МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УДМУРТСКОЙ РЕСПУБЛИКИ

АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ УДМУРТСКОЙ РЕСПУБЛИКИ «ТЕХНИКУМ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ А.В. ВОСКРЕСЕНСКОГО»

СОГЛАСОВАНО:	УТВЕРЖДЕНО:
_____	Директор АПОУ УР «ТРИТ имени А.В. Воскресенского»
_____/_____/	_____Е.А. Кривоногова
«____»_____20___ г.	«___»_____ 20___ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

специальность 11.02.15 Инфокоммуникационные сети и системы связи
квалификации выпускника – специалист
Форма обучения - очная

20___ г

Фонд оценочных средств рассмотрен и одобрен на заседании методического объединения профессионального цикла
Председатель методического объединения профессионального цикла
_____ Ильина А. В.
Протокол № _____
от «___»_____ 20___г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 11.02.15 Инфокоммуникационные сети и системы связи
Выполнение работ по профессии "Монтажник оборудования связи"

УТВЕРЖДАЮ
Заместитель директора по УМР автономного профессионального образовательного учреждения Удмуртской Республики «Техникум радиоэлектроники и информационных технологий имени А.В. Воскресенского»

_____ /_____/
«____» _____ 20___ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

Разработчик: Масалёв В. Г. АПОУ УР «ТРИТ им. А.В. Воскресенского»

Общие положения

Результатом освоения профессионального модуля является готовность обучающегося к выполнению основного вида деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и составляющих его профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ОПОП в целом.

Формой промежуточной аттестации по профессиональному модулю является экзамен по модулю.

1 Формы аттестации

1.1 Текущий контроль

1.1.1 Задания на практических занятиях

Перечень тем практических занятий:

Практическое занятие №1 Установка прав доступа с помощью СПО ЗИ. Считывание прав доступа с помощью СПО ЗИ (например, РЕВИЗОР-1XP). Регистрация пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1XP)

Практическое занятие №2 Законодательство в сфере защиты информации

Практическое занятие №3 Разработка политики безопасности объекта**.**

Практическое занятие №4 Установка и снятие СЗИ с помощью программы СЗИ НСД (например, Страж NT) **.**

Практическое занятие №5 Исследование возможностей управления пользователями с помощью СЗИ НСД

Практическое занятие №6 Исследование настройки маркировки документов с помощью СЗИ НСД

Практическое занятие №7 Разработка инструкции по организации защиты данных пользователя

Практическое занятие №8 Организация процедуры экстренной модификации

Практическое занятие №9 Разработка плана защиты и обеспечения непрерывной работы автоматизированной системы

Практическое занятие №10 Разработка концепции информационной безопасности организации

Практическое занятие №11 Ввод информации в САПР СЗИ. Расчет радиуса контролируемой зоны с помощью САПР СЗИ

Практическое занятие №12 Исследование механизма доступа в систему с использованием СПО ЗИ и УП

Практическое занятие №13 Сравнение средств защиты информации от НСД

Практическое занятие №14 Разработка алгоритма генерации одноразовых паролей

Практическое занятие №15 Организация разграничения доступа к ресурсам системы

Практическое занятие №16 Исследование механизма контроля и регистрации с использованием СПО ЗИ и УП

Практическое занятие №17 Исследование проблемных ситуаций с использованием СПО ЗИ и УП

Практическое занятие №18 Сравнение типов межсетевых экранов

Практическое занятие №19 Проведение анализа трафика сайта

Практическое занятие №20 Сравнение средств анализа защищенности

Практическое занятие №21 Исследование возможностей многофункционального поискового прибора

Практическое занятие №22 Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга

Практическое занятие №23 Исследование возможностей работы фильтров сетевых помехоподавляющих

Практическое занятие №24 Исследование уязвимостей и построение модели угроз объекта защиты.

Практическое занятие №25 Исследование возможностей устройства для защиты объектов информатизации

Практическое занятие №26 Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств

Практическое занятие №27 Организация мер по комплексному обследованию защищенности информационной системы

Практическое занятие №28 Исследование возможностей системы оценки защищенности оптических линий связи.

Практическое занятие №29 Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН.

Практическое занятие №30 Исследование возможностей системы оценки защищенности выделенных помещений.

Практическое занятие №31 Исследование возможностей индикаторов поля

Практическое занятие №32 Поиск и локализация скрытых видеокамер

Практическое занятие 33 Исследование методов защиты сотовых телефонов от несанкционированного прослушивания

Практическое занятие №34 Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов

Практическое занятие №35 Поиск устройств негласного съема информации с помощью многофункционального поискового прибора

Практическое занятие №36 Исследование методов криптографической защиты информации

Практическое занятие №37 Исследование работы генератора шума по сети электропитания и линиям заземления

Практическое занятие №38 Поиск и обнаружение радиоизлучающих средств (например, с помощью комплекса КРОНА-ПРО)

Практическое занятие №39 Разработка инструкции по аттестации объектов информатизации

Методические указания по выполнению практических занятий оформлены в виде отдельного документа по профессиональному модулю.

Примерное задание.

Практическое занятие №4 Установка и снятие СЗИ с помощью программы СЗИ НСД. (4 часа)

Цель работы: Ознакомление с установкой и снятием СЗИ НСД **Страж NT 3.0** и их использования, закрепить знания по теме «Обеспечение безопасности информационных технологий**».**

Способствовать формированию соответствующих общих и профессиональных компетенций: ОК 01, ОК 02, ОК 03, ОК 04, ПК 3.1, ПК 3.2, ПК 3.3.

