ВТОРОЙ НАЦИОНАЛЬНЫЙ ЧЕМПИОНАТ
«АБИЛИМПИКС-2017»

Компетенция «Информационная безопасность»

1. Описание компетенции

1.1. Актуальность компетенции

Интенсивное развитие средств связи и широкое внедрение информационных технологий во все сферы жизни делают все более актуальной проблему защиты информации. Насколько остро стоит проблема обеспечения безопасности информации говорит тот факт, что преступления в сфере передачи и обработки информации в ряде стран, по мнению специалистов, превратились в национальное бедствие. Проблема обеспечения безопасности передаваемой по каналам связи информации является комплексной и характеризуется способностью информации противостоять различного рода воздействиям, наносящим ущерб собственнику информации.

На сегодняшний день телекоммуникационные системы (ТС) обеспечивают эффективное выполнение бизнес-процессов как коммерческих, так и государственных предприятий. Вместе с тем повсеместное использование ТС для хранения, обработки и передачи информации приводит к повышению актуальности проблем, связанных с их защитой.

1.2. Требования к квалификации

Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.02 «Информационная безопасность телекоммуникационных систем» (утвержден приказом Министерства

образования и науки Российской Федерации от 13 августа 2010 г. № 1000) предъявляет ряд требований к данной специальности.

Техник по защите информации должен обладать профессиональными компетенциями, соответствующими видам деятельности:

- техническое обслуживание оборудования защищенных телекоммуникационных систем;
- применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем;
- участие в организации работ по обеспечению информационной безопасности телекоммуникационных систем.

2. Конкурсное задание

2.1. Цель

Задание было разработано с целью проверки следующих умений, установленных Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.02 «Информационная безопасность телекоммуникационных систем»:

- выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;
- производить установку и настройку типовых программно-аппаратных средств защиты информации;
- применять технические методы и средства защиты информации на выделенных объектах;
- решать частные технические задачи при аттестации объектов, помещений, технических средств;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации

2.2. Формат и структура Конкурсного задания

Конкурсное задание состоит из необходимости решения четырех отдельных задач:

Задача № 1 (15 мин.)

Исходя из анализа исходных данных определить класс защищенности государственной информационной системы в соответствии с приказом ФСТЭК России от 11 февраля 2013 года № 17.

Задача № 2 (15 мин.)

Оценив категории персональных данных и тип актуальных угроз определить необходимый уровень защищенности персональных данных при их обработке в информационной системе в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. N 1119.

Задача № 3 (15 мин.)

Установка программного обеспечения Secret Net, настройка подключения электронного замка «Secret Net Touch Memory Card» к Secret Net.

Задача № 4 (10 мин.)

Подготовка к работе, настройка и проведение поисковых работ с использованием измерителя спектра вторичных полей (детектора нелинейных переходов) NR-900 EMS.

2.3. Последовательность выполнения задания

Задача № 1

Исходные данные:

Информационная система ФГУП «Здравоохранение» функционирует на территории г. Москва и имеет сегменты в нескольких муниципальных образованиях и подведомственных организациях.

Обладателем информации экспертным методом было установлено, что в результате нарушения конфиденциальности информации возможны умеренные негативные последствия в финансовой и экономической областях деятельности организации.

Определить класс защищенности государственной информационной системы в соответствии с приказом ФСТЭК России от 11 февраля 2013 года № 17.

Решение:

Класс защищенности (К) = [уровень значимости информации; масштаб системы], где **УЗ** = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

1. Так как в результате нарушения одного из свойств безопасности информации (конфиденциальности) возможны умеренные негативные последствия в финансовой и экономической областях деятельности организации, то степень возможного ущерба определяется **средней**.

2. В случае, если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба, то информация имеет **средний** уровень значимости информации (**УЗ2**).

3. Информационная система имеет **региональный масштаб**, т.к. она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких подведомственных и иных организациях.

4. Исходя из анализа исходных данных и таблицы:

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3
УЗ 4	К3	К3	К4

класс защищенности информационной системы ФГУП «Здравоохранение» определен – К2.

Критерии оценки:

№	Критерий оценки	Баллы
1.	Знание порядка определения класса защищенности	5
2.	Умение анализировать исходные данные и формулировать выводы	5
3.	Правильность определения уровня значимости информации	5
4.	Правильность определения масштаба информационной системы	5
5.	Точность конечного результата	5

Задача № 2

Исходные данные:

В информационной системе ООО «Интерком» обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются для установления личности субъекта персональных данных.

Для информационной системы, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Определить необходимый уровень защищенности персональных данных при их обработке в информационной системе в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. N 1119.

Решение:

1. Т.к. в информационной системе ООО «Интерком» обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются для установления личности субъекта персональных данных, то данная информационная система является информационной системой, **обрабатывающей биометрические персональные данные.**

2. Если для информационной системы, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе, то для такой информационной системы **актуальны угрозы 2 типа**.

