Республиканская олимпиада профессионального мастерства обучающихся по профессиям и специальностям среднего профессионального образования

УГС 10.00.00 «Информационная безопасность»

Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности 15 марта 2017 г.

ПРОФЕССИОНАЛЬНОЕ КОМПЛЕКСНОЕ ЗАДАНИЕ

УФА 2017

Республиканская олимпиада профессионального мастерства обучающихся по профессиям и специальностям среднего профессионального образования
УГС 10.00.00 «Информационная безопасность»
Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности 15 марта 2017 г.

Профессиональное комплексное задание I уровень

Инвариантная часть тестового задания

Количество вопросов – 20.
Количество баллов за 1 правильный ответ:
- 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.

Максимальный результат – 5 баллов.
Время выполнения – 0,5 часа.

1. ИТ в профессиональной деятельности

Вопрос с выбором ответа - 0,1 балла

1.1 Какое из перечисленных ниже действий не является частью процесса управления конфигурациями?

Ответ:
а) конфигурирование и настройка операционной системы
б) передача официального запроса
в) конфигурирование оборудования
г) конфигурирование и настройка приложения

Вопрос с открытой формой ответа - 0,2 балла

1.2 На каком этапе проекта впервые должны быть учтены вопросы безопасности?
Ответ:

Вопрос на установление соответствия - 0,3 балла

1.3. Установите соответствие между уровнями модели OSI и типами данных

Ответ:
1 Физический
2 Канальный
3 Сетевой

4 Транспортный

1 Кадры
2 Биты
3 Блоки
4 Пакеты

Вопрос на установление правильной последовательности - 0,4 балла

1.4 Установите правильную последовательность уровней модели OSI

Ответ:
1 Канальный
2 Прикладной
3 Сетевой
4 Транспортный
5 Сеансовый
6 Представления
7 Физический

2. Оборудование, материалы, инструменты

Вопрос с выбором ответа - 0,1 балла

2.1 Ограждения сеткой относятся к :

Ответ:
а) предупредительным
б) основным
в) дополнительным
г) заградительным

Вопрос с открытой формой ответа - 0,2 балла

2.2 Какой прибор позволяет измерить уровень сигнала по акустическому каналу утечки информации.

Ответ:

Вопрос на установление соответствия - 0,3 балла

2.3 Установите соответствие между средствами защиты и каналами утечки информации

Ответ:
1 звукоизоляция
2 жалюзи
3 шредер
4 экранирование

1 вещественный КУИ
2 радио-электронный КУИ
3 акустический КУИ
4 оптический КУИ

Вопрос на установление правильной последовательности - 0,4 балла

Установите правильную последовательность обеспечения безопасности аппаратно-программного модуля доверенной загрузки:

Ответ:
1) Загрузку ОС
2) Загрузка CriptoBIOS
3) Идентификация пользователя по ключу и паролю АПМДЗ
4) Загрузка BIOS

3. Системы качества, стандартизации и сертификации

Вопрос с выбором ответа - 0,1 балла

Ответ:
3.1 Политика безопасности строится на основе
а) анализа рисков, признанных реальными для данной организации
б) стратегии управления защиты
в) программы действий, реализация которых обеспечит информационную безопасность;
г) финансовых данных

Вопрос с открытой формой ответа - 0,2 балла

3.2 Для чего предназначены стандарты информационной безопасности

Ответ:

Вопрос на установление соответствия - 0,3 балла

3.3 Установите соответствие этапов и действий согласно стандарта ИБ ISO27000

Ответ:
1 Оценка рисков
2 Пересмотр политик
3 Контроль факторов риска
4 Обработка рисков

1 Планирование и организация
2 Внедрение и эксплуатация
3 Мониторинг и аудит
4 Совершенствование

Вопрос на установление правильной последовательности - 0,4 балла

Установите последовательность жизненного цикла процесса разработки системы

Ответ:
1) разработка
2) сертификация
3) тестирование модулей
4) аккредитация

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

Вопрос с выбором ответа - 0,1 балла

4.1 Какой уровень шума считается максимально допустимым при работе оператора ПЭВМ?

