**Всероссийская олимпиада профессионального мастерства**

**Утверждено**

**протоколом заседания**

**ФУМО по (наименование ФУМО)**

**от** 10.042018 **№**336/180 -УМО

**Фонд оценочных средств**

**Всероссийской олимпиады профессионального мастерства**

**по укрупненной группе специальностей СПО**

**10.00.00 Информационная безопасность**

**код и наименование**

**Уфа 2018**

**ФОС разработан: Арефьевым А.В, Павловой А.Н., Ждановым Р.Р.**

(указываются авторы разработки )

**Рассмотрен на 1.** **Заседании ФУМО СПО ИБ от** 10.042018 **№**336/180 -УМО

**Рецензенты**

**1.** Макаренков С.А. эксперт ФУМО ВО ИБ, Председатель УМС по специальности 10.05.03 «Информационная безопасность автоматизированных систем», к.т.н.

**2**. Василевский В.В. эксперт ФУМО СПО ИБ, Сопредседатель УМС по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», к.в.н., доцент

**3.** Дмитриченко А. В., генеральный директор ООО НПП «Гарант Уфа»

**4.** Валеев Р. А., начальник центра информационных технологий, связи и защиты информации МВД по Республике Башкортостан

**Содержание**

1. **Спецификация Фонда оценочных средств.**
2. **Паспорт практического задания «Перевод профессионального текста».**
3. **Паспорт практического задания «Задание по организации работы коллектива».**
4. **Паспорт практического задания инвариантной части практического задания 2 уровня.**
5. **Паспорт практического задания вариативной части практического задания 2 уровня.**
6. **Оценочные средства (демоверсии, включающие инструкции по выполнению)**
7. **Индивидуальные ведомости оценок результатов выполнения участником практических заданий I уровня**
8. **Индивидуальная сводная ведомость оценок результатов выполнения участником заданий I уровня**
9. **Индивидуальные ведомости оценок результатов выполнения участником практических заданий 2 уровня**
10. **Индивидуальная сводная ведомость оценок результатов выполнения участником заданий 2 уровня**
11. **Сводная ведомость оценок результатов выполнения участниками заданий олимпиады**
12. **Методические материалы**

**Спецификация Фонда оценочных средств**

1. **Назначение Фонда оценочных средств**
   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»;

приказа Министерства образования и науки Российской Федерации от 29 октября 2013 г. № 1199 «Об утверждении перечня специальностей среднего профессионального образования»;

приказа Министерства образования и науки РФ от 18 ноября 2015 г. № 1350«О внесении изменений в перечни профессий и специальностей среднего профессионального образования, утвержденные приказом Министерства образования и науки Российской Федерации от 29 октября 2013 г. № 1199»;

регламента организации и проведения Всероссийской олимпиады профессионального мастерства обучающихся по специальностям среднего профессионального образования, утвержденного директором Департамента государственной политики в сфере подготовки рабочих кадров и ДПО Минобрнауки России Н.М. Золотаревой 27.02 2018 г.;

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 2 части - инвариантную и вариативную, всего 40 вопросов.

Инвариантная часть задания «Тестирование» содержит 20 вопросов по пяти 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 20 вопросов 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.

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** | **Откры=тая 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 | Оборудование, материалы, инструменты | 4 | 1 | 1 | 1 | 1 | 1 |
| 3 | Системы качества, стандартизации и сертификации | 4 | 1 | 1 | 1 | 1 | 1 |
| 4 | Охрана труда, безопасность жизнедеятельности, безопасность окружающей среды | 4 | 1 | 1 | 1 | 1 | 1 |
| 5 | Экономика и правовое обеспечение профессиональной деятельности | 4 | 1 | 1 | 1 | 1 | 1 |
|  | ИТОГО: | **20** |  |  |  |  | **5** |
|  | *Вариативный раздел тестового задания УГС10.00.00 Информационная безопасность* | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | Основы информационной безопасности | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | Организация и сопровождение электронного документооборота/ Криптографическая защита информации/ Криптографические средства и методы защиты информации | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | Технические методы и средства, технологии защиты информации/ Инженерно-техническая защита информации/ Применение инженерно-технических средств обеспечения информационной безопасности | 1 | 1 | 1 | 1 | 1 | 1 |
| 4 | Программно-аппаратные средства защиты информации/ Программно-аппаратные средства защищенных телекоммуникационных систем/ Программно-аппаратные средства обеспечения информационной безопасности | 1 | 1 | 1 | 1 | 1 | 1 |
| 5 | Обеспечение организации системы безопасности организации/Правовая защита информации/ | 1 | 1 | 1 | 1 | 1 | 1 |
|  | ИТОГО: | **20** |  |  |  |  | **5** |
|  | **ИТОГО:** | **40** |  |  |  |  | **10** |

\* Распределение заданий по вариативной части тестового задания является примерной, рекомендуемой для возможного использования

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 4.

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 1 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 2 задачи:

перевод текста, содержание которого включает профессиональную лексику.

ответы на вопросы по тексту.

Объем текста на иностранном языке составляет (1500-2000) знаков.

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

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 2 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 содержание работы, которую необходимо выполнить участнику для демонстрации определённого вида профессиональной деятельности в соответствии с требованиями ФГОС и профессиональных стандартов с применением практических навыков, заключающихся в проектировании, разработке, выполнении работ или изготовлении продукта (изделия и т.д.) по заданным параметрам с контролем соответствия результата существующим требованиям.

Количество заданий II уровня, составляющих общую или вариативную часть, одинаковое для специальностей или УГС 10.00.00 Информационная безопасность.

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 УГС 10.00.00 Информационная безопасность..

Инвариантная часть заданий II уровня представляет собой практическое задание, которые содержит 2- 3 задачи.

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

3.11. Вариативная часть задания II уровня формируется в соответствии со специфическими для каждой специальности, входящей в УГС 10.00.00 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 УГС 10.00.00 Информационная безопасность..

Вариативная часть задания II уровня содержит 2-3 задачи различных уровней сложности.

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: общая 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.03)**  **10.02.02(ОП.03)**  **10.02.03(ОП.04)** | **2. Оборудование, материалы, инструменты** | **0,1** | **0,2** | **0,3** | **0,4** |
| **10.02.01(ОП.01)**  **10.02.02(ОП.04)**  **10.02.03(ОП.03)** | **3. 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)** | **4. 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)** | **5. 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)** | **6. Основы информационной безопасности** | **0,1** | **0,2** | **0,3** | **0,4** |
| **10.02.01**  **(МДК 02.03)**  **10.02.02 (МДК02.01)**  **10.02.03 (МДК02.02)** | **7.** **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)** | **8 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)** | **9. 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)** | **10. 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 практические конкурсные задания I уровня: «Перевод профессионального текста (сообщения)» составляет 10 баллов.

4.8. 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 являются едиными для всех УГС СПО.

При выполнении 2 задачи в содержание критериев могут быть внесены дополнения (изменения) касающиеся конкретной УГС, которые не влияют на удельный вес каждого критерия.

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 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 (орфорграфические, 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).

Таблица 4

Критерии оценки 2 задачи

«Перевод профессионального текста (сообщения)»

(ответы на вопросы, аудирование, выполнение действия)

|  |  |  |
| --- | --- | --- |
| **№** | **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**

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 |
|  | Успешный эхо-запрос между узлами ПК-1 – ПК-4 | 1 | 0,1 |
|  | Успешный эхо-запрос между узлами ПК-2 – ПК-6 | 1 | 0,1 |
|  | Успешный эхо-запрос между узлами ПК-3 – ПК-6 | 1 | 0,1 |
|  | Успешный эхо-запрос между узлами ПК-1 – ПК-7 | 1 | 0,1 |
|  | Успешный эхо-запрос между узлами ПК-2 – ПК-8 | 1 | 0,1 |
|  | Успешный эхо-запрос между узлами ПК-3 – ПК-9 | 1 | 0,1 |
|  | Настройка пользователя Admin на маршрутизаторе DHCP | 1 | 0,1 |
|  | Настройка пользователя Admin на маршрутизаторе R1 | 1 | 0,1 |
|  | Настройка пользователя Admin на маршрутизаторе R2 | 1 | 0,1 |
|  | Настройка пользователя Admin на маршрутизаторе R3 | 1 | 0,1 |
|  | Настройка пользователя Admin на маршрутизаторе RB | 1 | 0,1 |
|  | Настройка пользователя Admin на коммутаторе S1 | 1 | 0,1 |
|  | Настройка пользователя Admin на коммутаторе S2 | 1 | 0,1 |
|  | Настройка пользователя Admin на коммутаторе SB | 1 | 0,1 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе DHCP | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R1 | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R2 | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R3 | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе RB | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе S1 | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе S2 | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе SB | 2 | 0,2 |
|  | Настройка доступа по протоколу SSH на маршрутизаторе DHCP | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на маршрутизаторе R1 | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на маршрутизаторе R2 | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на маршрутизаторе R3 | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на маршрутизаторе RB | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на коммутаторе S1 | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на коммутаторе S2 | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на коммутаторе SB | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе DHCP | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R1 | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R2 | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R3 | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе RB | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе S1 | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе S2 | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе SB | 3 | 0,3 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе DHCP | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R1 | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R2 | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R3 | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе RB | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе S1 | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе S2 | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе SB | 2 | 0,2 |
|  | Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе DHCP | 3 | 0,3 |
|  | Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R1 | 3 | 0,3 |
|  | Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R2 | 2 | 0,2 |
|  | Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R3 | 3 | 0,3 |
|  | Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе RB | 3 | 0,3 |
|  | Настройка баннера MOTD, шифрование незашифрованных паролей на коммутаторе S1 | 2 | 0,2 |
|  | Настройка баннера, шифрование незашифрованных паролей на коммутаторе S2 | 2 | 0,2 |
|  | Настройка баннера, шифрование незашифрованных паролей на коммутаторе SB | 2 | 0,2 |
|  | Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство DHCP | 3 | 0,3 |
|  | Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R1 | 3 | 0,3 |
|  | Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R2 | 3 | 0,3 |
|  | Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R3 | 3 | 0,3 |
|  | Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство RB | 3 | 0,3 |
|  | Настройка NTP-клиента на маршрутизаторе DHCP | 5 | 0,5 |
|  | Настройка NTP-клиента на маршрутизаторе R1 | 5 | 0,5 |
|  | Настройка NTP-клиента на маршрутизаторе R2 | 5 | 0,5 |
|  | Настройка NTP-клиента на маршрутизаторе R3 | 5 | 0,5 |
|  | Настройка NTP-клиента на маршрутизаторе RB | 5 | 0,5 |
|  | Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF\_GUARD) на маршрутизаторе R1 | 2 | 0,2 |
|  | Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF\_GUARD) на маршрутизаторе R2 | 2 | 0,2 |
|  | Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF\_GUARD) на маршрутизаторе R3 | 4 | 0,4 |
|  | Настройка именованного списка контроля доступа **NAT** на маршрутизаторе R3 | 1 | 0,1 |
|  | Настройка именованного списка контроля доступа **NAT** на маршрутизаторе RB | 1 | 0,1 |
|  | Настройка пула NAT R3POOL на маршрутизаторе R3 | 2 | 0,2 |
|  | Настройка статического NAT для сервера **Сервер** на маршрутизаторе R3 | 2 | 0,2 |
|  | Настройка пула NAT RBPOOL на маршрутизаторе RB | 2 | 0,2 |
|  | Настройка VPN-туннеля на маршрутизаторе R3 | 20 | 2 |
|  | Настройка VPN-туннеля на маршрутизаторе RB | 20 | 2 |
|  | Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45,** **VLAN60, VLAN75** на маршрутизаторе R1 | 10 | 1 |
|  | Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45,** **VLAN60, VLAN75** на маршрутизаторе R2 | 10 | 1 |
|  | Настройка протокола резервирования шлюза HSRP на маршрутизаторе R1 | 20 | 2 |
|  | Настройка протокола резервирования шлюза HSRP на маршрутизаторе R2 | 20 | 2 |
|  | Настройка VLAN, присвоение им имён на коммутаторе S1 | 5 | 0,5 |
|  | Настройка VLAN, присвоение им имён на коммутаторе S2 | 5 | 0,5 |
|  | Назначение портов доступа на интерфейсах коммутатора S1, включение функций PortFast и BPDU guard | 14 | 1,4 |
|  | Назначение портов доступа на интерфейсах коммутатора S2, включение функций PortFast и BPDU guard | 11 | 1,1 |
|  | Настройка функции Port Security на коммутаторе S1 | 12 | 1,2 |
|  | Настройка функции Port Security на коммутаторе S2 | 9 | 0,9 |
|  | 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 |
|  | Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S1 | 4 | 0,4 |
|  | Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S2 | 3 | 0,3 |
|  | 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 |
|  | 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 «Развертывание Удостоверяющего центра ViPNet в аккредитованном режиме»

|  |  |  |
| --- | --- | --- |
| № | Оцениваемый параметр | Количество баллов |
| 1 | Построение сети центра сертификации предприятия в аккредитованном режиме. В соответствии со схемой развертывания ViPNet в локальной сети:  - Создать сетевые узлы «Координатор; | 1 |
| 2 | - Создать клиентов «Администратор Центра сертификации», «Оператор ЦР\_СП» ; | 1 |
| 3 | - Создать пользователей сетевых узлов ; | 1 |
| 4 | - Настроить роли Publication Service и Registration Point для клиента «Оператор ЦР\_СП» | 1 |
| 5 | - Создать связи между пользователями | 1 |
| 6 | - Создать справочники СУ | 1 |
| 7 | - Установить Рутокен; | 1 |
| 8 | - Настроить новую БД | 1 |
| 9 | - Настроить Свойства удостоверяющего центра | 1 |
| 10 | - Настроить средство ЭП владельцев сертификата- ViPNet CSP 4.2 | 1 |
| 11 | - Настроить автоматический режим работы | 1 |
| 12 | - Настроить Место хранения контейнера ключа ЭЦП, тип создаваемого пароля | 1 |
| 13 | - Выдать дистрибутивы ключей для сетевых узлов | 1 |
| 14 | - Настроить параметры аутентификации пользователя | 1 |
| 15 | - Создать новый шаблон сертификата | 1 |
| 16 | - Создайте новую политику применения сертификатовАдминистратор центра сертификации» по Рутокену. | 2 |
| 17 | - Настроить, добавление в сертификаты информации о центрах регистрации | 2 |
| 18 | - Создать квалифицированный ключ электронной подписи и ключ проверки ЭП для пользователей сети ViPNet | 2 |
| 19 | - Издать сертификаты для пользователей своей сети, для узлов входящих в состав структуры сети УЦ. | 2 |
| 20 | - Настроить папку приёма и отправки файлов в УКЦ | 2 |
|  | Максимальное количество баллов | 25 баллов |

10.02.01 Задание 3 «Настройка системы учета рабочего времени «Guard Light»

|  |  |  |
| --- | --- | --- |
| № | Оцениваемый параметр | Количество баллов |
| 1 | - Осуществить подключениеь контроллера карточного доступа | 1 |
| 2 | - Осуществить подключение контроллера кодового доступа | 1 |
| 3 | - Создать базу данных работников предприятия согласно параметрам разрешенного доступа в подразделения «Офис» и «Склад» | 1 |
| 4 | - Создать отделы и настроить графики работы | 1 |
| 5 | - Вывести по ним отчет по работникам | 1 |
| 6 | - Настроить систему пожарной сигнализации | 1 |
| 7 | - Заблокировать доступ в праздничные и выходные дни | 1 |
| 8 | - Заблокировать доступ в связи с командировкой | 1 |
| 9 | - Настроить показ уведомлений при проходе работников на предприятии. | 1 |
| 10 | - Вывести отчет о обработке данных | 1 |
| Максимальное количество баллов | | 10 |

10.02.02 Задание 2 «Организация межсетевого защищенного взаимодействия с применением ПО ViPNet»

|  |  |  |
| --- | --- | --- |
| № | Оцениваемый параметр | Количество баллов |
| 1 | - Создать сетевые узлы | 1 |
| 2 | - В соответствии со схемой развертывания ViPNet в локальной сети создать клиентов | 1 |
| 3 | - Создать пользователей и зарегистрировать их на клиентах | 1 |
| 4 | - Построить межсерверный канал | 1 |
| 5 | - Построить межсерверные связи пользователей | 1 |
| 6 | - Создать справочники сетевых узлов для пользователей | 1 |
| 7 | - VM\_1Создать учетную запись Администратора сети ViPNet Настроить параметры; | 1 |
| 8 | - Выполнить настройку политики выдачи ключей | 1 |
| 9 | - Произвести выдачу дистрибутивов ключей для всех пользователей | 1 |
| 10 | - VM\_2 Развернуть рабочее место ViPNet Coordinator с соответствующими ключами | 1 |
| 11 | -VM\_3 Развернуть рабочее место ViPNet Coordinator с соответствующими ключами | 1 |
| 12 | \_VM\_4 Развернуть рабочее место ViPNet Администратор сети ViPNet Федеральной службы | 1 |
| 13 | - Инициировать межсетевое взаимодействие c инициатором ЦентрОфис к Федеральной службе | 1 |
| 14 | - Создайте индивидуальный симметричный межсетевой мастер-ключ, экспортируйте его на флеш. | 1 |
| 15 | - Произвести прием первичной межсетевой информации на рабочем месте Администратора сети Федеральной службы | 1 |
| 16 | - Установить связь Координатора ЦентрОфис и Координатора Федеральной службы | 2 |
| 17 | - Импортировать и использовать межсетевой мастер-ключ Главного администратора компании | 2 |
| 18 | - Произвести экспорт межсетевой информации сертификатов администраторов и списков аннулированных сертификатов. | 2 |
| 19 | - Создать ответную межсетевую информацию, сохранить на флеш, создать справочники и ключи передать сохраненный файл Администратору компании. | 2 |
| 20 | - Принять на VM\_1 ответную межсетевую информацию. | 2 |
| Максимальное количество баллов | | 25 |

10.02.02 Задание 3 «Настройка АПМДЗ ПАК «Соболь»

|  |  |  |
| --- | --- | --- |
| № | Оцениваемый параметр | Количество баллов |
| 1 | - Произвести Подключение АПМДЗ | 1 |
| 2 | - Произвести подключение блокировки по Reset; | 1 |
| 3 | - Произвести инициализацию устройства, настроить общие параметры | 1 |
| 4 | - Создать первичного администратора, произвести первичную смену пароля | 1 |
| 5 | - Произвести настройку контроля целостности, поставить на контроль файл | 1 |
| 6 | произвести настройку комплекса в режиме Администратора  - создать Администратора и пользователей  - настроить общие параметры | 1 |
| 7 | - Произвести вход пользователем | 1 |
| 8 | - Заблокировать пользователя неправильным входом | 1 |
| 9 | - Разблокировать пользователя | 1 |
| 10 | - Вывести отчет журнала событий | 1 |
| Максимальное количество баллов | | 10 |

10.02.03 Задание 2 «Администрирование системы защиты ViPNet»

|  |  |  |
| --- | --- | --- |
| № | Оцениваемый параметр | Количество баллов |
| 1 | - Создать сетевые узлы, клиентов зарегистрированных на соответствующем | 1 |
| 2 | - В соответствии с таблицей создать пользователей, зарегистрировать их на клиентах | 1 |
| 3 | - Построить межсерверный канал между «Координатором ЦентрОфис» и «Координатором Филиал». | 1 |
| 4 | - Построить связи пользователей согласно | 1 |
| 5 | - Создать справочники сетевых узлов для пользователей | 1 |
| 6 | - Создать учетную запись Администратора сети ViPNet , настроить параметры | 1 |
| 7 | - Выполнить настройку политики выдачи ключей | 1 |
| 8 | - Произвести выдачу дистрибутивов ключей для всех пользователей | 1 |
| 9 | - Произвести резервное копирование в ПО ViPNet Administrator УКЦ текущей конфигурации сети в ручном режиме | 1 |
| 10 | - Настроить автоматическое резервное копирование | 1 |
| 11 | - Установить ViPNet Client, установить ключи | 1 |
| 12 | - Создать учетную запись | 1 |
| 13 | -Установить ViPNet Administrator ЦУС,установить соединение с сервером | 1 |
| 14 | - Настроить Транспортный модуль обеспечивающий обмен служебными конвертами | 1 |
| 15 | - Выполнить модификацию сети, согласно предложенной схемы | 1 |
| 16 | - Создать группы узлов , выполнить настройки | 2 |
| 17 | - Произвести смену мастер ключей персональных ключей в УКЦ | 2 |
| 18 | - Объявить ключи скомпрометированными, выполнить действия по смене ключей | 2 |
| 19 | - Создать подразделения | 2 |
| 20 | - Создать политику безопасности блокирования | 2 |
| Максимальное количество баллов | | 25 |

10.02.03 Задание 3 «Настройка программного средства безопасности Secret Net Studio»

|  |  |  |
| --- | --- | --- |
| № | Оцениваемый параметр | Количество баллов |
| 1 | - Настройка «Политики и Регистрации событий» | 1 |
| 2 | - Настроить доступ к пользователю «adminsns» по идентификатору Рутокен | 1 |
| 3 | - Установить и настроить Рутокен | 1 |
| 4 | - Настроить параметры входа в систему | 1 |
| 5 | - Провести проверочные мероприятия выполненных настроек | 1 |
| 6 | - Произвести экспорт журнала | 1 |
| 7 | - Присвоить права администратора и скрыть пользователя с экрана приветствия | 1 |
| 8 | - Настроить контроль целостности | 1 |
| 9 | - Произвести проверку нарушения режима контроля целостности | 1 |
| 10 | - Выполнить аудит системы | 1 |
| Максимальное количество баллов | | 10 |

**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 час (академический).

Рекомендуемое максимальное время для выполнения отдельных заданий 2 уровня:

- 2 уровень Задание 1 Инвариантная часть – 3 часа

- 2 уровень Задание2 Вариативная часть – 3 часа

- 2 уровень Задание 3 Вариативная часть – 2 часа

**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 7,1С .

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 Windows 7, 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 Windows, (open source) – Project Libre.

Должна быть обеспечена возможность единовременного выполнения задания всеми участниками Олимпиады.

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

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 Windows, Microsoft Office Word, Cisco Packet Tracer 7.1, VirtualBox 5.2, ViPNet Администратор4, ViPNet Registration Point, ViPNet Publication Service, ViPNet Client, ViPNet Policy Manager, ViPNet Coordinator. SecretNet Studio8 «Guard Light», драйвер «Рутокен»

Используемое оборудование: - АПМДЗ ПАК «Соболь3.0»

- ПАК «Рутокен 32S»

- Флеш накопитель 8Гб, USB 3.0

- стенд СКУД «IronLogic»

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 индивидуальные сводные ведомости оценок результатов выполнения заданий I и II уровня.

7.2. На основе указанных в п.7.1.ведомостей формируется сводная ведомость, 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 3 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 Всероссийской олимпиады. Участники, имеющие второй и третий результаты, являются призерами Всероссийской 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 заданий 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.

**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/  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  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 | 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 - 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  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 | 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 - 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  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 |

**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 |
|  | Успешный эхо-запрос между узлами ПК-1 – ПК-4 | 1 | 0,1 |
|  | Успешный эхо-запрос между узлами ПК-2 – ПК-6 | 1 | 0,1 |
|  | Успешный эхо-запрос между узлами ПК-3 – ПК-6 | 1 | 0,1 |
|  | Успешный эхо-запрос между узлами ПК-1 – ПК-7 | 1 | 0,1 |
|  | Успешный эхо-запрос между узлами ПК-2 – ПК-8 | 1 | 0,1 |
|  | Успешный эхо-запрос между узлами ПК-3 – ПК-9 | 1 | 0,1 |
|  | Настройка пользователя Admin на маршрутизаторе DHCP | 1 | 0,1 |
|  | Настройка пользователя Admin на маршрутизаторе R1 | 1 | 0,1 |
|  | Настройка пользователя Admin на маршрутизаторе R2 | 1 | 0,1 |
|  | Настройка пользователя Admin на маршрутизаторе R3 | 1 | 0,1 |
|  | Настройка пользователя Admin на маршрутизаторе RB | 1 | 0,1 |
|  | Настройка пользователя Admin на коммутаторе S1 | 1 | 0,1 |
|  | Настройка пользователя Admin на коммутаторе S2 | 1 | 0,1 |
|  | Настройка пользователя Admin на коммутаторе SB | 1 | 0,1 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе DHCP | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R1 | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R2 | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе R3 | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на маршрутизаторе RB | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе S1 | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе S2 | 2 | 0,2 |
|  | Настройка длины ключа шифрования составляет 1024 бит для домена **olimp-spo.ru** на коммутаторе SB | 2 | 0,2 |
|  | Настройка доступа по протоколу SSH на маршрутизаторе DHCP | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на маршрутизаторе R1 | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на маршрутизаторе R2 | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на маршрутизаторе R3 | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на маршрутизаторе RB | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на коммутаторе S1 | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на коммутаторе S2 | 3 | 0,3 |
|  | Настройка доступа по протоколу SSH на коммутаторе SB | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе DHCP | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R1 | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R2 | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе R3 | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на маршрутизаторе RB | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе S1 | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе S2 | 3 | 0,3 |
|  | Настройка безопасного входа с локальной проверкой паролей на линиях VTY, консольном входе на коммутаторе SB | 3 | 0,3 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе DHCP | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R1 | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R2 | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе R3 | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на маршрутизаторе RB | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе S1 | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе S2 | 2 | 0,2 |
|  | Настройка отключения пользователя при бездействии в течении 5-ти минут на линиях VTY, консольном входе на коммутаторе SB | 2 | 0,2 |
|  | Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе DHCP | 3 | 0,3 |
|  | Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R1 | 3 | 0,3 |
|  | Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R2 | 2 | 0,2 |
|  | Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе R3 | 3 | 0,3 |
|  | Настройка баннера MOTD и минимальной длины паролей, шифрование незашифрованных паролей на маршрутизаторе RB | 3 | 0,3 |
|  | Настройка баннера MOTD, шифрование незашифрованных паролей на коммутаторе S1 | 2 | 0,2 |
|  | Настройка баннера, шифрование незашифрованных паролей на коммутаторе S2 | 2 | 0,2 |
|  | Настройка баннера, шифрование незашифрованных паролей на коммутаторе SB | 2 | 0,2 |
|  | Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство DHCP | 3 | 0,3 |
|  | Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R1 | 3 | 0,3 |
|  | Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R2 | 3 | 0,3 |
|  | Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство R3 | 3 | 0,3 |
|  | Настройка противодействия атакам типа «подбор пароля»: ограничение количества попыток входа на устройство RB | 3 | 0,3 |
|  | Настройка NTP-клиента на маршрутизаторе DHCP | 5 | 0,5 |
|  | Настройка NTP-клиента на маршрутизаторе R1 | 5 | 0,5 |
|  | Настройка NTP-клиента на маршрутизаторе R2 | 5 | 0,5 |
|  | Настройка NTP-клиента на маршрутизаторе R3 | 5 | 0,5 |
|  | Настройка NTP-клиента на маршрутизаторе RB | 5 | 0,5 |
|  | Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF\_GUARD) на маршрутизаторе R1 | 2 | 0,2 |
|  | Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF\_GUARD) на маршрутизаторе R2 | 2 | 0,2 |
|  | Настройка парольной защиты для работы протокола OSPF (алгоритм аутентификации – MD5 и пароль OSPF\_GUARD) на маршрутизаторе R3 | 4 | 0,4 |
|  | Настройка именованного списка контроля доступа **NAT** на маршрутизаторе R3 | 1 | 0,1 |
|  | Настройка именованного списка контроля доступа **NAT** на маршрутизаторе RB | 1 | 0,1 |
|  | Настройка пула NAT R3POOL на маршрутизаторе R3 | 2 | 0,2 |
|  | Настройка статического NAT для сервера **Сервер** на маршрутизаторе R3 | 2 | 0,2 |
|  | Настройка пула NAT RBPOOL на маршрутизаторе RB | 2 | 0,2 |
|  | Настройка VPN-туннеля на маршрутизаторе R3 | 20 | 2 |
|  | Настройка VPN-туннеля на маршрутизаторе RB | 20 | 2 |
|  | Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45,** **VLAN60, VLAN75** на маршрутизаторе R1 | 10 | 1 |
|  | Настройка именованных списков контроля доступа **VLAN15, VLAN30, VLAN45,** **VLAN60, VLAN75** на маршрутизаторе R2 | 10 | 1 |
|  | Настройка протокола резервирования шлюза HSRP на маршрутизаторе R1 | 20 | 2 |
|  | Настройка протокола резервирования шлюза HSRP на маршрутизаторе R2 | 20 | 2 |
|  | Настройка VLAN, присвоение им имён на коммутаторе S1 | 5 | 0,5 |
|  | Настройка VLAN, присвоение им имён на коммутаторе S2 | 5 | 0,5 |
|  | Назначение портов доступа на интерфейсах коммутатора S1, включение функций PortFast и BPDU guard | 14 | 1,4 |
|  | Назначение портов доступа на интерфейсах коммутатора S2, включение функций PortFast и BPDU guard | 11 | 1,1 |
|  | Настройка функции Port Security на коммутаторе S1 | 12 | 1,2 |
|  | Настройка функции Port Security на коммутаторе S2 | 9 | 0,9 |
|  | 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 |
|  | Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S1 | 4 | 0,4 |
|  | Настройка ограничения протокола DHCP на активных не доверенных портах доступа на 10 запросов на коммутаторе S2 | 3 | 0,3 |
|  | 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 |
|  | Настройка шлюза по умолчанию на коммутаторе SB | 1 | 0,1 |
| Максимальная оценка программы | | 350 |  |
| Максимальное количество баллов | |  | 35 |