Средства для выполнения работы:

– аппаратные: ПК;

– ПМ.03. «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» МДК 03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи.

I. Подготовка к выполнению практической работы:

I. Изучение теоретического материала работы по МДК.03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи по теме: «Обеспечение безопасности информационных технологий»

II. Теоретическая часть

Назначение программы

Система защиты информации от несанкционированного доступа «Страж NT» (версия 3.0) представляет собой комплекс средств защиты информации в автоматизированных системах на базе персональных компьютеров.

СЗИ «Страж NT» предназначена для комплексной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах на базе персональных ЭВМ. СЗИ «Страж NT» может использоваться при разработке систем защиты информации для автоматизированных систем до классов защищенности 3А, 2А и 1Б включительно в соответствии с требованиями Руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», а также для создания информационных систем обработки персональных данных до 1 класса включительно.

Условия применения

СЗИ «Страж NT» может устанавливаться на автономных рабочих станциях, рабочих станциях в составе рабочей группы или домена, серверах, в том числе в составе кластера. СЗИ «Страж NT» может функционировать на одно- и многопроцессорных компьютерных системах под управлением операционных систем Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 и Windows Server 2008 R2. Компьютер, на котором устанавливается СЗИ «Страж NT», должен удовлетворять требованиям, необходимым для загрузки операционной системы.

В силу особенностей реализации защитных механизмов СЗИ «Страж NT» существуют дополнительные требования к аппаратному обеспечению компьютера:

– загрузочный жесткий диск должен иметь не менее 63 секторов перед началом первого раздела (32 256 байтов);

– при использовании USB-клавиатуры и USB-идентификаторов пользователей в некоторых случаях требуется наличие не менее 2 контроллеров USB;

– в случае применения в качестве идентификаторов пользователей USB флэш- накопителей в BIOS компьютера должна быть включена поддержка таких устройств.

Тип файловой системы на жестких дисках компьютера не имеет значения, это может быть FAT 16, FAT 32 или NTFS. Жесткий диск компьютера, на котором установлена операционная система, должен иметь свободное пространство объемом не менее 30 Мб.

Перед началом установки СЗИ «Страж NT» рекомендуется установить все системное и прикладное программное обеспечение, предусмотренное на данном рабочем месте. Установка дополнительного программного обеспечения в процессе функционирования СЗИ «Страж NT» является нежелательной.

Для установки, настройки и управления функционированием СЗИ «Страж NT» должен быть назначен администратор системы защиты. Пользователь, выполняющий функции администратора системы защиты, должен быть создан перед началом установки системы защиты стандартными средствами операционной системы. При установке системы защиты на локальный компьютер администратор системы защиты должен быть включен в группу локальных администраторов. В случае установки системы защиты на компьютер, входящий в домен, администратор системы защиты должен входить в группу локальных администраторов компьютера, а также в группу администраторов домена. Администратор системы защиты должен иметь одинаковое имя и пароль для входа на всех компьютерах, на которых планируется установка СЗИ «Страж NT».

Администратор системы защиты должен быть подготовленным пользователем, знающим принципы функционирования и имеющим навыки работы с операционной системой и СЗИ «Страж NT».

Механизмы системы защиты

В СЗИ «Страж NT» реализована смешанная разрешительно-запретительная модель защиты информации с жестким администрированием. Система защиты представляет собой совокупность следующих основных подсистем:

– идентификации и аутентификации;

– разграничения доступа;

– контроля потоков информации;

– управление запуском программ;
– управления защитой;
– регистрации событий;
– маркировки документов;
– контроля целостности;
– стирания памяти;
– учета носителей информации;
– преобразования информации на отчуждаемых носителях;
– контроля устройств;
– тестирования системы защиты.

Подсистема идентификации и аутентификации обеспечивает опознание пользователей при входе в компьютер по персональному идентификатору и подтверждение подлинности путем запроса с клавиатуры личного пароля. Данная подсистема также обеспечивает блокировку экрана компьютера и идентификацию пользователя после такой блокировки.

Подсистема разграничения доступа реализует дискреционный и мандатный принципы контроля доступа пользователей к защищаемым ресурсам. Функционирование данной подсистемы основано на присвоении защищаемым объектам атрибутов защиты.

К атрибутам защиты ресурса, имеющим отношение к разграничению доступа, относятся:
– идентификатор безопасности владельца ресурса;
– список контроля доступа;
– режим запуска (для исполняемых файлов);
– метка конфиденциальности (гриф для неисполняемого файла или допуск для исполняемого файла).

Дискреционный принцип основан на сопоставлении полномочий пользователей и списков контроля доступа ресурсов (логических дисков, папок, файлов, принтеров).

Мандатный принцип контроля доступа реализован путем сопоставления при запросе на доступ к ресурсу меток конфиденциальности пользователя, прикладной программы и защищаемого ресурса.

Подсистема контроля потоков информации предназначена для управления операциями над ресурсами, имеющими различные метки конфиденциальности.

Подсистема запуска программ предназначена для обеспечения целостности и замкнутости программной среды и реализована путем разрешения для исполняемых файлов режима запуска. Если режим запуска программы не разрешен, то файл не является исполняемым и не может быть запущен пользователем ни при каких условиях.