Ответ:
а) 30 дБ
б) 50 дБ
в) 80 дБ
г) 70 дБ

Вопрос с открытой формой ответа - 0,2 балла

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

Ответ:

Вопрос на установление соответствия - 0,3 балла

4.3 Установите соответствие между требованиями и средствами защиты труда человека

Ответ:
1. Нормализация состава воздуха рабочей зоны
2. Нормализация климатических условий
3. Нормализация электромагнитных излучений
4. Нормализация производственного шума
5. Нормализация производственных вибраций

1 Вентиляция
2 Звукоизоляция
3 Виброзащита
4 Экранирование
5 Кондиционирование

Вопрос на установление правильной последовательности - 0,4 балла

4.4 Установите правильную последовательность этапов процессов управления охраной труда

Ответ:
1. Принятие решений, планирование мероприятий по охране труда
2. Выполнение запланированных мероприятий по охране труда
3. Подготовка к выполнению запланированных мероприятийпо охране труда
4. Анализ состояния охраны труда на предприятии
5. Контроль за ходом выполнения запланированных мероприятий по охране труда

5. Экономика и правовое обеспечение профессиональной деятельности

Вопрос с выбором ответа - 0,1 балла

5.1 Структура затрат на информационную безопасность предприятия - это:

Ответ:
а) состав затрат и часть каждого элемента в их общем объеме
б) все статьи затрат на информационную безопасность
в) часть каждого элемента затрат на информационную безопасность
г) калькуляция себестоимости затрат на информационную безопасность

Вопрос с открытой формой ответа - 0,2 балла

5.2 Назовите показатель сравнительной эффективности капиталовложений на информационную безопасность предприятия:

Ответ:

Вопрос на установление соответствия - 0,3 балла

5.3 Установите соответствие между мерами и документами

Ответ:
1. Административные меры
2. Законодательные меры
3. Процедурные меры
4. Программно-технические меры

1 Инструкция по защите компьютера
2 Политика безопасности предприятия
3. Должностные обязанности работников
4. Конституция РФ

Вопрос на установление правильной последовательности - 0,4 балла

5.4 Установите правильную последовательность анализа финансовой устойчивости

Ответ:
1. Анализ финансового состояния
2. Анализ хозяйственной деятельности
3. Управленческий анализ
4. Анализ вероятности наступления банкротства

Профессиональное комплексное задание I уровень

Вариативная часть тестового задания

Количество вопросов – 20.
Количество баллов за 1 правильный ответ:
- 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.

Максимальный результат – 5 баллов.
Время выполнения – 0,5 часа.

6. Основы информационной безопасности

Вопрос с выбором ответа - 0,1 балла

6.1 Действия злоумышленников относятся к …

Ответ:
а) угрозам преднамеренных воздействий
б) угрозам утечки информации
в) угрозам случайных воздействий
д) разглашению информации

Вопрос с открытой формой ответа - 0,2 балла

6.2 Под информационной безопасностью Российской Федерации понимается состояние …

Ответ:

Вопрос на установление соответствия - 0,3 балла

6.3 Установите соответствие между действием и определением

Ответ:
1 Логин
2 Пароль
3 Предоставление доступа
4 Проверка
5 Тест

1 Верификация
2 Авторизация
3 Аутентификация
4 Валидация
5 Идентификация

Вопрос на установление правильной последовательности - 0,4 балла

6.4 Установите последовательность степени важности информации от болееважного к менее важному

Ответ:
1 Совершенно секретно
2 Общедоступная информация
3 Секретно
4 Конфиденциальная информация
5 Особой важности

7. Криптографическая защита информации

Вопрос с выбором ответа - 0,1 балла

7.1 В алгоритмах электронной подписи подписывание производится …

Ответ:
а) закрытым ключом отправителя
б) закрытым ключом получателя
в) открытым ключом получателя
г) открытым ключом отправителя

Вопрос с открытой формой ответа - 0,2 балла

7.2 Как называется преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины с применением односторонних функций?
Ответ:

Вопрос на установление соответствия - 0,3 балла

7.3 Установите соответствие между алгоритмом шифрования и длиной ключа

Ответ:
1 DES
2 ГОСТ 28147-89
3 AES
4 3DES

1 168 бит
2 128/192/256 бит
3 256 бит
4 56 бит

Вопрос на установление правильной последовательности - 0,4 балла

Республиканская олимпиада профессионального мастерства обучающихся по профессиям и специальностям среднего профессионального образования
УГС 10.00.00 «Информационная безопасность»
Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности 15 марта 2017 г.

