Согласовано
Директор
Белгородского филиала
ПАО «РОСТЕЛЕКОМ»
_____ Г.Н. Кузьменко
от «25» февраля 2022 г.

Утверждаю
Директор ОГАПОУ
«Белгородский
индустриальный колледж»
_____ О.А. Шаталов
от «25» февраля 2022 г.

Фонд оценочных средств
Всероссийской олимпиады профессионального мастерства
по укрупненной группе специальностей СПО
10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

код и наименование

Белгород 2022

ФОС разработан в ОГАПОУ «Белгородский индустриальный колледж»

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

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

– Маламуд Элла Борисовна – преподаватель ОГАПОУ «Белгородский индустриальный колледж»;

– Сердюкова Надежда Анатольевна – преподаватель ОГАПОУ «Белгородский индустриальный колледж»;

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

Рецензенты

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

СОДЕРЖАНИЕ

I. Спецификация Фонда оценочных средств 4
II. Паспорт практического задания «Перевод профессионального текста» 21
III. Паспорт практического задания «Задание по организации работы коллектива» 24
IV. Паспорт практического задания инвариантной части практического задания II уровня 26
V. Паспорт практического задания вариативной части практического задания II уровня 28
VI. Индивидуальные ведомости оценок результатов выполнения участником практических заданий I уровня 31
VII. Индивидуальные ведомости оценок результатов выполнения участником практических заданий II уровня 32
VIII. Сводная ведомость оценок результатов выполнения участниками заданий олимпиады 33
IX. Оценочные средства выполнения участниками заданий олимпиады 34

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 Регионального этапа 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 Регионального этапа 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 I 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 **«Администрирование системы защиты ViPNet»** - 35 баллов.

Оценивание выполнения данного задания осуществляется следующим образом:

Критерии оценки

№	Оцениваемый параметр	Количество баллов
1	Запустить виртуальные машины, установить ПО, организовать схему ЛВС.	8
2	Создать сетевые узлы, клиентов зарегистрированных на соответствующем - В соответствии с таблицей, создать пользователей, зарегистрировать их на клиентах	4
3	Компрометация узла	2
4	Работоспособность сети	9
5	Удостоверяющий центр	12
Максимальное количество баллов		35

4.13. Максимальное количество баллов за выполнение вариативной части практического задания II уровня **«Настройка системы контроля информационных потоков и предотвращения неправомерных действий с информацией InfoWatch Traffic Monitor»** - 35 баллов.

Оценивание выполнения данного задания осуществляется следующим образом:

Критерии оценки

№	Оцениваемый параметр
1	Установлен стенд с Traffic Monitor в варианте All-in-one (PostgreSQL)
2	Установлена связь контроллера домена с Traffic Monitor
3	Создана виртуальная машина IWDM с Windows Server
4	Виртуальная машина IWDM введена в домен
5	Активирована лицензия IWTM
6	Проведена LDAP-синхронизация
7	Получена информация о пользователях и компьютерах компании, представленных на сервере-контроллере домена
8	Файл «*iwtm.txt*» создан на рабочем столе хостовой машины. В файле записаны IP-адреса и соответствующие им имена машин, токен для подключения IWDM, логины и пароли от учетных записей
9	Установлен на машину IWDM сервер безопасности InfoWatch Device Monitor
10	Синхронизирован IWDM с каталогом Active Directory (компьютеры и пользователи), и связан сервер IWDM с сервером IWTM
11	Создана виртуальная машина ARM-Agent
12	ARM-Agent введена в домен
13	Установлен на машину IWDM Crawler
14	Crawler настроен на автоматическое ежедневное сканирование ранее созданного каталога
15	Создан скриншот настройки сканера Crawler на рабочем столе хостовой машины в папке «Олимпиада_IWTM»
16	Выполнен перехват событий от Crawler и сохраните скриншот, демонстрирующий данный перехват событий на рабочем столе хостовой машины в папке «Олимпиада_IWTM»
17	Создан «белый список устройств» Device Monitor
18	Создан скриншот, демонстрирующий работу «белого списка устройств» Device Monitor на рабочем столе хостовой машины в папке «Олимпиада_IWTM»
19	Создан «черный список приложений»
20	Создан скриншот, демонстрирующий работу «черного списка устройств» Device Monitor на рабочем столе хостовой машины в папке «Олимпиада_IWTM»
21	Продемонстрирована интеграция Device Monitor с Active Directory
22	Создан скриншот, демонстрирующий интеграцию с Active Directory на рабочем столе хостовой машины в папке «Олимпиада_IWTM»

23	Выполнена выборка событий по условию
24	Создан скриншот, демонстрирующий работу запроса выборки событий по созданному условию на рабочем столе хостовой машины в папке «Олимпиада_IWTM»
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 (астрономический);

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

Рекомендуемое максимальное время для выполнения отдельных заданий 2 уровня:

- 2 уровень Задание 1 Инвариантная часть – 4 часа (астрономический).
- 2 уровень Задание 2 Вариативная часть – 4,5 часа (астрономический).