Подсистема управления защитой включает в себя следующие программы администрирования системы защиты:

Программа	Назначение
Установка и снятие системы защиты	Загрузка всех компонентов системы защиты информации, выполнение необходимых настроек в операционной системе, удаление всех компонентов при снятии системы защиты.
Настройка системы защиты	Установка параметров системы защиты информации, а также создание замкнутой программной среды, применение шаблонов настроек и другие сервисные функции.
Учет носителей	Настройка параметров работы системы защиты с носителями информации.
Менеджер пользователей	Управление пользователями системы защиты информации, их свойствами и персональными идентификаторами.
Менеджер файлов	Управление ресурсами, а также их защитными атрибутами.
Контроль устройств	Настройка правил работы системы защиты с устройствами компьютера.
Журнал событий	Работа с журналом событий системы защиты.
Редактор шаблонов настроек	Автоматизированное создание шаблонов настроек системы защиты.
Монитор системы защиты	Отображение состояния системы защиты, а также быстрый вызов функций управления системой защиты.

Подсистема регистрации обеспечивает регистрацию запросов на доступ к ресурсам компьютера и возможность выборочного ознакомления с регистрационной информацией и ее распечатки.

Подсистема маркировки документов обеспечивает автоматическое проставление учетных признаков в документах, выдаваемых на печать, а также регистрации фактов печати документов.

Подсистема контроля целостности предназначена для настройки и периодической проверки параметров целостности системы защиты, программного обеспечения и постоянных информационных массивов.

Подсистема стирания памяти реализует механизм заполнения нулями выделяемых программам областей оперативной памяти и стирания файлов на диске по команде удаления. В рамках данной подсистемы также реализовано стирание файла подкачки страниц по завершении сеанса работы.

Подсистема учета носителей информации позволяет управлять доступом к носителям информации в соответствии с разрешениями и параметрами, прописанными в журнале учета носителей.

Подсистема преобразования информации на отчуждаемых носителях позволяет включить дополнительную защиту для съемных носителей с помощью режима прозрачного преобразования всей информации на носителе.

Подсистема контроля устройств позволяет формировать необходимую конфигурацию устройств для пользователей в соответствии с установленными разрешениями.

Подсистема тестирования системы защиты предназначена для комплексного тестирования основных механизмов системы защиты, как на локальном компьютере, так и на удаленном, с использованием локальной вычислительной сети.

Подготовка к установке системы защиты

Перед установкой СЗИ «Страж NT» на компьютер следует провести ряд обязательных процедур:

1) проверить оперативную память компьютера, а также его жесткий диск на отсутствие вирусов;

2) убедиться в наличии на жестком диске свободного места, достаточного для установки и функционирования системы защиты;

3) убедиться, что на компьютере в данный момент не запущены какие-либо программы, препятствующие работе с системным реестром, выполняющие функции защиты от шпионского программного обеспечения и так далее.

4) убедиться в наличии исправного персонального идентификатора (в случае использования ГМД он должен быть отформатирован) и в возможности его чтения подсистемой идентификации

(см. раздел Тестирование подсистемы идентификации);

5) убедиться, что пароль пользователя, устанавливающего систему защиты, не содержит символов кириллицы и специальных знаков, а его длина не превышает 15 символов.

Тестирование подсистемы идентификации

Тестирование подсистемы идентификации предназначено для определения возможности чтения персональных идентификаторов в подсистеме идентификации до загрузки операционной системы. Тестирование подсистемы идентификации проводится до установки системы защиты информации.

Для запуска тестирования необходимо в BIOS Setup компьютера установить принудительную загрузку с носителя информации, на котором поставляется установочный комплект системы защиты. После появления диалога, приведенного на Рис. 1, необходимо предъявить необходимый персональный идентификатор.

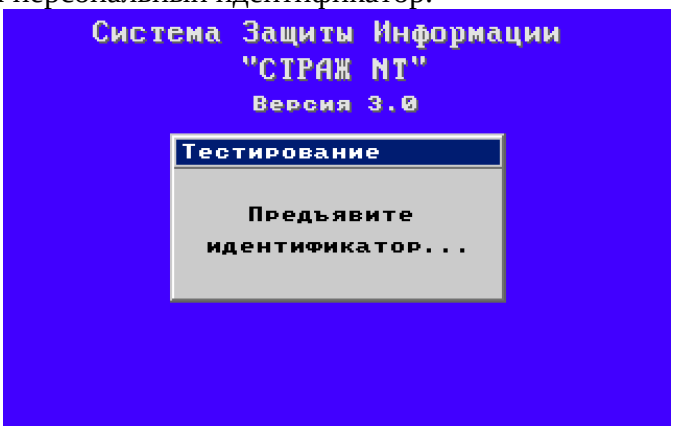


Рисунок 1 – Тестирование подсистемы идентификации

Тестирование считается успешным, если на экране появится сообщение, как на Рисунке 2.

