитель 8Гб, USB 3.0

6.5. Для лиц с ограниченными возможностями здоровья предусматриваются особые условия выполнения заданий.

7. Оценивание работы участника олимпиады в целом

7.1. Для осуществления учета полученных участниками олимпиады оценок заполняются ведомости оценок результатов выполнения заданий I и II уровня.

7.2. На основе указанных в п.7.1.ведомостей формируется сводная ведомость оценок результатов выполнения профессионального комплексного задания, в которую заносятся суммарные оценки в баллах за выполнение заданий I и II уровня каждым участником Олимпиады и итоговая оценка выполнения профессионального комплексного задания каждого участника Олимпиады, получаемая при сложении суммарных оценок за выполнение заданий I и II уровня.

7.3. Результаты участников заключительного этапа Всероссийской олимпиады ранжируются по убыванию суммарного количества баллов, после чего из ранжированного перечня результатов выделяют три наибольших результата, отличных друг от друга – первый, второй и третий результаты.

При равенстве баллов предпочтение отдается участнику, имеющему лучший результат за выполнение заданий II уровня.

Участник, имеющий первый результат, является победителем регионального этапа олимпиады. Участники, имеющие второй и третий результаты, являются призерами регионального этапа олимпиады.

Решение жюри оформляется протоколом.

7.4. Участникам, показавшим высокие результаты выполнения отдельного задания, при условии выполнения всех заданий, устанавливаются дополнительные поощрения.

Номинируются на дополнительные поощрения:

участники, показавшие высокие результаты выполнения профессионального комплексного задания по специальности или подгруппам специальностей УГС;

участники, показавшие высокие результаты выполнения отдельных задач, входящих в профессиональное комплексное задание;

участники, проявившие высокую культуру труда, творчески подошедшие к решению заданий.

II. ПАСПОРТ ПРАКТИЧЕСКОГО ЗАДАНИЯ «ПЕРЕВОД ПРОФЕССИОНАЛЬНОГО ТЕКСТА»

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.

Задание на перевод текста:

TEXT I.

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?

TEXT II.

PROTECTING INFORMATION SYSTEMS. COMPUTER CRIME

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. There are three important security threats that may damage information systems: computer crime, viruses, and disasters.

Internet-based crimes include scam, email fraud to obtain money or valuables, and phishing, bank fraud, to get banking information such as passwords of Internet bank accounts or credit card details. Piracy, the illegal copying and distribution of copyrighted software, information, music, and video files, is widespread.

To prevent system users from reading sensitive information, the company may use encryption software, which encodes, or scrambles, messages. Information security uses cryptography to transform information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. To read encrypted messages, users must use a key to convert them to regular text. Information that has been encrypted can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption.

Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit and while information is in storage. But as fast as software developers invent new and more elaborate protective measures, hackers seem to break through their defenses. So, security is an ongoing battle.

ANSWER THE QESTIONS

1. What is information security?
2. Identify the three important threats that may damage information systems.
3. What do Internet-based crimes include?
4. What must users do to read encrypted messages?
5. What is cryptography used for?

TEXT III.

INFORMATION SECURITY

Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. One of the tasks of information security is to defend information systems from illicit access. When computers are connected to a network, a problem at any place or position can influence the whole network. People with evil intentions may break into computer systems. Such actions are regarded as computer offenses.

One way that hackers gain access to secure information is through malware, which includes computer viruses, spyware, worms, and other programs. A computer virus is a very small program routine that infects the computer system and uses its resources to reproduce itself. Using strong antivirus software is one of the best ways of improving information security. Antivirus programs scan the system to check for any known malicious software, and most will warn the user if he or she is on a webpage that contains a potential virus.

Most operating systems include a basic antivirus program that will help protect the computer to some degree. Antivirus software can be downloaded for free online, although these programs may be less protection than paid versions.

Even the best antivirus programs usually need to be updated regularly to keep up with the new malware, and most software will alert the user when a new update is available for downloading. Running a full computer scan on a weekly basis is a good way to weed out potentially malicious programs.

ANSWER THE QESTIONS

1. What is information security?
2. How can hackers gain access to secure information?
3. What is a computer virus?
4. What is one of the best ways of improving information security?
5. What is a good way to weed out potentially malicious programs?

III. ПАСПОРТ ПРАКТИЧЕСКОГО ЗАДАНИЯ «ЗАДАНИЕ ПО ОРГАНИЗАЦИИ РАБОТЫ КОЛЛЕКТИВА»

№	**10.00.00 Информационная безопасность**								
1	10.02.01 Организация и технология защиты информации, № 805 от 28.07.2017 г.			10.02.02 Информационная безопасность телекоммуникационных систем, № 1000 от 13 августа 2014 г.			10.02.03 Информационная безопасность автоматизированных систем, № 806 от 28 июля 2014 г.		
2	ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.			ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.			ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.		
3	ОП.09. Менеджмент.			ОП.09. Менеджмент.			ОП.10. Менеджмент.		
4	Внедрение системы обеспечения безопасности электронного документооборота			Внедрение системы обеспечения безопасности телекоммуникационной информационной системы.			При разработке системы обеспечения безопасности автоматизированной информационной системы.		
5	Определение продолжительности проекта. Ответ: /количество рабочих дней/ Перечислить задачи, лежащие на критическом пути проекта. Ответ:/перечислить все этапы, лежащие на критическом пути проекта/	Оценка за правильный результат - балла несущественные погрешности в расчетах – минус 1 балл; частичное правильное решение задачи – минус 2 балла Оценка за правильный результат - 2 балла. частичное правильное	Максимальный балл - 10	Определение продолжительности проекта. Ответ: /количество рабочих дней/ Перечислить задачи, лежащие на критическом пути проекта. Ответ:/перечислить все этапы, лежащие на критическом пути проекта/	Оценка за правильный результат - балла несущественные погрешности в расчетах – минус 1 балл; частичное правильное решение задачи – минус 2 балла Оценка за правильный результат - 2 балла. частичное правильное решение задачи – минус 1 балл 5 баллов	Максимальный балл - 10	Определение продолжительности проекта. Ответ: /количество рабочих дней/ Перечислить задачи, лежащие на критическом пути проекта. Ответ:/перечислить все этапы, лежащие на критическом пути проекта/	Оценка за правильный результат - 3 балла несущественные погрешности в расчетах – минус 1 балл; частичное правильное решение задачи – минус 2 балла Оценка за правильный результат - 2 балла. частичное правильное решение задачи – минус 1 балл 5 баллов Оценка за правильный результат - 3 балла	Максимальный балл-10

	Распределить ресурсы по задачам проекта согласно таблице и определить стоимость проекта. Ответ:/ рублей/ После распределения ресурсов определить, какие ресурсы и в какое время перегружены. Ответ:/наименование перегруженного ресурса по датам/	решение задачи – минус 1 балл 5 баллов Оценка за правильный результат - 3 балла несущественные погрешности в расчетах – минус 1 балл; частичное правильное решение задачи – минус 2 балла Оценка за правильный результат - 2 балла частичное правильное решение задачи – минус 1 балл		Распределить ресурсы по задачам проекта согласно таблице и определить стоимость проекта. Ответ:/ рублей/ После распределения ресурсов определить, какие ресурсы и в какое время перегружены. Ответ:/наименование перегруженного ресурса по датам/	Оценка за правильный результат - 3 балла несущественные погрешности в расчетах – минус 1 балл; частичное правильное решение задачи – минус 2 балла Оценка за правильный результат - 2 балла частичное правильное решение задачи – минус 1 балл		Распределить ресурсы по задачам проекта согласно таблице и определить стоимость проекта. Ответ:/ рублей/ После распределения ресурсов определить, какие ресурсы и в какое время перегружены. Ответ:/наименование перегруженного ресурса по датам/	несущественные погрешности в расчетах – минус 1 балл; частичное правильное решение задачи – минус 2 балла Оценка за правильный результат - 2 балла частичное правильное решение задачи – минус 1 балл	