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

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, VM Ware Workstation 5.2, VipNet.

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, VMWare Workstation, Red Hat Linux Enterprise, Windows Server 2016 (образ), Windows 10 (образ), PostgreSQL, Traffic Monitor, Device Monitor, Crawler

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

INFORMATION SECURITY. DATA ENCRYPTION

The data transferred from one system to another over the public network can be protected by the method of encryption. On encryption, the data is encrypted by any encryption algorithm using the key. Only a user having access to the same key can decrypt the encrypted data. A single secret cryptographic key is used for both encryption and decryption. This method is known as a private key or symmetric key cryptography.

There are several standard symmetric key algorithms defined. Examples are AES, 3DES, and Blowfish. These standard symmetric algorithms are proven to be highly secured and time-tested. But the problem with these algorithms is the key exchange. The communicating parties require a shared secret, key, to be exchanged between them to have a secured communication. The security of the symmetric key algorithm depends on the secrecy of the key. Keys are typically hundreds of bits in length, depending on the algorithm used. Since there may be a number of intermediate points between the communicating parties through which the data passes, these keys cannot be exchanged online in a secured manner. In a large network, where there are hundreds of systems connected, the offline key exchange seems too difficult and even unrealistic.

The public-key cryptography is also known as asymmetric cryptography. Using a public key algorithm, a shared secret can be established online between communicating parties without the need for exchanging any secret key. In public-key cryptography, each user has a pair of cryptographic keys – a public key and a private key. Only the particular user /device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. The sender encrypts the message in such a way that only the recipient will be able to decrypt the message. A disadvantage of using public-key cryptography for encryption is speed. Asymmetric key algorithms are hundreds to thousands of times slower than symmetric key algorithms.

ANSWER THE QUESTIONS.

1. What is the method of protecting the data?
2. What method is used for both encryption and decryption?
3. What is a private key or symmetric key cryptography?
4. What standard symmetric algorithms do you know? What are their benefits?
5. What is the disadvantage of using public-key cryptography?

TEXT II

INFORMATION SECURITY. VIRUSES.

Another critical security challenge is presented by computer viruses, hidden programs that can work their way into computer systems and erase or corrupt data and programs. Viruses are programs that secretly attach themselves to other programs or files, known as the host, and change them or destroy data. Viruses can be programmed to become active immediately or to remain dormant for a period of time, after which the infections suddenly activate themselves and cause problems. A virus can reproduce by copying itself onto other programs stored in the same drive. It spreads as users install infected software on their systems or exchange files with others, usually by exchanging email, accessing electronic bulletin boards, trading disks, or downloading programs or data from unknown sources on the Internet. Because so many computers are interconnected, viruses can spread quickly, infecting all the computers linked on a local area network and then spreading over the Internet to other computers and networks. The main virus types include logic bombs, boot sector viruses, macro viruses, email viruses, companion viruses, cross-site scripting viruses, polymorphic viruses.

As viruses become more complex, the technology to fight them must increase in sophistication as well. The simplest way to protect against computer viruses is to install one of the many available antivirus software programs. There is no way to entirely stop the spread of computer viruses because new ones are created all the time. However, a number of excellent "vaccine" programs exist that search for and destroy viruses and prevent new ones from infecting your computer system. These programs continuously monitor systems for viruses and automatically eliminate any they spot. Anti-virus and anti-malware programs can provide real-time protection against the installation of malware on a computer. The software scans disk files at download time and blocks the activity of components known to represent malware. Users should regularly update antivirus software programs by going online to download the latest virus definitions.

ANSWER THE QUESTIONS.

1. What are viruses?
2. How does it spread?
3. What are the main virus types?
4. What is the simplest way to protect against computer viruses?
5. What do "vaccine" programs do?

TEXT III
DATA SECURITY

If the internet and information technology have made our lives simpler, it has also given birth to a number of security-based threats. Therefore, it has become equally important to protect your crucial data and other information with appropriate data security techniques and data privacy.

However, your first task at hand is identifying the confidential data that you want to protect from getting leaked out.

The hackers have become quite smart these days and so you need to be smarter than them to nullify any risk factors that exist.

As a computer owner, you not only have to be vigilant about the threats of viruses and worms penetrating the computer system but also various other hazards that are evil and dangerous for your confidential files and documents.

Here are some simple tips for protecting your data:

It is better to browse or surf the internet all alone. See to it that nobody is spying your browsing habits and gathering sensitive information from your computer.

Always write down your password at a safe and secure place and not on computer monitor screens.

When you are signing into your account the administrator usually offers you two options; remember the Password and Nope. Never choose the first option.

Don't disclose your password to anyone not even to your closest friend or relative.

You should keep on changing your password for duration of every few months. Never keep one password for any account too long.