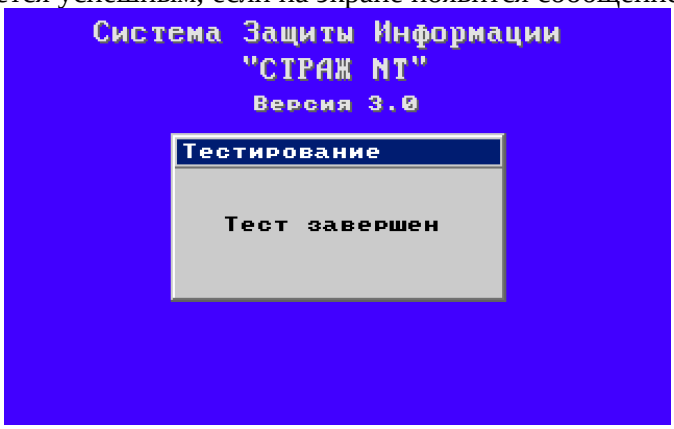
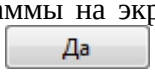


Рисунок 2 – Результат тестирования подсистемы идентификации

После появления сообщения о результатах тестирования следует перезагрузить компьютер.

Установка системы защиты

Для начала процесса установки СЗИ «Страж NT» необходимо установить компакт-диск в привод CD-ROM. При этом операционная система самостоятельно запустит **Мастер установки**. Если окно **Мастера установки** не появляется, необходимо запустить его самостоятельно, открыв в программе **Проводник** содержимое компакт-диска и запустив программу **GInstall.exe**. Если компьютер работает под управлением ОС старше MS Windows XP, и включен контроль учетных записей пользователей (UAC), при запуске программы на экране появится окно, как показано на Рис. 3. Для продолжения необходимо нажать кнопку 

.

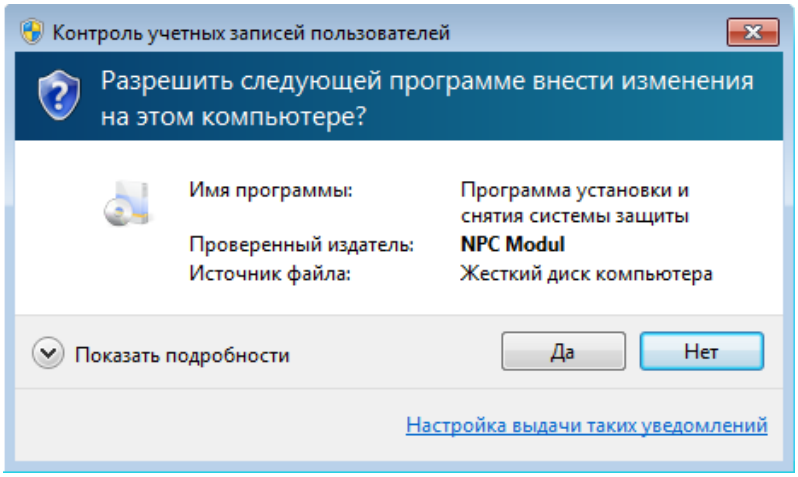


Рисунок 3 – Сообщение подсистемы контроля учетных записей пользователей

Если система защиты уже установлена на данном компьютере, **Мастер установки** проинформирует об этом и предложит снять систему защиты, иначе на экране появится окно, как показано на Рис. 4. Из **Мастера установки** можно выйти, нажав 

.

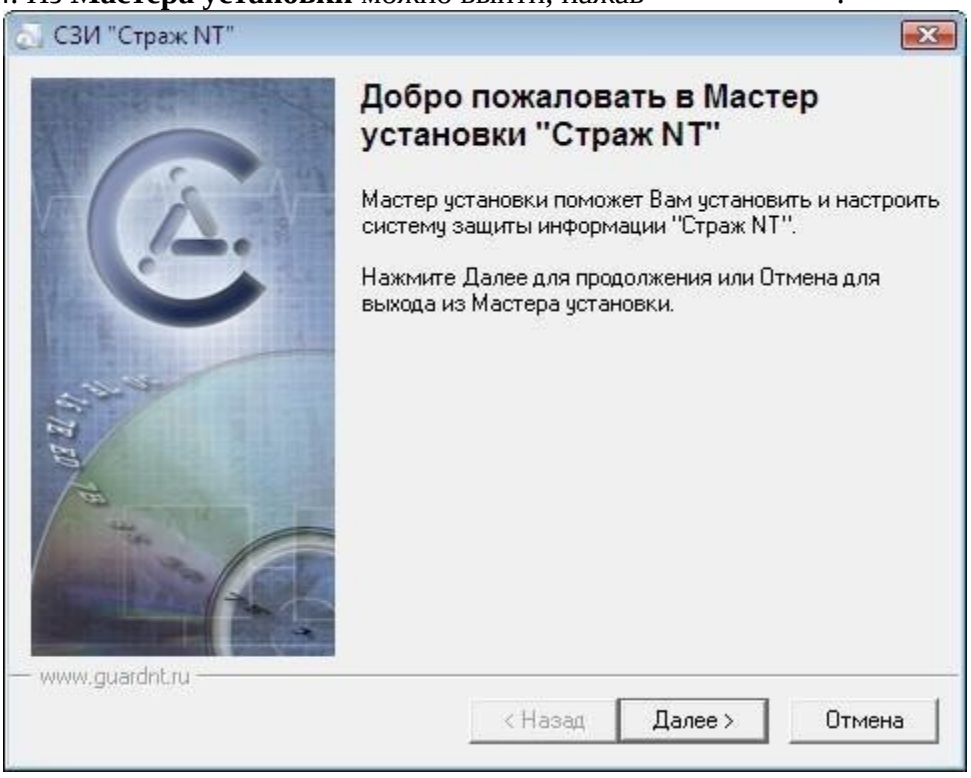


Рисунок 4 – Начальная страница Мастера установки

После нажатия кнопки 

на экране появится окно с текстом лицензионного соглашения (см. Рис. 5). Внимательно прочитайте его. Для продолжения установки системы защиты необходимо нажать кнопку **Я принимаю условия лицензионного соглашения**.