**Паспорт задания вариативной части II уровня**

Задание 2

|  |  |  |  |
| --- | --- | --- | --- |
| № | **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 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.  3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов | ПК 2.1. Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем.  ПК 2.2. Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем, их диагностику, обнаружение отказов, формировать предложения по их устранению.  ПК 2.3. Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем.  ПК 2.4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей | ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.  ПК 3.2. Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.  ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.  ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.  ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами. |
| 3 | 10.02.01 (МДК 03.02) | 10.02.02 (МДК 02.03) | 10.02.03 (МДК 02.01) |
| 4 | 10.02.01 Задание 2 «Развертывание Удостоверяющего центра ViPNet в аккредитованном режиме» | 10.02.02 «Организация межсетевого защищенного взаимодействия с применением ПО ViPNet» | 10.02.03 Задание 2 «Администрирование системы защиты ViPNet» |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5 | № | | Оцениваемый параметр | Количество баллов | № | Оцениваемый параметр | Количество баллов | № | Оцениваемый параметр | Количество баллов |
| 1 | | Построение сети центра сертификации предприятия в аккредитованном режиме. В соответствии со схемой развертывания ViPNet в локальной сети:  - Создать сетевые узлы «Координатор; | 1 | 1 | - Создать сетевые узлы | 1 | 1 | - Создать сетевые узлы, клиентов зарегистрированных на соответствующем | 1 |
| 2 | | - Создать клиентов «Администратор Центра сертификации», «Оператор ЦР\_СП» ; | 1 | 2 | - В соответствии со схемой развертывания ViPNet в локальной сети создать клиентов | 1 | 2 | - В соответствии с таблицей создать пользователей, зарегистрировать их на клиентах | 1 |
| 3 | | - Создать пользователей сетевых узлов ; | 1 | 3 | - Создать пользователей и зарегистрировать их на клиентах | 1 | 3 | - Построить межсерверный канал между «Координатором ЦентрОфис» и «Координатором Филиал». | 1 |
| 4 | | - Настроить роли Publication Service и Registration Point для клиента «Оператор ЦР\_СП» | 1 | 4 | - Построить межсерверный канал | 1 | 4 | - Построить связи пользователей согласно | 1 |
| 5 | | - Создать связи между пользователями | 1 | 5 | - Построить межсерверные связи пользователей | 1 | 5 | - Создать справочники сетевых узлов для пользователей | 1 |
| 6 | | - Создать справочники СУ | 1 | 6 | - Создать справочники сетевых узлов для пользователей | 1 | 6 | - Создать учетную запись Администратора сети ViPNet , настроить параметры | 1 |
| 7 | | - Установить Рутокен; | 1 | 7 | - VM\_1Создать учетную запись Администратора сети ViPNet Настроить параметры; | 1 | 7 | - Выполнить настройку политики выдачи ключей | 1 |
| 8 | | - Настроить новую БД | 1 | 8 | - Выполнить настройку политики выдачи ключей | 1 | 8 | - Произвести выдачу дистрибутивов ключей для всех пользователей | 1 |
| 9 | | - Настроить Свойства удостоверяющего центра | 1 | 9 | - Произвести выдачу дистрибутивов ключей для всех пользователей | 1 | 9 | - Произвести резервное копирование в ПО ViPNet Administrator УКЦ текущей конфигурации сети в ручном режиме | 1 |
| 10 | | - Настроить средство ЭП владельцев сертификата- ViPNet CSP 4.2 | 1 | 10 | - VM\_2 Развернуть рабочее место ViPNet Coordinator с соответствующими ключами | 1 | 10 | - Настроить автоматическое резервное копирование | 1 |
| 11 | | - Настроить автоматический режим работы | 1 | 11 | -VM\_3 Развернуть рабочее место ViPNet Coordinator с соответствующими ключами | 1 | 11 | - Установить ViPNet Client, установить ключи | 1 |
| 12 | | - Настроить Место хранения контейнера ключа ЭЦП, тип создаваемого пароля | 1 | 12 | \_VM\_4 Развернуть рабочее место ViPNet Администратор сети ViPNet Федеральной службы | 1 | 12 | - Создать учетную запись | 1 |
| 13 | | - Выдать дистрибутивы ключей для сетевых узлов | 1 | 13 | - Инициировать межсетевое взаимодействие c инициатором ЦентрОфис к Федеральной службе | 1 | 13 | -Установить ViPNet Administrator ЦУС,установить соединение с сервером | 1 |
| 14 | | - Настроить параметры аутентификации пользователя | 1 | 14 | - Создайте индивидуальный симметричный межсетевой мастер-ключ, экспортируйте его на флеш. | 1 | 14 | - Настроить Транспортный модуль обеспечивающий обмен служебными конвертами | 1 |
| 15 | | - Создать новый шаблон сертификата | 1 | 15 | - Произвести прием первичной межсетевой информации на рабочем месте Администратора сети Федеральной службы | 1 | 15 | - Выполнить модификацию сети, согласно предложенной схемы | 1 |
| 16 | | - Создайте новую политику применения сертификатовАдминистратор центра сертификации» по Рутокену. | 2 | 16 | - Установить связь Координатора ЦентрОфис и Координатора Федеральной службы | 2 | 16 | - Создать группы узлов , выполнить настройки | 2 |
| 17 | | - Настроить, добавление в сертификаты информации о центрах регистрации | 2 | 17 | - Импортировать и использовать межсетевой мастер-ключ Главного администратора компании | 2 | 17 | - Произвести смену мастер ключей персональных ключей в УКЦ | 2 |
| 18 | | - Создать квалифицированный ключ электронной подписи и ключ проверки ЭП для пользователей сети ViPNet | 2 | 18 | - Произвести экспорт межсетевой информации сертификатов администраторов и списков аннулированных сертификатов. | 2 | 18 | - Объявить ключи скомпрометированными, выполнить действия по смене ключей | 2 |
| 19 | | - Издать сертификаты для пользователей своей сети, для узлов входящих в состав структуры сети УЦ. | 2 | 19 | - Создать ответную межсетевую информацию, сохранить на флеш, создать справочники и ключи передать сохраненный файл Администратору компании. | 2 | 19 | - Создать подразделения | 2 |
| 20 | | - Настроить папку приёма и отправки файлов в УКЦ | 2 | 20 | - Принять на VM\_1 ответную межсетевую информацию. | 2 | 20 | - Создать политику безопасности блокирования | 2 |
|  | 10.02.01 Задание 3 «Настройка системы учета рабочего времени «Guard Light» | | | | 10.02.02 Задание 3 «Настройка АПМДЗ ПАК «Соболь» | | | 10.02.03 Задание 3 «Настройка программного средства безопасности Secret Net Studio» | | |
|  | № | Оцениваемый параметр | | Количество баллов | № | Оцениваемый параметр | Количество баллов | № | Оцениваемый параметр | Количество баллов |
| 1 | - Осуществить подключениеь контроллера карточного доступа | | 1 | 1 | - Произвести Подключение АПМДЗ | 1 | 1 | - Настройка «Политики и Регистрации событий» | 1 |
| 2 | - Осуществить подключение контроллера кодового доступа | | 1 | 2 | - Произвести подключение блокировки по Reset | 1 | 2 | - Настроить доступ к пользователю «adminsns» по идентификатору Рутокен | 1 |
| 3 | - Создать базу данных работников предприятия согласно параметрам разрешенного доступа в подразделения «Офис» и «Склад» | | 1 | 3 | - Произвести инициализацию устройства, настроить общие параметры | 1 | 3 | - Установить и настроить Рутокен | 1 |
| 4 | - Создать отделы и настроить графики работы | | 1 | 4 | - Создать первичного администратора, произвести первичную смену пароля | 1 | 4 | - Настроить параметры входа в систему | 1 |
| 5 | - Вывести по ним отчет по работникам | | 1 | 5 | - Произвести настройку контроля целостности, поставить на контроль файл | 1 | 5 | - Провести проверочные мероприятия выполненных настроек | 1 |
| 6 | - Настроить систему пожарной сигнализации | | 1 | 6 | произвести настройку комплекса в режиме Администратора  - создать Администратора и пользователей  - настроить общие параметры | 1 | 6 | - Произвести экспорт журнала | 1 |
| 7 | - Заблокировать доступ в праздничные и выходные дни | | 1 | 7 | - Произвести вход пользователем | 1 | 7 | - Присвоить права администратора и скрыть пользователя с экрана приветствия | 1 |
| 8 | - Заблокировать доступ в связи с командировкой | | 1 | 8 | - Заблокировать пользователя неправильным входом | 1 | 8 | - Настроить контроль целостности | 1 |
| 9 | - Настроить показ уведомлений при проходе работников на предприятии. | | 1 | 9 | - Разблокировать пользователя | 1 | 9 | - Произвести проверку нарушения режима контроля целостности | 1 |
| 10 | - Вывести отчет о обработке данных | | 1 | 10 | - Вывести отчет журнала событий | 1 | 10 | - Выполнить аудит системы | 1 |

**ОЦЕНОЧНЫЕ СРЕДСТВА**

**Тестовые задания**

1. **ИТ в профессиональной деятельности**

**Как называется программное или аппаратное обеспечение, которое препятствует несанкционированному доступу на компьютер?**

а. Сервер

б. Браузер

в. Брандмауэр

г. Архиватор

**World Wide Web – это служба Интернет, предназначенная для:**

а. Поиска и просмотра гипертекстовых документов, включающих в себя графику, звук и видео

б. Передачи файлов

в. Передачи электронных сообщений

г. Общения в реальном времени с помощью клавиатуры

**Какой из перечисленных ниже адресов является поисковой системой?**

а. http://www.letitbit.net

б. http://www.vk.com

в. http://www.narod.yandex.ru

г. http://www.google.ru

**Определите название сети, если компьютеры одной организации, связанные каналами передачи информации для совместного использования общих ресурсов и периферийных устройств и находятся в одном здании:**

а. Региональной

б. Территориальной

в. Локальной

г. Глобальной

**Назовите функции информационно-поисковой системы:**

а. Осуществлять поиск, вывод и сортировку данных

б. Осуществлять поиск и сортировку данных

в. Редактировать данные и осуществлять их поиск

г. Редактировать и сортировать данные

**Укажите, что обеспечивает система электронного документооборота:**

а. Массовый ввод бумажных документов

б. Управление электронными документами

в. Управление знаниями

г. Автоматизацию деловых процессов

**Независимость информации от чьего-то мнения определяет свойство - это..**

а. Обьективность

б. Актуальность

в. Достоверность

г. Полнота

**Выберите меры защиты, относящиеся к нормам поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе.**

а. Правовые (законодательные)

б. Организационные (административные и процедурные)

в. Технологические

г. Морально-этические

**Укажите назначение папки «Заметки»:**

а. Планирование личного расписания, встреч, событий и собраний

б. Информация о личных и деловых контактах

в. Планирование, ведение и учет задач

г. Создание различных примечаний

**Введение разделов в текстовый документ служит:**

а. Для изменения разметки документа на одной странице или на разных страницах

б. Для изменения разметки документа только на одной странице

в. Только для изменения порядка нумерации страниц документа

г. Для лучшей «читаемости» документа

**Типы данных в электронных таблицах MS Excel – это…**

а. Текст, число и формула

б. Текст и число

в. Константы, формулы и ошибки

г. Число и формула

**Медицинская автоматизированная информационная система – это…**

а. Совокупность программно-технических средств

б. Совокупность программно-технических средств, используемых в лечебно-профилактическом учреждении

в. База данных

г. Медицинская программа

**Автоматизированное рабочее место медицинского работника – это…**

а. Рабочее место, предназначенное для информационной поддержки

б. Рабочее место

в. Рабочее место, оснащенное средствами вычислительной техники для выполняемых профессиональных задач

г. Рабочее место, оборудованное программными средствами

**Какой из следующих пунктов лучше всего описывает ядро безопасности?**

1. программный компонент, который определяет, имеет ли пользователь право выполнять запрошенную операцию
2. программный компонент, который отслеживает действия и записывает информацию о событиях безопасности в журнал регистрации событий
3. программный компонент, который изолирует процессы, разделяет защищенный и реальный режимы
4. программный компонент, который работает в самом центре колец защиты и обеспечивает интерфейсы между доверенными и недоверенными объектами

**Что из перечисленного ниже входит в состав ядра безопасности?**

1. программное обеспечение, аппаратное обеспечение и прошивки
2. политика безопасности, защитные механизмы и структура системы
3. политика безопасности, механизмы защиты и программное обеспечение
4. программное обеспечение, аппаратное обеспечение и структура системы

**Операционная система выполняет все, за исключением какой из перечисленных ниже задач?**

1. задачи ввода/вывода
2. распределение памяти
3. доступ пользователей к представлениям базы данных
4. распределение ресурсов

**Что подразумевается, когда говорят, что компьютеры взаимодействуют друг с другом физически и логически?**

1. они взаимодействуют физически при подключении к магистральной сети, а логически – при взаимодействии в рамках одной локальной сети (LAN)
2. они взаимодействуют физически с помощью заголовков и окончаний, а логически – посредством физических соединений
3. они взаимодействуют физически через PVC, а логически – через SVC
4. они взаимодействуют физически с помощью электронов и сетевых кабелей, а логически – посредством различных уровней модели OSI

**Как называется программное или аппаратное обеспечение, которое препятствует несанкционированному доступу на компьютер?**

1. Сервер
2. Браузер
3. Брандмауэр
4. Архиватор

**World Wide Web – это служба Интернет, предназначенная для:**

1. Поиска и просмотра гипертекстовых документов, включающих в себя графику, звук и видео
2. Передачи файлов
3. Передачи электронных сообщений
4. Общения в реальном времени с помощью клавиатуры

**Иден­ти­фи­ка­тор не­ко­то­ро­го ре­сур­са сети Ин­тер­нет имеет сле­ду­ю­щий вид: http://www.olimpiada-profmast.ru/. Какая часть этого иден­ти­фи­ка­то­ра ука­зы­ва­ет на про­то­кол, ис­поль­зу­е­мый для пе­ре­да­чи ре­сур­са?**

1. www
2. olimpiada-profmast
3. http
4. ru

**Выберите правильный вариант записи ip - адреса:**

1. 198.165.2,5.3
2. 198.02.03
3. 198.256.02.02
4. 198.021.1-3

**В табличном процессоре Excel диапазон ячеек выглядит следующим образом:**

1. A1:B1
2. A1/B1
3. A1+B1
4. A1-B1

**Криптографические методы защиты информации предполагают:**

1. Использование алгоритмов шифрования
2. Установление специальных атрибутов файлов
3. Автоматическое дублирование данных на двух автономных носителях
4. Установление паролей на доступ к информации

**Проверка полномочий пользователя при его обращении к данным называется:**

1. Контролем доступа
2. Аутентификацией
3. Обеспечением целостности данных
4. Шифрованием

**Определите название сети, если компьютеры одной организации, связанные каналами передачи информации для совместного использования общих ресурсов и периферийных устройств и находятся в одном здании:**

1. Региональной
2. Территориальной
3. Локальной
4. Глобальной

**Региональная вычислительная сеть – это…**

1. Коммуникационная система, объединяющая абонентов, расположенных в различных странах
2. Коммуникационная система, которая связывает абонентов, расположенных на значительном расстоянии друг от друга
3. Коммуникационная система, которая объединяет абонентов, расположенных в пределах небольшой территории
4. Совокупность нескольких видов компьютерных сетей

**Сеть, в которой объединены компьютеры в различных странах, на различных континентах – это…**

1. Глобальная сеть
2. Локальная сеть
3. Региональная сеть
4. Вычислительная сеть

**Укажите, что обеспечивает система электронного документооборота:**

1. Массовый ввод бумажных документов
2. Управление электронными документами
3. Управление знаниями
4. Автоматизацию деловых процессов

**Что означает аббревиатура АСУ?**

1. Человеко-машинные система, в которых задача ПК состоит в предоставлении человеку необходимой информации для принятия решения
2. Информационные системы, основное назначение которых обработка и архивация больших объемов данных
3. Система управления устройствами, производственными установками, технологическими процессами, функционирующие без участия человека
4. Информационные системы автоматизированного создания эскизов, чертежей, схем

**Выберите меры защиты, относящиеся к нормам поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе.**

1. Правовые (законодательные)
2. Организационные (административные и процедурные)
3. Технологические
4. Морально-этические

**С помощью какой пиктограммы можно запустить программу MS Access?**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | Описание: http://i.ehow.com/images/a04/kj/pa/protect-ms-access-database-800X800.jpg | Описание: http://s1.iconbird.com/ico/2013/9/446/w512h5121380376652MetroUIMSOffice.png | Описание: https://www.shareicon.net/data/2015/12/12/205301_excel_300x300.png | Описание: http://studok.net/pictures/books/173800959.files/2012-07-29_5014fefdd10f2.jpg | |

**Какая из перечисленных ниже программ предназначена для создания буклетов, визиток?**

1. Microsoft Office Publisher
2. Microsoft Office Word
3. Microsoft Office Access
4. Microsoft Office Excel

**Какой кнопкой или их сочетанием прекратить показ слайдов и вернуться в режим редактирования в программе Microsoft PowerPoint?**

1. Tab
2. Alt + Shift
3. Enter
4. Esc

**Минимальным объект, используемый в растровом графическом редакторе, называется \_\_\_\_\_\_\_\_\_\_\_\_**

**В электронных таблицах выделена группа ячеек A1:В3. В эту группу входит \_\_ ячеек. Ответ запишите цифрой.**

**\_\_\_\_\_\_\_\_\_\_\_\_ редактор – это программа, предназначена для создания, редактирования и форматирования текстовой информации.**

**\_\_\_\_\_\_\_\_\_\_\_\_ – графический редактор, предназначенный для создания и редактирования изображений.**

**MODEM – это устройство для \_\_\_\_\_\_\_\_\_\_\_\_ информации.**

**Программа для просмотра WEB-страниц называется \_\_\_\_\_\_\_\_\_\_\_\_.**

**Единицей обмена физического уровня сети является \_\_\_\_\_\_\_\_\_\_\_\_.**

**В электронной таблице выделена группа ячеек А1:С2. Определите сколько ячеек входит в эту группу. Запишите ответ: \_\_\_\_\_\_\_\_\_\_\_\_.**

**Основными функциями текстовых редакторов являются: редактирование текста, \_\_\_\_\_\_\_\_\_\_\_\_ текста, вывод текста на печать.**

**Определенное количество информации, имеющее имя и хранящееся во внешней памяти на компьютере – это\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

**С какого знака начинается запись формулы в Excel (введите знак): \_\_\_\_\_\_\_\_\_\_\_\_.**

**Петабайт (Пбайт) равен \_\_\_\_\_\_\_\_\_\_\_\_терабайтам (Тбайт).**

**В документе MS Word текст, расположенный между двумя символами ¶ называется \_\_\_\_\_\_\_\_\_\_\_\_.**

**В Microsoft PowerPoint 2013 стандартным расширением файла, содержащего обычную презентацию, является \_\_\_\_\_\_\_\_\_\_\_\_.**

**Основным элементом электронной таблицы MS Excel 2013 является \_\_\_\_\_\_\_\_\_\_\_\_.**

**\_\_\_\_\_\_\_\_\_\_\_\_ - устройство для автоматического считывания с бумажных носителей и ввода в компьютер машинописных текстов, графиков, рисунков, чертежей.**

**Диапазон А1:В5 содержит \_\_\_ ячеек. (Ответ записывается в числовой форме, например, 30 или 5)**

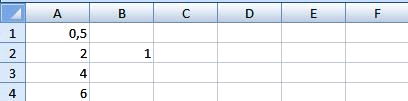
**Сетевая топология, при которой к одному центральному компьютеру присоединяются другие периферийные компьютеры, причем каждый из них использует свою отдельную линию связи, называется \_\_\_\_\_\_\_\_\_\_\_\_.**

**Сетевая топология, при которой каждый компьютер передает информацию всегда только одному компьютеру, следующему в цепочке, а получает информацию только от предыдущего компьютера в цепочке, и эта цепочка замкнута в круг, называется \_\_\_\_\_\_\_**

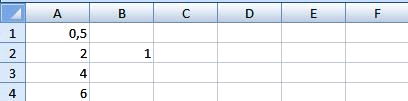
**Единицей обмена физического уровня сети является \_\_\_\_\_\_\_\_\_\_\_\_.**

**Протокол IP сети используется на \_\_\_\_\_\_\_\_\_\_\_\_ уровне модели OSI.**

**Дан фрагмент электронной таблицы. Содержимое ячейки В2 рассчитано по формуле =$А$1\*A2. Запишите, как будет выглядеть формула, если ее скопировать в нижестоящую ячейку В3?** Запишите ответ: \_\_\_\_\_\_\_\_\_\_\_\_



**Дан фрагмент электронной таблицы. В ней содержимое ячейки В2 рассчитано по формуле =$А$1\*A2. Формула скопирована из ячейки В2 в ячейку В3. Каков результат вычисления значения в ячейке В3?** Запишите ответ: \_\_\_\_\_\_\_\_\_\_\_\_



**\_\_\_\_\_\_\_\_\_\_\_\_ редактор – это программа, предназначена для создания, редактирования   
и форматирования текстовой информации.**

**\_\_\_\_\_\_\_\_\_\_\_\_ – графический редактор, предназначенный для создания и редактирования изображений**.

**Установите соответствие между программой и ее функцией:**

|  |  |
| --- | --- |
| 1. Создание презентаций | 1. Microsoft Word |
| 1. Текстовый редактор | 1. Microsoft Excel |
| 1. Создание публикаций | 1. Microsoft PowerPoint |
| 1. Редактор электронных таблиц | 1. Microsoft Publisher |

**Установите соответствие категорий программ и их описаний:**

|  |  |
| --- | --- |
| 1. Системные программы | 1. Обеспечивают создание новых компьютерных программ |
| 1. Прикладные программы | 1. Позволяют проводить простейшие расчеты и выбор готовых конструктивных элементов из обширных баз данных |
| 1. Инструментальные системы | 1. Организуют работу ПК выполняют вспомогательные функции |
| 1. Системы автоматизированного проектирования (CAD-системы) | 1. Обеспечивают редактирование текстов, создание рисунков и т.д. |

**Установите соответствие между комбинацией клавиш на клавиатуре и выполняемым действием:**

|  |  |
| --- | --- |
| 1. Сохранить документ | 1. Ctrl+Esc |
| 1. Закрыть активное окно | 1. Ctrl+S |
| 1. Открыть меню «Пуск» | 1. Ctrl+C |
| 1. Скопировать объект | 1. Alt+F4 |

**Установите соответствие между названиями клавиш и их функциями:**

|  |  |
| --- | --- |
| 1. F1 | 1. Удаляет символ справа от курсора |
| 1. Backspace | 1. Переключает режим дополнительной |
| 1. Delete | 1. Цифровой клавиатуры |
| 1. Num Lock | 1. Фиксирует верхний регистр алфавитной |
| 1. Caps Lock | 1. Клавиатуры |

**Определите соответствие между расширением файла и его содержанием:**

|  |  |
| --- | --- |
| 1. .exe | 1. Изображение |
| 1. .jpg | 1. Текст |
| 1. .doc | 1. Музыка |
| 1. .mp3 | 1. Программа |

**Установите соответствие типов файлов и обозначением расширений файлов:**

|  |  |
| --- | --- |
| 1. lett.doc | 1. Исполняемый файл |
| 1. lett.exe | 1. Графический файл |
| 1. lett.xls | 1. Текстовый документ |
| 1. lett.bmp | 1. Документ MS Word |
| 1. lett.txt | 1. Документ MS Excel |

**Укажите соответствие логотипа для всех 4 вариантов изображений:**

|  |  |
| --- | --- |
| 1. Описание: Описание: https://arhivurokov.ru/kopilka/uploads/user_file_5474c7ce6d836/diffierientsial-nyi-zachiet-informatsionnyie-tiekhnologhii-v-profiessional-noi-dieiatiel-nosti_1.png | 1. Microsoft PowerPoint |
| 1. Описание: Описание: https://arhivurokov.ru/kopilka/uploads/user_file_5474c7ce6d836/diffierientsial-nyi-zachiet-informatsionnyie-tiekhnologhii-v-profiessional-noi-dieiatiel-nosti_2.png | 1. Microsoft Word |
| 1. Описание: Описание: https://arhivurokov.ru/kopilka/uploads/user_file_5474c7ce6d836/diffierientsial-nyi-zachiet-informatsionnyie-tiekhnologhii-v-profiessional-noi-dieiatiel-nosti_3.png | 1. Microsoft Access |
| 1. Описание: Описание: https://arhivurokov.ru/kopilka/uploads/user_file_5474c7ce6d836/diffierientsial-nyi-zachiet-informatsionnyie-tiekhnologhii-v-profiessional-noi-dieiatiel-nosti_4.png | 1. Microsoft Excel |

**Установите изображения элементов блок-схемы с их назначением:**

|  |  |
| --- | --- |
| 1. Условие |  |
| 1. Начало/конец алгоритма |  |
| 1. Процесс |  |
| 1. Ввод/вывод данных |  |

**Укажите последовательность создания нумерации страниц в текстовом редакторе MS Word:**

1. Указать положение и выравнивание символа номера страницы
2. Нажать 
3. Выбрать команду «Номер страницы»
4. Открыть меню «Вставка»

**Укажите в правильной последовательности действия при создании папки на Рабочем столе**:

1. Щёлкнуть правой клавишей мыши
2. Ввести имя папки в поле ввода подписи
3. Выбрать команду создать – папка

**Расположите в правильной последовательности основные этапы разработки базы данных:**

1. Определение последовательности выполнения задач
2. Уточнение решаемых задач
3. Определение структуры данных
4. Анализ данных

**Установите последовательность этапов процесса создания базы данных:**

1. Определение связей между таблицами.
2. Усовершенствование структуры базы данных
3. Определение необходимых в таблице полей.
4. Ввод данных и создание других объектов базы данных.
5. Определение полей с уникальными значениями в каждой записи.
6. Определение цели создания базы данных
7. Определение таблиц, которые должна содержать база данных

**Укажите правильную последовательность поколений ЭВМ:**

1. Микропроцессорные ЭВМ
2. Ламповые ЭВМ
3. ЭВМ на интегральных схемах
4. Транзисторные ЭВМ

**Установите в хронологической последовательности этапы развития информационных технологий:**

1. «Электронная» технология
2. «Механическая» технология
3. «Ручная» технология
4. «Компьютерная» технология
5. «Электрическая» технология

**Установите единицы измерения объема информации по возрастанию:**

1. Бит
2. Мегабит
3. Мегабайт
4. Килобайт

**Мера цифровой информации в порядке увеличения:**

1. 1Терабайт
2. 100Гигабайт
3. 100Килобайт
4. 1Мегабайт

**Укажите последовательную цепочку элементов, образующую URL-адрес информационного ресурса:**

1. Имя каталога, в котором содержится нужный файл
2. Адрес сервера
3. Протокол
4. Имя файла

**Укажите последовательную цепочку элементов, образующую адрес электронной почты:**

1. Имя пользователя
2. Символ @
3. Домен
4. Имя почтового сервера.