ANSWER THE QUESTIONS:

1. How can you protect your crucial data and other information?
2. What is the first task for data protection?
3. Is it safe to write down your password on computer monitor screen?
4. Which option is safer to you: remember the password and nope?

How often does the author of the article advise you to change your password?

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.		
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.		
3	ОП.09. Менеджмент		
4	Внедрение системы обеспечения безопасности электронного документооборота		
5	Определение продолжительности проекта. Ответ: /количество рабочих дней/ Перечислить задачи, лежащие на критическом пути проекта. Ответ:/перечислить все этапы, лежащие на критическом пути проекта/ 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 - 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 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	Максимальный балл - 10

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

№	**10.00.00 Информационная безопасность**
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.
3	МДК 03.02
4	«Организация защищенной локально-вычислительной сети»

Критерии оценки

№	Оцениваемый параметр			Количество баллов
1.	Развертывание защищенной VPN сети	Сеть настроена по заданию	Неверная подсеть/прочее - вычесть 0.5 за каждый сегмент	2
		Работоспособен сервер ЦУС, УКЦ	Сеть 1, входит и работает, вычесть 0.5 за каждый отсутствующий компонент	2
		Клиент ЦУС установлен на незащищенный узел	Сеть 1, ЦУС на незащищенной машине, входит и работает	2
		Работоспособен клиент администратора, координатор филиала, клиент филиала	Сеть 1, входит, есть информация о сети (можно по скриншоту), вычесть 0.5 за каждый неработающий узел	2
2.	Работа с узлами и пользователями	Созданы и настроены пользователи и узлы (Админ), Клиент(ы)	2 шт, есть связи, вычесть 0,15 за каждый отсутствующий	2
		Созданы и настроены пользователи и узлы (Координатор)	2 шт, есть межсерверное взаимодействие, вычесть 0,15 за каждый отсутствующий	1
		Настроено взаимодействие между пользователями в сети	Настройка,	1
3.	Компрометация узла	Скомпрометированы ключи пользователя	Скриншот УКЦ/окна смены пароля, версия ключа >0	1
		Скомпрометированный пользователь работоспособен	Скриншот окна на предоставление резервного набора ключей, скриншот директории с резервными ключами + архив директории (после смены ключа); -0,9 если взаимодействие восстановлено через dst файл	1
4.		Настроен токен для входа на узел (админ)	Происходит вход с помощью токена. Если ключи в папке -0,7	2

	Работоспособность сети	Проверка проходит до всех узлов сети ЦО с филиала	Проверка с клиента филиал (если только скрин - вычесть 0.4)	2
		Проверка проходит до всех узлов сети Филиала с ЦО	Проверка с клиента админ (если только скрин - вычесть 0.4)	2
		Отправка текстовых сообщений	Чат работает, связь через координаторы, -0,20 за отсутствие скриншотов	1
		Отправка деловой почты	Письмо доходит, связь через координаторы. Вычесть 0,20 за отсутствие скриншотов	2
5.	Удостоверяющий центр	УКЦ работает в режиме УЦ	Есть скрины настройки УЦ	2
		Верно настроен сертификат	Прописаны поля, тип и т.д., без скринов вычесть 0.2	2
		Установлен и работоспособен Registration Point, Publication, TSP/OCSP	Запускается и работает, вычесть 0.4 за каждый нерабочий	2
		Осуществляется запрос и выдача ключей через Registration point	Есть скриншоты, есть сертификаты с успешным подтверждением, без скринов вычесть 0.3	1
		Сервис публикации подключен к УЦ общими папками	Есть общие каталоги, нет ошибок, без скринов вычесть 0.3	1
		Происходит публикация	Есть файлы, нет ошибок	1
		Работает и настроен сервис информирования	Работоспособен, без скринов вычесть 0.3	1
		Рассылаются уведомления	Работоспособен, без скринов вычесть 0.3	1
		Работает регистрация внешних пользователей	Выпуск сертификата, верные поля, без скринов вычесть 0.3	1
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)*
«Администрирование системы защиты ViPNet»	ОС Microsoft Windows10, Microsoft Office Word, ViPNet Администратор4, ViPNet Registration Point, ViPNet Publication Service, ViPNet Client, ViPNet Policy Manager, ViPNet Coordinator, VirtualBox 5.2 или VM Ware Workstation	Core i5 6400 2700 МГц ОЗУ 16 ГБ HDD1 ТБ USB 3.0;	Компьютерный класс

V. ПАСПОРТ ЗАДАНИЯ ВАРИАТИВНОЙ ЧАСТИ II УРОВНЯ

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	Задание «Настройка системы контроля информационных потоков и предотвращения неправомерных действий с информацией InfoWatch Traffic Monitor»