Материально-техническое обеспечение выполнения задания

Вид, выполняемой работы	Наличие прикладной компьютерной программы (наименование)	Наличие специального оборудования (наименование)	Наличие специального места выполнения задания *(учебный кабинет, лаборатория, иное)*
«Задание по организации работы коллектива»	ОС Microsoft Windows 10, (open source) – Project Libre.	примерная конфигурация компьютера Core i5 6400 2700 МГц ОЗУ 16 ГБ HDD1 ТБ USB 3.0;	Класс компьютерный

IV. ПАСПОРТ ПРАКТИЧЕСКОГО ЗАДАНИЯ ИНВАРИАНТНОЙ ЧАСТИ ПРАКТИЧЕСКОГО ЗАДАНИЯ II УРОВНЯ

Задание 1

№	**10.00.00 Информационная безопасность**		
1	10.02.01 Организация и технология защиты информации, № 805 от 28.07.2017 г.	10.02.02 Информационная безопасность телекоммуникационных систем, № 1000 от 13 августа 2014 г.	10.02.03 Информационная безопасность автоматизированных систем, № 806 от 28 июля 2014 г.
2	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 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 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей. ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях. ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.
3	10.02.01 (МДК 03.02)	10.02.02 (МДК 02.03)	10.02.03 (МДК 02.01)
4	«Организация защищенной локально-вычислительной сети»	«Организация защищенной локально-вычислительной сети»	«Организация защищенной локально-вычислительной сети»

№	Оцениваемый параметр	Оценка программы	Количество баллов
90.	Успешный эхо-запрос между узлами ПК-1 – ПК-4	1	0,1

91.	Успешный эхо-запрос между узлами ПК-2 – ПК-6	1	0,1
92.	Успешный эхо-запрос между узлами ПК-3 – ПК-6	1	0,1
93.	Успешный эхо-запрос между узлами ПК-1 – ПК-7	1	0,1
94.	Успешный эхо-запрос между узлами ПК-2 – ПК-8	1	0,1
95.	Успешный эхо-запрос между узлами ПК-3 – ПК-9	1	0,1
96.	Настройка пользователя Admin на маршрутизаторе DHCP	1	0,1
97.	Настройка пользователя Admin на маршрутизаторе R1	1	0,1
98.	Настройка пользователя Admin на маршрутизаторе R2	1	0,1
99.	Настройка пользователя Admin на маршрутизаторе R3	1	0,1
100.	Настройка пользователя Admin на маршрутизаторе RB	1	0,1
101.	Настройка пользователя Admin на коммутаторе S1	1	0,1
102.	Настройка пользователя Admin на коммутаторе S2	1	0,1
103.	Настройка пользователя Admin на коммутаторе SB	1	0,1
104.	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе DHCP	2	0,2
105.	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R1	2	0,2
106.	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R2	2	0,2
107.	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R3	2	0,2
108.	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе RB	2	0,2
109.	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе S1	2	0,2
110.	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе S2	2	0,2
111.	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе SB	2	0,2

112.	Настройка доступа по протоколу SSH на маршрутизаторе DHCP	3	0,3
113.	Настройка доступа по протоколу SSH на маршрутизаторе R1	3	0,3
114.	Настройка доступа по протоколу SSH на маршрутизаторе R2	3	0,3
115.	Настройка доступа по протоколу SSH на маршрутизаторе R3	3	0,3
116.	Настройка доступа по протоколу SSH на маршрутизаторе RB	3	0,3
117.	Настройка доступа по протоколу SSH на коммутаторе S1	3	0,3
118.	Настройка доступа по протоколу SSH на коммутаторе S2	3	0,3
119.	Настройка доступа по протоколу SSH на коммутаторе SB	3	0,3
120.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе DHCP	3	0,3
121.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R1	3	0,3
122.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R2	3	0,3
123.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R3	3	0,3
124.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе RB	3	0,3
125.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе S1	3	0,3
126.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе S2	3	0,3
127.	Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе SB	3	0,3
128.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе DHCP	2	0,2
129.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R1	2	0,2
130.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R2	2	0,2
131.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R3	2	0,2
132.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе RB	2	0,2

133.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе S1	2	0,2
134.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе S2	2	0,2
135.	Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе SB	2	0,2
136.	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе DHCP	3	0,3
137.	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R1	3	0,3
138.	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R2	2	0,2
139.	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R3	3	0,3
140.	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе RB	3	0,3
141.	Настройка баннера MOTD, шифрование незашифрованных паролей на коммутаторе S1	2	0,2
142.	Настройка баннера, шифрование незашифрованных паролей на коммутаторе S2	2	0,2
143.	Настройка баннера, шифрование незашифрованных паролей на коммутаторе SB	2	0,2
144.	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство DHCP	3	0,3
145.	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R1	3	0,3
146.	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R2	3	0,3
147.	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R3	3	0,3
148.	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство RB	3	0,3
149.	Настройка NTP-клиента на маршрутизаторе DHCP	5	0,5
150.	Настройка NTP-клиента на маршрутизаторе R1	5	0,5
151.	Настройка NTP-клиента на маршрутизаторе R2	5	0,5
152.	Настройка NTP-клиента на маршрутизаторе R3	5	0,5
153.	Настройка NTP-клиента на маршрутизаторе RB	5	0,5

154.	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R1	2	0,2
155.	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R2	2	0,2
156.	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R3	4	0,4
157.	Настройка именованного списка контроля доступа **NAT** на маршрутизаторе R3	1	0,1
158.	Настройка именованного списка контроля доступа **NAT** на маршрутизаторе RB	1	0,1
159.	Настройка пула NAT R3POOL на маршрутизаторе R3	2	0,2
160.	Настройка статического NAT для сервера **Сервер** на маршрутизаторе R3	2	0,2
161.	Настройка пула NAT RBPOOL на маршрутизаторе RB	2	0,2
162.	Настройка VPN-туннеля на маршрутизаторе R3	20	2
163.	Настройка VPN-туннеля на маршрутизаторе RB	20	2
164.	Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45, VLAN60, VLAN75** на маршрутизаторе R1	10	1
165.	Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45, VLAN60, VLAN75** на маршрутизаторе R2	10	1
166.	Настройка протокола резервирования шлюза HSRP на маршрутизаторе R1	20	2
167.	Настройка протокола резервирования шлюза HSRP на маршрутизаторе R2	20	2
168.	Настройка VLAN, присвоение им имён на коммутаторе S1	5	0,5
169.	Настройка VLAN, присвоение им имён на коммутаторе S2	5	0,5
170.	Назначение портов доступа на интерфейсах коммутатора S1, включение функций PortFast и BPDU guard	14	1,4
171.	Назначение портов доступа на интерфейсах коммутатора S2, включение функций PortFast и BPDU guard	11	1,1
172.	Настройка функции Port Security на коммутаторе S1	12	1,2
173.	Настройка функции Port Security на коммутаторе S2	9	0,9
174.	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
175.	Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S1	4	0,4
176.	Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S2	3	0,3