**Укажите в порядке возрастания объемы памяти:**

1. 20 бит
2. 10 бит
3. 2 байта
4. 1010 байт
5. 1 Кбайт

**Расположите в иерархическом порядке уровни памяти:**

1. Внешняя память (ВЗУ)
2. Основная память (ОП)
3. Регистровая кэш-память
4. Микропроцессорная память (МПП)

**Установите последовательность этапов моделирования:**

|  |
| --- |
| 1. Постановка задачи 2. Анализ результатов моделирования 3. Разработка модели 4. Компьютерный эксперимент |

**Укажите последовательность установки формата чертежа:**

1. Чертеж
2. Файл
3. Сервис
4. Создать
5. Формат
6. Параметры листа
7. Параметры
8. Текущий чертеж
9. Ок

**Установите правильную последовательность действий для вычисления данных по формуле в MS Excel:**

1. Нажать кнопку «Enter»
2. Выделить ячейку
3. Ввести формулу
4. Ввести знак =

**Установите правильную последовательность при создании диаграммы в MS Excel:**

1. выбрать вкладку «вставка»
2. создать таблицу с исходными данными
3. выбрать тип диаграммы
4. выделить диапазон ячеек таблицы

**Укажите последовательность этапов построения диаграммы в MS Excel с помощью мастера**

1. Выбор типа диаграммы
2. Настройки заголовков, осей, линии сетки, легенды, подписей и таблицы данных
3. Выбор расположения диаграммы
4. Выбор или уточнение источника данных

**Расставьте по порядку основные этапы подготовки текстового документа на компьютере:**

е

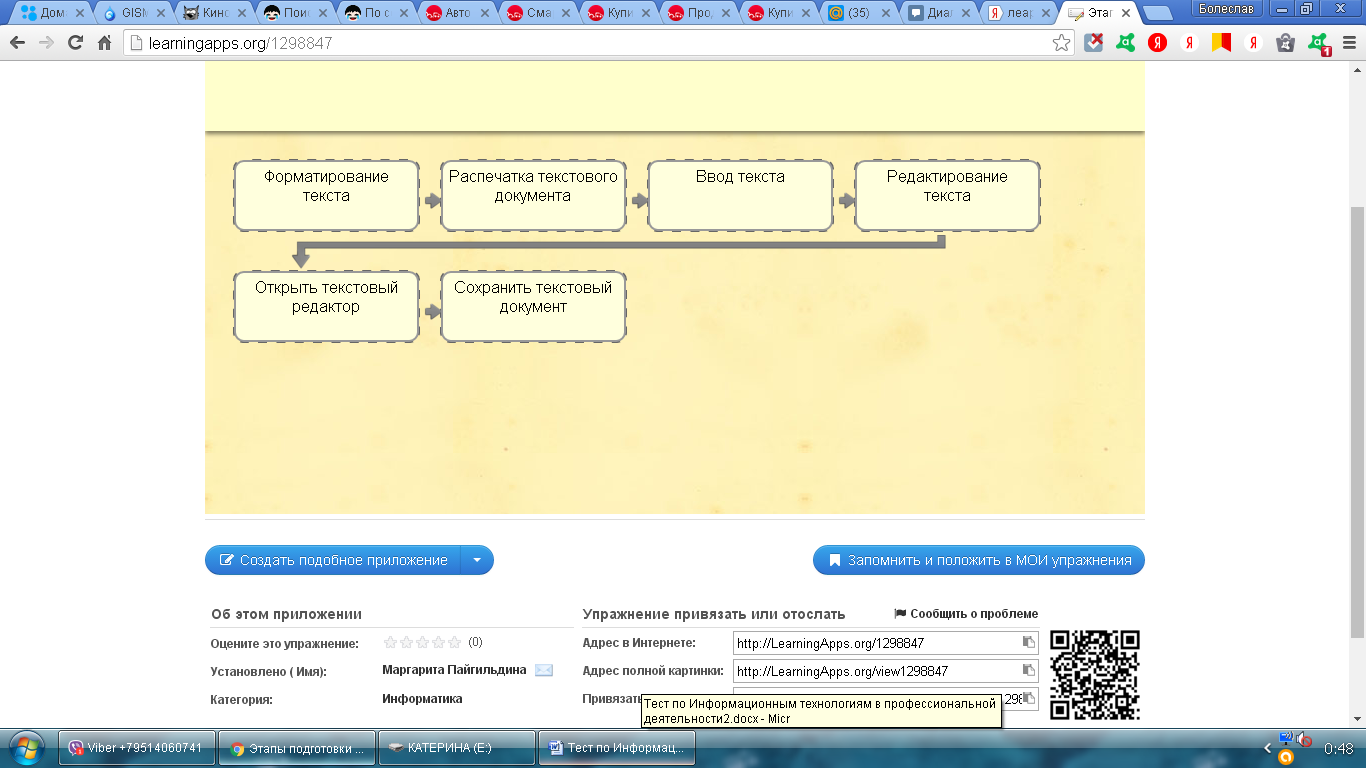
д

г

в

б

а



**2. Оборудование, материалы, инструменты**

**Ограждения сеткой относятся к …….. способам защиты:**

1. предупредительным
2. основным
3. дополнительным
4. заградительным

**Вибрационные и ударноконтактные извещатели относятся к…**

1. инфракрасным извещателям
2. ультразвуковым извещателям
3. барометрическим извещателям
4. радиоволновым извещателям
5. акустическим извещателям
6. инерционным извещателям
7. пьезоэлектрическим извещателям
8. сейсмическим извещателям

**Оптико-электронный извещатель предназначен для:**

1. обнаружения проникновения через двери и окна
2. обнаружения разбития окон
3. обнаружения источника ИК излучения
4. обнаружения возникновения задымления

**Электронный ключ Touch memory использует для хранения идентификатора:**

1. полупроводниковые элементы электронного носителя ПЗУ
2. магнитные носители
3. химико-физические свойства оптического носителя
4. полупроводниковые элементы электронного носителя ОЗУ

**Принцип обеспечения безопасности аппаратно-программного модуля доверенной загрузки:**

1. перехватывает работу компьютера прерывая загрузку BIOS, загружает CriptoBIOS и идентифицирует пользователя по ключу и паролю, после чего продолжает загрузку компьютера.
2. перехватывает работу компьютера до загрузки BIOS, загружает CriptoBIOS и идентифицирует пользователя по ключу и паролю, после чего продолжает загрузку компьютера.
3. перехватывает работу компьютера после загрузки BIOS, загружает CriptoBIOS и идентифицирует пользователя по ключу и паролю, после чего продолжает загрузку компьютера.
4. перехватывает работу компьютера прерывая загрузку ОС, загружает CriptoBIOS и идентифицирует пользователя по ключу и паролю, после чего продолжает загрузку компьютера.

**К средствам обеспечения защиты информации по акустическому каналу утечки информации относится:**

1. шумомер
2. тепловизор
3. сканер частот
4. детектор излучений

**К средствам обеспечения защиты информации по радиоэлектронному каналу утечки информации относится:**

1. шумомер
2. тепловизор
3. мультиметр
4. детектор излучений

**Звукоизоляция и экранирование помещений и технических средств обработки информации относится…**

1. к пассивным методам защиты
2. к активным методам защиты

**Системы электропитания, системы заземления относятся к…..**

1. средствам обеспечения ОИ (ОТСС)
2. средства обеспечения ОИ (ВТСС)

**Укажите средства, не требующие физического проникновения в защищаемые помещения:**

1. стетоскопы и лазерные микрофоны
2. проводниковые и лазерные микрофоны
3. закладки с передачей по сети 220 В
4. радиозакладки и направленные микрофоны

**В IBM BIOS повторяющийся короткий сигнал означает:**

1. неисправна клавиатура
2. неисправна видеосистема
3. неисправен блок питания
4. неисправна материнская плата

**Северный мост – это?**

1. контроллер-концентратор ввода-вывода
2. микросхема, отвечающая за возможность последовательной обработки запросов на прерывание от разных устройств
3. параллельный интерфейс подключения накопителей
4. контроллер-концентратор памяти

**Что такое интерфейс RS-232C?**

1. интерфейс обмена данными по последовательному коммуникационному порту СОМ
2. стандарт параллельного интерфейса для подключения периферийных устройств персонального компьютера
3. последовательная версия SCSI
4. интерфейс, предназначенный исключительно для подключения видеоадаптеров

**Какого интерфейса винчестеров не существует:**

1. IDE
2. SCSI
3. SASS
4. ESDI

**Какого уровня напряжения нет в блоке питания AT?**

1. 5 В
2. 3,3В
3. 12В
4. -12В
5. -5В

**Какое напряжение питания используется на шине PCI?**

1. 7В
2. 3.3В
3. 5,3В
4. 12В
5. -3.3В

**Накопитель использующий магнитную запись – это..**

а. HDD

б. SSD

в. DVD

г. CD

**Видеокарты, интегрированные в набор системной логики материнской платы, не имеют собственной видеопамяти и используют:**

1. часть постоянной памяти компьютера
2. часть памяти винчестера
3. часть оперативной памяти компьютера
4. часть кэш - памяти процессора

**\_\_\_\_\_\_\_\_\_\_\_\_\_ – процесс, осуществляемый с применением оптико-электронных устройств, предназначенных для визуального контроля или автоматического анализа изображений.**

**\_\_\_\_\_\_\_\_\_\_\_– это одно из устройств защитного плана, основной функцией которого является защита находящегося в помещении информационного объекта (устройства) от утечки информации через различные подслушивающие или улавливающие устройства (радиомикрофоны, цифровые и пленочные диктофоны, стетоскопы и т.д.) без вмешательства в процесс его эксплуатации.**

**\_\_\_\_\_\_ \_\_\_\_\_\_\_ – настольная микро-ЭВМ, имеющая эксплуатационные характеристики бытового прибора и универсальные функциональные возможности.**

**Специальная управляющая программа обычно поставляются в комплекте с устройством и предназначена для взаимодействия с операционной системой – это \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_– процессор (устройство, отвечающее за выполнение арифметических, логических операций и операций управления, записанных в машинном коде), реализованный в виде одной микросхемы или комплекта из нескольких специализированных микросхем**

**Установите соответствие между средствами ведения акустической разведки и их описанием:**

|  |  |
| --- | --- |
| * 1. трубчатые микрофоны органного типа | 1. приборы, преобразующие звуковые колебания в радиоволны для передачи информации на расстоянии посредством приёмо-передающих устройств |
| * 1. стетоскоп | 1. автономная группа из нескольких собранных в пучок открытых трубок разной длины, но одного диаметра, малого по сравнению с длиной любой из трубок этой группы; |
| * 1. радиомикрофоны | 1. приборы для регистрации микроколебаний ограждающих конструкций и инженерных коммуникаций возникающих при разговоре в помещении. |

**Установите соответствие между видами микрофонов и их описанием:**

|  |  |
| --- | --- |
| 1. трубчатые микрофоны органного типа | 1. несколько микрофонов, обычно располагаемых в ряд по прямой горизонтальной линии так, чтобы их оси были параллельны друг другу |
| 1. микрофонная решетка | 1. автономная группа из нескольких собранных в пучок открытых трубок разной длины, но одного диаметра, малого по сравнению с длиной любой из трубок этой группы; |
| 1. групповые микрофоны | 1. группа датчиков акустического давления, расположенных, как правило, в одной плоскости в шахматном или ином порядке |

**Установите соответствие между средствами защиты и их конкретными примерами :**

|  |  |
| --- | --- |
| 1. физические средства | 1. специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности |
| 1. аппаратные средства | 1. замки на дверях, решетки на ок­нах |
| 1. программные средства защиты | 1. ведение системного журнала |

**Установите соответствие компонента и его назначения:**

|  |  |
| --- | --- |
| 1. Монитор | а.Вывод информации |
| 2.Клавиатура | б.Обработка графической информации |
| 3.Видеокарта | в.Ввод информации |
| 4.Процессор | г.Арифметико-логическое вычисление |

**Установите соответствие между средствами защиты и их описанием:**

|  |  |
| --- | --- |
| 1. организационные средства защиты | 1. нормативно-правовые документы, регламентирующие порядок разработки, внедрения и эксплуатации ИС |
| 1. законодательные средства защиты | 1. регламентация производственной деятельности и использования компьютеров в сети |
| 1. морально-этические средства защиты | 1. всевозможные нормы по­ведения, которые традиционно сложились ранее, складываются по мере распространения информационных технологий в стране и в мире или специально разрабатываются |

**Установите соответствие между видом оборудования и его изображением:**

|  |  |
| --- | --- |
| 1. Роторная полуростовая вертушка |  |
| 1. Турникет типа «метро» |  |
| 1. Роторная понопрофильная вертушка |  |
| 1. Калитка |  |
| 1. Трипод |  |

**Установите соответствие между видом оборудования и его изображением:**

|  |  |
| --- | --- |
| 1. Карточка со штрихом |  |
| 1. Проксимити |  |
| 1. Перфорированная карточка |  |
| 1. PIN-код |  |
| 1. Электронная таблетка |  |
| 1. Смарт-карта |  |

**Установить соответствие между видом оборудования и его изображением:**

|  |  |
| --- | --- |
| 1. Сетевые контроллеры |  |
| 1. Радиочастотные считыватели и передатчики |  |
| 1. Биометрический считыватель |  |
| 1. Автономные однодверные контроллеры уличного и внутреннего исполнения |  |
| 1. PIN-клавиатуры и Proximity считыватели уличного и внутреннего исполнения |  |

**Установите правильную последовательность действий, раскрывающую принцип действия лазерной системы контроля оконных стёкол:**

1. когерентное лазерное излучение от стандартного источника направляется в сторону окна контролируемого помещения;
2. отраженное (по законам геометрической оптики) от внутреннего стекла часть излучения и попадает в приемник;
3. отраженное (по законам геометрической оптики) от внутреннего стекла часть излучения «возвращается» в направлении контрольного пункта.

**Установите правильную последовательность действий, раскрывающую принцип действия направленного микрофона с параболическим отражателем:**

1. возникает усиление звукового поля;
2. звуковые волны собираются в фокусе параболического рефлектора, складываясь в фазе;
3. звуковое поле передается на дополнительный внешний усилитель.
4. звуковые волны с осевого направления отражаются от параболического рефлектора.

**Установите правильный порядок, подключения оборудования:**

1. Подключение оборудования
2. Подготовка оборудования
3. Установка драйверов
4. Работа с оборудованием

**Установите правильный порядок, сборки компьютера:**

1. Подключение периферии
2. Установка материнской платы
3. Установка видеокарты
4. Включение компьютера
5. Настройка компьютера

**3.Системы качества, стандартизации и сертификации**

**Укажите международную организацию, занимающейся выпуском стандартов**

1. ISO
2. IEC
3. EAC
4. CEN

**Аккредитация – это…**

1. Официальное признание в том, что испытательная лаборатория правомочна проводить конкретные испытания
2. Документ, который орган по сертификации наделяет орган правом использовать знаки соответствия своей продукции
3. Процесс, устанавливающий правила определения результатов испытаний
4. Документ, устанавливающий руководящие принципы, характеристики различных видов деятельности

**Что является заключительным этапом жизненного цикла процесса разработки системы?**

1. аккредитация
2. сертификация
3. тестирование модулей
4. разработка

**Управление качеством – это часть системы менеджмента качества, направленная на …**

1. Создание уверенности в должном качестве объекта (продукции, процесса, системы)
2. Выполнение требований к качеству
3. Отслеживание конкретных результатов деятельности
4. Установление целей в области качества

**Стандартизация - это:**

1. Документ, принятый органами власти
2. Совокупность взаимосвязанных стандартов
3. Деятельность по установлению норм, требований, характеристик
4. Документ, в котором устанавливаются характеристики продукции

**Разность между значением величины, полученным в процессе измерений, и настоящим (действительным) значением данной величины – это …**

1. Относительная погрешность
2. Абсолютная погрешность
3. Приведенная погрешность
4. Динамическая погрешность

**Подтверждениями соответствия являются:**

1. Сертификация и декларация продукции
2. Сертификат и декларация соответствия
3. Знак соответствия
4. Сертификат и декларация и знак соответствия

**Укажите номер картинки, на которой изображен знак соответствия в системе ГОСТ Р**

|  |  |  |  |
| --- | --- | --- | --- |
| Описание: Описание: Картинка 4 из 22140 | Описание: Описание: Картинка 19 из 4108 | Описание: Описание: Картинка 13 из 4714 | Описание: Описание: http://www.sv-nn.ru/f/attach/58/5850-0824182359.jpg |
| а. | б. | в. | г. |

**Каков максимальный срок действия сертификата на продукцию?**

1. 2 года
2. 3 года
3. 4 года
4. 5 лет

**Объектом стандартизации не является:**

1. Продукция
2. Услуга
3. Процесс
4. Транспорт

**Политика безопасности строится на основе…**

1. анализа рисков, признанных реальными для данной организации
2. стратегии управления защиты
3. программы действий, реализация которых обеспечит информационную безопасность;
4. финансовых данных

**Политика безопасности оформляется…**

1. в виде документа, включающего описание проблемы, область применения, позицию организации, распределение ролей, санкции
2. в виде приказа о назначении ответственных лиц
3. в виде отчета обо всех действиях пользователей;
4. в виде инструкции по действию сотрудников в критических ситуациях

**Предназначение стандартов информационной безопасности**:

1. оценка уровня безопасности, обеспечиваемый продуктами ИТ
2. создание основы для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов ИТ
3. средство сравнения конкретных продуктов ИТ
4. практического решения вопросов управления информационной безопасностью

**Лицензирование это – …**

1. подтверждение соответствия продукции или услуг установленным требованиям и стандартам
2. процесс передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ
3. подтверждение подлинности отправителя и получателя информации
4. средство защиты информации от несанкционированного доступа

**Сертификация …**

1. основывается на Законе РФ "О государственной тайне"
2. регулируется секретными нормативными документами
3. это подтверждение соответствия продукции или услуг установленным требованиям или стандартам
4. осуществляется в соответствии с остальными пунктам

**Форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров, называется \_\_\_\_\_\_\_\_\_\_\_\_.**

**Степень соответствия присущих характеристик требованиям – это\_\_\_\_\_\_\_\_\_\_\_.**

**Документ, устанавливающий правила, руководящие принципы или характеристики различных видов деятельности или их результатов, называется \_\_\_\_\_\_\_\_\_\_\_\_.**

**\_\_\_\_\_\_\_\_\_\_\_\_ - это международная организация, сфера деятельности которой охватывает стандартизацию во всех областях, за исключением электроники и электротехники.**

**\_\_\_\_\_\_\_\_\_\_\_\_ - это совокупность свойств продукции, обусловливающих ее пригодность удовлетворять определенные потребности в соответствии с назначением.**

**Запишите в строке ответа аббревиатуру, обозначающую термин «Статистический менеджмент качества» \_\_\_\_\_\_\_\_\_\_\_\_.**

**Документом, регулирующим единство измерений в РФ, является \_\_\_\_\_\_\_\_\_\_\_\_.**

**Главным метрологическим органом РФ, который имеет исключительное право официального опубликования ГОСТов и ОКС, является \_\_\_\_\_\_\_\_\_\_\_\_.**

**Специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю, это - \_\_\_\_\_\_\_\_\_\_\_\_.**

**Отклонение результатов измерений от истинного (действительного) значения называется \_\_\_\_\_\_\_\_\_.**

**Установите соответствие между цифровыми обозначениями международных стандартов и их названиями:**

|  |  |
| --- | --- |
| 1. Управление качеством | 1. 14000 |
| 1. Экологический менеджмент | 1. 26000 |
| 1. Социальная ответственность | 1. 50001 |
| 1. Энергетический менеджмент | 1. 9000 |

**Установите соответствие между знаками и их названиями:**

|  |  |
| --- | --- |
| 1. Описание: Знак_соответствия.svg.png | 1. Знак обращения на рынке Российской Федерации |
| 1. Описание: EAC-black-on-white.gif | 1. Знак соответствия при обязательной сертификации в Российской Федерации |
| 1. Описание: 280px-Conformité_Européenne_(logo).svg.png | 1. Знак соответствия техническим регламентам Таможенного Союза ЕврАзЭС |
| 1. Описание: 6187754_Preview.jpg | 1. Знак соответствия требованиям директив стран Европейского Союза |

**Установите соответствие между названиями приставок для кратных единиц системы СИ и значениями их десятичных множителей:**

|  |  |
| --- | --- |
| 1. Гига | 1. 1012 |
| 1. Пета | 1. 109 |
| 1. Тера | 1. 1018 |
| 1. Экса | 1. 1015 |

**Установить соответствие между эталонами и их назначением:**

|  |  |
| --- | --- |
| 1. Рабочий эталон | 1. Предназначен для проверки сохранности государственного эталона и для замены его в случае порчи или утраты |
| 1. Эталон-копия | 1. Применяется для проверки сохранности государственного эталона или для его замены в случае порчи или утраты |
| 1. Эталон-свидетель | 1. Предназначен для передачи размеров единиц рабочим эталонам |
| 1. Эталон сравнения | 1. Применяется для передачи размера единицы образцовым средствам измерения высшей точности |

**Установите соответствие между термином и определением:**

|  |  |
| --- | --- |
| 1. Стандартизация | 1. Наука об измерениях, методах и средствах обеспечения их единства |
| 1. Метрология | 1. Деятельность, направленная на разработку и установление требований, норм, правил |
| 1. Сертификация | 1. Форма подтверждения соответствия объектов выдвинутым требованиям |

**Установите соответствие:**

|  |  |
| --- | --- |
| 1. Центральный орган по сертификации | а. Разрабатывает предложения по формированию единой политики сертификации в рамках системы |
| 2.Орган по сертификации | б. Управляет системой , организует работу и устанавливает общие правила проведения сертификации в системе |
| 3. Совет по сертификации | в. Выдает заключение о возможности распространения результатов испытаний, сертификатов соответствия |
| 4.Испытательный центр | г. Организует и проводит проверку условий производства сертифицируемой продукции |

**Установите соответствие между видом измерения и соответствующим ему определением:**

|  |  |
| --- | --- |
| 1. Прямое | 1. Измерение, при котором измеряемую величину определяют на основании известной функциональной зависимости |
| 1. Косвенное | 1. Одновременное измерение двух и более однородных величин с целью установления соотношения между ними |
| 1. Совместные | 1. Измерение, при котором измеряемую величину определяют непосредственно из опыта |
| 1. Динамические | 1. Разновременное измерение двух и более однородных величин с целью установления соотношения между ними |

**Установите соответствие между категорией стандарта и записью его названия:**

|  |  |
| --- | --- |
| 1. Государственный стандарт | 1. ИСО 9001:2000 |
| 1. Международный стандарт | 1. ПМГ 05-94 |
| 1. Инструкция | 1. МИ 2232-2000 ГСИ |
| 1. Правила | 1. ГОСТ Р 1.5-2012 |

**Установите соответствие между аббревиатурой и полным названием стандартов:**

|  |  |
| --- | --- |
| 1. ГОСТ | 1. Республиканский стандарт |
| 1. ОСТ | 1. Стандарт организация |
| 1. РСТ | 1. Отраслевой стандарт |
| 1. СТО | 1. Государственный стандарт |

**Укажите правильный порядок обозначения ГОСТа из системы ЕСКД:**

1. Год утверждения стандарта
2. Порядковый номер в группе
3. Номер группы
4. Класс

**Укажите правильную последовательность названий групп стандартов, входящих в единую систему технологической документации (ЕСТД), начиная с первой**:

1. Основополагающие стандарты ЕСТД
2. Методы расчета применяемости деталей и учета применяемости технологической документации
3. Система обозначения технологических документов
4. Правила оформления технологических документов на различные виды работ

**Установите правильную последовательность разделов Технического регулирования на продукцию**:

1. Применение стандартов
2. Требования к продукции
3. Государственный контроль
4. Подтверждение соответствия
5. Заключительные и переходные положения

**Установите последовательность работ по разработке стандартов:**

1. Уведомление о разработке стандартов
2. Публичное обсуждение проекта
3. Экспертиза технического комитета
4. Публикация стандарта
5. Утверждение стандарта

**Установите последовательность работ по проведению сертификации:**

1. Рассмотрение и принятия решения по заявке
2. Подача заявки на сертификацию
3. Отбор, идентификация образцов и их испытания
4. Инспекционный контроль за сертифицированной продукцией
5. Выдача сертификата соответствия

**Укажите в последовательности участников системы сертификации, начиная с заявителя:**

1. Органы сертификации
2. Испытательные лаборатории
3. Заявитель
4. Центральный орган сертификации

**Определите правильный алгоритм прохождения процесса стандартизации продукции, работ, услуг:**

1. Создание модели для стандартизируемой продукции, работ или услуг
2. Выбор продукции, работ или услуг, для которых будет проводиться стандартизация
3. Утверждение стандартов для созданной модели, стандартизация
4. Утверждение оптимального качества созданной модели

**Укажите верный алгоритм проведения процесса сертификации:**

1. Оценка соответствия объекта сертификации установленным требованиям
2. Заявка на сертификацию
3. Решение по сертификации
4. Анализ результатов оценки соответствия

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

**Какой уровень шума считается максимально допустимым при работе оператора ПЭВМ**

1. 30 дБ
2. 50 дБ
3. 80 дБ
4. 70 дБ

**Какое безопасное расстояние должно быть от глаз до монитора при работе на ПЭВМ**

1. 30…50 см
2. 50…60 см
3. 60…70 см
4. 90…100 см

**Какой организации предоставляется право устанавливать заключительный диагноз хронического профессионального заболевания?**