№	Оцениваемый параметр	Количество баллов
1	Установлен стенд с Traffic Monitor в варианте All-in-one (PostgreSQL)	4
2	Установлена связь контроллера домена с Traffic Monitor	2
3	Создана виртуальная машина IWDM с Windows Server	1
4	Виртуальная машина IWDM введена в домен	0,5
5	Активирована лицензия IWTM	0,5
6	Проведена LDAP-синхронизация	1
7	Получена информация о пользователях и компьютерах компании, представленных на сервере-контроллере домена	0,5
8	Файл «*iwtm.txt*» создан на рабочем столе хостовой машины. В файле записаны IP-адреса и соответствующие им имена машин, токен для подключения IWDM, логины и пароли от учетных записей	0,5
9	Установлен на машину IWDM сервер безопасности InfoWatch Device Monitor	3
10	Синхронизирован IWDM с каталогом Active Directory (компьютеры и пользователи), и связан сервер IWDM с сервером IWTM	1
11	Создана виртуальная машина ARM-Agent	1
12	ARM-Agent введена в домен	0,5

13	Установлен на машину IWDM Crawler	4
14	Crawler настроен на автоматическое ежедневное сканирование ранее созданного каталога	0,7
15	Создан скриншот настройки сканера Crawler на рабочем столе хостовой машины в папке «Олимпиада_IWTM»	0,3
16	Выполнен перехват событий от Crawler и сохраните скриншот, демонстрирующий данный перехват событий на рабочем столе хостовой машины в папке «Олимпиада_IWTM»	2
17	Создан «белый список устройств» Device Monitor	1,7
18	Создан скриншот, демонстрирующий работу «белого списка устройств» Device Monitor на рабочем столе хостовой машины в папке «Олимпиада_IWTM»	0,3
19	Создайн «черный список приложений»	1,7
20	Создан скриншот, демонстрирующий работу «черного списка устройств» Device Monitor на рабочем столе хостовой машины в папке «Олимпиада_IWTM»	0,3
21	Продемонстрирована интеграция Device Monitor с Active Directory	1,7
22	Создан скриншот, демонстрирующий интеграцию с Active Directory на рабочем столе хостовой машины в папке «Олимпиада_IWTM»	0,3
23	Выполнена выборка событий по условию	1,7
24	Создан скриншот, демонстрирующий работу запроса выборки событий по созданному условию на рабочем столе хостовой машины в папке «Олимпиада_IWTM»	0,3
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)*
«Настройка системы контроля информационных потоков и	ОС Microsoft Windows10, Microsoft Office Word, VMWare Workstation, Red Hat Linux Enterprise, Windows Server 2016 с установленным контроллером домена, Windows Server 2016	Core i5 6400 2700 МГц ОЗУ 16 ГБ HDD1 ТБ USB 3.0	Компьютерный класс

предотвращения неправомерных действий с информацией InfoWatch Traffic Monitor»	(образ), Windows 10 (образ), PostgreSQL, Traffic Monitor, Device Monitor, Crawler		

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 2022 году

Профильное направление Регионального этапа олимпиады _____
Специальность/специальности СПО _____ Региональный этап олимпиады _____
Дата выполнения задания «_____»_____2022 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 2022 году

Профильное направление Регионального этапа олимпиады _____
Специальность/специальности СПО _____ Региональный этап олимпиады _____
Дата выполнения задания «_____»_____2022 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		Суммарная оценка в баллах
		Инвариантная часть задания	Вариативная часть задания	

_____(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 2022 году

Профильное направление Регионального этапа олимпиады
_____

Специальность/специальности СПО

_____

Дата выполнения задания «_____»_____2022г.

№ 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

IX. 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.

Задание на перевод текста:

TEXT I

INFORMATION SECURITY. DATA ENCRYPTION

The data transferred from one system to another over the public network can be protected by the method of encryption. On encryption, the data is encrypted by any encryption algorithm using the key. Only a user having access to the same key can decrypt the encrypted data. A single secret cryptographic key is used for both encryption and decryption. This method is known as a private key or symmetric key cryptography.

There are several standard symmetric key algorithms defined. Examples are AES, 3DES, and Blowfish. These standard symmetric algorithms are proven to be highly secured and time-tested. But the problem with these algorithms is the key exchange. The communicating parties require a shared secret, key, to be exchanged between them to have a secured communication. The security of the symmetric key algorithm depends on the secrecy of the key. Keys are typically hundreds of bits in length, depending on the algorithm used. Since there may be a number of intermediate points between the communicating parties through which the data passes, these keys cannot be exchanged online in a secured manner. In a large network, where there are hundreds of systems connected, the offline key exchange seems too difficult and even unrealistic.

The public-key cryptography is also known as asymmetric cryptography. Using a public key algorithm, a shared secret can be established online between communicating parties without the need for exchanging any secret key. In public-key cryptography, each user has a pair of cryptographic keys – a public key and a private key. Only the particular user /device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. The sender encrypts the message in such a way that only the recipient will be able to decrypt the message. A disadvantage of using public-key cryptography for encryption is speed. Asymmetric key algorithms are hundreds to thousands of times slower than symmetric key algorithms.