Задание

1. Изучить программное обеспечение Страж NT 3.0:
2. Видеоурок №1. Установка и снятие СЗИ

Контрольные вопросы

1. Назовите основные принципы построения защищенных КС.
2. Дайте краткую характеристику этапов создания КСЗИ.
3. В чем заключается сущность специальных методов неформального моделирования?
4. Поясните сущность методов декомпозиции и макромоделирование.
5. Выполните сравнительный анализ подходов к оценке эффективности КСЗИ.

Критерии оценивания:

Оценка «5» ставится, если обучающийся выполнил все задания верно.
Оценка «4» ставится, если обучающийся выполнил правильно не менее ¾ заданий.
Оценка «3» ставится за работу, в которой правильно выполнено не менее ½ заданий. Оценка «2» ставится за работу, в которой не выполнено более половины заданий.

1.1.2 Устный опрос

Примерные вопросы:

1. Актуальность проблемы обеспечения безопасности информационных технологий.
2. Место и роль информационных систем в управлении бизнес-процессами.
3. Основные причины обострения проблемы обеспечения безопасности информационных технологий.
4. Основные понятия в области безопасности информационных технологий.
5. Информация и информационные отношения.

Критерии оценивания:

Оценка «5» ставится, если обучающийся ответил на все вопросы верно.
Оценка «4» ставится, если обучающийся ответил на не менее ¾ вопросов верно.
Оценка «3» ставится, если обучающийся ответил на не менее ½ вопросов верно.
Оценка «2» ставится, если обучающийся ответил на менее ½ вопросов верно.

1.1.3 Письменный опрос

Примерные вопросы:

1. В этом виде мошенничества недобросовестный оператор конфигурирует свой коммутатор для осуществления международных вызовов через не подозревающего об этом оператора. "Благодаря" недостаткам в конфигурации коммутационного оборудования пострадавшая сторона даже не будет подозревать о том, что вызовы являются международными. В результате недобросовестный оператор выставляет клиенту счет за международное соединение, однако сам платит только за междугородный или местный вызов. С другой стороны, пострадавшему оператору приходится платить по международным тарифам, получая заметно меньшую плату от оператора-мошенника. Определите вид мошенничества?
2. При построении модели угроз безопасности часто возникают сложности с выявлением и указанием факторов риска, которые могут быть реализованы в ИС. Упростить работу возможно используя банк данных угроз безопасности информации ФСТЭК России. Где находится эта электронная база?
3. Так как любое СЗИ содержит некий программный код, то можно предположить, что он обладает функциональностью, способствующей организации успешных атак в отношении защищаемых объектов. Как называются такие возможности, не указанные в документации или описанные с искажением, использование которых может привести к нарушению ИБ?
4. Какой способ защиты информации предполагает такие преобразования информации, вследствие которых она становится недоступной для злоумышленников или такой доступ существенно затрудняется, а также комплекс мероприятий по уменьшению степени распознавания самого объекта?
5. Как называется способ защиты информации, при котором пользователи и персонал объекта внутренне (т.е. материальными, моральными, этическими, психологическими и другими

мотивами) побуждаются к соблюдению всех правил обработки информации?

6. К каким средствам защиты относятся различные электронные и электронно-механические и т.п. устройства, схемно- встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации?

7. Механизм, посредством которого в системе может осуществляться информационный поток (передача информации) между сущностями в обход политики разграничения доступа называется?

8. Деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации, называется?

9. Средства шифрования, в которых часть криптопреобразований осуществляется с использованием ручных операций или автоматизированных средств, предназначенных для выполнения таких операций.

10. Если криптографическое СЗИ противостоит атакам, при создании которых участвовали специалисты в области разработки и анализа указанных средств, в том числе научно-исследовательские центры, была возможность проведения лабораторных исследований средств защиты, то такое СЗИ соответствует классу?

Критерии оценивания:

Оценка «5» ставится, если обучающийся выполнил всё задание верно.

Оценка «4» ставится, если обучающийся выполнил правильно не менее ¾ задания.

Оценка «3» ставится за работу, в которой правильно выполнено не менее ½ задания.

Оценка «2» ставится за работу, в которой не выполнено более половины задания.

1.1.4 Тестирование:

Примерные вопросы для тестирования:

1. Какая проблема безопасности характерна при предоставлении всеобщего доступа к внутренним ресурсам типовой корпоративной сети?

1.возможность внешних атак на внутренние ресурсы +

2. размытие периметра сети

3. отсутствие шифрования внутренних ресурсов

2. Какие проблемы решает криптография с открытыми ключами?

1.возможность отказа от произведенных действий +

2. низкая стойкость криптографии с симметричными ключами

3. невысокая скорость шифрования криптографии с симметричными ключами

4. распределение ключей +

3. К какому методу работы антивирусных программ относится следующее описание: создается специальный модуль для каждого контролируемого объекта (например, методом контрольной суммы или электронной подписи), далее периодически вычисляется контрольная сумма или электронная подпись контролируемого объекта, которая сверяется с хранящейся отдельно первоначально вычисленной.