1. Учреждению здравоохранения по месту жительства пострадавшего работника.
2. Центру профессиональной патологии, а также специализированным лечебно-профилактическим учреждениям, имеющим соответствующую лицензию
3. Медицинскому работнику организации

**На что имеет право каждый работник:**

1. На сохранение места работы и среднего заработка в случае приостановления работ вследствие нарушения требований охраны труда не по вине работника
2. На дополнительные компенсации при низком уровне травматизма и профзаболеваний в организации
3. На ежегодный медицинский осмотр за счёт средств работодателя

**Что должен делать специалист по охране труда на предприятии?**

1. Проведение специальной оценки условий труда
2. Стирка и ремонт средств индивидуальной защиты
3. Извещать своего непосредственного руководителя о любой ситуации, угрожающей жизни и здоровью людей, о каждом несчастном случае на производстве

**Как часто проводится повторный инструктаж?**

1. Ежегодно
2. Один раз в два года
3. Не реже одного раза в шесть месяцев

**Какова длительность непрерывной работы на компьютере без регламентированных перерывов?**

1. Не более 4 часов
2. Не более 2 часов
3. Не более 3 часов

**Продолжительность рабочей недели для подростков в возрасте 16-18 лет не должна превышать:**

1. 18 часов
2. 24 часа
3. 36 часов
4. 40 часов

**Какие производственные факторы относятся к опасным?**

1. Неправильное использование средств индивидуальной защиты
2. Недостаточная освещенность рабочего места
3. Неправильная организация рабочего места
4. Отсутствие лечебно-профилактического питания

**Что считается прогулом:**

1. Отсутствие на рабочем месте без уважительных причин в течении всего рабочего дня
2. Отсутствие на рабочем месте без уважительных причин более двух часов подряд в течение рабочего дня.
3. Отсутствие на рабочем месте без уважительных причин более четырех часов подряд в течение рабочего дня
4. Опоздание

**Что предусматривает дисциплинарная ответственность за нарушение законодательных и нормативных актов по безопасности труда должностными лицами?**

1. Наложение штрафа
2. Объявление дисциплинарного взыскания
3. Исправительные работы
4. Лишение свободы

**Какие устройства применяются для защиты от поражения электрическим током   
в случае повреждения изоляции?**

1. Автоматическое отключение
2. Защитное заземление
3. Защитное отключение
4. Все здесь указанные

**Основной задачей охраны труда является:**

1. Созидание и постоянное поддержание здоровых и безопасных условий труда
2. Обеспечение безопасности на производстве
3. Ликвидация несчастных случаев на производстве
4. Обеспечение выполнения законов об охране труда

**В какие сроки проводится повторный инструктаж на рабочем месте?**

1. Не реже одного раза в 6 месяцев, а для работников занятых на работах с повышенной опасностью раз в три месяца
2. Для работников занятых на работах с повышенной опасностью ежеквартально, для остальных ежегодно
3. Ежегодно для руководителей организации и раз в полгода для специалистов и служащих
4. Данный вид инструктажа не проводится

**О чем работник обязан немедленно известить своего руководителя?**

1. О любой ситуации угрожающей жизни и здоровью работника
2. О каждом несчастном случае пришедшим на производстве
3. Об ухудшении состояния своего здоровья
4. Обо всем вышеперечисленном

**На каких работах запрещается применение труда лиц в возрасте до 18 лет?**

1. На работах с вредными и опасными условиями труда
2. Подземных работах
3. На сверхурочных и ночных
4. Всех вышеназванных

**Какова минимальная продолжительность обеденного перерыва согласно Трудового Кодекса Российской Федерации?**

1. Не менее часа
2. Не менее 45 минут
3. Не менее 30 минут
4. На усмотрение руководителя

**Совокупность факторов производственной среды и трудового процесса, оказывающих влияние на работоспособность и здоровье работника это - …**

1. Условия труда
2. Охрана труда
3. Система управления охраной труда
4. Безопасность труда

**На кого возлагаются обязанности по обеспечению безопасных условий и охраны труда в организации?**

а.Работодатель

б. Профсоюзный орган

в. Служба охраны труда на предприятии

г. Отдел кадров

**По законодательству РФ в организациях создается служба охраны труда или вводится должность специалиста по охране труда при численности работников:**

1. 30 и более человек
2. 40 и более человек
3. 50 и более человек
4. 60 и более человек

**На расследование несчастных случаев при легких повреждениях отводится:**

1. 2 дня
2. 3 дня
3. 4 дня
4. 5 дней

**Укажите срок расследования тяжелых, групповых несчастных случаев и случаев со смертельным исходом?**

1. 7 дней
2. 8 дней
3. 9 дней
4. 15 дней

**Продолжительность отпуска без сохранения заработной платы по ТК РФ работникам, допущенным к вступительным испытаниям в образовательные организации высшего образования, составляет \_\_\_\_\_\_\_\_\_\_\_\_ календарных дней**

**Согласно ГОСТ 12.0.004-15 предусмотрено проведение следующих видов инструктажа: вводный, первичный и повторный на рабочем месте, \_\_\_\_\_\_\_\_\_\_\_\_, целевой**

**При воздействии на тело человека повышенной температуры в условиях повышенной влажности, обезвоживания и нарушения процесса терморегуляции организма возникает\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_**

**Вредный производственный фактор- это производственный фактор, воздействие которого на работника может привести к его\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Физическое повреждение организма под воздействием внешних факторов – это \_\_\_\_\_\_\_\_\_\_.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_ – это чрезвычайное событие техногенного характера, происшедшее по конструктивным, производственным, технологическим или эксплуатационным причинам, либо из-за случайных внешних воздействий, и заключающееся в повреждении, выходе из строя, разрушении технических устройств или сооружений.**

**При разрушении энергосберегающих ламп выделяются опасные для здоровья пары \_\_\_\_\_\_\_\_\_\_\_\_.**

**Состояние внутренней среды помещения, оказывающее воздействие на человека, характеризуемое показателями температуры воздуха и ограждающих конструкций, влажностью и подвижностью воздуха – это\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

**Гигиена труда – это область медицины, изучающая трудовую деятельность человека и производственную среду с точки зрения их влияния на организм, разрабатывающая меры и гигиенические нормативы, направленные на оздоровление условий труда и предупреждение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_заболеваний.**

**Установите соответствие между видом инструктажа по охране труда и временем его проведения:**

|  |  |
| --- | --- |
| 1. Вводный инструктаж | 1. Перед первым допуском к работе |
| 1. Первичный инструктаж | 1. Не реже одного раза в полгода |
| 1. Повторный инструктаж | 1. При выполнении разовых работ, не связанных с прямыми обязанностями по специальности |
| 1. Целевой инструктаж | 1. При поступлении на работу |

**Сопоставьте виды производственных травм в зависимости от вида травмирующего фактора:**

|  |  |
| --- | --- |
| 1. Баротравмы | 1. Вызваны ожогами и обморожениями |
| 1. Электротравмы | 1. Вызваны быстрым изменением атмосферного воздуха |
| 1. Психические | 1. Вызваны воздействием электрического тока |
| 1. Термические | 1. Вызваны тяжелыми психологическими потрясениями |

**Установите соответствие между факторами и названиями классов факторов:**

|  |  |
| --- | --- |
| 1. Физический фактор | 1. Недостаточная освещенность рабочей зоны |
| 1. Химический фактор | 1. Токсическое воздействие на организм человека |
| 1. Биологический фактор | 1. Воздействие на организм патогенных микроорганизмов и продуктов их деятельности |
| 1. Психофизиологический фактор | 1. Физические и нервные перегрузки |

**Установите правильную характеристику условий труда работников:**

|  |  |
| --- | --- |
| 1. Вредные | 1. Условия труда, при которых на работника не воздействуют опасные и вредные производственные факторы |
| 1. Опасные | 1. Условия труда, при которых на работника воздействуют вредные производственные факторы, в пределах предельно-допустимых уровней |
| 1. Оптимальные | 1. Условия труда, при которых уровни воздействия вредных и опасных производственных факторов превышают ПДУ |
| 1. Допустимые | 1. Условия труда, при которых на работника воздействуют вредные и опасные производственные факторы, которые в течение рабочего дня представляют угрозу жизни работника |

**Установите соответствие между измеряемым параметром микроклимата и освещения помещения и прибором для его измерения:**

|  |  |
| --- | --- |
| 1. Термометр | 1. Температура воздуха в помещении |
| 1. Гигрометр | 1. Уровень влажности воздуха в помещении |
| 1. Люксметр | 1. Освещенность рабочей зоны (световой поток) |
| 1. Электронный термогигрометр | 1. Температуру, влажность воздуха и др. параметры |

**Установите соответствие прохождения инструктажей по охране труда:**

|  |  |
| --- | --- |
| 1. Первичный | 1. Инструктаж проводится со всем личным составом подразделений ГПС, принятым на службу (работу), независимо от их образования, стажа работы по профессии |
| 1. Целевой | 1. Инструктаж проводится со всем личным составом, переводимым из одного подразделения ГПС в другое |
| 1. Вводный | 1. Инструктаж проводится при выполнении личным составом пожарных подразделений разовых работ, не связанных с прямыми обязанностями по специальности, с отметкой о нем в Журнале инструктажей |
| 1. Внеплановый | 1. Инструктаж проводится при введении новых стандартов, правил, инструкций по охране труда, а также изменений к ним |

**Установите соответствие между видом инструктажа и его целевой направленностью:**

|  |  |
| --- | --- |
| 1. Вводный | 1. Ознакомление с общими правилами и требованиями охраны труда в организации при приеме на работу |
| 1. Первичный | 1. Восстановление в памяти работника правил охраны труда, а также разбор имеющих место нарушений требований техники безопасности в практике организации. |
| 1. Повторный | 1. Изучение конкретных требований и правил обеспечения безопасности на конкретном оборудовании при выполнении конкретного процесса на рабочем месте. |
| 1. Внеплановый | 1. Изучение новых или переработанных стандартов, правил, инструкций по охране труда, при замене или модернизации оборудования, приспособлений и инструмента, для предупреждения несчастных случаев. |
| 1. Целевой | 1. Ознакомление с требованиями и правилами безопасности для конкретного события, мероприятия и несвязанного с основными обязанностями работника |

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

1. Убедиться в отсутствии пульса на сонной артерии и реакции зрачков на свет
2. Оттащить пострадавшего на безопасное расстояние
3. Приступить к реанимационным мероприятиям
4. Обесточить пострадавшего

**Укажите последовательность действий в универсальной схеме оказания первой помощи на месте происшествия**:

1. При наличии ран – наложить повязки
2. Если есть признаки переломов костей конечностей – наложить транспортные шины
3. Если нет сознания и нет пульса на сонной артерии – приступить к реанимации
4. Если нет сознания, но есть пульс на сонной артерии – повернуть на живот и очистить ротовую полость
5. При артериальном кровотечении – наложить повязки

**Укажите последовательность действий при оказании первой помощи пострадавшим в ЧС:**

а. Осуществить, немедленное прекращение поражающего фактора

б. Определить состояние пострадавшего(жив или мертв)

в.Наложить повязки и швы

г. Остановить артериальное кровотечение

д. Провести реанимацию

е. Транспортировать пострадавшего в соответствии с характером травмы

ж.Выяснить причины происшествия

**Укажите правильный порядок применения порошкового огнетушителя**:

1. Выдернуть чеку
2. Сорвать пломбу
3. Поднести огнетушитель к очагу горения
4. Нажать на верхнюю ручку запорно-пускового устройства
5. Направить сопло или шланг-раструб на очаг горения

**Укажите правильную последовательность оказания первой помощи пострадавшему работнику на производстве:**

1. Удалить пострадавшего из опасной зоны;
2. Оценить обстановку и прекратить действие повреждающего фактора;
3. Выявить признаки жизни и смерти;
4. Оказать первую доврачебную помощь;
5. Вызвать скорую медицинскую помощь.

**Укажите правильную последовательность мероприятий по охране труда при оформлении работника на работу:**

1. Проведение первичного инструктажа
2. Проверка знаний по охране труда
3. Проведение вводного инструктажа по охране труда
4. Обучение по охране труда

**Укажите правильную последовательность нормативно-правовых актов по охране труда в порядке увеличения их юридической силы:**

1. Трудовой кодекс Российской Федерации
2. Постановление Правительства Российской Федерации
3. Указы Президента Российской Федерации
4. Постановления федеральных министерств и ведомств

**Укажите правильную последовательность действий при использовании углекислотного огнетушителя:**

1. Выдернуть чеку
2. Направить раструб на очаг возгорания
3. Нажать рычаг
4. Сорвать пломбу

**Установите последовательность действий руководителя при несчастном случае, происшедшим на производстве:**

1. Сохранить до начала расследования несчастного случая все детали обстановки в том состоянии, в котором они были на момент происшествия
2. Принять неотложные меры по предотвращению развития аварийной ситуации и воздействия травмирующего фактора на других лиц
3. Сообщить работодателю или уполномоченному лицу о несчастном случае
4. Немедленно организовать первую помощь пострадавшему и при необходимости доставку его в учреждение здравоохранения

**Установите последовательность действий во время оказания первой медицинской помощи при сильном артериальном кровотечении:**

1. Наложить кровоостанавливающий жгут
2. Написать записку с указанием даты, часа наложения
3. Прижать артерию к костным выступам
4. Вызвать скорую помощь

**Установите последовательность оказания первой помощи при поражении электрическим током:**

1. укрыть, дать тепло
2. Обеспечить покой, наложить повязку
3. Отключить электроустановку
4. Оттянуть человека
5. Вызвать скорую помощь
6. Сделать искусственное дыхание

**Установите последовательность оказания первой помощи при обмороке:**

1. Освободить грудную клетку от одежды
2. Убедиться в наличии пульса
3. Надавить на болевую точку
4. Приподнять ноги

**Установите последовательность действий работодателя при несчастном случае на производстве:**

1. Сохранить до начала расследования несчастного случая обстановку, какой она была на момент происшествия или зафиксировать ее при помощи схем, фото- или видеосъемки
2. Принять неотложные меры по предотвращению аварийной ситуации
3. Организовать первую помощь пострадавшему, вызвать скорую помощь
4. Сформировать комиссию, организовать расследование несчастного случая
5. Проинформировать о несчастном случае соответствующие органы и организации

**Установите последовательность действий при обнаружении пожара в здании:**

1. Принять меры к тушению пожара
2. Эвакуировать людей из здания
3. Обесточить все доступные помещения
4. Сообщить по телефону 01 (мобильный 112) в пожарную часть

**Укажите последовательность инструктажей по охране труда которые должны проводиться в организации (ГОСТ 12.004-9 п.7):**

1. Первичный инструктаж на рабочем месте
2. Вводный инструктаж по охране труда
3. Повторный
4. Целевой

**Укажите последовательность действий в случаях поражением током:**

1. Обесточить потерпевшего
2. Если нет пульса на сонной артерии нанести удар по грудине и при его неэффективности приступить к проведению реанимации
3. В случае обильного кровотечения наложить жгуты
4. Если пульс на сонной артерии есть, но нет сознания более 4 минут – перевернуть на живот и приложить холод к голове
5. В случае повреждения конечностей наложить шины и холод
6. В случае термических и электрических ожогов – прикрыть пораженную поверхность чистой сухой тканью и приложить холод
7. Вызвать скорую помощь

**Установите последовательность оценки состояния пострадавшего:**

1. Цвет кожных покровов
2. Дыхание
3. Сознание
4. Пульс

**Определите иерархию проведения инструктажа по характеру, времени и последовательности**:

1. Повторный
2. Первичный на рабочем месте
3. Внеплановый
4. Вводный

**Определите последовательность действий при несчастном случае на производстве:**

1. Немедленно организовать первую помощь пострадавшему и при необходимости доставить в учреждение здравоохранения
2. Принять неотложные меры по предотвращению развития аварийной ситуации
3. Сохранить обстановку в том виде, в каком она была на момент происшествия, если это не угрожает жизни и здоровью других лиц и не ведёт к аварии
4. Обеспечить расследование несчастного случая и его учет

**5. Экономика и правовое обеспечение профессиональной деятельности**

**Структура затрат на информационную безопасность предприятия - это:**

1. состав затрат и часть каждого элемента в их общем объеме
2. все статьи затрат на информационную безопасность
3. часть каждого элемента затрат на информационную безопасность
4. калькуляция себестоимости затрат на информационную безопасность

**Назовите показатель сравнительной эффективности капиталовложений на информационную безопасность предприятия:**

1. объем выполняемых работ
2. производительность труда
3. трудоемкость
4. срок окупаемости

**В фонд заработной платы подразделения (организации) включаются:**

1. Оплата за отработанное время, начисленная работникам по тарифным планам и окладам
2. Оплата за выполненную работу по сдельным расценкам
3. Оплата за отработанное время, начисленная работникам по тарифным планам и окладам и оплата за выполненную работу по сдельным расценкам
4. Стоимость товаров или продуктов, выданных работникам в порядке натуральной оплаты труда

**Себестоимость продукции – это:**

1. Затраты материальных и трудовых ресурсов на производство и реализацию продукции или оказание услуг в денежном выражении
2. Количественные затраты материальных и трудовых ресурсов на производство и реализацию продукции или оказание услуг
3. Технологические затраты материальных и трудовых ресурсов на производство и реализацию продукции или оказание услуг
4. Затраты материальных и трудовых ресурсов на производство продукции или оказание услуг в денежном выражении

**Приговор суда, лишающий права гражданина заниматься предпринимательской деятельностью, является:**

1. Признанием гражданина недееспособным
2. Ограничением гражданина в правоспособности
3. Ограничением гражданина в дееспособности
4. Признанием гражданина несостоятельным

**За причиненный ущерб работник несет материальную ответственность:**

1. В размере 50 процентов от суммы ущерба
2. В пределах должностного оклада
3. В пределах среднего месячного заработка
4. В размере, не превышающем 50 000 рублей

**Продолжительность ежегодного основного оплачиваемого отпуска:**

1. 30 календарных дней
2. один месяц
3. 28 календарных дней
4. 24 рабочих дня

**Взыскания, применяемые к работнику работодателем, называются:**

1. Гражданско-правовыми
2. Административными
3. Уголовно-процессуальными
4. Дисциплинарными

**В чем состоит различие между производственным предприятием и фирмой:**

1. Предприятие осуществляет производственную деятельность, а фирма – коммерческую

(торговую) деятельность

1. Фирма – более широкое понятие, чем предприятие, и может включать несколько производственных или торговых предприятий
2. Различия между предприятием и фирмой нет

**К нормируемым оборотным средствам относятся:**

1. Все оборотные фонды
2. Все оборотные средства
3. Оборотные производственные фонды плюс готовая продукция на складе
4. Средства в расчетах, денежные средства, товары отгруженные, но не оплаченные покупателем

**Коммерческими признаются организации:**

1. Не имеющие статус юридического лица
2. Имеющие самостоятельную смету или баланс
3. Не ставящие основной целью получение прибыли
4. Преследующие в качестве основной цели своей деятельности извлечение прибыли

**Укажите тип банковских карт, позволяющий оплачивать услуги только в пределах доступного остатка на лицевом счете:**

1. Дебетовая карта
2. Кредитная карта
3. Дебетовая карта с подключенной услугой овердрафт
4. Любая банковская карта

**Укажите наличную валюту, в которой иностранец может рассчитываться в России:**

1. В долларах, евро, рублях
2. В долларах и рублях
3. Только в рублях
4. В валюте своей страны и рублях

**Работник получил доход в сумме 25.000 руб. После уплаты НДФЛ, в его распоряжении останется сумма равная….**

а.13250 руб.

б.23000 руб.

в.21750руб

г.20000 руб.

**Нормальная продолжительность рабочего времени в соответствии с Трудовым Кодексом Российской Федерации не может превышать:**

1. 40 часов в неделю
2. 36 часов в неделю
3. 8 часов в день
4. 7 часов в день

**Работники имеют право расторгнуть трудовой договор, заключенный на неопределенный срок, предупредив об этом работодателя письменно:**

1. За 2 дня
2. За 2 недели
3. За 1 месяц
4. За 3 месяца

**Постоянные издержки предприятия – это…**

1. Минимальные издержки, связанные с изготовлением продукции
2. Предельные издержки предприятия
3. Издержки, связанные с использованием производственных факторов, величина которых не зависит от объёма производимой продукции
4. Издержки, связанные с реализацией продукции

**Плата в выходной и нерабочий праздничный день производится:**

1. В двойном размере
2. В обычном размере
3. С увеличением в полтора раза
4. С увеличением в три раза

**Определите ситуацию, если обменный курс вырос с 25 до 30 рублей за доллар:**

1. Инфляция
2. Ревальвация
3. Дефляция
4. Девальвация

**Укажите, какой документ регламентирует отказ работника от работы в связи с условиями труда опасными для жизни:**

1. Конституция РФ
2. Постановление правительства РФ
3. Коллективный договор
4. Трудовой кодекс РФ

**Название гражданско-правового договора, когда предприятие, организация снимает жилье для своих сотрудников:**

1. Договор дарения
2. Договор аренды
3. Договор мены
4. Договор ренты

**Административная ответственность в Российской Федерации наступает для граждан, достигших возраста:**

1. 14 лет
2. 16 лет
3. 18 лет
4. 21 года

**Депутатом Государственной Думы может быть избран гражданин российской федерации, достигший на день голосования возраста:**

1. 18 лет
2. 25 лет
3. 21 года
4. 33 лет

**\_\_\_\_\_\_\_\_\_\_\_\_ - это отношение стоимости основных средств предприятия к средней годовой списочной численности рабочих.**

**\_\_\_\_\_\_\_\_\_\_\_\_ - это стоимость основных фондов, включающая стоимость (цену) приобретенного элемента основных фондов, а также затраты на доставку, монтаж, наладку, ввод в действие.**

**\_\_\_\_\_\_\_\_\_\_\_\_ - это финансовая несостоятельность организации.**

**Срок испытания для вновь принятого работника не может превышать \_\_\_ месяцев.**

**Экономическая категория, отражающая сущность расширенного воспроизводства; она характеризует степень достижения основных целей, присущих расширенному воспроизводству – это\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

**Минимальный уставный капитал для регистрации открытого акционерного общества составляет \_\_\_\_ МРОТ.**

**Прекращение деятельности юридического лица без перехода его прав и обязанностей к другим юридическим лицам называется \_\_\_\_\_\_\_\_\_\_\_\_.**

**Форма преобразования государственной собственности в частную называется \_\_\_\_\_\_\_\_\_\_\_\_.**

**Назовите основной документ при приеме на работу согласно ст. 65 Трудового кодекса РФ от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017).**

**Ответ: \_\_\_\_\_\_\_\_\_\_\_\_.**

**\_\_\_\_\_\_\_\_\_\_\_\_ - выдаваемое государством разрешение на осуществление определенных видов деятельности.**

**Формы организации и оплаты труда подразделения (организации) подразделяются на: \_\_\_\_\_\_\_\_\_\_\_\_ и повременную.**

**Установите соответствие между видами цен и их формулировкой:**

|  |  |
| --- | --- |
| 1. Свободные цены | 1. Устанавливаются на товары массового спроса |
| 1. Фиксированные цены | 1. Складываются на рынке под воздействием спроса и предложения независимо от влияния государственных органов |
| 1. Скользящие цены | 1. Устанавливаются почти в прямой зависимости от соотношения спроса и предложения |
| 1. Долговременные цены | 1. Устанавливаются государством в лице каких-либо органов власти и управления |

**Установите соответствие:**

|  |  |
| --- | --- |
| 1. Гражданское | а.Исправительные работы |
| 2. Трудовое | б.Замечание |
| 3. Административное | в.Дисквалификация |
| 4. Уголовное | г.Неустойка |

**Установите соответствие вида цены и её характеристики:**

|  |  |
| --- | --- |
| 1. Договорная цена | 1. Искусственно завышенная цена, ограничивающая ее снижение |
| 1. Регулируемая цена | 1. Искусственно заниженная цена, отграничивающая рост цены |
| 1. Цена «пола» | 1. Цена товара, которая устанавливается по соглашению сторон |
| 1. Цена «потолка» | 1. Цена, которая может отклоняться от базового уровня |

**Установите соответствие между терминами и их определениями:**

|  |  |
| --- | --- |
| 1. Первоначальная стоимость | 1. Стоимость основных фондов в момент прекращения их функционирования |
| 1. Восстановительная стоимость | 1. Складывается из цены на оборудование, затрат на транспорт и монтаж |
| 1. Остаточная стоимость | 1. Показывает, во сколько обошлось бы создание действующих основных фондов на момент переоценки с учётом морального износа |
| 1. Ликвидационная стоимость | 1. Полная первоначальная стоимость за вычетом износа |

**Установите соответствие между наказанием и его смыслом:**

|  |  |
| --- | --- |
| 1. Конфискация | 1. Принудительное безвозмездное обращение в собственность государства вещи, явившейся орудием совершения или предметом административного правонарушения |
| 1. Дисквалификация | 1. Лишение физического лица права занимать руководящие должности в исполнительном органе управления юридического лица, входить в совет директоров, осуществлять управление юридическим лицом, в том числе в качестве предпринимательской деятельности |
| 1. Административный арест | 1. Содержание нарушителя в условиях изоляции от общества |

**Установите соответствие между термином и отраслью права:**

|  |  |
| --- | --- |
| 1. Дееспособность | 1. Трудовое право |
| 1. Работник | 1. Административное право |
| 1. Предупреждение | 1. Предпринимательское право |
| 1. Прибыль | 1. Гражданское право |

**Установите соответствие между конкретными ситуациями и типом правоотношений, который они иллюстрируют:**

|  |  |
| --- | --- |
| 1. Семейное | 1. Семья нашла клад во время ремонта дома |
| 1. Административное | 1. Работник без уважительной причины не вышел на работу |
| 1. Трудовое | 1. Гражданка оформила опеку над племянником |
| 1. Гражданское | 1. Гражданин нарушил правила дорожного движения |

**Установите соответствие между названиями организационно-правовых форм предпринимательства и их характеристиками:**

|  |  |
| --- | --- |
| 1. Производственный кооператив | 1. Коммерческая организация, уставный капитал которой разделен на определенное количество долей, каждая из которых выражена ценной бумагой (акцией), удовлетворяющей обязательные права участников общества (акционеров по отношению к обществу) |
| 1. Государственное учреждение | 1. Договорное объединение участников для предпринимательской деятельности |
| 1. Акционерное общество | 1. Добровольное объединение граждан на основе членства для совместной хозяйственной деятельности, основанной на их личном участии и объединении его членам индивидуальных взносов |
| 1. Товарищество | 1. Государственное или муниципальное предприятие, не наделенное правом собственности на закрепленное за ним собственником имущество (имущество неделимое и не может быть распределено по долям, частям, вкладам) |
| 1. Унитарное предприятие | 1. Некоммерческая организация, созданная собственником для осуществления управленческих, социально-культурных или иных функций некоммерческого характера и финансируемая им полностью или частично |

**Установите соответствие типа организации его характеристике:**

|  |  |
| --- | --- |
| 1. Государственное (муниципальное) унитарное предприятие | 1. Основано на личном трудовом или ином участии и объединении его членов |
| 1. Производственный кооператив | 1. Имущество является неделимым и не может быть распределено по вкладам (долям), в том числе между работниками предприятия |
| 1. Общество с ограниченной ответственностью | 1. Участники несут солидарную ответственность по его обязательствам своим имуществом в одинаковом для всех кратном размере стоимости их вкладов |
| 1. Общество с дополнительной ответственностью | 1. Участники не отвечают по обязательствам и несут риск убытков, связанных с деятельностью общества, в пределах стоимости внесенных ими вкладов |

