Согласовано Региональный Совет работодателей	Согласовано Центр по компетенции	Утверждено Региональный организационный комитет
«__»_____ 2017г.	«__»_____ 2017г.	«__»_____ 2017г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

по компетенции «Информационная безопасность»
региональный этап чемпионата «Абилимпикс - 2017» г. Москва

Согласовано с
Представителями
общественных организаций
инвалидов:

Разработано:
Главный эксперт по компетенции Грибаков Сергей Леонидович

Москва
2017

1. Описание компетенции

Компетенция «Информационная безопасность» входит в «ТОП-50 наиболее востребованных и перспективных профессий» в соответствии с лучшими зарубежными стандартами и передовыми технологиями. Утверждено приказами Министерства образования и науки Российской федерации от 09 декабря 2016 года № 1551, №1553 в виде Федеральных образовательных стандартов среднего профессионального образования 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Имея решающую роль в повседневном функционировании, техник по защите информации имеет спрос в организациях различных масштабов коммерческого и государственного сектора. Информация конфиденциального характера нуждается в защите, следовательно - в защите нуждаются все элементы системы: ПК, автоматизированные системы, сеть, сетевое оборудование, периметр объекта и т.п. Техник по защите информации несет ответственность за настройку оборудования и программного обеспечения по защите информации, надежное функционирование автоматизированных систем предприятия, поддержание информационной безопасности.

Информационная безопасность требует широкий спектр познаний и навыков в области информационных технологий. В связи с быстрым развитием этой области, требования к техникам по защите информации постоянно возрастают.

Техник по защите информации должен уметь:

- обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных

систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;

- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;
- организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;
- настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- использовать типовые программные криптографические средства, в том числе электронную подпись;
- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
- применять технические средства для криптографической защиты информации конфиденциального характера;
- применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;
- применять инженерно-технические средства физической защиты объектов;
- выявлении технических каналов утечки информации; применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;
- проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
- проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

2. Конкурсное задание

Цель

В рамках выполнения поставленной задачи показать высокий уровень мастерства в компетенции «Информационная безопасность» за максимально короткое время.

Время на выполнение задания

3 часа.

Требования

- Участники и Эксперты обязаны соблюдать Регламент организации и проведения чемпионата «Абилимпикс»;
- Участникам запрещается приносить с собой какие-либо носители информации, а также иметь доступ к сети Интернет во время выполнения работы или перерывах;
- Сообщить экспертам о необходимости установить дополнительное вспомогательное ПО, оборудование минимум за 3 суток до начала соревнования;
- Эксперты определяют рассадку до начала конкурса путем жеребьевки;
- Участники должны немедленно проинформировать Экспертов в случае обнаружения дефектов в оборудовании;
- Участники должны следовать указаниям Экспертов в случае обнаружения дефектов в оборудовании;
- Участники должны уведомить Экспертов, когда завершат выполнение задания.

Задание

1. Задание
    1.1.1. Дана хеш сумма слова e242f36f4f95f12966da8fa2efd59992
    Необходимо определить алгоритм расшифровки и расшифровать слово.
2. Задание
    2.1.1. Установить необходимое программное обеспечение для работы с сертификатами (находится в папке Участник на рабочем столе виртуальной машины).
    2.1.2. Настроить браузер для работы с центром сертификации.
    2.1.3. Зайти на сайт www.cryptopro.ru/ui и создать новый сертификат, в поле Общее имя - указать Фамилию и Имя через пробел.
    2.1.4. Сохранить полученный сертификат на компьютер.
    2.1.5. Установить сертификат через КриптоПро.
    2.1.6. Зайти в программу КриптоАРМ и убедиться, что сертификат является действительным.
    2.1.7. Зашифровать файл shifr из папки Участник с помощью криптопровайдера Crypto-Pro GOST R 34.10-2001, используя собственный сертификат.
3. Задание
    3.1.1. В папке Участник на рабочем столе находится файл certyficat.
    3.1.2. Установить сертификат с контейнером на компьютер.
    3.1.3. Расшифровать файл shifr_1 в папке Участник, используя данный

сертификат.