177.	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
178.	Настройка шлюза по умолчанию на коммутаторе SB	1	0,1
Максимальная оценка программы		350	
Максимальное количество баллов			35

Материально-техническое обеспечение выполнения задания

Вид, выполняемой работы	Наличие прикладной компьютерной программы (наименование)	Наличие специального оборудования (наименование)	Наличие специального места выполнения задания *(учебный кабинет, лаборатория, иное)*
«Организация защищенной локально-вычислительной сети»	ОС Microsoft Windows10, Microsoft Office Word, Cisco Packet Tracer 7.2.1, VirtualBox 5.2	Core i5 6400 2700 МГц ОЗУ 16 ГБ HDD1 ТБ USB 3.0;	Компьютерный класс

V. ПАСПОРТ ЗАДАНИЯ ВАРИАТИВНОЙ ЧАСТИ II УРОВНЯ

Задание 2

1	10.02.01 Организация и технология защиты информации, № 805 от 28.07.2017 г.	
2	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	
3	10.02.01 (МДК 03.02)	
4	10.02.01 Задание 2 «Настройка АПМДЗ ПАК «Соболь» и программного средства безопасности Secret Net Studio»	
№	Оцениваемый параметр	Количество баллов

1	- Произвести Подключение АПМДЗ, блокировки по Reset, управление блокировкой корпуса.	1
2	- Произвести инициализацию устройства, настроить общие параметры. Создать первичного администратора, произвести первичную смену пароля	1
3	Произвести настройку контроля целостности, поставить на контроль файл	1
4	произвести настройку комплекса в режиме Администратора - создать Администратора и пользователей - настроить общие параметры	1
5	- Произвести вход пользователем. Заблокировать пользователя неправильным входом. Разблокировать пользователя. Вывести отчет журнала событий	1
6	- Установить Secret Net Studio	1
7	- Настройка «Политики и Регистрации событий»	1
8	- Настроить доступ к пользователю «adminsns» по идентификатору Рутокен	1
9	- Настроить параметры входа в систему Провести проверочные мероприятия выполненных настроек Произвести экспорт журнала	1
10	- Выполнить аудит системы	1

Материально-техническое обеспечение выполнения задания

10.02.03 Задание 2 «Настройка АПМДЗ ПАК «Соболь» и программного средства безопасности Secret Net Studio»	ОС Microsoft Windows10, Microsoft Office Word, SecretNet Studio8, драйвер «Рутокен»	Core i5 6400 2700 МГц ОЗУ 16 ГБ HDD1 ТБ USB 3.0; - АПМДЗ ПАК «Соболь3.0» - ПАК «Рутокен 32S» - Флеш накопитель 8Гб, USB 3.0	Отвертка крестовая, отвертка часовая	Компьютерный класс

VI. ИНДИВИДУАЛЬНЫЕ ВЕДОМОСТИ ОЦЕНОК РЕЗУЛЬТАТОВ ВЫПОЛНЕНИЯ УЧАСТНИКОМ ПРАКТИЧЕСКИХ ЗАДАНИЙ I УРОВНЯ

ВЕДОМОСТЬ

оценок результатов выполнения комплексного задания I уровня
Регионального этапа олимпиады профессионального мастерства обучающихся
по специальностям среднего профессионального образования
в 2020 году

Профильное направление Регионального этапа олимпиады _____
Специальность/специальности СПО _____ Региональный этап олимпиады _____
Дата выполнения задания «_____»_____2020 г.

Член жюри _____
(фамилия, имя, отчество, место работы)

№ п/п	Номер участника, полученный при жеребьевке	Оценка в баллах за выполнение комплексного задания I уровня в соответствии с №№ заданий			Суммарная оценка в баллах
		1	2	3	

_____(подписи членов жюри)

VII. ИНДИВИДУАЛЬНЫЕ ВЕДОМОСТИ ОЦЕНОК РЕЗУЛЬТАТОВ ВЫПОЛНЕНИЯ УЧАСТНИКОМ ПРАКТИЧЕСКИХ ЗАДАНИЙ II УРОВНЯ

ВЕДОМОСТЬ

оценок результатов выполнения комплексного задания II уровня
Регионального этапа олимпиады профессионального мастерства обучающихся
по специальностям среднего профессионального образования
в 2020 году

Профильное направление Регионального этапа олимпиады _____
Специальность/специальности СПО _____ Региональный этап олимпиады _____
Дата выполнения задания «_____»_____2020 г.

Член жюри _____
(фамилия, имя, отчество, место работы)

№ п/п	Номер участника, полученный при жеребьевке	Оценка в баллах за выполнение комплексного задания II уровня в соответствии с №№ заданий						Суммарная оценка в баллах
		Общая часть задания			Вариативная часть задания			
		4.1	4.2	4.3	5.1	5.2	5.3	

_____(подписи членов жюри)

VIII. СВОДНАЯ ВЕДОМОСТЬ ОЦЕНОК РЕЗУЛЬТАТОВ ВЫПОЛНЕНИЯ УЧАСТНИКАМИ ЗАДАНИЙ ОЛИМПИАДЫ

СВОДНАЯ ВЕДОМОСТЬ
оценок результатов выполнения профессионального комплексного задания
Регионального этапа олимпиады профессионального мастерства обучающихся
по специальностям среднего профессионального образования
в 2020 году

Профильное направление Регионального этапа олимпиады
_____

Специальность/специальности СПО

_____

Дата выполнения задания «_____»_____2020г.

№ п/п	Номер участника, полученный при жеребьевке	Фамилия, имя, отчество участника	Наименование субъекта образовательной организации	Оценка результатов выполнения профессионального комплексного задания в баллах		Итоговая оценка выполнения профессионального комплексного задания в баллах	Занятое место
				Комплексное задание I уровня	Комплексное задание II уровня		
1	2	3	4	5	6	7	8

Председатель организационного комитета _____ _____
подпись фамилия, инициалы

Председатель жюри _____ _____
подпись фамилия, инициалы

Члены жюри: _____ _____
подпись фамилия, инициалы

X. Оценочные средства выполнения участниками заданий олимпиады

Задания I уровня включают следующие задания:

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

Инвариантная часть задания «Тестирование» содержит 16 вопросов по четырем тематическим направлениям, из них 4 – закрытой формы с выбором ответа, 4 – открытой формы с кратким ответом, 4 - на установление соответствия, 4 - на установление правильной последовательности. Тематика, количество и формат вопросов по темам инвариантной части тестового задания едины для всех специальностей СПО.

Вариативная часть задания «Тестирование» содержит 24 вопроса не менее, чем по двум тематическим направлениям. Тематика, количество и формат вопросов по темам вариативной части тестового задания формируются на основе знаний, общих для специальностей, входящих в УГС, по которой проводится Олимпиада.