**Установите последовательность действий при расчете производительности труда:**

1. Определение стоимости одной единицы продукции
2. Расчет стоимости валовой продукции подразделения (организации)
3. Определение численности промышленно-производственного персонала
4. Расчет объёма выпускаемой продукции
5. Определение отношения валовой продукции к численности промышленно-производственного персонала

**Установите последовательность действий при расчете показателя фондоотдачи подразделения (организации):**

1. Определение стоимости одной единицы продукции
2. Расчет стоимости валовой продукции подразделения (организации)
3. Определение общей стоимости основных производственных фондов подразделения (организации)
4. Расчет объёма выпускаемой продукции
5. Определение отношения валовой продукции к общей стоимости основных производственных фондов подразделения (организации)

**Установите рациональную последовательность процесса ценообразования на товары(услуги):**

а. Анализ цен конкурентов

б. Выбор методов ценообразования

в.Установление окончательной цены

г. Выбор цели ценообразования

д.Определение спроса

е. Анализ издержек

**Укажите в правильной последовательности структуру бизнес-плана:**

1. Организационный план
2. Описание товаров, работ или услуг, которые собирается предлагать фирма
3. Маркетинговый план
4. Финансовый план
5. Резюме проекта или концепция бизнеса
6. Характеристика будущего бизнеса и отрасли его функционирования

**Установите последовательность расчета себестоимости:**

1. Производственная себестоимость (себестоимость готовой продукции)
2. Технологическая себестоимость
3. Цеховая себестоимость
4. Полная себестоимость, или себестоимость реализованной (отгруженной) продукции

**Установите порядок заключения трудового договора:**

1. Наступление испытательного срока
2. Подача письменного заявления работником
3. Знакомство работника с условиями труда и оплаты
4. Предъявление соискателем необходимых документов, конкурс документов претендентов
5. Приказ работодателя о приеме на работу
6. Подписание трудового договора

**Расположите источники трудового права по юридической силе:**

1. Трудовой кодекс РФ
2. Указ Президента РФ
3. Конституция РФ
4. Закон субъекта РФ

**Установите правильную последовательность расчёта розничной цены продукции:**

1. Прибыль продукции
2. Себестоимость продукции
3. Наценка посредника
4. НДС
5. Наценка продавца

**Установить правильную последовательность расширения дееспособности гражданина РФ:**

1. Быть принятым на работу
2. Совершать мелкие бытовые сделки
3. Возглавить кооператив
4. Вступать в брак
5. Избираться в Государственную Думу

**Расположите факторы внешней среды прямого воздействия на работу предприятия по значимости для успешной работы в рыночной экономике:**

1. Конкуренты
2. Посредники
3. Поставщики
4. Потребители

**Установите последовательность этапов регистрации юридического лица:**

1. Представление документов на регистрацию в ИФНС
2. Заключение между учредителями договора об учреждении общества
3. Принятие участниками решения об открытии фирмы
4. Открытие расчетного счета фирмы
5. Изготовление печати

**Установите порядок приема сотрудника на работу:**

1. Подготовка приказа о приеме на работу
2. Ознакомление нового сотрудника с внутренними документами организации под роспись
3. Оформление личной карточки
4. Проверка предоставленных соискателем документов
5. Согласование и подписание трудового договора
6. Внесение сведений в трудовую книжку

**Установите этапы лицензирования деятельности:**

1. Уведомление соискателя лицензии о принятом решении
2. Выдача лицензии
3. Принятие лицензирующим органом решения о выдаче или отказе в выдаче лицензии
4. Представление соискателем лицензии документов в лицензирующий орган
5. Плата соискателем лицензионного сбора за предоставление лицензии
6. Проведение проверки соответствия соискателя лицензии лицензионным требованиям и условиям

**Выберите правильную последовательность действий работодателя и работника при установлении факта дисциплинарного проступка в соответствии с Трудовым кодексом РФ в действующей редакции:**

1. Ознакомление с приказом
2. Установление факта дисциплинарного проступка
3. Издание приказа
4. Истребование объяснения от работника
5. Установление предела дисциплинарного взыскания

**Укажите правильную последовательность этапов определения уровня рентабельности:**

1. Расчёт выручки от реализации
2. Определение затрат на реализацию
3. Определение полной себестоимости
4. Расчет прибыли

**Укажите правильный порядок образования чистой прибыли в организации:**

1. Прибыль до налогообложения
2. Прибыль от продажи
3. Чистая прибыль
4. Налог на прибыль

**Расставьте формы оборотных средств по естественным стадиям кругооборота оборотных средств на предприятии:**

1. Готовая продукция,
2. Сырье,
3. Денежные средства на закупку,
4. Незавершенное производство

**Установите правильную последовательность расчета амортизационных отчислений на единицу продукции:**

1. Нормы амортизации
2. Амортизационные отчисления на единицу продукции
3. Амортизационные отчисления на весь объем продукции в год
4. Полная балансовая стоимость основного средства

**Установите порядок формирования цен во всех звеньях товаропроводящей цепочки:**

1. Розничная цена продавца
2. Себестоимость продукции у производителя
3. Оптовая цена посредника
4. Цена производителя

**6. Основы информационной безопасности**

**Информация это -**

а) сведения, поступающие от СМИ

б) только документированные сведения о лицах, предметах, фактах, событиях

в) сведения о лицах, предметах, фактах, событиях, явлениях и процессах

независимо от формы их представления

г) только сведения, содержащиеся в электронных базах данных

**Какими официальными документами информация отнесена к объектам гражданских прав?**

а) УК РФ

б) Законом РФ "О праве на информацию"

в) ГК и законом РФ "Об информации, информатизации и защите информации"

г) Конституцией РФ

**Информация, зафиксированная на материальном носителе, с реквизитами,**

**позволяющими ее идентифицировать, называется**

а) достоверной

б) конфиденциальной

в) документированной

г) коммерческой тайной

**Формы защиты интеллектуальной собственности -**

а) авторское, патентное право и коммерческая тайна

б) интеллектуальное право и смежные права

в) коммерческая и государственная тайна

г) гражданское и административное право

**Потенциальная возможность нарушения защиты – это..**

а)Угроза

б) Уязвимость

в) Риск

г) Обязательство

**По принадлежности информационные ресурсы подразделяются на**

а) государственные, коммерческие и личные

б) государственные, не государственные и информацию о гражданах

в) информацию юридических и физических лиц

г) официальные, гражданские и коммерческие

**К негосударственным относятся информационные ресурсы**

а) созданные, приобретенные за счет негосударственных учреждений и организаций и физических лиц

б) созданные, приобретенные за счет негосударственных предприятий и физических лиц

в) полученные в результате дарения юридическими или физическими лицами

**По доступности информация классифицируется на**

а) открытую информацию и государственную тайну

б) конфиденциальную информацию и информацию свободного доступа

в) информацию с ограниченным доступом и общедоступную информацию

г) виды информации, указанные в остальных пунктах

**К конфиденциальной информации относятся документы, содержащие**

а) государственную тайну

б) законодательные акты

в) "ноу-хау"

г) сведения о золотом запасе страны

**К конфиденциальной информации не относится**

а) коммерческая тайна

б) персональные данные о гражданах

в) государственная тайна

г) "ноу-хау"

**Вопросы информационного обмена регулируются (...) правом**

а) гражданским

б) информационным

в) конституционным

г) уголовным

**Согласно ГК РФ интеллектуальная собственность это**

а) информация, полученная в результате интеллектуальной деятельности индивида

б) литературные, художественные и научные произведения

в) изобретения, открытия, промышленные образцы и товарные знаки

г) исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности

**Интеллектуальная собственность включает права, относящиеся к**

а) литературным, художественным и научным произведениям, изобретениям и открытиям

б) исполнительской деятельности артиста, звукозаписи, радио- и телепередачам

в) промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям

г) всему, указанному в остальных пунктах

**Конфиденциальная информация это**

а) сведения, составляющие государственную тайну

б) сведения о состоянии здоровья высших должностных лиц

в) документированная информация, доступ к которой ограничивается в

соответствии с законодательством РФ

г) данные о состоянии преступности в стране

**Какая информация подлежит защите?**

а) информация, циркулирующая в системах и сетях связи

б) зафиксированная на материальном носителе информация с реквизитами,

позволяющими ее идентифицировать

в) только информация, составляющая государственные информационные ресурсы

г) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

**Система защиты государственных секретов определяется Законом**

а) "Об информации, информатизации и защите информации"

б) "Об органах ФСБ"

в) "О государственной тайне"

г) "О безопасности"

**Государственные информационные ресурсы не могут принадлежать**

а) физическим лицам

б) коммерческим предприятиям

в) негосударственным учреждениям

г) всем перечисленным субъектам

**Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает**

а) Указ Президента "Об утверждении перечня сведений, относящихся к

государственной тайне"

б) ГК РФ

в) Закон "Об информации, информатизации и защите информации"

г) Конституция

**Классификация и виды информационных ресурсов определены**

а) Законом "Об информации, информатизации и защите информации"

б) Гражданским кодексом

в) Конституцией

г) всеми документами, перечисленными в остальных пунктах

**Определение понятия "конфиденциальная информация" дано в**

а) ГК РФ

б) Законе "О государственной тайне"

в) Законе "Об информации, информатизации и защите информации"

г) УК РФ

**Формой правовой защиты литературных, художественных и научных произведений является (...) право**

а) литературное

б) художественное

в) авторское

г) патентное

**Запрещено относить к информации с ограниченным доступом**

а) законодательные акты, информацию о чрезвычайных ситуациях и информацию о

деятельности органов государственной власти (кроме государственной тайны)

б) только информацию о чрезвычайных ситуациях

в) только информацию о деятельности органов государственной власти (кроме государственной тайны)

г) документы всех библиотек и архивов

**Формой правовой защиты изобретений является**

а) институт коммерческой тайны

б) патентное право

в) авторское право

г) все, перечисленное в остальных пунктах

**К коммерческой тайне могут быть отнесены**

а) сведения не являющиеся государственными секретами

б) сведения, связанные с производством и технологической информацией

в) сведения, связанные с управлением и финансами

г) сведения, перечисленные в остальных пунктах

**Является ли авторское право, патентное право и КТ формами защиты интеллектуальной собственности?**

а) да

б) нет

в) только авторское и патентное

г) только КТ

**Каким законом в РФ защищаются права исполнителей и производителей фонограмм?**

а) "О правовой охране программ для ЭВМ и баз данных"

б) "Об авторском праве и смежных правах"

в) "Патентный закон РФ"

г) закон еще не принят

**Закон "Об авторском праве и смежных правах" защищает права**

а) исполнителей (актеров, певцов и т.д.)

б) производителей фонограмм

в) организации эфирного и кабельного вещания

г) всех лиц, перечисленных в остальных пунктах

**Какой законодательный акт содержит сведения по защите коммерческой тайны?**

а) Закон "Об авторском праве и смежных правах"

б) Закон "О коммерческой тайне"

в) Патентный закон

г) Закон "О правовой охране программ для ЭВМ и баз данных"

**К информации ограниченного доступа не относится**

а) государственная тайна

б) размер золотого запаса страны

в) персональные данные

г) коммерческая тайна

**Система защиты государственных секретов**

а) основывается на Уголовном Кодексе РФ

б) регулируется секретными нормативными документами

в) определена Законом РФ "О государственной тайне"

г) осуществляется в соответствии с п.а)-в)

**Действие Закона "О государственной тайне" распространяется**

а) на всех граждан и должностных лиц РФ

б) только на должностных лиц

в) на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне

г) на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения

**К государственной тайне относится...**

а) информация в военной области

б) информация о внешнеполитической и внешнеэкономической деятельности

государства

в) информация в области экономики, науки и техники и сведения в области

разведывательной и оперативнорозыскной деятельности

г) все выше перечисленное

**Документы, содержащие государственную тайну снабжаются грифом**

а) "секретно"

б) "совершенно секретно"

в) "особой важности"

г) указанным в п.а)-в)

**Гриф "ДСП" используется**

а) для секретных документов

б) для документов, содержащих коммерческую тайну

в) как промежуточный для несекретных документов

г) в учебных целях

**Порядок засекречивания состоит в установлении следующих принципов:**

а) целесообразности и объективности

б) необходимости и обязательности

в) законности, обоснованности и своевременности

г) всех выше перечисленных

**Предельный срок пересмотра ранее установленных грифов секретности составляет**

а) 5 лет

б) 1 год

в) 10 лет

г) 15 лет

Действия, принимаемые для достижения информационного превосходства в интересах национальной военной стратегии, осуществляемые путем влияния на информацию и информационные системы противника при одновременной защите собственной информации своих информационных систем – это..

**Срок засекречивания сведений, составляющих государственную тайну**

а) составляет 10 лет

б) ограничен 30 годами

в) устанавливается Указом Президента РФ

г) ничем не ограничен

**За нарушения законодательства РФ о ГТ предусматривается (...) ответственность**

а) уголовная и административная

б) гражданско-правовая

в) дисциплинарная

г) указанная в п.1-3

**Не подлежат засекречиванию**

а) сведения о чрезвычайных происшествиях и катастрофах

б) сведения об объемах государственного заказа

в) сведения о дислокации особо важных объектах

г) сведения о лицах сотрудничающих с правоохранительными органами

**Факты угроз общественной безопасности являются**

а) информацией свободного доступа

б) информацией обязательного доведения

в) служебной тайной

г) государственной тайной

**Коммерческая информация имеет ценность (выбрать все варианты)**

а) в силу ее неизвестности третьими лицами

б) при отсутствии ее в свободных источниках

в) при обеспечении защиты такой информации

г) при контроле за действиями персонала.

**Профессиональная тайна - это**

а) тайна связи

б) медицинская тайна

в) военная тайна

г) служебная тайна

**Профессиональная тайна это**

а) милицейская тайна

б) тайна исповеди

в) персональные данные

г) коммерческая тайна

**Служебная тайна – конфиденциальная информация ставшая известной в государственных органах и органах местного самоуправления с силу выполнения**

а) служебной деятельности

б) профессиональной деятельности

в) коммерческой деятельности

г) предпринимательской деятельности

**Персональные данные это**

а) биографические данные

б) биометрические данные

в) статистические данные

г) публикации средств массовой информации

**Виды доступа к информации(выбрать все варианты)**

а) свободный доступ

б) обязательное доведение

в) персональные данные

г) предоставление информации по запросу

**Информация не может быть предоставлена по запросу, если она является(выбрать все варианты)**

а) общедоступной информацией

б) сведениями обязательного доведения

в) государственной тайной

г) коммерческой тайной

д) персональными данными

**Дестабилизирующим фактором является(выбрать все варианты)**

а) ошибка

б) сбой

в) экранирование

г) отказ

д) зашумление

е) стихийное бедствие

**Дестабилизирующим фактором является(выбрать все варианты)**

а) количественная недостаточность

б) ущерб

в) качественная недостаточность

г) использование шифрования

д) побочные явления;

е) злоумышленные действия

**Количественной недостаточностью является**

а) действия людей специально направленные на нарушение защищенности

б) физическая нехватка одного или нескольких элементов системы

в) несовершенство конструкции или организации системы безопасности

г) временное нарушение работоспособности системы безопасности

**Качественной недостаточностью является**

а) недостаточная квалификация персонала

б) несовершенство конструкции или организации системы безопасности

в) действия людей специально направленные на нарушение защищенности

г) физическая нехватка одного или нескольких элементов системы

**Отказом является**

а) неправильное одноразовое выполнение функций

б) явление, сопутствующее выполнению элементом системы своих функций

в) временное нарушение работоспособности системы

г) нарушение работоспособности системы, приводящие к невыполнению ею своих функций

**Сбоем является**

а) временное нарушение работоспособности системы

б) неправильное одноразовое выполнение функций

в) явление, сопутствующее выполнению элементом системы своих функций

г) несовершенство конструкции или организации системы безопасности

**Ошибкой является**

а) явление, сопутствующее выполнению элементом системы своих функций

б) недостаточная квалификация персонала

в) неправильное одноразовое выполнение функций

г) физическая нехватка одного или нескольких элементов системы

**Побочное явление - это**

а) явление, сопутствующее выполнению элементом системы своих функций

б) недостаточная квалификация персонала

в) временное нарушение работоспособности системы

г) разглашение информации

**Действия, принимаемые для достижения информационного превосходства в интересах национальной военной стратегии, осуществляемые путем влияния на информацию и информационные системы противника при одновременной защите собственной информации своих информационных систем – это\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   «зашифрование» данных, состоящий в преобразовании открытых данных в зашифрованные, и «расшифрование» данных, соответственно выполняющего преобразование зашифрованных данных в открытые.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_открытые данные данные, не подвергнутые криптографическому преобразованию.**

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ —* это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.**

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ —* информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *—* это желаемый результат защиты информации.**

**Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *—* степень соответствия результатов защиты информации поставленной цели.**

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ —* деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.**

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ —* деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.**

**Установите соответствие между терминами**

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

**Установите соответствие:**

|  |  |
| --- | --- |
| 1.Конфиденциальность | А. Хеш-функция |
| 2.Целостность | Б. Шифрование |
| 3.Разграничение доступа | В. Аутентификация |
| 4.Авторство | Г. Электронная подпись |

**Установите соответствие между понятиями и их определениями.**

|  |  |
| --- | --- |
| 1. Конфиденциальность | 1. Возможность ознакомиться с информацией имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями. |
| 1. Целостность | 1. Возможность внести изменение в информацию должны иметь только те лица, кто на это уполномочен. |
| 1. Доступность | 1. Возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени. |
| 1. Учет | 1. Все значимые действия лица, выполняемые им в рамках, контролируемых системой безопасности, должны быть зафиксированы и проанализированы. |

**Установите соответствие между видом тайны и информационным активом**

|  |  |
| --- | --- |
| 1. Государственная | 1. Сведения о запасах стратегических ресурсов |
| 1. Коммерческая | 1. Биометрические данные граждан |
| 1. Профессиональная | 1. Сведения об обороте предприятия |
| 1. Персональные данные | 1. Сведения о факте обращения гражданина за оказанием медицинской помощи |

**Установите соответствие между видом тайны и информационным активом**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вид тайны | |  | Информационный актив | |
| 1. | Государственная |  | А | Сведения о запасах стратегических ресурсов |
| 2. | Коммерческая | Б | Сведения об обороте предприятия |
| 3. | Служебная | В | Базы данных пенсионного фонда граждан |
| 4. | Профессиональная | Г | Сведения о регистрации сделок с недвижимостью |
| 5. | Персональные данные | Д | Биометрические данные граждан |

**Сопоставить дестабилизирующие факторы и соответствующие им действия**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Дестабилизирующий фактор | |  | Действия | |
| 1. | Сбой |  | А. | Отключение компьютера из-за пониженного уровня питания |
| 2. | Отказ |  | Б. | Выход из строя блока питания компьютера |
| 3. | Ошибка |  | В. | Зависание компьютера |
| 4. | Стихийное бедствие |  | Г. | пожар |
| 5. | Количественная недостаточность |  | Д. | Нехватка персонала |
| 6. | Качественная недостаточность |  | Е. | Устаревшее оборудование |
| 7. | Злоумышленные действия |  | Ж. | диверсия |
| 8. | Побочное явление |  | З. | Паразитные наводки |

**Установите последовательность этапов создание системы защиты информации:**

1. выбор контрмер, обеспечивающих информационную безопасность;

2. определение политики информационной безопасности;

3. определение границ управления информационной безопасностью объекта;

4. анализ уязвимости;

1. проверка системы защиты;
2. составление плана защиты;
3. реализация плана защиты (управление системой защиты).

**Установите последовательность оценки безопасности в процессе разработки ИТ на наибо­лее важных этапах.**

1. оценка профиля защиты;

2. оценка задания по безопасности;

3. оценка реализованных механизмов безопасности.

**Установите последовательность по формированию Перечня и определению сведений, составляющих служебную или коммерческую тайну, должна состоять из следующих этапов**:

1.составление предварительного перечня сведений, содержащих служебную или коммерческую тайну, для структурных подразделений (отделов, служб) организации;

2. определение возможного ущерба, наступающего в результате несанкционированного распространения сведений, включаемых в Перечень;

3. определение затрат на защиту рассматриваемых сведений;

4. принятие решения о включении сведений в окончательный вариант Перечня;

5. составление обобщенного Перечня и рассмотрение его на заседании ЭК;

6. оформление результатов работы по формированию Перечня.

7. определение преимуществ открытого использования рассматриваемых сведений по сравнению с закрытым;

**Установите последовательность анализа сведений, составляющих служебную или коммерческую тайну:**

1. установить места их разработки, накопления и хранения;

2. оценить возможности по перекрытию этих каналов;

3. определить, какие сведения организации могут быть отнесены к служебной или коммерческой тайне;

4. проанализировать соотношение затрат и доходов по использованию различных технологий, обеспечивающих защиту служебной или коммерческой тайны;

5. выявить потенциальные каналы утечки таких сведений;

6. назначить сотрудников, ответственных за каждый участок системы обеспечения безопасности.

**Подход к реализации защитных мероприятий по обеспечению информационной безопасности должен соответствовать следующей последовательности:**

1.Оценка угроз

2.Анализ риска

3 Определение способов защиты

4.Определение состава средств информационной системы

5.Анализ уязвимых элементов информационной системы

6. Определение функций защиты

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

**Какую длину ключа имеет алгоритм шифрования DES?**

а) 256 байт

б) 56 бит

в) 128 байт

г) 1024 бит

**Алгоритм шифрования PGP является:**

а) комбинированным использованием симметричного и асимметричного алгоритмов

б) симметричным

в) асимметричным

г) цифровой подписи

**Алгоритм шифрования RSA основан на сложности:**

а) разложения произведения двух простых чисел на множители

б) вычисления десятичных логарифмов

в) модулярной арифметики

г) сложности вычисления точки на эллиптической кривой

**Алгоритм шифрования ГОСТ 28147-89 использует длину ключа:**

а) 256 бит

б) 56 бит

в) 128 байт

г) 1024 бит

**Алгоритм шифрования ГОСТ 28147-89 является:**

а) симметричным

б) асимметричным

в) комбинированным

г) многоалфавитным

**Ассиметричное шифрование использует:**

а) 2 ключа

б) 1 ключ

в) электронный ключ

г) электронную подпись

**В алгоритмах электронной подписи распознавание авторства производится:**

а) закрытым ключом отправителя

б) закрытым ключом получателя

в) открытым ключом получателя

г) открытым ключом отправителя

**В ассиметричных алгоритмах расшифрование производится:**

а) закрытым ключом отправителя

б) закрытым ключом получателя

в) открытым ключом получателя

г) открытым ключом отправителя

**В омофоническом шифре частотность появления символьных комбинаций стремится к:**

а) 1%

б) 2%

в) 10%

г) 100%

**Длина ключа электронной подписи ГОСТ3410-94 составляет:**

а) 56 бит

б) 1024 бит

в) 256 бит

г) 128 байт

**Замену символов с открытого текста, соответствующими символами алфавита криптотекста называют:**

а) шифром замены

б) простейшим шифром

в) блочным шифром

г) шифром подстановки

**Как называют в ГОСТе режим электронной кодовой книги (ЕСВ):**

а) режим простой замены

б) режим сцепления блоков шифротекста

в) режим обратных связей по выбору

г) режим счетчика

**Какое свойство информационной безопасности обеспечивается хеш-функцией?**

а) целостность

б) конфиденциальность

в) безотказность

г) готовность

**Какое свойство информационной безопасности обеспечивается шифрованием?**

а) безотказность

б) доступность

в) конфиденциальность

г) целостность

**Какой алгоритм шифрования стал прообразом для отечественного ГОСТ28147-89?**

а) DES

б) AES

в) ГОСТ 34.10

г) DSA

**Какой из перечисленных ниже алгоритмов основан на сложности разложения больших чисел:**

а) DES

б) AES

в) RSA

г) Диффи-Хеллман

**Ключ- это:**

а) информация необходимая для беспрепятственного шифрования и расшифровывания сообщения

б) сообщение необходимое для расшифровывания информации

в) конечное множество используемых информационных знаков

г) бесконечное множество используемых символов

**Контроль целостности передаваемых по сетям данных осуществляется посредством:**

а) аудита событий

б) аутентификации данных

в) вычисления значения хеш-функции

г) межсетевого экранирования

**Юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом – это\_\_\_\_\_\_\_\_\_\_**

а)Удостоверяющий центр

б) Репозиторий

в)Центр обновления ПО

г) Доверенный центр сертификации

**Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения:**

а) число раундов шифрования

б) разрядность блока

в) ключ

г) алгоритм шифрования

**Криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись, разработанная в 1977 году, называется:**

а) алгоритм шифрования RSA

б) алгоритм DSA

в) алгоритм DSS

г) алгоритм SHA

**Криптосистемы с последовательным выполнением преобразований над элементами открытого текста называются:**

а) поточными шифрами

б) двоичными аддитивными шифрами

в) блочными шифрами

г) криптосистемами с ключом однократного применения

**Линейное шифрование данных, основанное на поточном способе шифрования называется:**

а) гаммированием

б) подстановкой

в) перестановкой

г) имитовставкой

**Наука об обеспечении секретности и / или аутентичности (подлинности) передаваемых сообщений:**

а) криптография

б) ЭЦП

в) криптоанализ

г) стеганография

**По принципу Керкгоффса в криптосистеме секретным должно быть:**

а) ключ

б) алгоритм

в) время шифрования

г) используемый алфавит

д) длина ключа

**При использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы называются:**

а) симметричными криптосистемами

б) простыми криптосистемами

в) гибридными криптосистемами

г) ассиметричными криптосистемами

**Происхождение термина «криптография»:**

а) от слова «тайнопись»

б) от слова «шифрование»

в) от термина «скремблирование»

г) от термина «кодирование»

**Процесс наложения по определенному закону гамма-шифра на открытые данные:**

а) имитовставка

б) хэширование

в) гаммирование

г) ЭЦП

**Процесс, в ходе которого шифрованный текст преобразуется в исходный, называется:**

а) дешифрование

б) шифрование

в) преображение

г) искажение

**Разрядность 3DES равна:**

а) 112 бит

б) 56 бит

в) 168 бит

г) 256 бит

**Разрядность шифруемых блоков данных RSA:**

а) меньше разрядности ключа

б) произвольная

в) равна разрядности ключа

г) больше разрядности ключа

**Симметричное шифрование использует:**

а) 1 ключ

б) 2 ключа

в) электронный ключ

г) электронную подпись

**Системы, где с помощью открытого ключа шифруют ключ блочного криптоалгоритма, а само сообщение шифруют с помощью этого симметричного секретного ключа, называют:**

а) гибридные(комбинированные) криптосистемы

б) криптосистема RSA

в) электронная подпись

г) криптографические протоколы

**Сколько циклов замены выполняет DES?**

а) 32

б) 16

в) 64

г) 56

**Совокупность действий инструкций, команд, вычислений), выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата называется:**