Установите последовательностьдействий при выполнении алгоритма Диффи-Хеллмана

Ответ:
1. Каждая сторона вычисляет открытый ключ
2. Стороны устанавливают открытые параметры p и g
3. Каждая сторона генерирует случайное натуральное число a — закрытый ключ
4. Обмен открытыми ключами с удалённой стороной
5. Вычисление общего секретного ключа

8. Инженерно-техническая защита информации

Вопрос с выбором ответа - 0,1 балла

8.1 Побочные излучения и наводки относятся к …

Ответ:
а) угрозам преднамеренных воздействий
б) угрозам утечки информации
в) угрозам случайных воздействий
д) разглашению информации

Вопрос с открытой формой ответа - 0,2 балла

8.2 К какому каналу утечки информации относится наблюдение злоумышленника за объектом защиты

Ответ:

Вопрос на установление соответствия - 0,3 балла

8.3 Установите последовательность между элементами схем и Акустоэлектрическими преобразователями

Ответ:
1 Громкоговоритель
2 Трансформатор

3 Конденсатор
4 ультразвуковые преобразователи

1 Магнитострикционный АЭП
2 Электродинамический АЭП
3 Пьезоэлектрический АЭП
4 Емкостной АЭП

Вопрос на установление правильной последовательности - 0,4 балла

8.4 установите правильную последовательность этапов поискового мероприятия радиозакладного устройства

1 Локализация с применением тепловизора
2 Применение анализатора спектра
3 Измерение частотометром обнаруженных локаций
4 Проверка помещения индикатором/детектором излучений
5 Проверка с применением сканирующего приемника

9. Программно-аппаратная защита информации

Вопрос с выбором ответа - 0,1 балла

9.1 Спуфинг –это…

Ответ:
а) изменение данных
б) фальсификация IP-адреса
в) анализ сетевого трафика
г) посредничество в обмене незашифрованными ключами

Вопрос с открытой формой ответа - 0,2 балла

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

Ответ:

Республиканская олимпиада профессионального мастерства обучающихся по профессиям и специальностям среднего профессионального образования
УГС 10.00.00 «Информационная безопасность»
Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности 15 марта 2017 г.

Вопрос на установление соответствия - 0,3 балла

9.3 Установите соответствие между моделью управления доступом

Ответ:
1 Мандатная
2 Ролевая
3 Дискреционная
4 Верификационная

1 Проверка доступа
2 Объединение субъектов
3 Матрица доступа
4 Объединение объектов

Вопрос на установление правильной последовательности - 0,4 балла

9.4 Установите последовательность выполнения SSL/TLS соединения

Ответ:
1) Генерируется сеансовый ключ для защищенного соединения.

2) Устанавливается зашифрованное соединение.

3) Сервер отправляет клиенту свой цифровой сертификат, подписанный удостоверяющим центром, и открытый ключ сервера.

4) Клиент может связаться с сервером доверенного центра сертификации, который подписал сертификат сервера, и проверяет, валиден ли сертификат сервера.

5) Клиент устанавливает соединение с сервером и запрашивает защищенное подключение.

6) Клиент предоставляет список алгоритмов шифрования, Сервер выбирает и сообщает клиенту, какой алгоритм использовать.

Республиканская олимпиада профессионального мастерства обучающихся по профессиям и специальностям среднего профессионального образования
УГС 10.00.00 «Информационная безопасность»
Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности 15 марта 2017 г.

10. Организационно-правовая защита информации

Вопрос с выбором ответа - 0,1 балла

10.1 Лицензирование это -

Ответ:
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

Вопрос с открытой формой ответа - 0,2 балла

10.2 Сертификация это -

Ответ:

Вопрос на установление соответствия - 0,3 балла

10.3 Установите соответствие по регулированию функций контроля органов РФ

Ответ:
1.ФСБ
2 ФСТЭК
3 Роскомнадзор
4 ФСО

1 Криптографическая защита информации
2 Защита персональных данных
3Защита правительственной связи
4 Защита несанкционированного доступа

Вопрос на установление правильной последовательности - 0,4 балла

10.4 Последовательность аттестации объектов информатизации

Ответ:
1 Ознакомление с объектом информатизации
2 Проверка организационной документации и нормативных документов
3 Оформление документов
4 Проверка технической документации ИС
5 Экспертная оценка выявления КУИ

Профессиональное комплексное задание I уровень
Практические задания

Задание выполняется на компьютере с использованием инженерного калькулятора.

Количество задания – 2.
Количество баллов за правильный ответ – 10.
Максимальный результат – 20 баллов.
Время выполнения – 1 час.