1.использование резидентного сторожа

2. вакцинация +

3. эвристический анализ

4. использование ревизора

4. Какого механизма оперативного реагирования на события не существует?

1. извещение администратора

2. запуск системы обнаружения атак +

3. подача сигнала тревоги

4. блокировка рабочей станции

5. Каковы основные требования к диспетчеру доступа?
1. шифрование наиболее важных операций
2. полнота контролируемых операций +
3. доступность
4. минимизация накладных расходов +

1.1.5 Доклад

Выступление с докладом по теме: «Перспективные направления развития средств комплексной защиты информации».

Требования к оформлению материалов.

Используемый текстовый редактор – Microsoft Word, размер страницы - А4, шрифт - Times New Roman, кегль шрифта - 14, интервал - однострочный, поля - по 2 см со всех сторон, абзацный отступ - 1 см. Графические материалы (рисунки, схемы, диаграммы) должны быть внедрены в основной текст.

Критерии оценки:

- **оценка «отлично»** выставляется обучающемуся, если доклад, содержание которого основано на глубоком и всестороннем знании темы, изученной литературы, изложен логично, аргументировано и в полном объеме. Основные понятия, выводы и обобщения сформулированы убедительно и доказательно;

- **оценка «хорошо»** оценивает доклад, основанный на твердом знании исследуемой темы. Возможны недостатки в систематизации или в обобщении материала, неточности в выводах. Студент твердо знает основные категории, умело применяет их для изложения материала;

- **оценка «удовлетворительно»** оценивает доклад, который базируется на знании основ предмета, но имеются значительные пробелы в изложении материала, затруднения в его изложении и систематизации, выводы слабо аргументированы, в содержании допущены теоретические ошибки;

- **оценка «неудовлетворительно»** оценивает доклад, в котором обнаружено неверное изложение основных вопросов темы, обобщений и выводов нет. Текст доклада целиком или в значительной части дословно переписан из первоисточника без ссылок на него.

1.2 Формы промежуточной аттестации по профессиональному модулю

Наименование междисциплинарных курсов, практик	Формы аттестации	
	Текущий контроль	Промежуточная аттестация (курс/семестр)
МДК 03.01 Защита информации в инфокоммуникационных системах и сетях связи МДК 03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи	– тестирование; – письменный опрос; – устный опрос; – оценка выступления с докладом; – оценка результатов выполнения практических работ; – экспертное наблюдение выполнения практических работ.	Дифференцированный зачет

УП 03.01 Учебная практика	оценка процесса и результатов выполнения видов работ учебной практики	Дифференцированный зачет
ПП 03.01 Производственная практика	оценка процесса и результатов выполнения видов работ производственной практики	Дифференцированный зачет

2.2.1 Тесты к промежуточной аттестации по дисциплине:

Дифференцированный зачет по МДК.03.01 проводится в форме тестирования. Тест содержит 100 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом),выбираемых случайным образом программой из каждого блока (первый блок 150 вопросов, второй блок 150 вопросов) заданий по 10 вопросов. Время тестирования – 4 академических часа.

Блок заданий закрытого типа Формируемые компетенции ПК.3.1		
1.	Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …	1.С одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой - ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды. 2.С одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на еѐ функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации. 3.Способна противостоять только информационным угрозам, как внешним так и внутренним. 4.Способна противостоять только внешним информационным угрозам.
2.	Информационная безопасность – это…	1.Состояние защищѐнности информационной среды. 2.Сохранность информационных ресурсов. 3.Защита конфиденциальности, целостности и доступности информации. 4.Все ответы не верны.
3.	Какие решения направлены на обеспечение информационной безопасности?	1.Высокопроизводительные системы защиты каналов. 2.Автоматизированные системы в защищенном исполнении. 3.Защита периметра информационной системы. 4.Все ответы верны.
4.	В качестве стандартной модели безопасности часто приводят модель из трёх категорий, каких?	1.Конфиденциальность. 2.Целостность. 3.Доступность. 4.Надежность.
5.	Какие существуют основные уровни обеспечения защиты информации?	1.Законодательный. 2.Организационно-административный. 3.Программно-технический (аппаратный). 4.Физический. 5.Вероятностный. 6.Распределительный.
Блок заданий закрытого типа Формируемые компетенции ПК.3.2		
1.	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?	1.Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования. 2.Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации. 3.Улучшить контроль за безопасностью этой информации. 4.Снизить уровень классификации этой информации.
2.	Какая категория является наиболее рискованной для компании с точки	1.Сотрудники. 2.Хакеры.