	Задание 1 уровня - этап «Тестирование» - Инвариантная часть				
		Вопрос с выбором ответа - 0,1 балл;	Вопрос с открытой формой ответа - 0,2 балла;	Вопрос на установление соответствия - 0,3 балла;	Вопрос на установление правильной последовательности - 0,4 балла.
10.02.01 **10.02.02** **10.02.03**	**1. ИТ в профессиональной деятельности**	Как называется программное или аппаратное обеспечение, которое препятствует несанкционированному доступу на компьютер? а. Брандмауэр в. Сервер в. Браузер г. Архиватор	Минимальным объект, используемый в растровом графическом редакторе, называется …	Установите соответствие между программой и ее функцией: Создание презентаций -Microsoft PowerPoint Текстовый редактор - Microsoft Word Создание публикаций- Microsoft Publisher Редактор электронных -таблиц Microsoft Excel	Установите единицы измерения объема информации по возрастанию: а. Бит б. Килобайт в. Мегабит г. Мегабайт
10.02.01 **10.02.02** **10.02.03**	**2. Системы качества, стандартизации и сертификации**	Поле, ограниченное верхним и нижним предельными отклонениями относительно номинального размера, называется: а. Поле допуска б. Поле значений	Добровольное подтверждение соответствия осуществляется по инициативе …	1. Установите соответствие между цифровыми обозначениями международных стандартов и их названиями: 1 Управление качеством А - ISO9000 2 Экологический менеджмент Б - ISO14000 3 Информационная безопасность	Укажите последовательность участников системы сертификации, начиная с заявителя: 1 Заявитель 2 Органы сертификации

		в. Поле точности г. Поле готовности		В – ISO27000 4 Г. Энергетический менеджмент Г – ISO 50001	3 Испытательная лаборатория 4 Центральный орган сертификации
10.02.01 10.02.02 10.02.03	**3. Охрана труда, безопасность жизнедеятельности, безопасность окружающей среды (охрана окружающей среды, «зеленые технологии»)**	Продолжительность рабочей недели для подростков в возрасте 16-18 лет не должна превышать а. 36 часов б. 18 часов в. 24 часа г. 40 часов	Гражданская оборона- это система … по подготовке и защите населения, материальных и культурных ценностей на территории РФ от опасностей, возникающих при ведении военных действий или вследствие этих действий.	Установите соответствие между видом инструктажа по охране труда и временем его проведения: 1Вводный инструктаж - При поступлении на работу 2 Первичный инструктаж - Перед первым допуском к работе 3 Повторный инструктаж - Не реже одного раза в полгода 4 Целевой инструктаж - При выполнении разовых работ, не связанных с прямыми обязанностями по специальности	Укажите правильную последовательность действий при использовании углекислотного огнетушителя: а. Сорвать пломбу б. Выдернуть чеку в. Направить раструб на очаг возгорания г. Нажать рычаг
10.02.01 10.02.02 10.02.03	**4. Экономика и правовое обеспечение профессиональной деятельности**	Себестоимость продукции – это: а. Затраты материальных и трудовых ресурсов на производство и реализацию продукции или	… - это финансовая несостоятельность организации. Ответ: Банкротство	Установите соответствие между термином и отраслью права: 1Дееспособность -Гражданское право 2Работник - Трудовое право 3Предупреждение - Административное право 4Прибыль - Предпринимательское право	Расположите источники трудового права по юридической силе: а. Конституция РФ б. Трудовой кодекс РФ в. Указ Президента РФ г. Закон субъекта РФ

		оказание услуг в денежном выражении б. Количественные затраты материальных и трудовых ресурсов на производство и реализацию продукции или оказание услуг в. Технологические затраты материальных и трудовых ресурсов на производство и реализацию продукции или оказание услуг г. Затраты материальных и трудовых ресурсов на производство продукции или оказание услуг в денежном выражении			
Задание 1 уровня - этап «Тестирование» - Вариантная часть					

10.02.01 (ОП06) **10.02.02 (ОП05)** **10.02.03 (ОП01)**	**5. Основы информационной безопасности**	Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением, это… Ответ: 1. Пользователь информации 2. Владелец информации 3. Собственник информации 4. Носитель информации *[ГОСТ Р 50922-96 Защита информации.*	Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, это…	Установите соответствие: 1.Защита информации от утечки - Деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками 2. Защита информации от несанкционированного воздействия - Деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации	Согласно модели PDCA (Цикл Шухарта – Деминга) выделяется 4 этапа создания системы обеспечения информационной безопасности (СОИБ) в следующей последовательности: Ответ: 1.Планирование СОИБ 2.Реализация СОИБ 3.Проверка СОИБ 4.Совершенствование СОИБ

		Основные термины и определения]		3. Защита информации от непреднамеренного воздействия -Деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации 4. Защита информации от разглашения - Деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации	

				[ГОСТ Р 50922-96 Защита информации. Основные термины и определения]	
10.02.01 (ОП06) **10.02.02 (ОП05)** **10.02.03 (ОП01)**	**5. Основы информационной безопасности**	Формы защиты интеллектуальной собственности – это… а) авторское, патентное право и коммерческая тайна б) интеллектуальное право и смежные права в) коммерческая и государственная тайна г) гражданское и административное право	… - это система официальных взглядов на обеспечение национальной безопасности страны в информационной сфере	Установите соответствие между терминами 1. Целостность - Свойство информации сохранять свою структуру и содержание в процессе передачи и хранения 2. Конфиденциальность - Статус, предоставленный данным и определяющий требуемую степень защиты 3. Доступность - Возможность субъекта ознакомления с информацией 4. Достоверность - Свойство информации, выражающееся в строгой принадлежности субъекту, являющемуся источником информации	Подход к реализации защитных мероприятий по обеспечению информационной безопасности должен соответствовать следующей последовательности: 1. Определение состава средств информационной системы 2. Анализ уязвимых элементов информационной системы и оценка угроз 3. Анализ риска 4. Определение способов защиты
10.02.01 (МДК02.03)	**6. Организация и сопровождение электронного документооборота/ Криптографическая**	Действующий российский криптографический стандарт, определяющий	Процесс нормального применения криптографического преобразования открытого текста на основе	Установите соответствие: 1.Ключ - Изменяемый элемент (параметр), каждому значению которого однозначно	Установите правильный порядок выполнения преобразований в шифре AES: Ответ:

10.02.02 (МДК02.01) **10.02.03 (МДК02.02)**	**защита информации/ Криптографические средства и методы защиты информации**	алгоритм и процедуру вычисления хеш-функции, это… Ответ: 1.ГОСТ Р 34.11-2012 2. ГОСТ Р 34.10-2012 3. ГОСТ Р 34.13-2015 4. ГОСТ Р 34.12-2015	алгоритма и ключа, в результате которого возникает шифрованный текст, это…	соответствует одно из отображений, реализуемых криптосистемой 2.Пароль - Конфиденциальная информация аутентификации, обычно состоящая из строки знаков 3.Пин-Код - персональный идентификационный номер 4.MAC-— уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet. *[ГОСТ Р ИСО 7498-2-99]*	1.SubBytes 2.ShiftRows 3.MixColumns 4.AddRoundKey *[Federal Information Processing Standards Publication 197 November 26, 2001 Specification for the ADVANCED ENCRYPTION STANDARD (AES)]*
10.02.01 (МДК03.01) **10.02.02 (МДК02.02)** **10.02.03 (МДК03.01)**	**7 Технические методы и средства, технологии защиты информации/ Инженерно-техническая защита информации/ Применение инженерно-технических средств обеспечения**	Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера,	Токи и напряжения в токопроводящих элементах, вызванные электромагнитным излучением, емкостными и индуктивными связями, это… *[ГОСТ Р 51275-99 Защита информации. Объект информатизации.*	Установите соответствие: 1. Перехват -Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов 2. Утечка (информации) по техническому каналу - Неконтролируемое	Установите последовательность принципа классификации факторов, воздействующих на защищаемую информацию: 1. Подкласс 2. Группа