Практическое задание 1 «Перевод профессионального текста»

RFC2196 представляет собой руководство по определению процедур и политики безопасности для узлов, которые имеют связь с Интернет.

```
Network Working Group                                          B. Fraser
Request for Comments: 2196                                        Editor
FYI: 8                                                          SEI/CMU
Obsoletes: 1244                                          September 1997
Category: Informational


...
1.6  Risk Assessment

1.6.1  General Discussion

   One of the most important reasons for creating a computer security
   policy is to ensure that efforts spent on security yield cost
   effective benefits.  Although this may seem obvious, it is possible
   to be mislead about where the effort is needed.  As an example, there
   is a great deal of publicity about intruders on computers systems;
   yet most surveys of computer security show that, for most
   organizations, the actual loss from "insiders" is much greater.

   Risk analysis involves determining what you need to protect, what you
   need to protect it from, and how to protect it.  It is the process of
```

```
   examining all of your risks, then ranking those risks by level of
   severity.  This process involves making cost-effective decisions on
   what you want to protect.  As mentioned above, you should probably
   not spend more to protect something than it is actually worth.

   A full treatment of risk analysis is outside the scope of this
   document.  [Fites 1989] and [Pfleeger 1989] provide introductions to
   this topic.  However, there are two elements of a risk analysis that
   will be briefly covered in the next two sections.
   Identifying the assets
   Identifying the threats
   For each asset, the basic goals of security are availability,
   confidentiality, and integrity.  Each threat should be examined with
   an eye to how the threat could affect these areas.

1.6.2  Identifying the Assets

   One step in a risk analysis is to identify all the things that need
   to be protected.  Some things are obvious, like valuable proprietary
   information, intellectual property, and all the various pieces of
   hardware; but, some are overlooked, such as the people who actually
   use the systems. The essential point is to list all things that could
   be affected by a security problem.
   One list of categories is suggested by Pfleeger [Pfleeger 1989]; this
   list is adapted from that source.
   Hardware: CPUs, boards, keyboards, terminals, workstations, personal
   computers, printers, disk drives, communication lines, terminal servers,
   routers.
   Software: source programs, object programs, utilities, diagnostic
   programs, operating systems,  communication programs.
   Data: during execution, stored on-line, archived off-line, backups, audit
   logs, databases, in transit over communication media.
   People: users, administrators, hardware maintainers.
   Documentation: on programs, hardware, systems, local administrative
   procedures.
   Supplies: paper, forms, ribbons, magnetic media.
```

Задача 1: выполнить перевод текста

Задача 2 :Найти в предложенном тексте:

- пункты проведения анализа рисков;
- перечень объектов информационной среды.

Выполнить их перевод на русский язык.

Республиканская олимпиада профессионального мастерства обучающихся по профессиям и специальностям среднего профессионального образования
УГС 10.00.00 «Информационная безопасность»
Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности 15 марта 2017 г.

Практическое задание 2 «Задание по организации работы коллектива»

Проект по созданию системы обеспечения информационной безопасности для организации состоит из ряда этапов. Фрагмент проекта представлен в таблице и содержит наименование этапов, продолжительность в рабочих днях при выполнении работы сотрудниками, календарные сроки и последовательность этапов.

№ п.п	Название задачи	Специалист	Длительность, раб. дн.	Календарные сроки, дата начала – дата окончания этапа	Количество нерабочих дней за период	Описание зависимости
1	Предпроектное обследование	Специалист ИБ	10	01.09.2015 - 04.09.2015	-	-
2	Формирование требований к системе	Специалист ИБ	4	05.09.2015 – 13.09.2015	4	Начинается после 1
3	Обсуждение и согласование технических решений	Специалист ИБ	8	14.09.2015 – 24.09.2015	2	Начинается после 2
4	Проведение монтажных работ	Техник	29	25.09.2015 – 20.10.2015	8	Проводится параллельно с 5
5	Проведение пусконаладочных работ	Техник	12	15.10.2015 – 28.10.2015	4	Проводится параллельно с 4
6	Проведение предварительных испытаний	Специалист ИБ Техник	7	29.10.2015 – 03.11.2015	2	Начинается после 5

На выполнении каждого этапа задействованы сотрудники, фрагмент перечня которых с распределением по этапам представлен в таблице.

Задача 1: Требуется определить количество техников и специалистов по информационной безопасности на соответствующем этапе, требуемое для выполнения этапа проекта в указанный календарный срок, если продолжительность одного рабочего дня составляет 8 часов и каждый сотрудник занят полный рабочий день - 5 баллов.

Задача 2: Составить диаграмму Ганта - 5 баллов.

Республиканская олимпиада профессионального мастерства обучающихся по профессиям и специальностям среднего профессионального образования
УГС 10.00.00 «Информационная безопасность»
Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности 15 марта 2017 г.

Профессиональное комплексное задание 2 уровень

Инвариантная часть

«Анализ «Политики ИБ Компании»

Задание:

Изучите документ «Политика информационной безопасности Компании».

Определите, допущены ли в нём ошибки. Исправьте их с отметкой в правых полях. Каждая выявленная ошибка – 1балл. Всего - 25 баллов.

Дополните по собственному мнению документ дополнительными пунктами. Оценивается жюри дополнительными 0 - 10 баллами.