а) шифрованием

б) алгоритмом

в) протоколом

г) дешифрованием

**Стеганография это:**

а) скрытие самого факта передачи информации

б) скрытие смысла передаваемой информации

в) сжатие информации

г) замена смысловых конструкций

**Текст- это:**

а) упорядоченный набор из элементов алфавита

б) конечное множество комбинаций символов алфавита

в) информация необходимая для шифрования и расшифровывания сообщения

г) алгоритм шифрования

**Тот из двух ключей асимметричной системы, который свободно распространяется – это..?**

а) смарт-карта

б) закрытый ключ

в) электронный ключ

г) открытый ключ

**Установление санкционированным получателем (приемником) того факта, что полученное сообщение послано санкционированным отправителем (передатчиком) называется:**

а) авторизацией

б) идентификацией

в) аутентификацией

г) контролем целостности информации

**Функции, для которых легко найти функцию прямого отображения и нельзя найти обратное называются:**

а) нелинейные функции

б) линейные функции

в) односторонние функции

г) функции преобразования

**Функция, предназначенная для сжатия подписываемого документа до нескольких десятков, или сотен бит называется:**

а) хэш- функцией

б) логарифмической функцией

в) тригонометрической функцией

г) ЭЦП

**Процесс взаимной аутентификации подразумевает, что:**

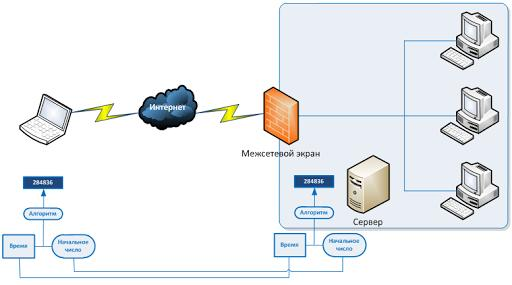
а) пользователь аутентифицируется системой, а система аутентифицируется пользователем

б) пользователь аутентифицируется на двух системах одновременно

в) пользователь аутентифицируется сервером, а затем – процессом

г) пользователь аутентифицируется, получает билет, а затем с помощью билета аутентифицируется службой

**Работу чего из перечисленного ниже иллюстрирует этот рисунок:**



а) Rainbow-таблицы

б) одноразовые пароли

в) атака по словарю

г) строгая аутентификация

**Характеристика шифра, определяющая его стойкость к шифрованию без знания ключа, называется:**

а) криптостойкость

б) аутентификация

в) идентификация

г) секретность

**Защита от навязывания ложной информации-это\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Данные, передаваемые без использования криптографии- это\_\_\_\_\_\_\_\_\_\_**

**Данные, полученные после применения криптосистемы- это\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Данные, присоединенные, либо полученные в результате криптографического преобразования к набору данных, позволяющие получателю набора данных подтвердить подлинность источника и целостность набора данных и обеспечить защиту против подделки, например, со стороны получателя – это\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Зашифрованные данные подвергнутые криптографическому преобразованию**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей .**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности возможных для данного алгоритма преобразований.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  совокупность криптоключей, существует временное ограничение в отношении ключевой информации – с течением времени она подлежит замене.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ физические устройства, со структурой, которая понятна средствам их использующих, и которые планируется применять для размещения на них ключевой информации.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ключевая информация, помещенная на ключевой носитель.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  защита системы шифрованной связи от навязывания ложных данных .**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ такое состояние информации, при котором «…отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право».**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ процесс аналитического получения противником открытого текста без предварительного полного знания всех элементов криптографической системы.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ защита данных при помощи криптографического преобразования данных .**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_криптографическое преобразование преобразование данных при помощи шифрования и (или) выработки имитовставки.**

**Установите последовательность шифров и длин ключа:**

|  |  |
| --- | --- |
| 1.DES | А.128/192/256 бит |
| 2.AES | Б.56 бит |
| 3.ГОСТ 28147-89 | В.256 бит |
| 4.3DES | Г.168 бит |

**Установите соответствие:**

|  |  |
| --- | --- |
| 1RSA | А Сложность вычисления дискретных логарифмов в конечном поле |
| 2Эль-Гамаль | Б Сложность разложения произведения двух простых чисел на множители |
| 3ГОСТ Р 34.10-2012 | В Сложность поиска квадратных корней составного числа |
| 4Криптосистема Рабина | Г Сложность вычисления дискретного логарифма в группе точек эллиптической кривой |

**Установите соответствие для алгоритмов и длины хеш-функций:**

|  |  |
| --- | --- |
| 1 MD5 | А 128 |
| 2 SHA1 | Б 256/512 |
| 3 ГОСТ34.11.-2012 | В 160 |
| 4 SHA-512 | Г 512 |

**Установите соответствие между описанием и видом ЭЦП**

|  |  |
| --- | --- |
| 1. Простая электронная подпись | 1. Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. |
| 1. Неквалифицированная электронная подпись | 1. Электронная подпись, которая: получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; создается с использованием средств электронной подписи. |
| 1. Квалифицированная электронная подпись | 1. Электронная подпись, которая: получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; создается с использованием средств электронной подписи; ключ проверки электронной подписи указан в квалифицированном сертификате; для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с  Федеральным законом от 6 апреля 2011 года N 63-ФЗ |

**Установите соответствие:**

|  |  |
| --- | --- |
| 1.Ключ | А Изменяемый элемент (параметр), каждому значению которого однозначно соответствует одно из отображений, реализуемых криптосистемой |
| 3.Пин-Код | Б уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet. |
| 2.Пароль | В Конфиденциальная информация аутентификации, обычно состоящая из строки знаков |
| 4.MAC | Г персональный идентификационный номер |

**Упорядочите пошаговый алгоритм получения электронной цифровой подписи**

1. Выбрать какая электронная подпись (ЭП) вам нужна
2. Выбрать Удостоверяющий центр (УЦ)
3. Заполнить и отправить заявку в УЦ
4. Получить счет на оплату и оплатить его
5. Предоставить в УЦ все необходимые документы (сканы)
6. Приехать в УЦ с оригиналами документов для получения ЭП.

**Установите последовательность действий при подписании документа электронной цифровой подписью**

1. Открытие электронного документа
2. Создание хеш-функции
3. Шифрование хеш-функции закрытым ключом
4. Создание электронной подписи
5. Соединение подписи с документом

**Установите последовательность развития шифров**

1.моноалфавитные шифры

2. полиалфавитне шифры

3. шифры с открытым ключом

4. электромеханические устройства полиалфавитных шифров

5. математические шифры с секретным ключом

**Установите последовательность развития**  **криптографии**

1.Формальная криптография

2.Научная криптография

3. Наивная криптография.

4. Компьютерная криптография

**Установите последовательность шифрования алгоритмом DES:**

* + 1. Шифрованый текст
    2. Исходный текст
    3. Конечная перестановка
    4. Начальная перестановка
    5. Шифрование заменой

**Установите правильный порядок аккредитации УЦ:**

1. Рассмотрение заявления, а также комплектности и содержания документов, представленных УЦ, осуществляется уполномоченным органом в течение 20 календарных дней со дня приема заявления.

2. Уполномоченный орган в срок, не превышающий 10 календарных дней со дня принятия решения об аккредитации, уведомляет УЦ о принятом решении и выдает свидетельство об аккредитации

3. Оформление заключения о возможности/ невозможности предоставления УЦ аккредитации в течении 5 дней.

4. Уполномоченный орган принимает решение в форме издания организационно-распорядительного акта о предоставлении аккредитации и об изготовлении квалифицированного сертификата с использованием средств головного УЦ в течении 5 дней.

**Установите последовательность шифрования алгоритмом AES:**

1.вычисление всех раундовых ключей

2. сдвиг в форме с использованием различающихся величин

3. подстановка байтов с помощью основной таблицы S-Box

4. сложение формы и раундового ключа

5.смешивание данных внутри каждого столбца матрицы (формы)

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

**Наиболее надежным считается построение контролируемой зоны по принципу:**

а) независимые КЗ

б) пересекающиеся КЗ

в) вложенные КЗ

г) комбинированные КЗ

**Под абсолютной системой защиты понимается**

а) система обеспечивающая 100% защиту

б) система, обеспечивающая полную защиту при любых угрозах

в) система способная адаптироваться к новым угрозам

г) система, обеспечивающая максимальную скрытность

**Проявления стихии относятся**

а) угрозам преднамеренных воздействий

б) угрозам утечки информации

в) угрозам случайных воздействий

д) разглашению информации

**Разговоры сотрудников за пределами контролируемой зоны относятся**

а) угрозам преднамеренных воздействий

б) угрозам утечки информации

в) угрозам случайных воздействий

д) разглашению информации

**Надежность системы контроля доступа построена основана на**

а) конфиденциальности PIN-кода

б) уникальности идентификационного номера

в) хранении номера в контроллере

г) установки пароля на карту доступа

**Когда охранники являются лучшим выбором в качестве механизма физического контроля доступа?**

а) когда необходимо принимать обдуманные решения в различных ситуациях

б) когда требуется выявлять вторжения

в) когда бюджет безопасности мал

г) когда внедрены меры контроля доступа

**Электронный ключ Touch memory использует в качестве идентификатора:**

а) комбинацию букв, цифр и символов

б) сгенерированный код

в) уникальную биометрическую характеристику

г) идентификационный номер

**Акустический извещатель предназначен для:**

а) обнаружения разбития окон

б) обнаружения проникновения через двери и окона

в) обнаружения возникновения задымления

г) обнаружения источника ИК излучения

**Важными объектами являются:**

а) помещения для работы с гос. тайной

б) хранилища банков

в) торговые комплексы

г) жилые помещения

**Во внерабочее время должно использоваться освещение**:

а) аварийное

б) тревожное

в) дежурное

г) основное

**Ворота из деревянных конструкций 40мм относятся к:**

а) 3 класс

б) 1класс

в) 2 класс

г) 4 класс

**Для защиты бумажных носителей используют сейф классом:**

а) класс а

б) класс д

в) класс б

г) класс в

**Для защиты окон помещения от наблюдения и взлома используют**:

а) полимерную пленку

б) решетки

в) армированные стекла

г) стеклопакет

**Для защиты территории от проезда транспорта используют:**

а) выдвижные препятствия

б) шлагбаум

в) сигнализацию

г) видеонаблюдение

**Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств?**

а) Контролируемая зона

б) Выделенное помещение

в) Территория

г) Объект

**Для защиты ценных документов необходимо использовать:**

а) шкаф

б) хранилище

в) металлический ящик

г) сейф

**Для защиты электронных носителей используют сейф классом:**

а) класс а

б) класс д

в) класс в

г) класс б

**Для оповещения проникновения на территорию используют:**

а) сигнализацию

б) выдвижные препятствия

в) шлагбаум

г) видеонаблюдение

**Для регистрации событий на территории используют:**

а) шлагбаум

б) сигнализацию

в) выдвижные препятствия

г) видеонаблюдение

**Состояние порта СКУД «нормально открытый» означает**

а) по умолчанию разомкнут

б) по умолчанию «нет доступа»

в) по умолчанию замкнут

г) по умолчанию передает сигнал тревоги, а не включает его в месте своего нахождения

**Идентификатор для обеспечения доступа в системе управления контролем доступа:**

а) сравнивается с эталонной базой значений хэш

б) сравнивается с эталонной базой истинных значений

в) сравнивается с базой разработчика

г) вычисляется из эталонных данных

**Идентификатор Проксимити-карт использует для активации:**

а) электро-магнитное поле

б) магнитное поле

в) электрическое поле

г) ИК-канал

**Как используется протокол запрос/ответ в случае применения токенов?**

а) служба аутентификации генерирует запрос, а токен выполняет проверку и генерирует ответ на основе запроса

б) этот протокол не используется, применяется криптография

в) токен запрашивает у пользователя имя и пароль

г) токен запрашивает пароль пользователя у базы данных, в которой хранятся учетные данные

**Класс прочности ограждения вычисляется:**

а) берется усредненное значение

б) по самому надежному участку

в) по самому слабому участку

г) не имеет значения

**Магнитоконтактный извещатель предназначен для:**

а) обнаружения проникновения через двери и окон

б) обнаружения возникновения задымления

в) обнаружения разбития окон

г) обнаружения источника ИК излучения

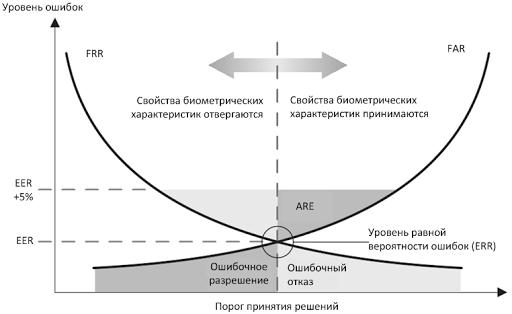
**Металлическое кованное ограждение является защитой от:**

а) наблюдения

б) проникновения

в) подслушивания

г) излучения

**Объяснение какой из приведенных ниже концепций показано на рисунк**е:

а) уровень пересечения вероятности ошибок

б) ошибки третьего рода

в) уровень ошибочных разрешений равен уровню ошибочных отказов в системах, которые имеют высокий уровень пересечения вероятности ошибок

г) биометрия является общепринятой технологией

**Особоважными объектами являются:**

а) правительственные здания

б) кассовые залы банков

в) жилые помещения

г) территории

**Пожарный дымовой извещатель работает в :**

а) Свч-диапазоне

б) ультрафиолетовом диапазоне

в) инфракрасном диапазоне

г) контактный

**При каких условиях безопасность системы является самой эффективной и экономичной?**

а) если она спроектирована и реализована с самого начала разработки системы

б) если она спроектирована и реализована как безопасный и доверенный внещний интерфейс

в) если она специально спроектирована для противодействия определенным видам атак

г) если система была оптимизирована перед добавлением в нее безопасности

**Примером какого типа функций безопасности является просмотр журналов регистрации событий?**

а) служебного расследования

б) сдерживающий (устрашающий)

в) превентивный

г) корректирующий

**Система управления контролем доступа не может быть построена идентификаторе:**

а) проксимити

б) Touch memory

в) ДСЧ

г) биометрическом

**Почему в случае, если безопасность имеет важное значение, следует использовать оптоволоконный кабель?**

а) он обеспечивает мощные функции для выявления и исправления ошибок при передаче данных

б) он обеспечивает более высокую скорость передачи данных и менее подвержен помехам

в) он выполняет мультиплексирование данных, что вызывает сложности у атакующих

г) перехват данных очень сложен

**Убрать лишнее: Приемоконтрольный прибор позволяет:**

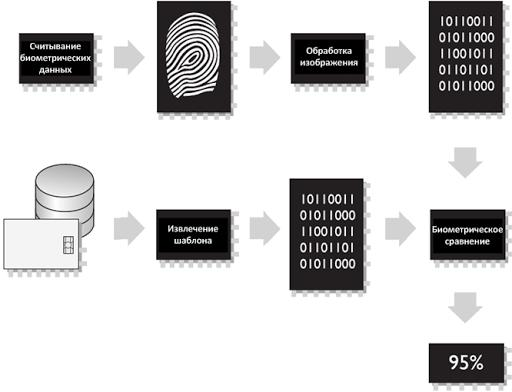
а) отключать РПДИ

б) регистрировать РПДИ

в) удалять РПДИ

г) конфигурировать РПДИ

Что из перечисленного ниже имеет отношение к этому рисунку:



а) уровень авторизации

б) уровень пересечения вероятности ошибок

в) проверка личности

г) уровень ошибок аутентификации

**Что из перечисленного ниже не является задерживающим механизмом?**

а) предупреждающие знаки

б) замки

в) внутренние защитные средства

г) контроль доступа

**Что из перечисленного ниже не относится к логике управления доступом?**

а) идентификационные карты

б) шифрование

в) сетевая архитектура

г) матрица контроля доступа

**Что из приведенного ниже не является правильным утверждением в отношении электростатической системы выявления вторжений?**

а) она может использоваться в качестве системы выявления вторжений для больших областей (помещений)

б) она выявляет уязвимости ПЭМИН

в) она контролирует баланс между электрической емкостью и индуктивностью объекта.

г) она может выявить проникновение нарушителя в определенные границы вокруг объекта

**Что из приведенного ниже является примером защиты от ослепления?**

а) направление света в сторону точек входа и от постов охраны

б) использование объективов с автоматической регулировкой диафрагмы с коротким фокусным расстоянием

в) использование дежурного освещения, которое исходит от камер видеонаблюдения

г) обеспечение использование системой освещения положительного давления

**Что обеспечивает наилучшую аутентификацию?**

а) что человек имеет

б) что человек знает

в) кем человек является

г) что человек имеет и знает

**Что означает аутентификация?**

а) подтверждение прав пользователя

б) авторизация пользователя

в) идентификация пользователя

г) регистрация пользователя

**Что является наиболее частой проблемой с датчиками, выявляющими вибрацию, при их использовании для безопасности периметра?**

а) они вызывают ложные срабатывания

б) они могут быть обезврежены путем направления определенных электрических сигналов в защищаемую область

в) источники энергии для них могут быть легко отключены

г) они создают помехи для компьютерного оборудования

**Что является первым шагом, который нужно предпринять при выявлении пожара?**

а) активировать оповещение о необходимости покинуть здание

б) отключить систему СКУД и активировать открытие пожарных выходов

в) определить тип пожара

г) активировать систему пожаротушения

**Пожарный ИК извещатель предназначен для**:

а) обнаружения разбития окон

б) обнаружения проникновения через двери и окона

в) обнаружения возникновения задымления

г) обнаружения источника ИК излучения

**Пожарный контактный извещатель предназначен для**:

а) обнаружения разбития окон

б) обнаружения проникновения через двери и окона

в) обнаружения возникновения задымления

г) подачи синала тревоги на пост охраны

**Электронный ключ TouchMemory использует для активации**:

а) электро-магнитное поле

б) магнитное поле

в) электрическое поле

г) контактное соединение

**Ключи TouchMemory доступа обеспечивают следующую пропускную способность:**

а) высокую

б) среднюю

в) низкую

г) крайне низкую

**Биометрический доступ обеспечивает следующую пропускную способность:**

а) высокую

б) среднюю

в) низкую

г) крайне низкую

**К способам обеспечения защиты информации по акустическому каналу утечки информации относится:**

а) зашумление

б) фильтрация

в) сканирование

г) экранирование

**К способам обеспечения защиты информации от побочных электромагнитных излучений относится:**

а) зашумление

б) фильтрация

в) сканирование

г) экранирование

**К способам обеспечения защиты информации от побочных электромагнитных наводок относится:**

а) зашумление

б) фильтрация

в) сканирование

г) заземление

**К средствам обеспечения защиты информации по оптическому каналу утечки информации относится:**

а) использование жалюзи

б) звукоизоляция

в) экранирование

г) заземление

**К средствам обеспечения защиты информации по вещественному каналу утечки информации относится:**

а) маркирование

б) звукоизоляция

в) экранирование

г) заземление

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_ - это набор формальных правил, которые регламентируют функционирование механизма информационной безопасности.**

**Процедура проверки подлинности заявленного пользователя – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_- процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий м доступных ресурсов системы (сети).**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_- создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа.**

**Составление списка объектов, которые будут подлежать защите, и субъектов, которые задействованы в данном информационном пространстве, и будут влиять на информационную защиту системы, - это\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Свойство информации, заключающееся в ее существовании в неизменном виде по отношению к некоторому фиксированному состоянию и адекватности (полноты и точности) отображения объекта предметной области независимо от формы представления этой информации, называется \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

**Субъективно определяемое свойство информации, указывающее на необходимость ограничения круга доступа к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней, называется \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

**\_\_\_\_\_\_\_\_\_\_ помещение – это помещение (служебный кабинет, актовый зал, конференц-зал и т.д.), специально предназначенное для проведения секретных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).**

**\_\_\_\_\_\_\_\_\_\_ помещение – это помещение (служебный кабинет, актовый зал, конференц-зал и т.д.), специально предназначенное для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций переговоров и т.п.).**

**\_\_\_\_\_\_\_\_ – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.**

**\_\_\_\_\_\_\_\_ – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.**

**\_\_\_\_\_\_\_\_ – это   слабость актива или управления, эксплуатация которой приведёт к реализации одной или нескольких угроз.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_- это сущность в пределах области действия функции безопасности объекта оценки, которая содержит или получает информацию, и над которой субъекты выполняют операции**

**\_\_\_\_\_\_\_\_ – сотрудник предприятия, который причиняет или планирует причинение ущерба активам организации или помогает в такой акции внешнему нарушителю.**

**Установите соответствие классификации помещений в зависимости от наличия технических средств охраны:**

|  |  |
| --- | --- |
| ***Наименование зоны*** | ***Наличие технических средств охраны*** |
| 1. Зона высшей защиты | 1. Нет |
| 1. Регистрационная зона | 1. Средства наблюдения |
| 1. Зона усиленной защиты | 1. Охранная сигнализация |
| 1. Режимная зона | 1. Охранная сигнализация, система контроля доступа |
| 1. Наблюдаемая зона | 1. Охранная сигнализация, система контроля доступа, технические средства защиты информации |
| 1. Свободная зона | 1. Охранная сигнализация, система контроля доступа, технические средства защиты информации, инженерное усиление |

**Установите соответствие между техническими каналами утечки информации и средствами получения информации:**

1 Акустический ТКУИ а. Стетоскоп

2 Оптический ТКУИ б. тепловизор

3 Радиоэлектронный ТКУИ в. кейлоггер

4 Вещественный ТКУИ г.отходы делопроизводства

**Установите соответствие классификации помещений в зависимости от условий доступа сотрудников (к одному условию может быть отнесено несколько зон)**

|  |  |
| --- | --- |
| *Наименование зоны* | *Условия доступа сотрудников* |
| 1. Зона высшей защиты | 1. Свободный |
| 1. Регистрационная зона |
| 1. Зона усиленной защиты | 1. По спецпропускам |
| 1. Режимная зона |
| 1. Наблюдаемая зона | 1. По служебным удостоверениям или идентификационным картам |
| 1. Свободная зона |

**Установите соответствие классификации охраняемых объектов по типу охраны**

|  |  |
| --- | --- |
| 1. Объекты с простым типом охраны | 1. Для патрулирования объекта используется автотранспорт, охранники экипированы огнестрельным оружием и специальными средствами, используют собак, наиболее значимые помещения оборудованы средствами видеоконтроля территории объекта |
| 1. Объекты с комбинированным типом охраны | 1. Путем периодического обхода охраняемой территории без использования огнестрельного оружия и специальных средств |
| 1. Объекты с усложненным типом охраны | 1. Сотрудники используют специальные средства и служебных собак, часть помещений на охраняемом объекте выведа на пульт централизованного наблюдения |

**Установите соответствие между содержанием мероприятия и его названием**

|  |  |
| --- | --- |
| 1. Спецпроверка | 1. Выявление электронных устройств, предназначенных для негласного получения сведений в технических средствах, обрабатывающих конфиденциальные данные |
| 1. Специсследование | 1. Использование контрольно-измерительной аппаратуры по выявлению возможных технических каналов утечки конфиденциальных сведений |
| 1. Спецобследование | 1. Проведение работ по выявлению электронных устройств, предназначенных для негласного получения сведений в помещениях, где циркулирует конфиденциальная информация |

**Упорядочите распределение утечек по каналам от большего к меньшему**

1. Сеть (браузер, Cloud)
2. Электронная почта
3. Бумажные документы
4. Кража/потеря оборудования

**Упорядочить этапы проведения специальной проверки технических средств:**

1 прием-передача технического средства, формирование исходных данных для составления программы проведения специальной проверки

2 разработка программы проведения специальной проверки технического средства

3 анализ результатов специальной проверки, оформление отчетных документов

1. проведение технических проверок

**Установите последовательность разработки системы защиты:**

1.Определение границ управления информационной безопасностью объекта;

2.Анализ уязвимости;

3.Выбор контрмер, обеспечивающих информационную безопасность; 4.Определение политики информационной безопасности;

5.Проверка системы защиты;

6.Составление плана защиты;

7.Реализация плана защиты

**Упорядочить содержание мероприятий на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе**

1Организация работ по защите информации в ходе создания и эксплуатации объектов информатизации и их систем защиты информации

2Содержание аналитического обоснования необходимости создания системы защиты информации

3Содержание технического задания на разработку системы защиты информации

4Содержание работ на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе

5Выполняемые работы на предпроектной стадии по обследованию объекта информатизации

**Упорядочить стадии создания системы защиты информации:**

1. Стадия проектирования (разработки проектов), включает разработку системы защиты информации в составе объекта информатизации;

2. Предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания системы защиты информации и технического (частного технического) задания на ее создание;

3. Стадия ввода в действие системы защиты информации, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствующие требования безопасности информации.

**Упорядочить работы на предпроектной стадии по обследованию объекта информатизации**

1.Определяется перечень сведений конфиденциального характера подлежащих защите;

2.Определяется класс защищенности в автоматизированной системе;

3.Определяются мероприятия по обеспечению конфиденциальности информации на этапе проектирования объекта информатизации.

4. Определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта;

5. Определяются технические средства и системы, предполагаемые к использованию в разработанной автоматизированной системе и в системах связи, темные и прикладные программы средств, имеющиеся на рынке и предполагаемые к разработке;

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

**На программу за последнее время несколько раз устанавливались патчи, но недавно ее основной исполняемый файл был заражен опасным вирусом. Антивирусная программа сообщает, что лечение зараженного файла приведет к его повреждению. Какое действие является наиболее правильным в этом случае?**

а) восстановить с резервной копии незараженную версию файла с установленными патчами

б) выполнить лечение файла и обратиться к производителю для его восстановления

в) сделать резервную копию и затем выполнить лечение файла

г) заменить файл на его копию, сделанную вчера

**Причина макро-вирусы так распространены?**

а) язык, на котором пишутся макросы, очень прост в использовании

б) они быстро распространяются

в) они могут заражать любую платформу

г) они активируются по событиям, обычно происходящим на любой системе

**При использовании дискреционного управления доступом, кто имеет полномочия предоставления прав доступа к данным**?

а) владелец

б) пользователь

в) администратор безопасности

г) политика безопасности

**Системы, построенные на основе модели OSI, считаются открытыми системами.** Что это означает?

а) они построены с использованием принятых на международном уровне протоколов и стандартов, поэтому они могут легко взаимодействовать с другими открытыми системами

б) по умолчанию в них не настроен механизм аутентификации

в) они имеют проблемы совместимости

г) они построены с использованием принятых на международном уровне протоколов и стандартов, поэтому при их использовании можно выбирать, с какими типами систем они будут взаимодействовать

**Что из перечисленного ниже должно сделать веб-приложение при выявлении неправильной транзакции?**

а) создать контрольную точку

б) выполнить откат и восстановить первоначальные данные

в) прервать выполнение транзакций, пока неправильная транзакция не будет исправлена

г) сформировать отчет об ошибке

**Что из перечисленного ниже лучше всего описывает логическую бомбу?**

а) она выполняет какое-либо действие при наступлении определенных условий

б) она используется для перемещения информационных активов с одного компьютера на другой

в) она может самостоятельно «размножаться»

г) она выполняет как полезные действия, так и вредоносные

**Что из перечисленного ниже является наилучшим описанием протокола IP?**

а) протокол с предварительным установлением соединения, который обеспечивает адресацию и маршрутизацию пакетов

б) протокол без предварительного установления соединения, который обеспечивает установление, поддержку и уничтожение диалога (сеанса)

в) протокол без предварительного установления соединения, который обеспечивает адресацию и маршрутизацию пакетов

г) протокол с предварительным установлением соединения, который упорядочивание пакетов, выявление ошибок и управление потоком

**Что из приведенного ниже соответствует последовательности уровней 2, 5, 7, 4 и 3?**

а) канальный, сеансовый, прикладной, транспортный и сетевой

б) канальный, транспортный, прикладной, сеансовый и сетевой

в) сетевой, сеансовый, прикладной, сетевой и транспортный

г) сетевой, транспортный, прикладной, сеансовый и представительский

**Что происходит на сеансовом уровне?**

а) управление диалогом (сеансом)

б) маршрутизация

в) упорядочивание пакетов

г) адресация

**Что такое процедура?**

а) пошаговая инструкция по выполнению задачи

б) правила использования программного и аппаратного обеспечения в компании

в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) обязательные действия

**Для чего используется Nmap?**

а) исследования безопасности сети

б) подключение к сети

в) облегчения поиска

г) управления системой

**Для чего используется сниффер?**

а) исследования безопасности сети

б) подключение к сети

в) перехват пакетов в сети

г) управления системой

**Тип атаки с применением сниффера?**

а) пассивная, прослушивание сети

б) активная, переполнение буфера

в) активная, использование спецпрограмм

г) активная, сетевая разведка

**Что необходимо сделать перед установкой обновления ОС?**

а) выполнить резервное копирование служебной информации

б) создать дубликат жесткого диска

в) создать контрольную точку восстановления

г) выполнить резервное копирование пользовательской информации

**Что такое логический порт?**

а) логический адрес для идентификации процесса

б) IP-адрес

в) МАС-адрес

г) разъем

**Что такое служба?**

а) протокол

б) процесс клиент-сервер

в)приложение запускаемые системой вне зависимости от статуса пользователя

г) поток данных

**Для хранения Файлов, предназначенных для общего доступа пользователей сети, используется …**

а) файл-сервер

б) клиент-сервер

в) рабочая станция

г) коммутатор

**Транспортный протокол (TCP) обеспечивает …**

а) разбиение файлов на IP- пакеты в процессе передачи и сборку Файлов в процессе получения

б) прием, передачу и выдачу одного сеанса связи

в) предоставление в распоряжение пользователя уже переработанную информацию

г) доставку информации от компьютера-отправителя к компьютеру-получателю

**Конфигурация (топология) локальной компьютерной сети, в которой все рабочие станции соединены с Файл-сервером, называется …**

а) шинной

б) кольцевой

в) радиальной (звездообразной)

г) древовидной

**Скорость передачи данных по каналу связи измеряется количеством передаваемых..?**

а) битов информации в секунду

б) байтов в минуту

в) слов в минуту

г) символов в секунду

**В модели OSI все сетевые функции разделены на … уровней.**

а) 5

б) 7

в) 6

г) 8

**Сетевой протокол – это …**

а) набор соглашений о взаимодействиях в компьютерной сети

б) последовательная запись событий, происходящих в компьютерной сети

в) правила интерпретации данных, передаваемых по сети

г) согласование различных процессов во времени

**Эталонная модель обмена информацией открытой системы получила название модели …**

а) OSI

б) ISO

в) OIS

г) SIO

**Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)**

а) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения

б) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

г) МЭ работают только на прикладном, сетевом, канальном уровне, а СОВ – еще и на физическом

**Сервис безопасности:**

а) регулирование конфликтов

б) инверсия паролей

в) идентификация и аутентификация

г) кэширование записей

**Наиболее эффективное средство для защиты от сетевых атак**

а) посещение только «надёжных» Интернет-

б) использование антивирусных программ

в) узлов использование сетевых экранов или «firewall»

г) использование только сертифицированных программ-броузеров при доступе к сети Интернет

**Деятельность клавиатурных шпионов**

а) находясь в оперативной памяти записывают все, что пользователь вводит с клавиатуры и передают своему хозяину

б) находясь в оперативной памяти следят за вводимой информацией. Как только пользователь вводит некое кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором

в) находясь в оперативной памяти следят за вводимой пользователем информацией и по команде хозяина производят нужную ему замену одних символов (или групп символов) другими

г) передают хозяину марку и тип используемой пользователем клавиатуры

**Для чего используется пароль?**

а) аутентификация

б) идентификация

в) регистрация

г) авторизация

**Для чего предназначен канальный уровень?**

а) кадрирование

б) «сквозное» (end-to-end) соединение

в) управление диалогом (сеансом)

г) синтаксис данных

**Для чего предназначен представительский уровень?**

а) синтаксис и форматирование данных

б) адресация и маршрутизация

в) «сквозное» (end-to-end) соединение

г) кадрирование

**Если в системе происходит сбой, что позволяет начать обработку с момента, предшествующего сбою?**

а) контрольная точка

б) словарь данных

в) метаданные

г) инструмент интеллектуального анализа данных (data-mining)

**Если операционная система позволяет следующему субъекту использовать некий объект без его предварительной надежной очистки, какую проблему безопасности это вызывает?**

а) раскрытие остаточных данных

б) несанкционированный доступ к привилегированным процессам

в) утечка данных по скрытым каналам

г) компрометация домена выполнения

**Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?**

а) улучшить контроль за безопасностью этой информации

б) снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

г) снизить уровень классификации этой информации

**Зачем для автоматизации анализа журналов регистрации событий безопасности применяются экспертные системы?**

а) для выявления вторжений

б) для предотвращения вторжений

в) чтобы убедиться, что используется наилучший метод доступа

г) чтобы собрать статистику отклонений от базового уровня

**Кто перехватывает вводимые пользователем пароли и отправляет их по некоторому адресу?**

а) троянская программа

б) вирус

в) червь

г) логическая бомба

**Изолированная среда обеспечивает**

а) доступность системы

б) конфиденциальность данных

в) целостность данных

г) работоспособность системы

**Как работает инкапсуляция данных и стек протоколов?**

а) каждый протокол или сервис на каждом уровне модели OSI добавляет собственную информацию к данным по мере их перемещения вниз по стеку протоколов

б) пакет инкапсулирован и растет по мере прохождения от одного маршрутизатора к другому

в) пакет инкапсулирован и растет по мере прохождения вверх по стеку протоколов

**Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?**

а) сотрудники

б) хакеры

в) атакующие

г) контрагенты (лица, работающие по договору)

**Какая модель реализует матрицы контроля доступа для управления взаимодействием субъектов с объектами**

а) мандатная

б) дискреционная

в) централизованная

г) децентрализованная

**Какая модель управления доступом является групповой?**

а) ролевая

б) мандатная

в) на основе идентификации

г) дискреционная

**Какая модель управления доступом является полномочной** ?

а) на основе идентификации

б) ролевая

в) мандатная

г) дискреционная

**Какое преимущество с точки зрения безопасности имеют прошивки над обычным программным обеспечением?**

а) их трудно изменить без физического доступа

б) они требуют меньше памяти

в) они не нужны для реализации политики безопасности

г) их проще перепрограммировать

**Какой вид вредоносного программного обеспечения «размножается» с использованием ресурсов зараженной системы?**

а) червь

б) вирус

в) троянская программа

г) составной вирус

**Какой из перечисленных ниже видов вредоносного программного обеспечения «размножается», добавляя свой код к другим программам?**

а) троянская программа

б) червь

в) вирус

г) любой вредоносный код

**Какой тип атаки пытается перебрать все возможные варианты?**

а) брутфорс

б) по словарю

в) человек-по-середине

г) спуфинг

**Цель полного перебора комбинаций «brute forse attacks»**

а) блокирование трафика

б) подбор пароля

в) доступ к сетевым ресурсам

г) изменение данных

**Указать верную последовательность стадии жизненного цикла компьютерного вируса**

а) открытие исполняемого файла

б) анализ заголовков на корректность

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

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

д) инициализация стека и формирование начального заполнения регистров процессора

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

д) передача управления по адресу первой инструкции исполняемого файла

**Постоянное наблюдение за объектами и субъектами, влияющими на безопасность информационную организации, а также сбор, анализ и обобщение результатов наблюдений – это\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1 Мониторинг

2Нотаризация

3Туннелирование

4Перехват

[**Компьютерная сеть**](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C)**, состоящая из некоторого количества**[**хостов**](http://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82)**, обычно используется для нелегальной или неодобряемой деятельности — рассылки**[**спама**](http://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B0%D0%BC)**, перебора**[**паролей**](http://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C)**на удалённой системе, атак на**[**отказ в обслуживании**](http://ru.wikipedia.org/wiki/DDoS)

а) руткит

б) ботнет

в) бекдор

г) кейлоггер

**Упорядочить уровни модели OSI начиная с верхнего:**

а) прикладной

б) сеансовый

в) канальный

г) транспортный

д) сетевой

е) представительный

ж) физический

Установите соответствие между видом протокола и уровнем модели OSI

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Протокол | |  | Уровень модели OSI | |
| 1. | FTP |  | А | Канальный |
| 2. | TCP | Б | Транспортный |
| 3. | IP | В | Прикладной |
| 4. | Ethernet | Г | Сетевой |

**Процесс сравнения двух уровней спецификации средств вычислительной техники или систем автоматизированных на надлежащее соответствие – это\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Под угрозой удаленного администрирования в компьютерной сети понимается угроза\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_ в аппаратном обеспечении - это устройство, выполняющее некоторые недокументированные функции, обычно в ущерб пользователю данной информационной системы.**

**\_\_\_\_\_\_\_\_\_\_\_ - это программа, перехватывающая пакеты, поступающие к данной станции, в том числе и те, которые станция при нормальной работе должна проигнорировать.**

**Компьютерный вирус, скрывающийся под видом добропорядочной программы\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Использование брандмауэров относят к \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ методам антивирусной защиты.**

**Установите соответствие:**

|  |  |
| --- | --- |
| 1.Червь | А.программа, которая делает копии самой себя |
| 2.Межсетево́й экра́н, | Б. программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами |
| 3.VPN | Г. разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно. |
| 4.Троя́нская программа | В. обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети |

**Установите соответствие между классификацией компьютерных вирусов и их описанием:**

|  |  |
| --- | --- |
| 1. файловые вирусы; | а) заражают файлы-документы и электронные таблицы популярных офисных приложений; |
| 2. загрузочные вирусы; | б) внедряются в выполняемые файлы, либо создают файлы; |
| 3. макровирусы. | в) записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик жесткого диска, либо меняют указатель на активный boot-сектор. |

**Установите соответствие между классификацией компьютерных вирусов и их описанием:**

|  |  |
| --- | --- |
| 1. Резидентные; | 1. Полностью или частично скрывают себя в системе. Наиболее распространенным примером вирусов является перехват запросов операционной системы на чтение/запись зараженных объектов; |
| 1. Полиморфик-вирусы; | 1. Оставляют в оперативной памяти ПК свою некую часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них; |
| 1. Стелс-вирусы. | 1. Достаточно труднообнаружимые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. |

**Установите соответствие между автоматизированной системой и классом защищенности от несанкционированного доступа**

|  |  |
| --- | --- |
| 1Б | Многопользовательские автоматизированные системы с разными правами доступа, обрабатывающие государственную тайну категории «совершенно секретно» |
| 1Г | Многопользовательские автоматизированные системы с разными правами доступа, обрабатывающие конфиденциальную информацию |
| 2А | Многопользовательские автоматизированные системы с равными правами доступа, обрабатывающие государственную тайну |
| 3Б | Однопользовательские автоматизированные системы, обрабатывающие конфиденциальную информацию |

**Установите соответствие между информационной системой и типом угроз**

|  |  |
| --- | --- |
| 1 Угрозы 1-го типа | А Информационная система, для которой актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе |
| 2 Угрозы 2-го типа | Б Информационная система, для которой актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе |
| 3 Угрозы 3-го типа | В Информационная система, для которой актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе. |

**Установите правильную последовательность действий, раскрывающую аутентификацию пользователей на основе функционального метода парольной защиты:**

1. пользователь вычисляет результат функции y=f(x) и возвращает его в систему.
2. при входе в АС подсистема аутентификации генерирует случайную последовательность x, которая передается пользователю.
3. при совпадении указанных результатов подлинность пользователя считается доказанной;
4. система сравнивает собственный вычисленный результат с полученным от пользователя.

**Установите правильную последовательность действий, раскрывающую процедуру аутентификации пользователя (П) при входе в компьютерную систему (С):**

1. П: ввод логического имени (ID);
2. П: ввод идентифицирующей информации;
3. С: проверка наличия ID в регистрационной базе данных. Если пользователь с таким именем зарегистрирован, то запрос его идентифицирующей информации;
4. С: запрос имени, под которым пользователь зарегистрирован в базе данных учетных записей КС (логического имени пользователя или так называемого логина);
5. С: допуск пользователя к работе в КС;
6. С: проверка совпадения Р с идентифицирующей информацией для пользователя ID в регистрационной базе данных

**Установите последовательность событий при входе пользователя в компьютерную систему**

1. Идентификация
2. Аутентификация
3. Авторизация

**Установите последовательность мероприятий для обеспечения защиты информации, содержащейся в информационной системе**

а. Формирование требований к защите информации, содержащейся в информационной системе

б. Разработка системы защиты информации информационной системы

в. Внедрение системы защиты информации информационной системы

г. Аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие

д. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

е. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации

**Расположите нарушителей по уровню возрастания возможностей, предоставляемых им штатными средствами АС и СВТ**

* 1. Запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации
  2. Возможность создания и запуска собственных программ с новыми функциями по обработке информации
  3. Возможность управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования
  4. Весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации

**Установите последовательность загрузки компьютера с установленным АПМДЗ:**

1 Загрузка BIOS

2Загрузка КриптоBIOS

3 Аутентификация АПМДЗ

4 Зарузка ОС

**10. Обеспечение организации системы безопасности организации/Правовая защита информации/**

**Организационное и правовое обеспечение информационной безопасности/Организационно-правовое обеспечение информационной безопасности**

**Что понимают под термином «политика безопасности»?**

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

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

в) специфические потребности организации

г) деятельность в компьютерной информационной системе организации

**Что предписывают процедуры безопасности?**

а) устанавливают доступ к активам и приложениям

б) определяют конкретные задачи безопасности

в) определяют ответственных лиц

г) описывают роли и обязанности ответственных лиц

**Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ – это\_\_\_\_\_\_\_**

а) Лицензирование

б) Сертификация

в) Аккредитация

г) Апробация

**Область применения политики безопасности включает**

а) аппаратные ресурсы предприятия

б) программные ресурсы предприятия

в) информационные ресурсы предприятия

г) все ресурсы, входящие в локальную сеть предприятия

**Санкции за нарушение политики безопасности**

а) штраф

б) выговор

в) понижение в должности

г) санкции вплоть до увольнения

**Количество уровней политики безопасности**

а) 2

б) 3

в) 4

г) 5

**Верхний уровень политики безопасности определяет**

а) решения затрагивающие организацию целиком

б) решения, касающиеся отдельных аспектов информационной безопасности, но важных для различных систем

в) решения связанные с конкретными сервисами

г) решения связанные с конкретными ролями

**К верхнему уровню политики безопасности относится**

а) формулировка целей, которые преследует организация в области информационной безопасности

б) позиция организации в отношении к доступу в Интернет

в) вопросы прав доступа к объектам поддерживаемые сервисом

г) условия чтения и модификации данных

**К среднему уровню политики безопасности относится**

а) формирование или пересмотр комплексной программы обеспечения информационной безопасности

б) общее описание запрещенных действий и наказаний за них

в) кто имеет право на доступ к объектам, поддерживаемым сервисом

г) формулировку управленческих решений по вопросам реализации программы безопасности

**К нижнему уровню политики безопасности относится**

а) формирование или пересмотр комплексной программы обеспечения информационной безопасности

б) общее описание запрещенных действий и наказаний за них

в) вопросы организации удаленного доступа к сервису

г) формулировка целей, которые преследует организация в области информационной безопасности

**Расставить по порядку цели программы реализации политики безопасности**

а) управление рисками

б) координация, деятельность в области информационной безопасности, пополнение и распределение ресурсов

в) стратегическое планирование

г) контроль деятельности в области ИБ

**Расставить по порядку жизненный цикл информационного сервиса программы безопасности**

а) эксплуатация

б) закупка

в) инициация;

г) установка

д) выведение из эксплуатации

**Интересы в информационной сфере Российской Федерации определяются сбалансированностью интересов**

а) личности, общества, государства

б) граждан, партий, государства

в) лиц, объединений, страны

г) людей, сообществ, страны

**Интересы общества в информационной сфере**

а) обеспечении интересов государства, упрочнении демократии, создании правового социального государства

б) обеспечении интересов личности, на использование информации в интересах осуществления не запрещенной законом деятельности

в) обеспечении суверенитета и территориальной целостности

г) обеспечении интересов личности, упрочнении демократии, создании правового социального государства

**Интересы государства в информационной сфере заключаются в**

а) обеспечении суверенитета, территориальной целостности России, политической, экономической и социальной стабильности

б) обеспечении монополизации информационного рынка России отечественными информационными средствами

в) вытеснении с отечественного рынка импортных средств информатизации, телекоммуникации и связи

г) формировании военной доктрины государства

**Доктрина ИБ РФ служит для**

а) формирования государственной политики в информационной сфере

б) обострения международной конкуренции в информационной сфере

в) разработки политики информационной войны в информационной сфере

г) обеспечении монополизации информационного рынка России

**Сколько составляющих национальных интересов в информационной сфере выделено в доктрине ИБ**

а) 3

б) 4

в) 5

г) 6

д) 8

**Информация это**

а) сведения независимо от формы их представления

б) данные в цифровой форме представления

в) сообщения средств массовой информации

г) отражение окружающего мира в виде сигналов и знаков

**Деятельность иностранных военных, разведывательных структур в области информационных технологий относится к**

а) внутренним источникам угроз

б) внешним источникам угроз

в) криминогенных угроз безопасности

г) антропогенным источникам угроз

**Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?**

а) актуальные и адекватные политики и процедуры безопасности

б) эффективные защитные меры и методы их внедрения

в) поддержка высшего руководства

г) проведение тренингов по безопасности для всех сотрудников

**Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?**

а) когда стоимость контрмер превышает ценность актива и потенциальные потери

б) никогда, для обеспечения хорошей безопасности нужно учитывать и снижать все риски

в) когда риски не могут быть приняты во внимание по политическим соображениям

г) когда необходимые защитные меры слишком сложны

**Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?**

а) руководство

б) владельцы данных

г) пользователи

д) администраторы

**Кто является основным ответственным за определение уровня классификации информации?**

а) высшее руководство

б) руководитель среднего звена

в) владелец

г) пользователь

Что (или кто) определяет, какую модель управления доступом следует использовать компании – дискреционную, мандатную или недискреционную?

а) политика безопасности

б) администратор

в) культура

г) уровень безопасности

**Что из перечисленного ниже лучше всего описывает то, что дает компаниям ролевое управление доступом в части снижения административных расходов?**

а) членство пользователей в ролях может быть легко отменено, новые пользователи включаются в соответствующие роли при назначении на работу

б) позволяет принимать решения о том, кто может и кто не может иметь доступ к ресурсам тем людям, которые лучше всего знают эти ресурсы

в) обеспечивает централизованный подход к управлению доступом, что освобождает от обязательств руководителей подразделений

г) обеспечивает реализацию политик безопасности, стандартов и руководств на уровне всей компании

**Что самое главное должно продумать руководство при классификации данных?**

а) оценить уровень риска и отменить контрмеры

б) типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

в) необходимый уровень доступности, целостности и конфиденциальности

г) управление доступом, которое должно защищать данные

**Что является заключительным шагом разрешения использования системы в конкретной среде?**

а) аккредитация

б) сертификация

в) оценка безопасности и присвоение рейтинга

г) проверка

**Что является заключительным этапом жизненного цикла процесса разработки системы?**

а) тестирование модулей

б) сертификация

в) аккредитация

г) разработка

**Экспертная система использует все перечисленные элементы, за исключением**

а) механизм циклических рассуждений

б) автоматическая логическая обработка

в) общие методы поиска решений проблем

г) механизм логических выводов

**Лицензирование это -**

а) подтверждение соответствия продукции или услуг установленным требованиям и

стандартам

б) процесс передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ

в) подтверждение подлинности отправителя и получателя информации

г) средство защиты информации от несанкционированного доступа

**Сертификация**

а) основывается на Законе РФ "О государственной тайне"

б) регулируется секретными нормативными документами

в) это подтверждение соответствия продукции или услуг установленным требованиям или стандартам

г) осуществляется в соответствии с остальными пунктами

**Документ, дающий право на осуществление указанного вида деятельности в течении определенного времени называется**

а) сертификатом

б) свидетельством

в) лицензией

г) аттестатом

**Сертификат на средство защиты информации**

а) подтверждает подлинность передаваемых документов

б) дает право на пользование данным средством

в) это документ, подтверждающий соответствие средства требованиям по безопасности информации

г) выдается пользователям сети Интернет

**К лицензируемым видам деятельности относится разработка, производство, реализация и сервисное обслуживание**

а) шифровальных и специальных технических средств

б) защищенных систем телекоммуникаций

в) программных средств защиты информации

г) всех перечисленных средств

**Перечень видов деятельности в области защиты информации, на которые выдаются лицензии, определен**

а) нормативными документами ФСБ

б) ФЗ№99 "О лицензировании отдельных видов деятельности"

в) Указом Президента РФ N334 от 03.04.95г.

г) Законом "Об информации..."

**Вопросы лицензирования в области защиты информации регулируются**

а) Законом "О государственной тайне"

б) ПП № 333 "О лицензировании деятельности предприятий..."

в) ФЗ№99 "О лицензировании отдельных видов деятельности"

г) всеми перечисленными документами

**К законодательной базе лицензирования и сертификации в РФ не относится Закон**

а) "О сертификации продукции и услуг"

б) "О стандартизации"

в) "О защите прав потребителей"

г) "О лицензировании деятельности предприятий"

**Заниматься лицензированием и сертификацией в РФ в области защиты информации поручено**

а) МВД

б) СВР

в) ФСБ и ФСТЭК

г) организациям, перечисленным в остальных пунктах

**Органами, уполномоченными на ведение лицензионной деятельности, являются**

а) ФСБ

б) Служба внешней разведки

в) ФСТЭК

г) службы, перечисленные в остальных пунктах

**Продление срока действия лицензии проводится**

а) в порядке, установленном для ее переоформления

б) руководством ФСБ или ФСТЭК

в) после оплаты госпошлины

г) автоматически, при отсутствии нарушений

**Что является правовой основой лицензирования и сертификации в РФ**?

а) международные конвенции по охране интеллектуальной собственности

б) выдача лицензий и сертификатов

в) совокупность нормативно-правовых актов в этой области

г) все, перечисленное в остальных пунктах

**Лицензирование в области защиты информации является**

а) желательным

б) обязательным только для физических лиц

в) не обязательным для государственных предприятий

г) обязательным

**Лицензия разрешает осуществлять конкретный вид деятельности**

а) в течении установленного срока

б) на всей территории РФ

в) в учреждениях РФ, находящихся за рубежом

г) в соответствии с остальными пунктами

**Нормы, устанавливающие порядок организации и осуществления деятельности по защите ГТ**

а) определяются руководством предприятия

б) даны в ГК РФ

в) определяются Законом "О государственной тайне"

г) изложены в нормативных документах ФСТЭК

**Для получения лицензии требуется**

а) аттестация руководителя предприятия

б) специальная экспертиза заявителя

в) регистрация предприятия на территории РФ

г) все, перечисленное в остальных пунктах

**Национальный орган по сертификации России**

а) ФСТЭК

б) СВР

в) ФСБ

г) определяется Правительством РФ

**Срок действия лицензии в области защиты информации**

а) зависит от вида деятельности

б) не может быть менее 3-х лет

в) не превышает 5-и лет

г) бессрочно

**Сертификат в области защиты информации выдается на**

а) 3 года

б) 7 лет

в) срок до 5 лет

г) неограниченное время

**Основанием для отказа в выдаче лицензии является**

а) наличие в документах, представленных заявителем, недостоверной информации

б) отрицательное заключение экспертизы

в) отрицательное заключение государственной аттестации руководителя

предприятия

г) все, вышеперечисленное в остальных пунктах

**Национальная экономическая безопасность – это**

а) состояние экономики и институтов власти, при котором обеспечивается гарантированная защита национальных интересов, гармоничное, социально направленное развитие страны в целом, достаточный экономический и оборонный потенциал даже при наиболее неблагоприятных вариантах развития внутренних и внешних процессов

б) защищенность экономических отношений, определяющих прогрессивное развитие экономического потенциала страны и обеспечивающих повышение уровня благосостояния всех членов общества, его отдельных социальных групп и формирующих основы обороноспособности страны от опасностей и угроз.