	информационной безопасности	транспортные средства, а также в технические средства и системы обработки информации), это… Ответ: 1. Закладочное устройство 2. Программная закладка 3. Программный вирус 4. ВТСС *[ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения]*	*Факторы, воздействующие на информацию. Общие положения]*	распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации 3. Уязвимость (автоматизированной информационной системы) - Недостаток или слабое место в автоматизированной информационной системе, которые могут быть условием реализации угрозы безопасности, обрабатываемой в ней информации 4. Угроза (безопасности информации) - Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации *[Р 50.1.053-2005 Информационные технологии. Основные термины и*	3. Подгруппа 4.Вид 5.Подвид *[ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения]*

				определения в области технической защиты информации]	
10.02.01 (МДК03.02) **10.02.02 (МДК02.03)** **10.02.03 (МДК02.01)**	**8. Программно-аппаратные средства защиты информации/ Программно-аппаратные средства защищенных телекоммуникационных систем/ Программно-аппаратные средства обеспечения информационной безопасности**	Состояние ресурсов автоматизированной информационной системы, при котором обеспечивается реализация информационной технологии с использованием именно тех ресурсов, к которым субъект, имеющий на это право, обращается, это… 1 Подлинность 2 Конфиденциальность 3 Целостность 4 Доступность *[Р 50.1.053-2005 Информационные технологии.*	Сигнал, по параметрам которого может быть определена защищаемая информация, это.. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации]*	Установите соответствие между уязвимостью и методом защиты: Загрузка нештатной ОС –Защита Secure boot Отключение /обход СЗИ – запуск Measured Boot Изменение параметров СЗИ – Защита SPI Flash Обход функций СЗИ – Защита гипервизора	Установите последовательность загрузки компьютера с установленным АПМДЗ: 1.Запуск встроенной ОС (Embedded OS) 2. Аутентификация пользователя 3.Контроль целостности 4. Передача управления BIOS

		Основные термины и определения в области технической защиты информации]			
10.02.01 (МДК 01.01/МДК 02.01) **10.02.02 (МДК03.01)** **10.02.03 (ОП03)**	**9. Обеспечение организации системы безопасности организации/Правовая защита информации/ Организационное и правовое обеспечение информационной безопасности/Организационно-правовое обеспечение информационной безопасности**	Сочетание вероятности нанесения ущерба и тяжести этого ущерба, это… 1. Риск 2. Ущерб 3. Опасность 4.Безопасность *[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты]*	Потенциальная причина инцидента, который может нанести ущерб системе или организации, это… *[ГОСТ Р ИСО/МЭК 13335-1 — 2006]*	Установите соответствие: Правовой документ – Кодекс РФ Организационно-распорядительный документ – Инструкция администратора безопасности Нормативный документ – ГОСТ Р Информационно справочный документ - Акт ввода в эксплуатацию СЗИ	Установите последовательность способов уменьшения риска (в порядке приоритетов): 1.Разработка безопасного в своей основе проекта 2.Защитные устройства и персональное защитное оборудование 3.Информация по установке и применению 4.Обучение *[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты]*

I уровень
Практическое задание «Перевод профессионального текста (сообщения)»

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.

Задание на перевод текста:

TEXT I.

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?

TEXT II.

PROTECTING INFORMATION SYSTEMS. COMPUTER CRIME

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. There are three important security threats that may damage information systems: computer crime, viruses, and disasters.

Internet-based crimes include scam, email fraud to obtain money or valuables, and phishing, bank fraud, to get banking information such as passwords of Internet bank accounts or credit card details. Piracy, the illegal copying and distribution of copyrighted software, information, music, and video files, is widespread.

To prevent system users from reading sensitive information, the company may use encryption software, which encodes, or scrambles, messages. Information security uses cryptography to transform information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. To read encrypted messages, users must use a key to convert them to regular text. Information that has been encrypted can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption.

Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit and while information is in storage. But as fast as software developers invent new and more elaborate protective measures, hackers seem to break through their defenses. So, security is an ongoing battle.

ANSWER THE QESTIONS

1. What is information security?
2. Identify the three important threats that may damage information systems.
3. What do Internet-based crimes include?
4. What must users do to read encrypted messages?
5. What is cryptography used for?

TEXT III.

INFORMATION SECURITY

Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. One of the tasks of information security is to defend information systems from illicit access. When computers are connected to a network, a problem at any place or position can influence the whole network. People with evil intentions may break into computer systems. Such actions are regarded as computer offenses.

One way that hackers gain access to secure information is through malware, which includes computer viruses, spyware, worms, and other programs. A computer virus is a very small program routine that infects the computer system and uses its resources to reproduce itself. Using strong antivirus software is one of the best ways of improving information security. Antivirus programs scan the system to check for any known malicious software, and most will warn the user if he or she is on a webpage that contains a potential virus.

Most operating systems include a basic antivirus program that will help protect the computer to some degree. Antivirus software can be downloaded for free online, although these programs may be less protection than paid versions.

Even the best antivirus programs usually need to be updated regularly to keep up with the new malware, and most software will alert the user when a new update is available for downloading. Running a full computer scan on a weekly basis is a good way to weed out potentially malicious programs.

ANSWER THE QESTIONS

1. What is information security?
2. How can hackers gain access to secure information?
3. What is a computer virus?
4. What is one of the best ways of improving information security?
5. What is a good way to weed out potentially malicious programs?

Практическое задание I уровня «Организация работы в коллективе»

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».

Критерии оценки

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

Задание

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

При определении продолжительности проекта учесть производственный календарь, действующий на территории Республики Башкортостан.

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

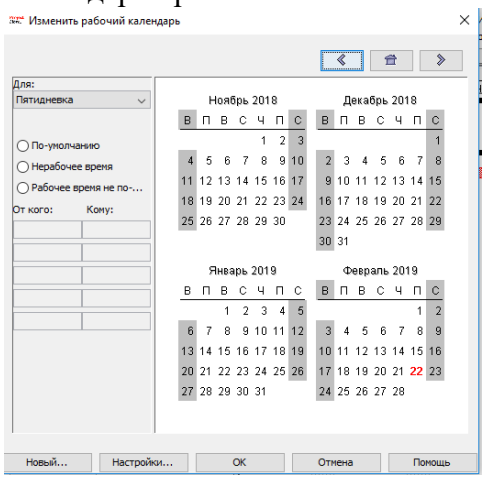
4. После распределения ресурсов определить, какие ресурсы и в какое время перегружены. (Ответ занести в файл)

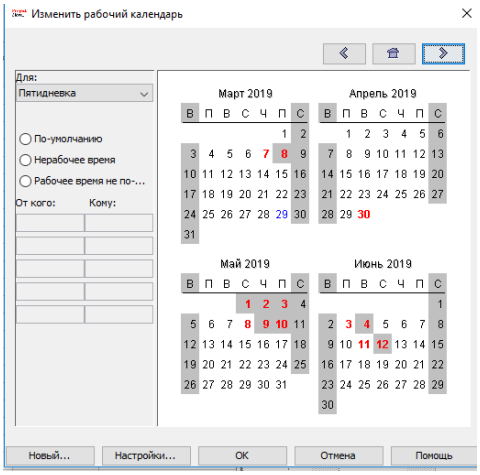
Форма представления результатов выполнения задания