Максимальная оценка – 35 баллов.

Документ будет предоставлен на олимпиаде

ПРИМЕР

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Общие положения

1.1 Настоящая политика информационной безопасности предусматривает принятие необходимых мер в целях защиты активов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Компании.

1.2 Ответственность за соблюдение информационной безопасности несет каждый сотрудник Компании, при этом первоочередной задачей является обеспечение безопасности всех активов Компании.

1.3 Целями настоящей Политики являются:

- сохранение конфиденциальности критичных информационных ресурсов;
-
-

2. Требования и рекомендации

2.1 В отношении всех собственных информационных активов Компании, активов, находящихся под контролем Компании, а также активов, используемых для получения доступа к инфраструктуре Компании, ответственность должна быть разделена поровну между всеми работниками Компании.

2.2 Все работы в пределах офисов Компании выполняются в соответствии с официальными должностными обязанностями только на любых компьютерах Компании.

Республиканская олимпиада профессионального мастерства обучающихся по профессиям и специальностям среднего профессионального образования
УГС 10.00.00 «Информационная безопасность»
Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности 15 марта 2017 г.

2.3 Внос в здания и помещения Компании личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы Компании разрешен.

…

Номер ошибки	Исходный текст с ошибкой(подчеркнуто)	Вариант исправления	Баллы за правильное исправление
1	1.2 Ответственность за соблюдение информационной безопасности несет каждый сотрудник Компании, при этом первоочередной задачей является обеспечение безопасности всех активов Компании.	…работник…согласно Трудовому Кодексу РФ	
2	2.1 В отношении всех собственных информационных активов Компании, активов, находящихся под контролем Компании, а также активов, используемых для получения доступа к инфраструктуре Компании, ответственность должна быть разделена поровну между всеми работниками Компании.	…ответственность должна быть назначена за соответствующим работником…	
3	2.2 Все работы в пределах офисов Компании выполняются в соответствии с официальными должностными обязанностями на любых компьютерах Компании.	…только на компьютерах, разрешенных к использованию в Компании.	
4	2.3 Внос в здания и помещения Компании личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а	…производится только при согласовании с Департаментом защиты информации	

	также вынос их за пределы Компании разрешен.	Компании.	

…

Профессиональное комплексное задание - 2 уровень

Вариативная часть

с учетом специфики специальности

Задание: Обеспечить защиту автоматизированных рабочих мест с учетом специфики специальности.

Количество выполняемых пунктов задания 30
Каждый выполненный пункт – 1 балл.
Оценивается жюри дополнительными 0 - 10 баллами.
Максимальная оценка – 35 баллов.
Время выполнения задания 2 часа.

Вводные данные:

Конфигурация компьютера: Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz ОЗУ 2048 МБ HDD160 Гб NVIDIA GeForce 9600 GT (512 МБ)

ОС Windows 7 Professional SP1

Аппаратно-программный ключ Рутокен S 32К(драйверы, утилиты, описание с http://www.rutoken.ru/, лицензия freeware)

Программа шифрования VeraCript v1.7 (программа, описание https://veracrypt.codeplex.com/, лицензия freeware)

Программа восстановления и надежного удаления файлов Recuva(Программа, описание, https://www.piriform.com/recuva, лицензия freeware)

Межсетевой экран D-Link DFL-260E

USB флеш накопитель 8Гб

1. Организация восстановления штатными средствами ОС Windows 7 Professional SP1.

2 Организация доступа в систему штатными средствами ОС Windows 7 Professional SP1.

3. Администрирование учетных записей штатными средствами ОС Windows 7 Professional SP1.

4. Настройка автозагрузки носителей штатными средствами ОС Windows 7 Professional SP1.

5. Настройка дискреционной и ролевой моделей доступа штатными средствами ОС Windows 7 Professional SP1.

6. Архивирование информации штатными средствами ОС Windows 7 Professional SP1.

7. Шифрование штатными средствами ОС Windows 7 Professional SP1.

8. Применение токенов безопасности в ОС Windows 7 Professional SP1.

9. Применение прикладной программы шифрования VeraCript v1.7

10. Применение прикладной программа Recuva.

Вариативная часть 10.02.02

11. Настройка активных соединения и открытых портов штатными средствами ОС Windows 7 Professional SP1.

12 Организация VPN соединения с применением межсетевого экрана D-Link DFL-260E

Вариативная часть 10.02.03

11.Настройка целостности программной среды штатными средствами ОС Windows 7 Professional SP1.

12. Генерация ключей и сертификатов PKI штатными средствами ОС Windows 7 Professional SP1 с применением токенов безопасности (Рутокен S).