ANSWER THE QUESTIONS.

1. What is the method of protecting the data?
2. What method is used for both encryption and decryption?
3. What is a private key or symmetric key cryptography?
4. What standard symmetric algorithms do you know? What are their benefits?
5. What is the disadvantage of using public-key cryptography?

TEXT II

INFORMATION SECURITY. VIRUSES.

Another critical security challenge is presented by computer viruses, hidden programs that can work their way into computer systems and erase or corrupt data and programs. Viruses are programs that secretly attach themselves to other programs or files, known as the host, and change them or destroy data. Viruses can be programmed to become active immediately or to remain dormant for a period of time, after which the infections suddenly activate themselves and cause problems. A virus can reproduce by copying itself onto other programs stored in the same drive. It spreads as users install infected software on their systems or exchange files with others, usually by exchanging email, accessing electronic bulletin boards, trading disks, or downloading programs or data from unknown sources on the Internet. Because so many computers are interconnected, viruses can spread quickly, infecting all the computers linked on a local area network and then spreading over the Internet to other computers and networks. The main virus types include logic bombs, boot sector viruses, macro viruses, email viruses, companion viruses, cross-site scripting viruses, polymorphic viruses.

As viruses become more complex, the technology to fight them must increase in sophistication as well. The simplest way to protect against computer viruses is to install one of the many available antivirus software programs. There is no way to entirely stop the spread of computer viruses because new ones are created all the time. However, a number of excellent "vaccine" programs exist that search for and destroy viruses and prevent new ones from infecting your computer system. These programs continuously monitor systems for viruses and automatically eliminate any they spot. Anti-virus and anti-malware programs can provide real-time protection against the installation of malware on a computer. The software scans disk files at download time and blocks the activity of components known to represent malware. Users should regularly update antivirus software programs by going online to download the latest virus definitions.

ANSWER THE QUESTIONS.

1. What are viruses?
2. How does it spread?
3. What are the main virus types?
4. What is the simplest way to protect against computer viruses?
5. What do "vaccine" programs do?

TEXT III
DATA SECURITY

If the internet and information technology have made our lives simpler, it has also given birth to a number of security-based threats. Therefore, it has become equally important to protect your crucial data and other information with appropriate data security techniques and data privacy.

However, your first task at hand is identifying the confidential data that you want to protect from getting leaked out.

The hackers have become quite smart these days and so you need to be smarter than them to nullify any risk factors that exist.

As a computer owner, you not only have to be vigilant about the threats of viruses and worms penetrating the computer system but also various other hazards that are evil and dangerous for your confidential files and documents.

Here are some simple tips for protecting your data:

It is better to browse or surf the internet all alone. See to it that nobody is spying your browsing habits and gathering sensitive information from your computer.

Always write down your password at a safe and secure place and not on computer monitor screens.

When you are signing into your account the administrator usually offers you two options; remember the Password and Nope. Never choose the first option.

Don't disclose your password to anyone not even to your closest friend or relative.

You should keep on changing your password for duration of every few months. Never keep one password for any account too long.

ANSWER THE QUESTIONS:

1. How can you protect your crucial data and other information?
2. What is the first task for data protection?
3. Is it safe to write down your password on computer monitor screen?
4. Which option is safer to you: remember the password and nope?

How often does the author of the article advise you to change your password?

Практическое задание I уровня «Организация работы в коллективе»

1. Оформить в среде MS Project начальные условия (плановые сроки и режим работы) по выполнению проекта в соответствии с исходными данными.

2. Выполнить планирование последовательности и продолжительности работ. Определить бюджет проекта (смету расходов) и сроки выполнения работ в среде MS Project.

3. Исходные данные

3.1. Заданный способ планирования по времени: начала проекта (начало проекта запланировано с даты 1 этапа исходных данных.

3.2. Наименование и примерная последовательность работ без учета их параллельного выполнения заданы в таблицах 1.1-1.3.

3.3. Изменение режима работы: четыре дня из состава возможных рабочих дней приходятся на праздники; в предпраздничные дни рабочий день сокращается на час; в связи с ужесточением сроков поставок предполагается использовать работу в субботние дни (всего – четыре дня).

3.4. Планирование суммарных задач, ввод вех, установление суммарной задачи проекта, установление и изменение связей, ограничений, крайнего срока, повторяющихся задач могут уточняться организаторами олимпиады перед началом работы.

Вариант 1. Таблица 1.1 Бизнес-план для открытия мастерской по производству мебели.