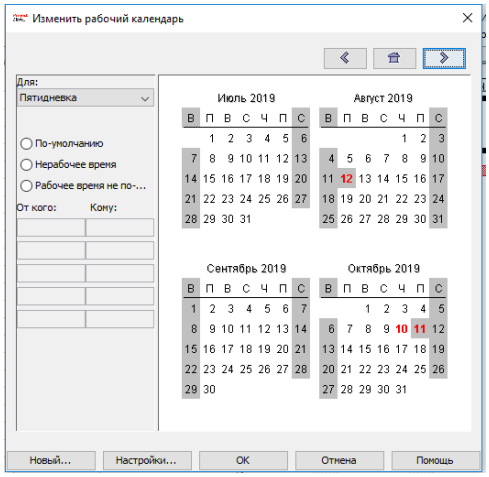
1	Продолжительность проекта, раб. дни	117
2	Критический путь	Предпроектное обследование, обсуждение и согласование технических решений, разработка эскизного проекта, разработка технического проекта, разработка комплекта рабочей документации, разработка комплекта сметной документации, разработка программы и методики испытаний, поставка необходимых программных и технических средств, проведение монтажных работ, проведение пусконаладочных работ, предварительные испытания, опытная эксплуатация, приемочные испытания
3	Стоимость проекта, руб.	929 850

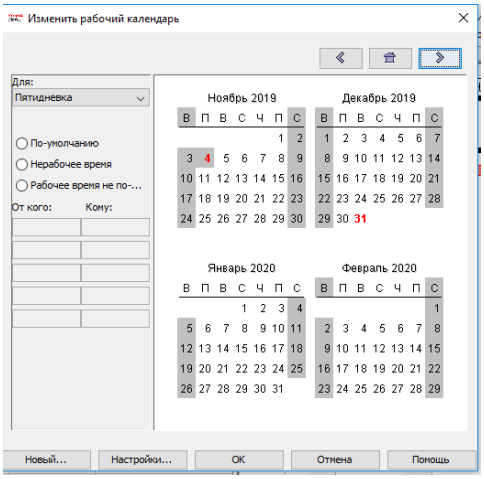
4	Перегруженные ресурсы	Наименование ресурса	Календарные даты перегрузки ресурса	
			с	по
		Гл. инженер	10.01.2019 14.01.2019	11.01.2019 15.01.2019
		Специалист по ИБ 1	10.01.2019 14.01.2019	11.01.2019 15.01.2019
		ГИП	25.02.2019 04.03.2019	01.03.2019 04.03.2019

Календарь проекта









- черные – рабочие дни
- красные – выходные и праздничные дни
- черные с* - предпраздничные сокращенные на 1 час дни

Результаты выполнения заданий I уровня:

№ п/п	Номер участника, полученный при жеребьевке	Оценка в баллах за выполнение I этапа задания в соответствии с №№ вопросов и задач			Суммарная оценка в баллах
		Тестирование	Перевод текста	Организация работы в коллективе	
1	HCEP	5,9	7	8	20,9
2	FLQ9	7,5	6	6	19,5
3	B3C3	4,1	6	9	19,1
4	Y289	5,7	7	6	18,7
5	3WDT	7	2	9	18
6	T4FG	6	4	8	18
7	O3MP	6,5	4	7	17,5
8	MN2J	5,5	3	9	17,5

9	O9A4	4,9	3	9	16,9
10	0PPQ	5,7	2	9	16,7
11	LMB0	3,4	5	8	16,4
12	9MGL	5,3	3	6	14,3
13	6CON	4,6	2	7	13,6
14	WVNC	4,6	1	7	12,6
15	R5QB	5,5	4	3	12,5
16	WBOH	2,6	4	5	11,6
17	1QBC	5,1	3	3	11,1
18	J4TU	5	3	3	11
19	VE4A	3,6	2	5	10,6
20	7J72	5,6	3	1	9,6
21	RWS1	4,3	2	3	9,3
22	IBYD	3,4	2	2	7,4
23	NRX8	3,3	3	1	7,3
24	6CUH	4,3	0	3	7,3
25	GNH8	4,9	2	0	6,9

Анализ выполнения заданий I уровня

Необходимо отметить хороший уровень подготовки по теоретической части. Большинство студентов справились с 50 и более процентами выполнения тестовой части заданий. Студенты показали хорошие знания в таких разделах, как информационные технологии в профессиональной деятельности, системы качества, охрана труда.

Вместе с тем стоит отметить, что сложными оказались вопросы на знание стандартизации и сертификации, безопасности жизнедеятельности, вопросы, предполагающие ввод значений, а не их выбор из предложенных вариантов.

Целесообразно внести в практику образовательного процесса специальную проверку знаний на основе ввода (указания) соответствующих терминов.

Следует констатировать сниженный уровень умений по переводу с иностранного языка профессионального текста, особенно в части применения сложившейся в русском языке профессиональной терминологии.

Задачи на организацию работы коллектива выполнены студентами на высоком уровне, трудности при этом вызвали вопросы определения сроков перегрузки трудовых ресурсов с учетом производственного календаря.

В целом содержание заданий I уровня соответствует содержанию основных образовательных программ, по которым обучаются участники олимпиады.

2 уровень
Практическое задание №1
«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	10.0.30.2	255.255.255.0
	Gi0/0.45	10.0.45.2	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.