в) комплекс международных условий сосуществования договоренностей и институциональных структур, при котором каждому государству – члену мирового сообщества, обеспечивается возможность свободно избирать и осуществлять свою стратегию социального и экономического развития, не подвергаясь внешнему и политическому давлению и рассчитывая на невмешательство, понимание и взаимоприемлемое и взаимовыгодное сотрудничество со стороны остальных государств

**Основным ответственным лицом за определение уровня классификации информации является \_\_\_\_\_\_\_\_\_\_\_\_.**

**Интересы \_\_\_\_\_\_\_\_\_ состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России в политической, экономической и социальной стабильности, безусловном обеспечении законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества**

**Действия третьей стороны, цель которых подтвердить (с помощью сертификата соответствия) то, что изделие (в том числе программное средство) или услуга соответствует определенным стандартам или другим нормативным документам – это\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Эффективная программа безопасности требует сбалансированного применения организационных и \_\_\_\_\_\_\_\_\_\_\_\_ методов.**

**Субъект персональных данных может отозвать свое согласие на обработку \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_.**

**Концепция защиты информации, циркулирующая в помещениях или технических системах коммерческого объекта, требует не периодического, а \_\_\_\_\_\_\_\_\_\_\_\_ контроля в зоне расположения объекта.**

**Установите соответствие между ролями обязанностями, определяемыми в политике безопасности**

|  |  |
| --- | --- |
| Роль | Обязанность |
| 1. Руководитель подразделения | А Доведение положений политики безопасности до пользователей и за контакты с ними |
| 2. Администраторы локальной сети | Б Обеспечение непрерывного функционирования сети и реализация технических мер безопасности |
| 3. Администраторы сервисов | В Выполнение правил и процедур политики безопасности |
| 4. Пользователи | Г Построение защиты в соответствии с общей политикой безопасности |

**Установите соответствие:**

|  |  |
| --- | --- |
| 1.Аудит | А Объединение нескольких рисков в один риск, направленное на более глубокое понимание совокупного риска. |
| 2.Аттестация | Б Проверка, выполняемая компетентным органом (лицом) с целью обеспечения независимой оценки степени соответствия программных продуктов или процессов установленным требованиям |
| 3.Аккредитация | В Официальное признание правомочий осуществлять какую-либо деятельность. |
| 4 Агрегирование | Г Подтверждение экспертизой и представлением объективных доказательств того, что конкретные требования к конкретным объектам полностью реализованы. |

**Установите соответствие между названием закона, номером и датой его принятия**

|  |  |
| --- | --- |
| 1. 152-ФЗ от 27 июля 2006 | 1. "О персональных данных" |
| 1. 149-ФЗ от 27 июля 2006 | 1. "Об информации, информационных технологиях и о защите информации" |
| 1. 99-ФЗ от 04 мая 2011 | 1. "О лицензировании отдельных видов деятельности" |
| 1. [5485-1 от 21 июля 1993 г.](https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/107-zakony/362-zakon-rossijskoj-federatsii-ot-21-iyunya-1993-g-n-5485-1) | 1. "О государственной тайне" |

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

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

**Установите соответствие между содержанием понятия и его названием**

|  |  |
| --- | --- |
| 1. Лицензирование | 1. Получение специального разрешения на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности |
| 1. Аккредитация | 1. Официальное признание компетентности физического или юридического лица выполнять работы в определенной области |
| 1. Сертификация | 1. Подтверждение соответствия объектов требованиям технических регламентов, документам по стандартизации или условиям договоров |
| 1. Нотификация | 1. Уведомлением изготовителя о технических и криптографических характеристиках товара, являющегося шифровальным (криптографическим) средством |
| 1. Нострификация |  |

**Установите соответствие между содержанием действия и его названием**

|  |  |
| --- | --- |
| 1. Распространение | 1. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц |
| 1. Предоставление | 1. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц |
| 1. Обработка | 1. Любое действие (операция) совершаемое с использованием средств автоматизации с персональными данными |
| 1. Обработка | 1. Совокупность действий, совершаемых без использования средств автоматизации с персональными данными |
| 1. Обезличивание | 1. Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных |
| 1. Блокирование |  |

**Установите соответствие между содержанием лицензии и органом, выдающим лицензию**

|  |  |
| --- | --- |
| 1. Роскомнадзор | 1. Лицензирование деятельности в области телевизионного вещания и радиовещания; в области оказания услуг связи |
| 1. ФСБ | 1. Лицензирование деятельности, связанной с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну |
| 1. ФСБ | 1. Лицензирование деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации |
| 1. ФСТЭК | 1. Лицензирование деятельности по технической защите конфиденциальной информации |
| 1. ФСО |  |

**Установите правильный порядок засекречивания информации, составляющей государственную тайну (ГТ):**

а) правительство вносит предложение о Перечне должностных лиц органов государственной власти и управле¬ния, наделенных полномочиями по отнесению сведений к ГТ;

б) правительство разрабатывает Правила отнесения сведе¬ний, составляющих ГТ, к различным степеням секретности;

в) закон определяет категории сведений, отнесенных к ГТ;

г) руководители ведомств на основании соответствующих документов издают приказы, вводящие в действие и детализирующие в перечни засекречиваемых сведений;

д) межведомственная комиссия по защите государственной тайны разрабатывает Перечень сведений, отнесенных к ГТ;

е) руководители органов власти и управления, наделенные соответствующими полномочиями по засекречиванию информации, осуществляют политику государства в области защиты информации;

ж) президент РФ утверждает Перечень сведений, отнесенных к ГТ и Перечень должностных лиц органов государственной власти и управле-ния, наделенных полномочиями по отнесению сведений к государствен-ной тайне.

**Установите правильную последовательность комплекса мероприятий, проводимых на предприятии по определению сведений, являющихся коммерческой тайной (КТ):**

а) вырабатывается первоначальный вариант Перечня сведений, составляющих КТ предприятия;

б) перечень утверждается руководителем предприятия и доводится до исполнителей в полном объеме или в части их касающейся;

в) анализируются поступившие предложения по формировании. Перечня сведений, составляющих КТ предприятия, и готовится окончательный вариант Перечня сведений.

г) создается комиссия из числа квалифицированных специалистов ведущих структурных подразделений, которая будет выполнять экспертные функции;

д) выделяется ответственный за работу по определению сведений, являющихся КТ, который совместно со службой безопасности (СБ) организует и осуществляет весь комплекс работ.

**Установите последовательность порядка проведения аттестации объектов информатизации:**

1. Подача заявки на рассмотрение и проведение аттестации;

2. Проведение предварительного специального обследования аттестуемого объекта информатизации;

3. Разработка программы и методики аттестационных испытаний;

4. Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации;

5. Проведение аттестационных испытаний объекта информатизации;

Установите последовательность процессов в системе менеджмента информационной безопасности (СМИБ) в соответствии с моделью PDCA

а. Разработка СМИБ

б. Внедрение и функционирование СМИБ

в. Проведение мониторинга и анализа СМИБ

г. Поддержка и улучшение СМИБ

**Установите последовательность мер по защите персональных данных при их обработке, которые должен принимать оператор в соответствии с федеральным законом от 27 июля 2007 152-ФЗ**

а. Назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных

б. Издание оператором, являющимся юридическим лицом, локальных актов по вопросам обработки персональных данных

в. Применение правовых, организационных и технических мер по обеспечению безопасности персональных данных

г. Осуществление внутреннего контроля или аудита соответствия обработки персональных данных требованиям 152-ФЗ и принятым в соответствии с ним нормативным правовым актам

д. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения 152-ФЗ

е. Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, локальными актами по вопросам обработки персональных данных, и обучение указанных работников

**Установите порядок проведения аттестации и контроля объектов информатизации по требованиям безопасности**

а. Подача и рассмотрение заявки на аттестацию

б. Предварительное ознакомление с аттестуемым объектом

в. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости)

г. Разработка программы и методики аттестационных испытаний;

д. Заключение договоров на аттестацию

е. Проведение аттестационных испытаний объекта информатизации

ж. Оформление, регистрация и выдача "Аттестата соответствия"

з. Осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации

и. Рассмотрение апелляций

**Установите последовательность разработки модели угроз ИСПДн:**

а. Описать ИСПДн

б. Определить пользователей ИСПДн

в. Определить тип ИСПДн

г. Определить исходный уровень защищенности ИСПДн

д. Определить вероятность реализации угроз в ИСПДн

е. Определить возможность реализации угроз в ИСПДн

ж. Оценить опасность угроз

з. Определить актуальность угроз в ИСПДн

**1 уровень Практическое задание «Перевод профессионального текста (сообщения)»**

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 27002 Second edition 2013-10-01

Information technology — Security techniques — Code of practice for

information security controls

Technologies de l’information — Techniques de sécurité — Code de

bonne pratique pour le management de la sécurité de l’information

© ISO/IEC 2013

Объем контрольного участка текста на иностранном языке (1500-2000) знаков и контрольные вопросы будут предоставлены участнику перед выполнением задания.

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

**1 уровень Практическое задание «Задание по организации работы коллектива»**

При разработке системы обеспечения информационной безопасности для предприятия выполняются следующие этапы:

1 Предпроектное обследование;

2 Формирование требований к системе обеспечения информационной безопасности (СОИБ) и разработка технического задания на её создание;

3 Проектирование системы обеспечения информационной безопасности:

4 Внедрение системы обеспечения информационной безопасности:

4.1 Поставка необходимых программных и технических средств;

4.2 Проведение монтажных и пусконаладочных работ по созданию СОИБ.

**Задание**. При реализации данного проекта требуется обеспечить сбалансированное распределение трудовых и временных ресурсов между работами проекта.

1. Определение продолжительности проекта. Ответ: /количество рабочих дней/ - Оценка за правильный результат - 3 балла
2. Перечислить задачи, лежащие на критическом пути проекта. Ответ:/перечислить все этапы, лежащие на критическом пути проекта/ Оценка за правильный результат - 2 балла.
3. Распределить ресурсы по задачам проекта согласно таблице и определить стоимость проекта. Ответ:/ рублей/ - Оценка за правильный результат - 3 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

**Используемое программное обеспечение (open source)** – Project Libre

**Используемая литература:**

1. <https://www.projectlibre.com/>
2. Управление проектом. Основы проектного управления : учебник / коллектив

авторов; под ред. проф. М.Л. Разу. — 3-е изд., перераб. и доп. — М. : КНОРУС, 2010. — 760 c.

**2 уровень Инвариантная часть задание1**

**Практическое задание в Cisco Packet Tracer (www.netacad.com)**

**Описание ПО и оборудования для моделирования сети**

Для выполнения задания необходимо ПО Cisco Packet Tracer v.7.1.1. Получить лдоступ к ПО можно тремя способами:

1. в результате прохождения курса сетевой академии Cisco ([www.netacad.com](http://www.netacad.com)), расположенного по ссылке https://www.netacad.com/ru/courses/intro-packet-tracer/ ;
2. отправить на почту организаторов Олимпиады данные участников (ФИО на русском и английском языках, e-mail участника). После этого участник Олимпиады будет зарегистрирован в сетевой академии Cisco ФГБОУ ВО УГАТУ и получит доступ к вышеуказанному ПО;
3. если учебное заведение является участником программы Сетевых академий Cisco;

**2 уровень Вариативная часть Задание2**

10.02.01 Задание 2 «Развертывание Удостоверяющего центра ViPNet в аккредитованном режиме»

<https://infotecs.ru/downloads/besplatnye-produkty/>

<https://infotecs.ru/downloads/documentacii/>

10.02.02 «Организация межсетевого защищенного взаимодействия с применением ПО ViPNet»

<https://infotecs.ru/downloads/besplatnye-produkty/>

<https://infotecs.ru/downloads/documentacii/>

10.02.03 Задание 2 «Администрирование системы защиты ViPNet»

<https://infotecs.ru/downloads/besplatnye-produkty/>

<https://infotecs.ru/downloads/documentacii/>

**2 уровень Вариативная часть Задание3**

10.02.01 Задание 3 «Настройка системы учета рабочего времени «Guard Light»

Инструкции, руководство, программное обеспечение <https://ironlogic.ru/il_new.nsf/htm/ru_guardlight>

10.02.02 Задание 3 «Настройка АПМДЗ ПАК «Соболь»

Инструкции, руководство, программное обеспечение <https://www.securitycode.ru>

10.02.03 Задание 3 «Настройка программного средства безопасности Secret Net Studio»

Инструкции, руководство, программное обеспечение <https://www.securitycode.ru>

**Спецификация ФОС УГС 10.00.00 «Информационная безопасность»**

**Алгоритм формирования содержания задания I уровня «Тестирование»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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.03)**  **10.02.02(ОП.03)**  **10.02.03(ОП.04)** | **2. Оборудование, материалы, инструменты** | **0,1** | **0,2** | **0,3** | **0,4** |
| **10.02.01(ОП.01)**  **10.02.02(ОП.04)**  **10.02.03(ОП.03)** | **3. 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)** | **4. 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)** | **5. 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)** | **6. Основы информационной безопасности** | **0,1** | **0,2** | **0,3** | **0,4** |
| **10.02.01 (МДК 02.03)**  **10.02.02 (МДК02.01)**  **10.02.03 (МДК02.02)** | **7.** **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)** | **8 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)** | **9. 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 (МДК 01.01/МДК 02.01)**  **10.02.02 (МДК03.01)**  **10.02.03 (ОП03)** | **10. 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** |
| **Максимальная сумма баллов** | **10** | | | |

**Алгоритм формирования содержания задания I уровня «Перевод»**

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 27002 Second edition 2013-10-01

Information technology — Security techniques — Code of practice for

information security controls

Technologies de l’information — Techniques de sécurité — Code de

bonne pratique pour le management de la sécurité de l’information

© ISO/IEC 2013

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 (орфорграфические, 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.

**10.02.01 ОГСЭ.03. Иностранный язык**

**10.02.02** **ОГСЭ.03. Иностранный язык**

**10.02.03** **ОГСЭ.03. Иностранный язык**

**Алгоритм формирования содержания задания I уровня «Задание по организации работы коллектива»**

При разработке системы обеспечения информационной безопасности для предприятия выполняются следующие этапы:

1 Предпроектное обследование;

2 Формирование требований к системе обеспечения информационной безопасности (СОИБ) и разработка технического задания на её создание;

3 Проектирование системы обеспечения информационной безопасности:

4 Внедрение системы обеспечения информационной безопасности:

4.1 Поставка необходимых программных и технических средств;

4.2 Проведение монтажных и пусконаладочных работ по созданию СОИБ.

**Задание**. При реализации данного проекта требуется обеспечить сбалансированное распределение трудовых и временных ресурсов между работами проекта.

|  |  |  |
| --- | --- | --- |
| № задания | Тип задания | Оценка |
| 1.1 | Определение продолжительности проекта. Ответ: /количество рабочих дней/ | - Оценка за правильный результат - 3 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. |
| Итого: | | 5 баллов |
| 2.1 | Распределить ресурсы по задачам проекта согласно таблице и определить стоимость проекта. Ответ:/ рублей/ | - Оценка за правильный результат - 3 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 |
| Итого | | 5 баллов |
| Максимальный результат | | 10 баллов |

**10.02.01 (ОП.08, ОП.09)**

**10.02.02 (ОП.08, ОП.09)**

**10.02.03 (ОП.09, ОП.10)**

**Алгоритм формирования содержания задания II уровня Инвариантная часть**

Задание:

Используя документацию, реализуйте приведённые ниже требования:

На **всех устройствах** согласно таблице адресациинастройте 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,** 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 с локальной проверкой паролей на линиях VTY, консольном входе, линиях AUX сетевых устройств;
  + незашифрованные пароли необходимо зашифровать;
  + установить баннер MOTD «This is a secure system. Authorized Access Only!»;
  + настроить NTP:
    - NTP-сервер 192.168.0.2;
    - ключ №1;
    - аутентификация по алгоритму MD5 c паролем Ufa2018;
  + 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:**

* 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, RB** настройте статическиемаршрутыв Интернет по умолчанию.

**Маршрутизатор DHCP:**

* настройте службы DHCP для VLAN 15, 30, 45, 60, 75:
  + используйте слово **LAN\_Х**в качестве имени пула (с учетом регистра), где Х – 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:**

* настройте преобразование NAT:
  + настройте именованный список контроля доступа с именем **NAT**, содержащий одну запись. Сначала разрешите все IP-адреса, принадлежащие адресному пространству **10.0.0.0/16**;
  + далее настройте статический NAT для сервера **Сервисы**, заменяяего внутреннийадрес на адрес 209.165.24.40;
  + настройте динамическую трансляцию NAT с использованием PAT, указав выбранное имя пула, маску /30 и следующие два общедоступных адреса для R3: 209.165.24.34 и 209.165.24.35;
  + настройте динамическую трансляцию NAT с использованием PAT, указав выбранное имя пула, маску /30 и следующие два общедоступных адреса для RB: 209.165.24.50 и 209.165.24.51;
* настройте VPN-туннель между маршрутизаторами (для пар подсетей 192.168.0.0/24–192.168.1.0/24, 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 создать расширенный список контроля доступа **110**):
  + первая фаза:
    - политика (приоритет) – 1;
    - тип алгоритма шифрования – **AES**;
    - тип алгоритма обеспечения целостного данных – **SHA**;
    - группа – 2;
    - тип аутентификации – с заранее заданным ключом (pre-share);
    - пароль – **VPN\_P@55w0rd**;
  + 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**;
* настройте именованные списки контроля доступа **FROM\_IN** для ограничения доступа из ЛВС:
  + разрешите для всех VLAN доступ по протоколам HTTP и HTTPS к любым веб-серверам в Интернете;
  + разрешите доступ по протоколу ICMP для сообщений типа **echo-reply**, **unreachable**, **source-quench** и запретите все остальные сообщения протокола ICMP;
* настройте именованные списки контроля доступа **FROM\_OUT** для ограничения доступа из Интернета:
  + разрешите доступ по протоколу TCP, если соединение было установлено из ЛВС для всех VLAN;
  + разрешите доступ по протоколу ICMP для сообщений типа **echo**, **parameter-problem**, **packet-too-big**, **source-quench** и запретите все остальные сообщения протокола ICMP;
  + включите защиту от спуфинга от:
    - узла 0.0.0.0;
    - узла 255.255.255.255;
    - всех частных диапазонов подсетей;
    - подсети 127.0.0.0/8;
    - подсети 224.0.0.0/4.

**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 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 назначить группу резервирования 2, приоритет 110, отслеживание интерфейса Gi0/2.

**Коммутаторы S1, S2:**

* настройте сети VLAN, присвойте им имена и выполните назначение портов доступа;
* включите функцию PortFast для портов доступа;
* 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 35, 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 защиты от атак, связанных с протоколами ARP(DAI) и DHCP(DHCP Snooping):
  + для VLAN 15, 30,45,60,75;
  + примените её на интерфейсе Port-channel 1 коммутатора S1 и на интерфейсе Fa0/24 коммутатора S2;
* настройте защиту IP Source guard для всех портов;
* настройте защиту Loop guard по умолчанию.

**Коммутатор SB:**

* выполните назначение портов доступа;
* включите функцию PortFast для портов доступа;
* 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:
  + 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, 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 защиту IP Source guard для всех портов.

**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.

1. Получить доступ с узлов ПК-1, ПК-2, ПК-3 к серверу **Сервисы** попротоколуHTTP.

**Максимальный результат – 35 баллов**

**10.02.01 (МДК 03.02)**

**10.02.02 (МДК 02.03)**

**10.02.03 (МДК 02.01**

**Задание II уровня Вариативная часть**

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

С помощью технологии виртуальных машин *VirtualBox* для выполнения задания смоделирована корпоративная сеть организации.

VirtualBox 5.2

ОС Windows7

VM\_1,VM\_4 ViPNet Administrator

ViPNet Client

ViPNet Policy Manager

VM\_2,VM\_3 ViPNet Client

ViPNet Coordinator

|  |  |  |
| --- | --- | --- |
| № | НАЗВАНИЕ СЕТЕВОГО УЗЛА | Имя пользователя СЕТЕВОГО УЗЛА |
| 1 | Главный администратор | Admin |
| 2 | Помощник Администратора | Secadmin |
| 3 | Пользователь1 Офис | User1 |
| 4 | Пользователь2 Филиал | User2 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Схема связей пользователей | CoordinatorOffice | Secadmin | AdminSecuruty | User1 | CoordinatorSubsidiary | User2 |
| CoordinatorOffice | xx | \* | \* | \* | \* |  |
| Admin | \* | xx | \* |  |  |  |
| Secadmin | \* | \* | xx |  |  |  |
| User1 | \* |  |  | xx |  | \* |
| CoordinatorSubsidiary | \* |  |  |  | xx | \* |
| User2 |  |  |  | \* | \* | xx |

Задание 2.1 Создание структуры защищенной сети:

- создать структуру защищенной сети в соответствии с заданной схемой;

- настроить связи пользователей в ;

- сформировать дистрибутивы ключей для сетевых узлов в УКЦ

- создать резервную копию конфигурации сети в ручном режиме;

- настроить автоматическое ежедневное резервное копирование данных

Задание 2.2 Развертывание рабочего места Администратора безопасности:

- установить ViPNet Client

- установить связь с сервером

- сохранить отчет о структуре сети ViPNet в файл

- ограничить обмен информацией в чате.

Задание 2.3 Модификация защищенной сети

- настроить транспортный модуль;

- добавить новый сетевой узел, сформировать справочники и ключи;

- создать группу узлов;

- создать нового пользователя;

**10.02.01**

- произвести смену мастер ключей;

- сформировать новый сертификат ключей проверки электронной подписи;

- объявить ключи одного из пользователей скомпрометированными;

- произвести смену ключей скомпрометированного пользователя;

**10.02.03**

-установить ViPNet Policy Manager;

- создать подразделения;

- создать политики безопасности с ограничением доступа к соц.сетям и блокированием открытого трафика на рабочем месте одного из пользователей;

- вывести журнал IP пакетов.

**10.02.02**

- установить ViPNet Coordinator

- развернуть защищенную сеть, настроить межсетевое взаимодействие с использованием симметричного межсетевого мастер-ключа.

- проверить взаимодействие узлов;

**Максимальная оценка 25 баллов**

**10.02.01 (МДК 03.02)**

**10.02.02 (МДК 02.03)**

**10.02.03 (МДК 02.01)**

**Задание II уровня Вариативная часть**

**Задание 3**

**10.02.01**  3.1 Произвести настройку системы учета рабочего времени «Guard Light»

Программное обеспечение «Guard Light», позволяет управлять работой контроллеров и обрабатывать полученную с них информацию.

3.1 Включить всё оборудование и запустить программу;

- на закладке «конвертеры» подключить к программе конвертеры;

- на закладке «контроллеры» подключить к программе контроллеры;

- на закладке «работа с базой» настроить временные зоны контроллеров;

- создать отделы;

- создать записи работников.

3.2 Для контроля трудовой дисциплины создать отдел и график работы, настроить:

- Начало рабочего дня в отделе;

- Окончание рабочего дня;

- Начало обеда;

- Окончание обеда;

- Короткий день;

- Окончание короткого дня;

- Тип графика работы – с ночной сменой;

3.3 Создать и настроить работников и карты работников и администратора:

Форма имеет следующие поля:

- Должность;

- Фамилия работника;

- Имя;

- Отчество;

- Дата рождения;

- Комментарий – он будет отображаться в списке работников (например, местный телефон);

- Дополнительная информация – несколько строк текста связанных с данным работником (например, номер паспорта, домашний адрес и телефоны);

- Блокировка позволяет отменить доступ работника во всех контроллерах на случай его поездки в командировку или отпуск. Это не позволит использовать его карту в его отсутствие;

3.4 Произвести настройку режимов доступа согласно заданию

3.5 Вывести отчет о обработки данных

**10.02.02**  3.1 Произвести настройку ПАК «Соболь»

- выключить компьютер, открыть корпус системного блока, произвести установку плат;

- произвести переподключение блокировки по Reset;

3.2 Произвести инициализацию устройства

-отформатировать ключевой носитель

- настроить общие параметры(инициализации)

- расчет контрольных сумм

- создать первичного администратора

3.3 Контроль целостности

- произвести настройку контроля целостности

- создать файл, поставить на контроль КЦ

3.4 Произвести вход в систему в режиме Администратора

- произвести настройку комплекса

- создать Администратора и пользователей

- настроить общие параметры

3.5 произвести вход пользователем

- изменить файл

- зайти администратором, найти в журнале событий запись контроля целостности

**10.02.03**  3.1 Произвести локальную настройку Secret Net Studio в соответствии с заданными параметрами:

- настроить политику группы "Вход в систему"по паролю и идентификатору на токене безопасности;

- настроить регистрацию событий, журнал и теневое копирование;

3.2 Произвести настройку контроля целостности:

- создать файл, настроить реакцию на отказ, задать расписание, сформировать задание,структуру, эталоны

-внести изменение в файл, произвести проверку целостности, найти записи в журнале.

3.3 Настроить сервер безопасности

- произвести настройку управления подчинением защищаемых компьютеров серверу безопасности SNS согласно задания

3.4. Настройка работы с электронными идентификаторами

- настроить размещение ключей на USB-носителе, копию ключей разместить на токене, проверить идентификатор.

3.5 Настроить полномочия доступа к внешним носителям

- установите запрет всем пользователям на использование незарегистрированных USB-флеш-накопителей (всех, кроме подключенного в настоящий момент).

**Максимальная оценка 10 баллов**

**10.02.01 (МДК03.01)**

**10.02.02 (МДК 02.02)**

**10.02.03 (МДК 03.01)**

СВОДНАЯ ВЕДОМОСТЬ

оценок результатов выполнения заданий I уровня

заключительного этапа

Всероссийской олимпиады профессионального мастерства

в 2018 году

УГС10.00.00 Информационная безопасность

Перечень специальностей:

10.02.01 Организация и технология защиты информации,

10.02.02 Информационная безопасность телекоммуникационных систем,

10.02.03 Информационная безопасность автоматизированных систем

Дата «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_

Член (ы) жюри \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

фамилия, имя, отчество, место работы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  п/п | Номер участника, полученный при жеребьевке | Оценка по каждому заданию | | | Суммарная оценка |
| Тестирование | Перевод текста (сообщения) | Организация работы коллектива |
|  |  |  |  |  |  |

\_\_\_\_\_\_\_\_\_(подпись члена (ов) жюри)

ВЕДОМОСТЬ

оценок результатов выполнения практического задания II уровня

заключительного этапа

Всероссийской олимпиады профессионального мастерства

в 2018 году

УГС10.00.00 Информационная безопасность

Перечень специальностей:

10.02.01 Организация и технология защиты информации,

10.02.02 Информационная безопасность телекоммуникационных систем,

10.02.03 Информационная безопасность автоматизированных систем

Дата «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_

Член (ы) жюри \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

фамилия, имя, отчество, место работы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  п/п | Номер участника, полученный при жеребьевке | Оценка за выполнение  Задач задания | | | Суммарная оценка в баллах |
| 1 | 2 | 3 |
|  |  |  |  |  |  |

\_\_\_\_\_\_\_\_\_(подпись члена (ов) жюри)

СВОДНАЯ ВЕДОМОСТЬ

оценок результатов выполнения практических заданий II уровня

заключительного этапа

Всероссийской олимпиады профессионального мастерства

в 2018 году

УГС10.00.00 Информационная безопасность

Перечень специальностей:

10.02.01 Организация и технология защиты информации,

10.02.02 Информационная безопасность телекоммуникационных систем,

10.02.03 Информационная безопасность автоматизированных систем

Дата «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_

Член (ы) жюри \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

фамилия, имя, отчество, место работы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Номер участника, полученный при жеребьевке | Оценка за выполнение заданий II уровня | | Суммарная оценка |
| Инвариантная часть | Вариативная часть |
|  |  |  |  |  |

\_\_\_\_\_\_\_\_\_(подпись члена (ов) жюри)

СВОДНАЯ ВЕДОМОСТЬ

оценок результатов выполнения профессионального комплексного задания

заключительного этапа

Всероссийской олимпиады профессионального мастерства

в 2018 году

УГС10.00.00 Информационная безопасность

Перечень специальностей:

10.02.01 Организация и технология защиты информации,

10.02.02 Информационная безопасность телекоммуникационных систем,

10.02.03 Информационная безопасность автоматизированных систем

Дата «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Номер  участника,  полученный при жеребьевке | Фамилия, имя, отчество  участника | Наименование субъекта Российской Федерации  и образовательной организации | | Оценка результатов выполнения профессионального комплексного задания  в баллах | | | Итоговая оценка выполнения профессионального комплексного задания | Занятое  место (номинация) |
| Суммарная оценка за выполнение заданий  I уровня | Суммарная оценка за выполнение заданий  2 уровня | |
| 1 | 2 | 3 | 4 | | 5 | 6 | | 10 | 11 |
|  |  |  |  | |  |  | |  |  |
| Председатель рабочей группы (руководитель  организации –организатора олимпиады) | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  фамилия, инициалы | | | |
| Председатель жюри | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  фамилия, инициалы | | | |
| Члены жюри: | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  фамилия, инициалы | | | |

**Методические материалы**

**1 уровень задание «Тестирование»**

Литература:

1.ГОСТ Р ИСО 7498-2-99

2. ГОСТ Р 52863-2007

3. ГОСТ Р 50922-2006

4. ГОСТ Р 51188-98

5. РД Защита от НСД

6. ГОСТ Р 51897- 2011/Руководство ИСО 73:2009 /ISO GUIDE 73-2009

7. ПРИКАЗ Минкомсвязи России от 23.11.2011 №320 Об аккредитации удостоверяющих центров

8. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. Родичев Ю.А Издательство Питер, 2017 г.

9.  Информационная безопасность. История защиты информации в России А. Бабаш, Е.Баранова, Д. Ларин Книжный дом Университет 2013 г.

10. Основы информационной безопасности. Учебное пособие С. Нестеров ЛАНЬ 2016 г.

11. Введение в информационную безопасность автоматизированных систем. Учебное пособие Бондарев В.В. Издательство МГТУ 2016 г.