3. Согласно Постановления Правительства РФ от 1 ноября 2012 г. N 1119, с учетом анализа исходных данных информационной системы, если для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные, то **для информационной системы ООО «Интерком» устанавливается необходимость обеспечения 2-го уровня защищенности персональных данных.**

Критерии оценки:

№	Критерий оценки	Баллы
1.	Знание порядка определения необходимости обеспечения уровней защищенности персональных данных	5
2.	Умение анализировать исходные данные и формулировать выводы	5
3.	Правильность определения категории обрабатываемых персональных данных	5
4.	Правильность определения типа актуальных угроз	5
5.	Точность конечного результата	5

Задача № 3

Порядок выполнения

Установка клиента Secret Net.

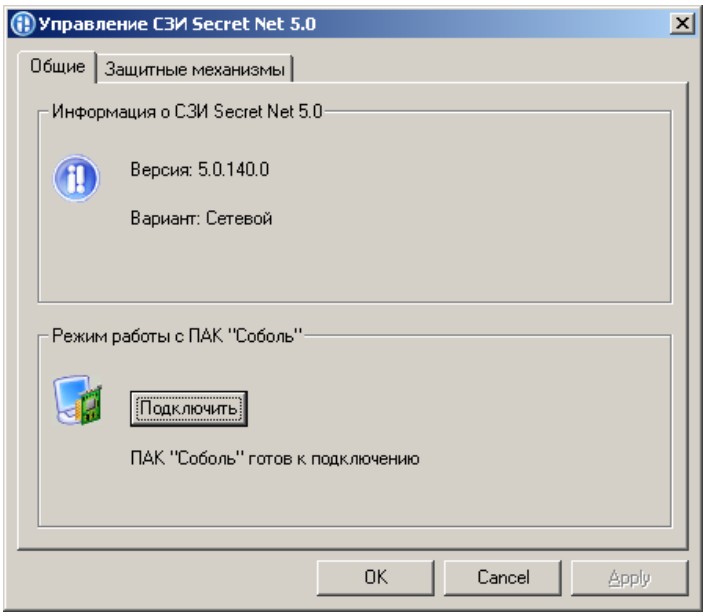
- Местоположение дистрибутивов сообщит преподаватель. Местоположение по умолчанию – S:\Secret Net\Setup

- Следует действовать с учетом особенностей, указанных ниже.

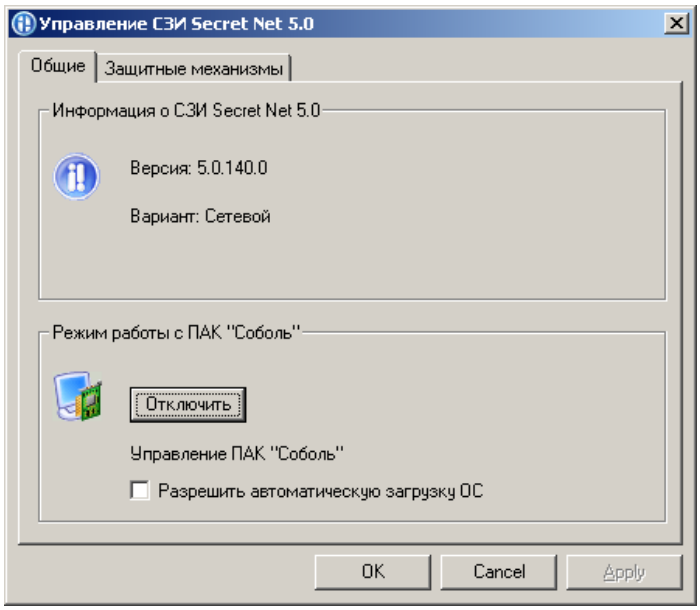
- Лицензионный номер сообщит преподаватель.

Настройка интеграции Secret Net с ЭЗ «Secret Net Touch Memory Card»

Настройка интеграции Secret Net с ЭЗ «Secret Net Touch Memory Card» осуществляется с помощью элемента управления «Управление СЗИ Secret Net», располагающегося в Панели управления:



Следует нажать на кнопку «Подключить». После этого диалог настроек примет следующий вид:



Автоматическая загрузка ОС, которую здесь можно установить, означает: после включения компьютера ЭЗ «Secret Net Touch Memory Card» отображает приглашение на предъявление персонального идентификатора, после чего, если в течение 30 секунд ожидания никто не предъявил идентификатор, происходит загрузка ОС от имени пользователя AUTOLOAD. Такой режим целесообразно устанавливать, если ЭЗ «Secret Net Touch Memory Card» и Secret Net установлены на сервере, работающем круглосуточно и допускающем возможность дистанционной перезагрузки.