	зрения вероятного мошенничества и нарушения безопасности?	3.Атакующие. 4.Контрагенты (лица, работающие по договору).
3.	Что подразумевает принцип «разделение обязанностей»?	1.Для выполнения критических или необратимых операций требуется участие нескольких независимых пользователей. 2.Данный принцип требует создания механизма подотчётности пользователей, позволяющего отследить моменты нарушения целостности информации. 3.Порядок передачи привилегий должен полностью соответствовать организационной структуре предприятия.
4.	Что такое процедура?	1.Правила использования программного и аппаратного обеспечения в компании. 2.Пошаговая инструкция по выполнению задачи. 3.Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах. 4.Обязательные действия.
5.	Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?	1.Поддержка высшего руководства. 2.Эффективные защитные меры и методы их внедрение. 3.Актуальные и адекватные политики и процедуры безопасности. 4.Проведение тренингов по безопасности для всех сотрудников.
Блок заданий закрытого типа Формируемые компетенции ПК.3.3		
1.	Межсетевые экраны какого типа устанавливают на физическом периметре информационных систем?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
2.	Межсетевые экраны какого типа устанавливаются на логической границе информационных систем?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
3.	Межсетевые экраны какого типа предназначены для размещения на мобильных или стационарных узлах информационных систем?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
4.	Межсетевые экраны какого типа осуществляют разбор http(s)-трафика между веб-сервером и клиентом?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
5.	Межсетевые экраны какого типа работают с промышленными протоколами передачи данных?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»

Блок заданий открытого типа

Формируемые ПК.3.1

1.Преднамеренное указание неверных данных при заключении контракта или невыполнение абонентом контрактных условий оплаты, когда нарушитель с самого начала не планирует платить за услуги или же в какой-то момент времени отказывается от их отплаты называется?

2. Проникновение в компьютерную систему безопасности для удаления механизмов защиты или переконфигурирования системы с целью несанкционированного использования сети называется?

3. Неправомочное изготовление (клонирование) телефонных трубок или платежных телефонных карточек с фальшивыми идентификаторами абонентов, номеров и платежных отметок называется?

4.Неправомочное вмешательство в бизнес-процедуры (например, биллинг) с целью уменьшения оплаты услуг связи называется?

5. Для идентификации мошенничества важно определить его источники, от которых исходит угроза. Перечислите основные виды мошенничества?

Блок заданий открытого типа

Формируемые ПК.3.2

1.Перечислите основные уровни обеспечения защиты информации?

2.Режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду называется?

3.Защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах государственного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости называется?

4.Обязанность не разглашать того, что стало известно лицу в силу его профессиональной деятельности; сюда принадлежит тайна исповеди, врачебная, адвокатская, нотариальная, служебная (канцелярская), тайна совещаний присяжных заседателей называется?

5.Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации называется?

Блок заданий открытого типа

Формируемые ПК.3.3

1.Для каких целей используется физическая защита информации?

2. Какие задачи решаются при создании системы физической защиты?

3. Что такое периметр безопасности?

4. Какие средства, реализующие контроль за информацией, направленной в АС или исходящей из нее, выполняющие фильтрацию информации по заданным критериям, рассматриваются ФСТЭК в качестве СЗИ?

5.Какие средства автоматизируют процесс контроля событий в сети с проведением анализа этих событий с целью поисках признаков инцидента ИБ?

Критерии оценивания:

– оценка «отлично» выставляется обучающемуся, если процент результативности (в % выполнения) составляет 90–100%;

– оценка «хорошо» ставится в том случае, если верные ответы составляют 71–89% от общего количества;

– оценка «удовлетворительно» соответствует работа, содержащая 51–70% правильных ответов;

– оценка «неудовлетворительно» соответствует работа, содержащая менее 50% правильных ответов.

2 Результаты освоения модуля

2.1 Профессиональные и общие компетенции

В результате контроля и оценки по профессиональному модулю осуществляется комплексная проверка следующих общих, профессиональных и дополнительные компетенций:

Общие компетенции	Показатели оценки результата
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	-грамотность устной и письменной речи; - ясность формулирования и изложения мыслей
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	Эффективность выполнения правил ТБ вовремя учебных занятий, при прохождении учебной и производственной практик
ОК 09. Использовать информационные технологии	- эффективность использования

в профессиональной деятельности	информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.
Профессиональные компетенции	Показатели оценки результата
ПК 3.1 Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	- классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно; - анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный; - возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно; - мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме; - недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выявлены в полном объеме; - тестирование систем с целью определения уровня защищенности выполнено, уровень защищенности определен верно
ПК 3.2 Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи	- для обеспечения информационной безопасности выбраны оптимальные способы; - выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях

ПК 3.3 Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования	- мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными; - политика безопасности сетевых элементов и логических сетей разработана в полном объеме; - расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми стандартами; - установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи выполнена в соответствии с отраслевыми стандартами; - конфигурирование автоматизированных систем и информационно-коммуникационных сетей осуществлено в соответствии с политикой информационной безопасности и отраслевыми стандартами; - базы данных максимально защищены при помощи специализированных программных продуктов; - ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами

3.Промежуточная аттестация

3.1 Оценка освоения теоретического курса профессионального модуля

3.1.1 Задания к промежуточной аттестации по МДК.03.02

Список типовых практических заданий:

1. Выполните сканирование логических дисков с помощью СПО ЗИ (например, РЕВИЗОР-
2. Получите список пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1XP).
3. Создайте отчет на базе СПО ЗИ (например, РЕВИЗОР-1XP).
4. Установите права доступа с помощью СПО ЗИ.
5. Выполните считывание прав доступа с помощью СПО ЗИ (например, РЕВИЗОР-1XP).
6. Постройте модель угроз объекта защиты.
7. Разработайте комплексную систему инженерно-технической защиты информации на объекте.
8. Выполните поиск и локализацию скрытых видеокамер (например, с помощью прибора ОПТИК-2).
9. Проанализируйте методы защиты сотовых телефонов от несанкционированного прослушивания (например, с помощью изделия Ладья-ИВТ).
10. Продемонстрируйте на практике возможности системы оценки защищенности выделенных помещений.