Наименование и последовательность работ	Ответственные исполнители	Продолжительность цикла, дни	Единицы назначения
1. Аренда и подготовка помещения	Директор	19 апреля	Разовый взнос 20000 руб.
	Директор, менеджер, рабочий	20 апреля (2 дня)	100%, 100%, 100%
2.Закупка основного производственного оборудования (верстаки, стеллажи, наборы инструментов)	Директор Менеджер Инженер 1	22 апреля (2 дня)	50%, 100%, 50%
	Верстаки; Наборы инструментов		(по цене - 5000 руб.); (по цене - 10000 руб.)
3.Транспортировка и установка оборудования	Менеджер грузовики	24 апреля (1 день)	50% 2 шт 300р/час

3.1. Аренда грузовика;			
3.2. Установка	Менеджер Инженер 1 Инженер 2	24 апреля (3 дня)	50%, 100%, 100%
4.Закупка и транспортировка расходных материалов (доски, клей и т.д.)	Менеджер Водитель Материалы Бензин – 26 рублей за 1 литр	27 апреля (2 дня)	100% 100% 15000 руб. 300 л
5. Запуск и тестирование оборудования	Рабочий Инженер 1	29 апреля (3 дня)	100%, 100%

Таблица 1.1.1. Оплата трудовых ресурсов:

Директор	40000 в месяц
Рабочий	300 рублей в час
Менеджер	30000 в месяц
Инженер 1	400 рублей в час
Водитель	4000 рублей по договору (фиксированная сумма)
Инженер 2	1000 рублей в день

Вариант 2. Таблица 1.2 Бизнес-план для открытия летнего кафе.

Наименование и последовательность работ	Ответственные исполнители	Продолжительность цикла, дни	Единицы назначения
1. Аренда и подготовка помещения, подбор кадров	аренда	16 мая (2 дня)	Разовый взнос 25000 руб
	Директор Менеджер Рабочий		100% 100% 100%
2.Закупка основного производственного оборудования (верстаки, стеллажи, наборы инструментов)	Директор Менеджер	18 мая (2 дня)	50% 100%
	печки - микроволновки по цене 3000 руб.; палатки по 5000 рублей; одноразовая посуда по 1000 руб.; мебель по 5 000 руб.		2 шт 3 шт 2 компл 5 компл

3.Транспортировка и установка оборудования 3.1. Аренда 2-х грузовиков и перевозка	Менеджер Грузовики	20 мая (1 день)	50% 2 шт. по 300 руб./час
3.2. Установка оборудования	инженер рабочий	20 мая (2 дня)	50% 100 %
4. Закупка долгохранящихся продуктов (мука) и их транспортировка	Менеджер Водитель	22 мая (2 дня)	100% 100%
	Мука по 20 руб. за 1 кг Бензин – 27 рублей за 1 литр		50 кг 200 литров

Таблица 1.2.1. Оплата трудовых ресурсов:

Директор	50000 в месяц
Рабочий	100 рублей в час
Менеджер	30000 в месяц
Инженер	300 рублей в час
Водитель	2000 рублей по договору (фиксированная сумма)

Вариант 3.

Определение проекта – закупка партии товара в Белоруссии:

1.Задача 1. Менеджер по закупкам, проанализировав заявки от дилеров и складские запасы, принимает решение о закупке товара. Составляет докладную о закупке и передает её директору.

2. Задача 2. Директор согласовывает закупочные цены и сроки с поставщиком. После согласования поставщик присылает счет. Бухгалтерия оплачивает счет.

3. Задача 3. Менеджер оформляет договор о транспортных услугах с фирмой «Авто-Транс». Заказывает транспорт (2 машины с прицепом и водителями).

4. Задача 4. Автомашины фирмы «Авто-Транс» едут в Белоруссию.

5. Задача 5. Поставщик (фирма «БелМастер») загружает машины и передает сопроводительные документы.

6. Задача 6. Рейс Белоруссия – Россия. Вернувшись в Россию, автомашины приезжают на таможенный пункт, где растаможивают товар. Задачу можно разделить на 3 подзадача: Рейс до таможни; Таможенный сервис; Рейс от таможни до склада фирмы.

7. Задача 7. Автомашины приезжают на склад фирмы, грузчики разгружают товар.

8. Задача 8. Бухгалтерия проверяет отчетность и оплачивает счет за грузоперевозки.

Таблица 1.3 Бизнес-план для открытия летнего кафе.

Задача	Ответственные	Продолжительность цикла, дни	Единицы назначения	Оплата
1.	Менеджер	2 (9 марта)	100%	30000 р/мес
2	Директор	4 (10 марта)	50%	50000 р/мес
	Бухгалтер		100%	40000 р/мес
	товар		Разовая сумма	9000000 руб
3	Менеджер	1 (13 марта)	-	100%
4	Услуги фирмы Авто-Транс (водители + транспорт)	3 (14 марта)	200	4000 руб /день за 1 машину
5	Услуги фирмы «БелМастер»	1 (17 марта)	-	30000 руб
6.1	Услуги фирмы Авто-Транс (водители + транспорт	1 (18 марта)	200%	4000 руб/день за одну машину
6.2	Услуги таможни	2 (19-20 марта)	-	Оплата – 30000 рублей
6.3	Услуги фирмы АвтоТранс (водители + транспорт)	2 (21-22 марта)	200%	4000 руб./ день за одну машину
7	Зав. складом	2 (23 -24 марта)	100%	25000 р/мес
	Грузчики склада - 4		400%	2000 руб/день
	Автопогрузчик с водителем		100%	25000 руб/мес
	бензин		100 л	20 р/л
8	Менеджер	2 (24 марта)	100%	-
	Бухгалтер		100%	-
	Директор		100%	-

Дополнительные условия - Работа фирмы Автотранс - без выходных. Обратите внимание – задачи 2, 3, 8 начинаются с опережением!