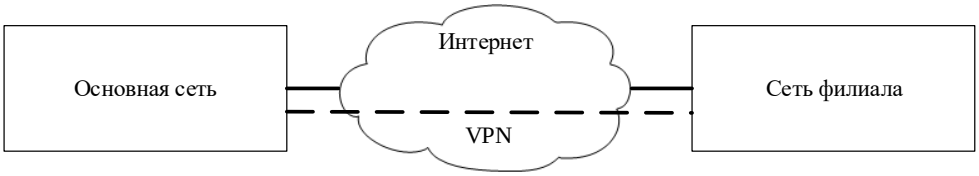


Рисунок 1 – Общая топология сети

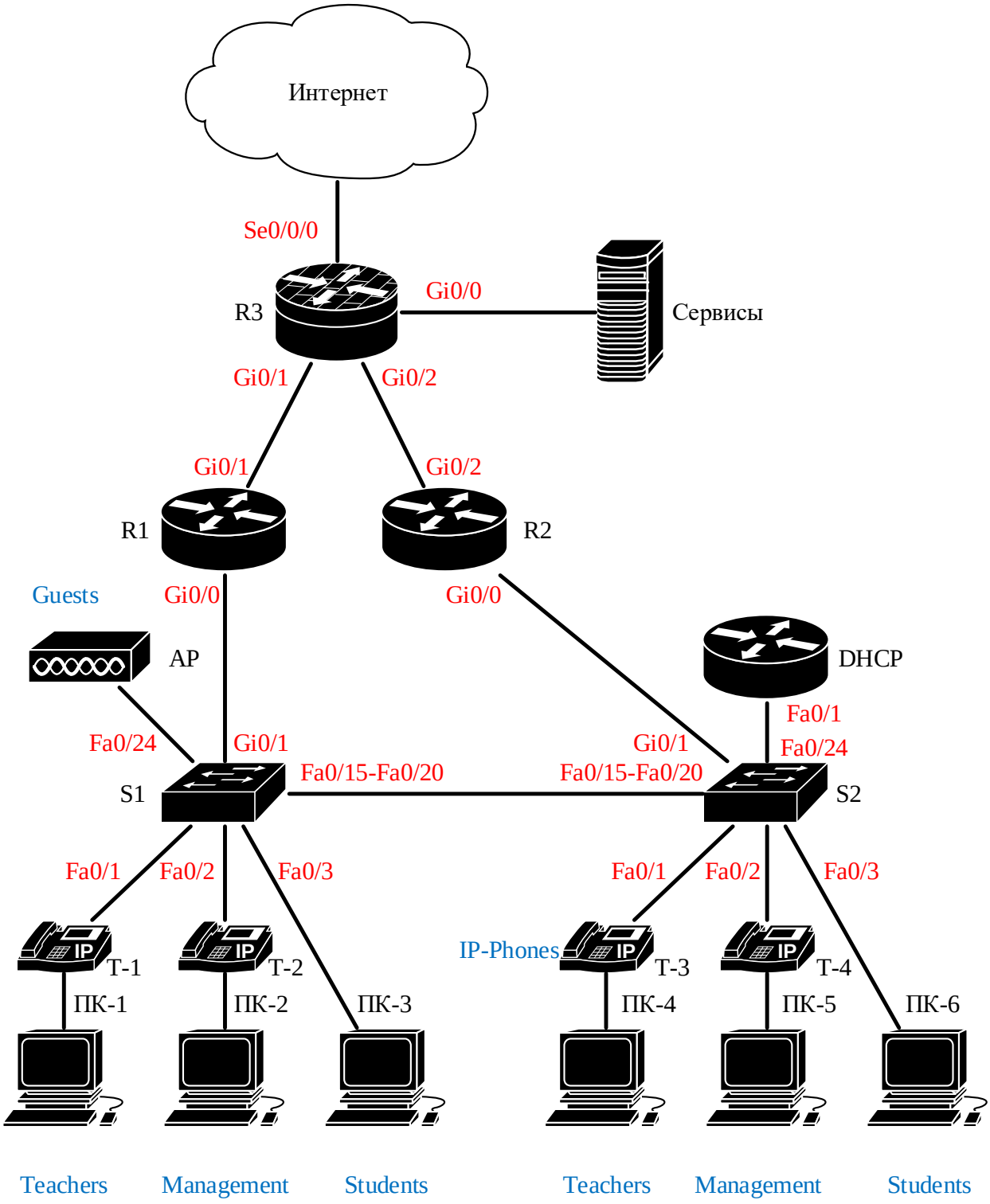


Рисунок 2 – Топология основной сети
(синим цветом указана принадлежность портов к VLAN)