1. Войти на компьютер от имени учетной записи Administrator Вашего компьютера

2. Подключить ЭЗ «Secret Net Touch Memory Card» к Secret Net

- Открыть в Панели управления элемент «Управление СЗИ Secret Net»
- Нажать на кнопку «Подключить». Дождаться завершения операции

Критерии оценки:

№	Критерий оценки	Баллы
1.	Знание теоретических основ применения СЗИ «Secret Net»	7
2.	Навыки по выполнению основных операций в ОС	5
3.	Правильность установки программного обеспечения Secret Net	5
4.	Точность настройки подключения электронного замка «Secret Net Touch Memory Card» к Secret Net.	5
5.	Возвращение настроек в исходное состояние	3

Задача № 4

Порядок выполнения:

а) Теоретическая часть

Измеритель спектра вторичных полей (детектор нелинейных переходов) “NR-900EMS” предназначен для поиска скрытно установленных технических средств съема информации, содержащих полупроводниковые компоненты.

К ним могут относиться:

радиомикрофоны; микрофонные усилители; проводные микрофоны; устройства, в которых для передачи информации и управления их работой используется инфракрасный или ультразвуковой диапазон; средства видео- и звукозаписи и др.

б) Подготовка к работе

1. Включить изделие, при этом установится режим «LISTEN»

2. Установить максимальную чувствительность приемников кнопкой «-» на пульте управления прибора.

3. Оценить помеховую обстановку на частотах приема, направляя антенную систему в разные стороны и подключая головные телефоны к выходам 2-й и 3-й гармоники приемника кнопкой «3/2».

При наличии помех кнопками «+»/ «-»

установить такое ослабление входного сигнала, чтобы сигнал помехи не прослушивался в головных телефонах.

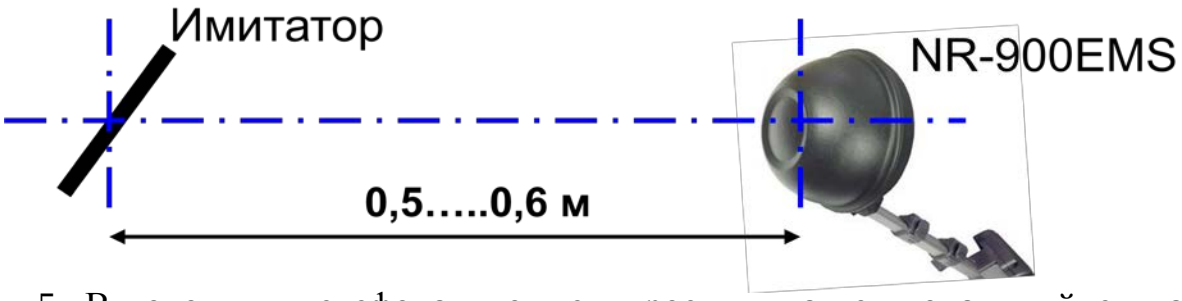
в) Проверка работоспособности

1. Повторно нажать на пульте управления кнопку включения (включить режим «300»).

2. Расположить штатный имитатор в свободном месте, где отсутствует какая-либо радиоэлектронная аппаратура.

3. Установить максимальную мощность передатчика Pmax с помощью кнопки «PWR» .

4. Направить антенную систему изделия в сторону имитатора с расстояния 0,5-0,6 м.



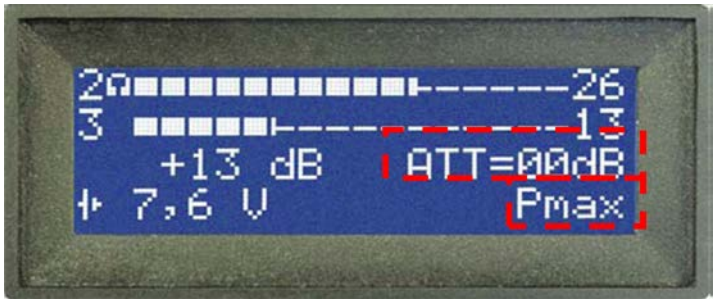
5. В головных телефонах должен прослушиваться тональный сигнал, а на экране ЖКИ - отображаться уровень 2-й и 3-й гармоник принимаемого сигнала.

6. Постепенное удаление имитатора из зоны облучения (при неизменном положении антенной системы прибора) должно приводить к снижению уровня звукового сигнала в головных телефонах и уменьшению уровня сигнала отображаемого на экране ЖКИ.

г) Проведение поисковых работ

Проведение поиска полупроводниковых элементов, осуществляется, по возможности, при максимальной выходной мощности передатчика и максимальной чувствительности приемника (Pmax и ATT = 00 dB).