3.5. Ввод ограничений означает, что данная задача начинается до времени окончания предшествующей задачи (например, за один день – опережение (-1д)), или после – запаздывание (+5д). Опережение и запаздывание могут задаваться в процентах (%).

2 уровень
Практическое задание №1
«Администрирование системы защиты ViPNet»

Технологии этого модуля: технологии защиты сетевого трафика VPN VipNET, PKI-системы (ViPNet УЦ, Publication Service и др.)

Задание

Задание 1.1. Установка ПО ViPNet Administrator для создания защищённой сети:

- Установить и настроить рабочее место администратора VipNet: центр управления сетью (серверное и клиентское приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ).

Если были произведены изменения паролей, IP-адресов и так далее, необходимо отразить это в отчете.

Задание 1.2. Установка ПО ViPNet Coordinator и ПО VipNet Client на соответствующие виртуальные машины:

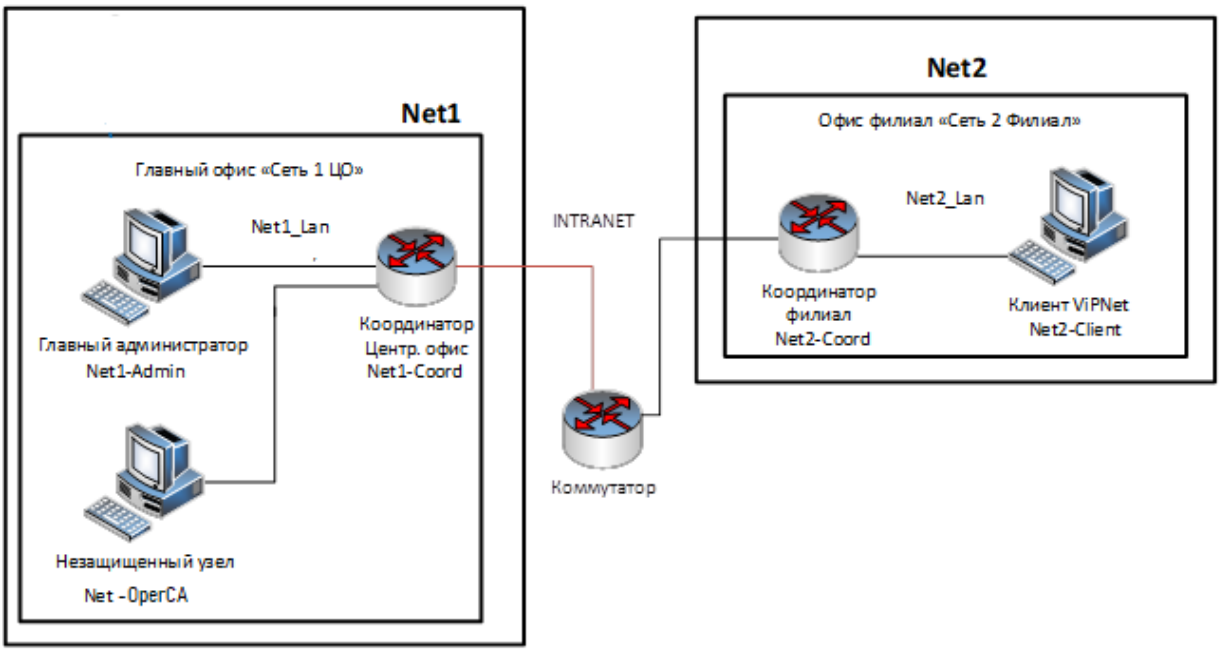
- На компьютере на Net1-Admin (ЦО) установить ПО ViPNet Client (Windows), рабочее место администратора;
- На компьютере на Net1-Coord (ЦО) установить ПО ViPNet Coordinator (Windows);
- На компьютере на Net2-Coord (Филиал) установить ПО ViPNet Coordinator (Windows);
- На ВМ на Net2-Client (филиал) установить ПО ViPNet Client, рабочее место пользователя;

Необходим скриншот первого запуска приложения.

Задание 2. Защита локально-вычислительной сети предприятия с применением ПО ViPNet

Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

Схема сети, которую требуется создать, приведена ниже.



В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).

Таблица 1 Узлы защищенной сети если УКЦ и ЦУС на одной машине.