4. Задание
   1.1. Шифр Цезаря файл с текстом и шаг даны: Чфцкзуфзёуое_Ёжосотхорч шаг 6 Необходимо получить фразу.

Задание для соревнования может быть изменено до 30%.

Критерии оценки

№	Описание критерия	Баллы
1	Определение Алгоритма шифрования	5
2	Расшифровка хеш-суммы	10
3	Установка и настройка КриптоПРО	5
4	Установка КриптоАРМ	5
5	Установка и настройка КриптоПРО Browser plug-in	5
6	Настройка браузера для работы с центром сертификации	10
7	Создание сертификата	10
8	Установка сертификата через программу КритоПРО	5
9	Проверка сертификата в ПО КритоАРМ на действительность	10
10	Шифровка файла Shifr созданным сертификатом	5
11	Установка сертификата с закрытым ключом	5
12	Расшифровка файла shifr_1	10
13	Определение фразы (Шифр Цезаря)	10
14	Установка корневого сертификата	5
	Всего	100

- Баллы начисляются коллегией Экспертов согласно критериям оценки.
- Решение по начислению баллов принимается большинством голосов Экспертов. Главный эксперт не участвует в начислении баллов. В случае, равенства голосов Экспертов, решающий голос имеет Главный эксперт.
- При частичном выполнении задачи, коллегия Экспертов в праве начислить часть баллов, вплоть до десятых долей балла.
- При равном количестве баллов участник, закончивший работу раньше, в итоговом протоколе поднимается выше участника с равным количеством баллов, но потратившим на выполнение задания больше количество времени.
- Все спорные вопросы решаются коллегией Экспертов вместе с Главным экспертом. Главный эксперт имеет право вето.
- Любые решения, касаемые вопросов проведения чемпионата и оценки задания оформляются протоколом за подписью коллегии Экспертов.

3. Требования охраны труда и техники безопасности

Техника безопасности Общие требования безопасности

Настоящая инструкция распространяется на допущенных на площадку соревнований

лиц, эксплуатирующих средства вычислительной техники и сетевое оборудование. Инструкция содержит общие указания по безопасному применению электрооборудования площадки соревнований. Требования настоящей инструкции являются обязательными, отступления от нее не допускаются. К самостоятельной эксплуатации электроаппаратуры допускается только лица не моложе 18 лет.

Требования безопасности перед началом работы

Перед началом работы следует убедиться в исправности электропроводки, выключателей, штепсельных розеток, при помощи которых оборудование включается в сеть, наличии заземления компьютера, его работоспособности.

Требования безопасности во время работы

Для снижения или предотвращения влияния опасных и вредных факторов необходимо соблюдать Санитарные правила и нормы, гигиенические требования к видео-дисплейным терминалам, персональным электронно-вычислительным машинам и организации работы.

Во избежание повреждения изоляции проводов и возникновения коротких замыканий не разрешается: вешать что-либо на провода, закрашивать и белить шнуры и провода, закладывать провода и шнуры за газовые и водопроводные трубы, за батареи отопительной системы, выдергивать штепсельную вилку из розетки за шнур, усилие должно быть приложено к корпусу вилки.

Для исключения поражения электрическим током запрещается: часто включать и выключать компьютер без необходимости, прикасаться к экрану и к тыльной стороне блоков компьютера, работать на средствах вычислительной техники и сетевом оборудовании мокрыми руками, а также иметь на рабочем месте тару с водой или другой жидкостью, работать на средствах вычислительной техники и периферийном оборудовании, имеющих нарушения целостности корпуса, нарушения изоляции проводов, неисправную индикацию включения питания, с признаками электрического напряжения на корпусе, класть на средства вычислительной техники и периферийном оборудовании посторонние предметы.

Запрещается под напряжением очищать от пыли и загрязнения электрооборудование.

Запрещается проверять работоспособность электрооборудования в неприспособленных для эксплуатации помещениях с токопроводящими полами, сырых, не позволяющих заземлить доступные металлические части.

Недопустимо под напряжением проводить ремонт средств вычислительной техники и периферийного оборудования.

Ремонт электроаппаратуры производится только специалистами техниками с соблюдением необходимых технических требований.