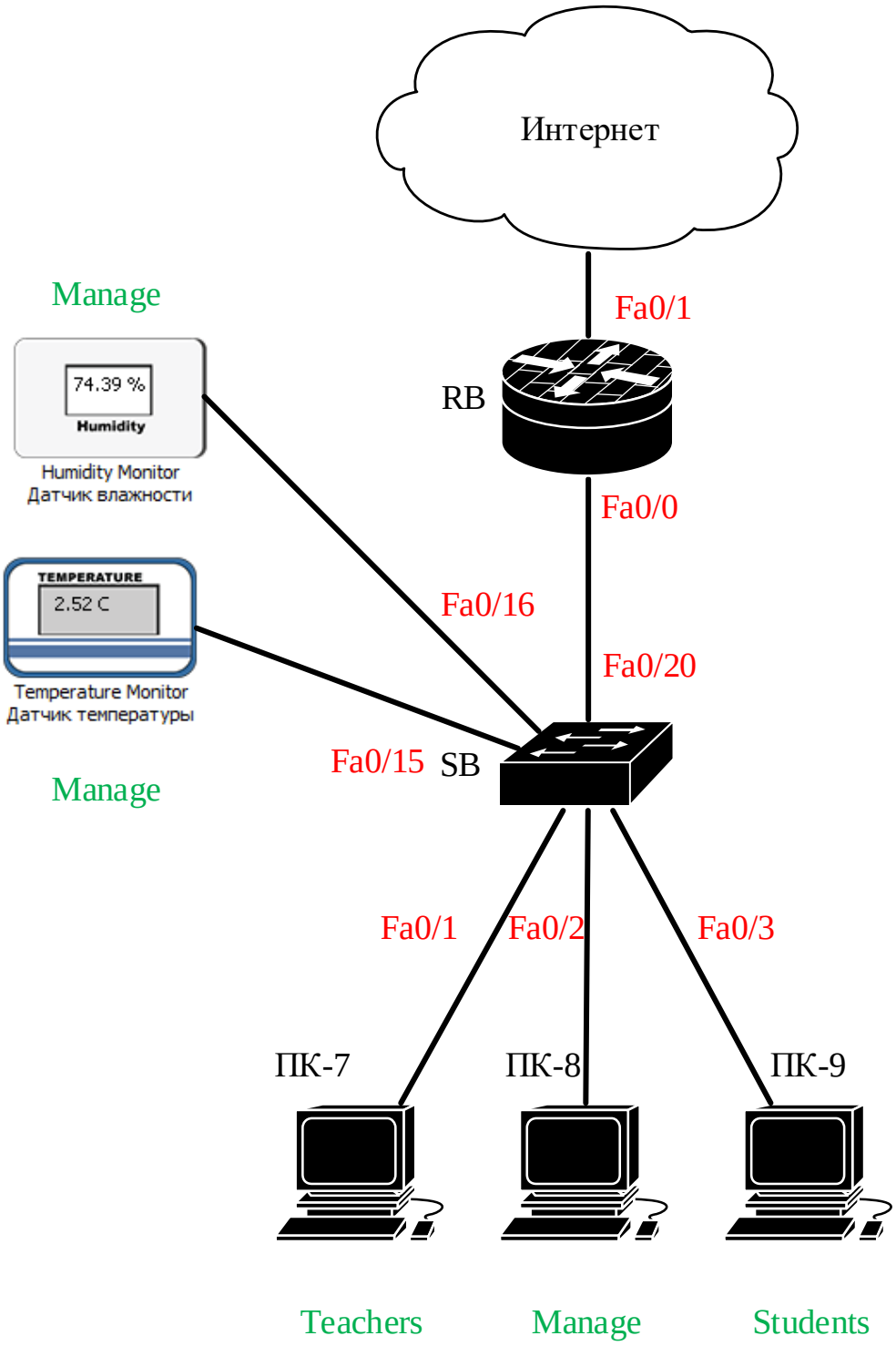


Рисунок 3 – Топология сети филиала

Критерии оценки

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
1	Успешный эхо-запрос между узлами ПК-2 – ПК-6	1	0,1
1	Успешный эхо-запрос между узлами ПК-3 – ПК-6	1	0,1
1	Успешный эхо-запрос между узлами ПК-1 – ПК-7	1	0,1
1	Успешный эхо-запрос между узлами ПК-2 – ПК-8	1	0,1
1	Успешный эхо-запрос между узлами ПК-3 – ПК-9	1	0,1
1	Настройка пользователя Admin на маршрутизаторе DHCP	1	0,1
1	Настройка пользователя Admin на маршрутизаторе R1	1	0,1
1	Настройка пользователя Admin на маршрутизаторе R2	1	0,1
1	Настройка пользователя Admin на маршрутизаторе R3	1	0,1
1	Настройка пользователя Admin на маршрутизаторе RB	1	0,1
1	Настройка пользователя Admin на коммутаторе S1	1	0,1
1	Настройка пользователя Admin на коммутаторе S2	1	0,1
1	Настройка пользователя Admin на коммутаторе SB	1	0,1
1	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе DHCP	2	0,2
1	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R1	2	0,2
1	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R2	2	0,2
1	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R3	2	0,2
1	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе RB	2	0,2
1	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе S1	2	0,2
1	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе S2	2	0,2
2	Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе SB	2	0,2
2	Настройка доступа по протоколу SSH на маршрутизаторе DHCP	3	0,3
2	Настройка доступа по протоколу SSH на маршрутизаторе R1	3	0,3
2	Настройка доступа по протоколу SSH на маршрутизаторе R2	3	0,3
2	Настройка доступа по протоколу SSH на маршрутизаторе R3	3	0,3
2	Настройка доступа по протоколу SSH на маршрутизаторе RB	3	0,3
2	Настройка доступа по протоколу SSH на коммутаторе S1	3	0,3
2	Настройка доступа по протоколу SSH на коммутаторе S2	3	0,3
2	Настройка доступа по протоколу SSH на коммутаторе SB	3	0,3

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

2	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе DHCP	3	0,3
2	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R1	3	0,3
2	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R2	2	0,2
2	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R3	3	0,3
2	Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе RB	3	0,3
2	Настройка баннера MOTD, шифрование незашифрованных паролей на коммутаторе S1	2	0,2
2	Настройка баннера, шифрование незашифрованных паролей на коммутаторе S2	2	0,2
2	Настройка баннера, шифрование незашифрованных паролей на коммутаторе SB	2	0,2
2	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство DHCP	3	0,3
2	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R1	3	0,3
2	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R2	3	0,3
2	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R3	3	0,3
2	Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство RB	3	0,3
2	Настройка NTP-клиента на маршрутизаторе DHCP	5	0,5
2	Настройка NTP-клиента на маршрутизаторе R1	5	0,5
2	Настройка NTP-клиента на маршрутизаторе R2	5	0,5
2	Настройка NTP-клиента на маршрутизаторе R3	5	0,5
2	Настройка NTP-клиента на маршрутизаторе RB	5	0,5
2	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R1	2	0,2
2	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R2	2	0,2

2	Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF_GUARD) на маршрутизаторе R3	4	0,4
2	Настройка именованного списка контроля доступа **NAT** на маршрутизаторе R3	1	0,1
2	Настройка именованного списка контроля доступа **NAT** на маршрутизаторе RB	1	0,1
2	Настройка пула NAT R3POOL на маршрутизаторе R3	2	0,2
2	Настройка статического NAT для сервера **Сервер** на маршрутизаторе R3	2	0,2
2	Настройка пула NAT RBPOOL на маршрутизаторе RB	2	0,2
2	Настройка VPN-туннеля на маршрутизаторе R3	20	2
2	Настройка VPN-туннеля на маршрутизаторе RB	20	2
2	Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45, VLAN60, VLAN75** на маршрутизаторе R1	10	1
2	Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45, VLAN60, VLAN75** на маршрутизаторе R2	10	1
2	Настройка протокола резервирования шлюза HSRP на маршрутизаторе R1	20	2
2	Настройка протокола резервирования шлюза HSRP на маршрутизаторе R2	20	2
2	Настройка VLAN, присвоение им имён на коммутаторе S1	5	0,5
2	Настройка VLAN, присвоение им имён на коммутаторе S2	5	0,5
2	Назначение портов доступа на интерфейсах коммутатора S1, включение функций PortFast и BPDU guard	14	1,4
2	Назначение портов доступа на интерфейсах коммутатора S2, включение функций PortFast и BPDU guard	11	1,1
2	Настройка функции Port Security на коммутаторе S1	12	1,2
2	Настройка функции Port Security на коммутаторе S2	9	0,9
2	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
2	Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S1	4	0,4
2	Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S2	3	0,3
2	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
2	Настройка шлюза по умолчанию на коммутаторе SB	1	0,1

Максимальная оценка программы	350	
Максимальное количество баллов		35

Задание II уровня Вариативная часть

с учетом специфики специальности

Задание № 2

10.02.01 «Настройка ПАК «Соболь» и «Secret Net Studio»

Задание выполняется на компьютере.
Используемое оборудование и ПО:
- ПАК «Соболь 3.0», DVD ПАК «Соболь»
- Рутокен PIN: 12345678, драйверы Рутокен
- USB-флеш
- Электронный ключ iButton
- ПО «Secret Net Studio» 8.4

Баллы выставляются по отчетам действий на usb-флеш носителе!!!

№	Задание	Количество баллов
1	Произвести установку и настройку ПАК «Соболь» в компьютер. Произвести переподключение кнопки Reset через ПАК «Соболь». Настроить режим сторожевого таймера	3
2	Произвести инициализацию устройства в автономном режиме. Настроить общие параметры системы. Зарегистрировать пользователей: *Администратор* - пароль Gfhjkm1 (с идентификатором Рутокен.) *Пользователь* - пароль 87654321 и идентификатор iButton;	3
3	Произвести настройку контроля целостности - на рабочем столе создать текстовый файл с именем шифра участника. Изменение файла должно быть зафиксировано в журнале ПАК «Соболь».	3
4	Заблокировать вход в систему *Пользователя* после 3 неверных попыток входа. Заблокировать компьютер по времени ввода параметров идентификации.	4
5	Создать файл внешнего журнала и произвести экспорт журнала на usb- внешний носитель.	3
6	Удалить пользователя. Перенести учетную запись администратора на iButton. (В дальнейшем для входа ПАК Соболь использовать iButton). Установить ПАК Соболь в режим работы совместно с «Secret Net Studio».	2
7	Установить «Secret Net Studio», лицензии с папки на рабочем столе. Настроить параметры учетной записи администратора. Настроить идентификатор Рутокен для входа в «Secret Net Studio» для хранения пароля и хранения закрытого ключа и входа в ПАК «Соболь».	3
8	Настроить политики безопасности SNS обеспечивающие: - Запрет вторичного входа; - Блокирование компьютер при изъятии идентификатора;	3

	- Усиленную аутентификацию; - Регистрацию неверных аутентификационных данных; - Длину пароля 8 символов; - Срок хранения журнала - 30дней; - Оповещение о тревогах; - Количество циклов затирания по требованию ГОСТ Р 50739-95;	
9	Поставить на контроль целостности «Secret Net Studio» графический файл. Изменить файл. Изменение файла должно быть зафиксировано в журнале «Secret Net Studio».	4
10	Настроить контроль устройств. Запретить: - BlueThooth; - WI-FI модули; - Подключение сотовых телефонов - Подключение электронных идентификаторов и считывателей, кроме Рутокен S.	3
11	Вывести отчет журнала «Secret Net Studio» и журнала безопасности на usb-флеш носитель.	4
Максимальное количество баллов за задание 2		35