Вирт. машина	Название сетевого узла	ПО VipNet	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1-Admin (ЦО)	Главный администратор (VM)	ViPNet Administrator (ЦУС клиент и сервер + УКЦ) ViPNet Client	ОС Windows Server	Admin
Net1-Coord (ЦО)	Координатор Центр Офис (VM)	ViPNet Coordinator	ОС Windows 10	CoordinatorOffice
Net2-Coord (Филиал)	Координатор Филиал (VM)	ViPNet Coordinator	ОС Windows 10	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал (VM)	ViPNet Client	ОС Windows 10	User2

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	**Coordinator Office**	**Admin**	**Coordinator Subsidiary**	**User2**
CoordinatorOffice	×	*	*	

Admin	*	×		*
CoordinatorSub	*		×	*
User2		*	*	×

Задание II уровня Вариативная часть

с учетом специфики специальности

10.02.01 «Настройка системы контроля информационных потоков и предотвращения неправомерных действий с информацией InfoWatch Traffic Monitor»

Используемое ПО:

- VMWare Workstation
- Red Hat Linux Enterprise
- Windows Server 2016 с установленным контроллером домена
- Windows Server 2016 (образ)
- Windows 10 (образ)
- PostgreSQL
- Traffic Monitor
- Device Monitor
- Crawler

Вам предоставлена в виртуальной среде виртуальная машина с контроллером домена. На нем развернут каталог Active Directory со всеми сотрудниками компании.

Создайте новую машину Red Hat Linux, на которой установите сервер безопасности InfoWatch Traffic Monitor (задайте ей имя IWTM). Сервер и СУБД должны быть установлены на одной виртуальной машине со следующими параметрами:

- виртуальный диск размером 80 – 100 ГБ в динамическом режиме;
- 2 процессора, 2 логических ядра;
- 8ГБ ОЗУ.

Параметры IWTM для установки: версия - Enterprise, СУБД - PostgreSQL.

Установите связь контроллера домена с Traffic Monitor.

Создайте новую виртуальную машину Windows Server, на которой установите операционную систему Windows Server (задайте ей имя IWDM). Введите машину в домен.

Активируйте лицензию IWTM.

Получите информацию о пользователях и компьютерах компании, представленных на сервере-контроллере домена, с помощью LDAP-синхронизации.

Запишите IP-адреса и соответствующие им имена машин, токен для подключения IWDM, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные Вами) системы в текстовом файле «*iwtm.txt*» на рабочем столе хостовой машины.

Установите на машину IWDM сервер безопасности InfoWatch Device Monitor.

Сервер безопасности InfoWatch Device Monitor и СУБД должны быть установлены на одной виртуальной машине. СУБД, которую необходимо установить - PostgreSQL.

При установке IWDM настройте пользователя для доступа к консоли управления: officer с паролем xxXX1234.

Синхронизируйте IWDM с каталогом Active Directory (компьютеры и пользователи) и свяжите сервер IWDM с сервером IWTM.

Создайте новую виртуальную машину Windows, на которой установите операционную систему Windows 10 (задайте ей имя ARM-Agent). Введите машину в домен.

Установите InfoWatch Device Monitor Agent на виртуальную машину ARM-Agent с помощью задачи первичного распространения (без формирования пакета установки) в IWDM.

Запишите IP-адреса и соответствующие им имена машин, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные Вами) системы в текстовом файле “iwtm.txt” на рабочем столе хостовой машины.

Установите на машину IWDM Crawler.

- Name of Traffic Monitor database (SID): postgres
- Username: iwtm_linux

Password: xxXX1234

Настройте Crawler на автоматическое ежедневное сканирование ранее созданного каталога и зафиксируйте выполнение задания скриншотом настройки Crawler в Web-консоли IWTM.

Сохраните скриншоты настройки сканера Crawler на рабочем столе хостовой машины в папке «Олимпиада_IWTM».

Выполните перехват событий от Crawler и сохраните скриншот, демонстрирующий данный перехват событий на рабочем столе хостовой машины в папке «Олимпиада_IWTM».

Настройте свою политику и правила для Device Monitor и сохраните скриншот, демонстрирующий работу своей политики и правил для Device Monitor на рабочем столе хостовой машины в папке «Олимпиада_IWTM».

Создайте «белый список устройств» Device Monitor и сохраните скриншот, демонстрирующий работу «белого списка устройств» Device Monitor на рабочем столе хостовой машины в папке «Олимпиада_IWTM».

Создайте «черный список приложений» и сохраните скриншот, демонстрирующий работу «чёрного» списка приложений Device Monitor на рабочем столе хостовой машины в папке «Олимпиада_IWTM».

Продемонстрируйте интеграцию Device Monitor с Active Directory. Сохраните скриншот, демонстрирующий интеграцию с Active Directory на рабочем столе хостовой машины в папке «Олимпиада_IWTM».

Выполните выборку событий по условию. Сохраните скриншот, демонстрирующий работу запроса выборки событий по созданному Вами условию на рабочем столе хостовой машины в папке «Олимпиада_IWTM».