Это обеспечивает наибольшую эффективность обнаружения объектов поиска.



Сравнивая значения уровней принимаемых сигналов на частотах 2-ой и 3-ей гармоник зондирующего сигнала и оценивая их соотношение можно сделать вывод о типе обнаруженного объекта.

Существенное превышение сигнала **2-ой** гармоники с высокой степенью вероятности говорит о наличии в зоне облучения **изделия с полупроводниковыми элементами промышленного производства.**

В противном случае наиболее вероятно, что источником сигнала-отклика является **коррозийный нелинейный отражатель.**

Критерии оценки:

№	Критерий оценки	Баллы
1.	Знание теоретических основ применения NR-900 EMS	5
2.	Правильность подготовки устройства к работе	5
3.	Правильность проверки работоспособности изделия	5
4.	Точность проведения поисковых работ	5
5.	Правильность определения обнаруженного элемента	5

3. Требования охраны труда и техники безопасности

1. Общее положения:

1.1 К работе в компьютерном классе допускаются лица, ознакомленные с данной инструкцией по технике безопасности и правилами поведения.

1.2 Работа учащихся в компьютерном классе разрешается только в присутствии преподавателя (инженера, лаборанта).

1.3 Во время занятий посторонние лица могут находиться в классе только с разрешения преподавателя.

1.4 Во время перемен между уроками проводится обязательное проветривание компьютерного кабинета с обязательным выходом учащихся из класса.

1.5 Помните, что каждый учащийся в ответе за состояние своего рабочего места и сохранность размещенного на нем оборудования.

2. Перед началом работы необходимо:

2.1 Убедиться в отсутствии видимых повреждений на рабочем месте.

2.2 Разместить на столе тетради, учебные пособия так, что бы они не мешали работе на компьютере.

2.3 Принять правильною рабочую позу (п. 5 данной инструкции).

2.4 Посмотреть на индикатор монитора и системного блока и определить, включён или выключен компьютер. Переместите мышь, если компьютер находится в энергосберегающем состоянии, или включить монитор и системный блок, если он был выключен.

3. При работе в компьютерном классе категорически запрещается:

3.1 Находиться в классе в верхней одежде.

3.2 Класть одежду и сумки на столы.

3.3 Находиться в классе с напитками и едой.

3.4 Работать за компьютером с грязными или мокрыми руками.

3.5 Располагаться сбоку или сзади от включенного монитора.

3.6 Присоединять или отсоединять кабели, трогать разъемы, провода и розетки.

3.7 Передвигать компьютеры и мониторы.

3.8 Открывать системный блок.

3.9 Включать и выключать компьютеры самостоятельно.

3.10 Пытаться самостоятельно устранять неисправности в работе аппаратуры.

3.11 Перекрывать вентиляционные отверстия на системном блоке и мониторе.

3.12 Ударять по клавиатуре, нажимать бесцельно на клавиши.

3.13 Класть книги, тетради и другие вещи на клавиатуру, монитор и системный блок.

3.14 Удалять и перемещать чужие файлы.

3.15 Приносить и запускать компьютерные игры.

4. Находясь в компьютерном классе, учащиеся обязаны:

4.1 Соблюдать тишину и порядок.

4.2 Выполнять требования преподавателя и лаборанта.

4.3 Находясь в сети работать только под своим именем и паролем.

4.4 Соблюдать режим работы.

4.5 При появлении рези в глазах, резком ухудшении видимости, невозможности сфокусировать взгляд или навести его на резкость, появления боли в пальцах и кистях рук, усиления сердцебиения немедленно покинуть рабочее место, сообщить о происшедшем преподавателю и обратиться к врачу.

4.6 После окончания работы завершить все активные программы и корректно выключить компьютер.

4.7 Оставить рабочее место чистым.

5. Работая за компьютером, необходимо соблюдать правила:

5.1 Расстояние от экрана до глаз – 70 – 80 см (расстояние вытянутой руки).

5.2 Вертикально прямая спина.

5.3 Плечи опущены и расслаблены.

5.4 Ноги на полу и не скрещены.

5.5 Локти, запястья и кисти рук на одном уровне.

5.6 Локтевые, тазобедренные, коленные, голеностопные суставы под прямым углом.

6. Требования безопасности в аварийных ситуациях:

6.1 При появлении программных ошибок или сбоях оборудования учащийся должен немедленно обратиться к преподавателю (лаборанту).

6.2 При появлении запаха гари, необычного звука немедленно прекратить работу, и сообщить преподавателю (лаборанту).

4. Инфрастркутурный лист

1. Персональный компьютер, клавиатура, мышь.
2. СЗИ «Secret Net»
3. Нелинейный радиолокатор NR 900-EMS
4. Стол, стул
5. Тетрадь для записи проводимых расчетов, ручка.