Во избежание поражения электрическим током, при пользовании электроприборами нельзя касаться одновременно каких-либо трубопроводов, батарей отопления, металлических конструкций, соединенных с землей.

При пользовании электроэнергией в сырых помещениях соблюдать особую осторожность.

Требования безопасности по окончании работы

После окончания работы необходимо обесточить все средства вычислительной техники

и сетевое оборудование. В случае необходимости оставить включенными только оборудование, указанное экспертами.

Требования безопасности в аварийных ситуациях

При обнаружении неисправности немедленно обесточить электрооборудование, оповестить экспертов. Продолжение работы возможно только после устранения неисправности.

При обнаружении оборвавшегося провода необходимо немедленно сообщить об этом экспертам, принять меры по исключению контакта с ним людей. Прикосновение к проводу опасно для жизни.

Во всех случаях поражения человека электрическим током немедленно вызывают врача.

До прибытия врача нужно, не теряя времени, приступить к оказанию первой помощи пострадавшему.

Необходимо немедленно начать производить искусственное дыхание, наиболее эффективным из которых является метод «рот в рот» или «рот в нос», а также наружный массаж сердца.

Искусственное дыхание пораженному электрическим током производится вплоть до прибытия врача.

На рабочем месте запрещается иметь огнеопасные вещества.

В помещениях запрещается:

а) разжигать огонь;

б) включать электрооборудование, если в помещении пахнет газом;

в) курить;

г) сушить что-либо на отопительных приборах;

д) закрывать вентиляционные отверстия в электроаппаратуре.

Источниками воспламенения являются:

а) искра при разряде статического электричества;

б) искры от электрооборудования;

в) искры от удара и трения;

г) открытое пламя.

При возникновении пожароопасной ситуации или пожара персонал должен немедленно принять необходимые меры для его ликвидации, одновременно оповестить о пожаре администрацию.

Помещения с электрооборудованием должны быть оснащены огнетушителями.

4. Инфраструктурный лист

Список предоставляемых материалов

№	Название	Описание	Кол-во на человека	Примечание
1				
2	Бумага для лазерной печати	А4	50	1 пачка (500 листов) на всех
3	Ручка	синяя	1	гелиевая
4	Аптечка	типовая		1 на площадку
5	Огнетушитель	типовой		1 на площадку

Список объектов, установленных на площадке соревнований
Материальное оборудование

№	Назначение	Название	Описание	Кол-во
1	Оборудование для участников	стол	1400х700 мм	1 на участника
2		стул	офисный	1 на участника
3		ПК	Intel Core i5 или быстрее, 8GB RAM и более, 500GB HDD и более, ОС WINDOWS 8.1, Монитор 22 дюйма и более, мышь, клавиатура, доступ к точке доступа участника через wi-fi карту компьютера или сетевой кабель, подключение компьютеров к сети интернет	1 на участника
6		ИБП	Не менее 1000 VA	1 на 2^{x} участников
7		Удлинитель	220В, 2 метра, 6 розеток	1 на участника

Программные средства

№	Назначение	Название	Описание	Кол-во
7	Программное обеспечение	Windows 7	Утановленная для работы в VMware Workstation	
8		КриптоПро CSP 4.0)	Exe файл	на рабочем столе виртуальной машины

9		КриптоАРМ 5 Обновление 4.1	Exe файл	на рабочем столе виртуальной машины
10		КриптоПро ЭЦП Browser plug-in	Exe файл	на рабочем столе виртуальной машины
12		VMware Workstation 12.5 Player for Windows	установленная	на рабочем столе ПК участника

Оборудование для общего пользования

1	Оборудование экспертов и общего пользования	стол	1400x700 мм	4
2		стул	офисный	10
3		ПК	ПК или ноутбук экспертов	1
4		ИБП	Не менее 1000 VA	1
7		Принтер или МФУ	Лазерный, ч/б	1
8		Удлинитель	220В, 2 метра, 6 розеток	1

Резервное оборудование

№	Назначение	Название	Описание	Кол-во
1		ПК участника	типовое	1
5		Удлинитель	типовой	2