Критерии оценки

Оценка «5» «отлично» - при ответе на теоретический вопрос обучающийся показывает полные и глубокие знания программного материала, логично и аргументировано отвечает на поставленный вопрос, а также дополнительные вопросы, показывает высокий уровень

теоретических знаний; обучающийся самостоятельно и правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия, ссылаясь на нормативно-правовую базу.

Оценка «4» «хорошо» - при ответе на теоретический вопрос обучающийся показывает глубокие знания программного материала, грамотно его излагает, достаточно полно отвечает на поставленный вопрос и дополнительные вопросы, умело формулирует выводы; в тоже время при ответе допускает несущественные погрешности; обучающийся самостоятельно и в основном правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия.

Оценка «3» «удовлетворительно» - при ответе на теоретический вопрос обучающийся показывает достаточные, но не глубокие знания программного материала; при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами; для получения правильного ответа требуется уточняющие вопросы; обучающийся в основном решает учебно-профессиональные задачи (задания), допускает несущественные ошибки, слабо аргументирует свое решение, используя в основном понятия.

Оценка «2» «неудовлетворительно» - при ответе на теоретический вопрос дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками; обучающийся не решил учебно-профессиональные задачи (задания).

3.1.2 Вопросы к промежуточной аттестации по МДК.03.02

Список вопросов:

1. Основные понятия информационной безопасности.
2. Сущность и понятия защиты информации.
3. Значение информационной безопасности и ее место в системе национальной безопасности.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.
6. Виды и источники угроз информационной безопасности Российской Федерации.
7. Доктрина информационной безопасности Российской Федерации.
8. Состояние информационной безопасности РФ и основные задачи по ее обеспечению.
9. Государственная система обеспечения информационной безопасности Российской Федерации.
10. Регуляторы в области информационной безопасности.
11. Основы криптографии.
12. Структура криптосистемы.
13. Основные методы криптографического преобразования данных.
14. Требования, предъявляемые к криптографическим системам.
15. Симметричные и ассиметричные криптосистемы.
16. Шифрование методом замены.
17. Шифрование методом перестановки.
18. Шифрование методом гаммирования.
19. Криптосистемы с открытым ключом.
20. Основы шифрования с открытым ключом.

Критерии оценки

Оценка «5» «отлично» - при ответе на теоретический вопрос обучающийся показывает полные и глубокие знания программного материала, логично и аргументировано отвечает на поставленный вопрос, а также дополнительные вопросы, показывает высокий уровень теоретических знаний; обучающийся самостоятельно и правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия, ссылаясь на нормативно-правовую базу.

Оценка «4» «хорошо» - при ответе на теоретический вопрос обучающийся показывает глубокие знания программного материала, грамотно его излагает, достаточно полно отвечает на поставленный вопрос и дополнительные вопросы, умело формулирует выводы; в тоже время при ответе допускает несущественные погрешности; обучающийся самостоятельно и в основном правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия.

Оценка «3» «удовлетворительно» - при ответе на теоретический вопрос обучающийся показывает достаточные, но не глубокие знания программного материала; при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами; для получения правильного ответа требуется уточняющие вопросы; обучающийся в основном решает учебно-профессиональные задачи (задания), допускает несущественные ошибки, слабо аргументирует свое решение, используя в основном понятия.

Оценка «2» «неудовлетворительно» - при ответе на теоретический вопрос дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками; обучающийся не решил учебно-профессиональные задачи (задания).

Требования к дифференцированному зачету по учебной и (или) производственной практике

Требования к дифференцированному зачету по учебной практике

Целью оценки по учебной практике является установление степени освоения практического опыта и умений.

Дифференцированный зачет по учебной практике выставляется на основании данных аттестационного листа (характеристики профессиональной деятельности обучающегося на практике) с указанием: видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика

Форма аттестационного листа

(характеристика профессиональной деятельности обучающегося во время учебной практики)

Аттестационный лист
по учебной практике ПМ 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем

1. _____
(Ф.И.О. студента)

2. АПОУ УР «ТРИТ имени А.В. Воскресенского»
(наименование учебного заведения)

11.02.15 Инфокоммуникационные сети и системы связи»
(специальность)

3. Место проведения практики _____
(наименование организации юридический адрес)

4. Сроки проведения практики _____

5. Количество часов ___72_____

6. Виды и объем работ, выполненных обучающимся во время учебной практики

№ п/п	Виды работ	Коды проверяемых результатов (ПК, ПО, У)	Объем работ (часы)	Качество выполненных работ (баллы)	
				Максимальное количество баллов	Результат

5.Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика_____
_____

«____»_____2025 г. Руководитель практики _____/_____

мп Ответственное лицо организации _____/_____

Критерии оценивания

Оценка по 5-балльной шкале	«5»	«4»	«3»	«2»
Оценка по 100-балльной шкале	91-100	81-90	71-80	Менее 70
Вербальная оценка	отлично	хорошо	удовлетвори тельно	Неудовлетворит ельно

Дифференцированный зачет по учебной практике считается сданным, если обучающийся набирает 71-100 баллов.

Требования к дифференцированному зачету по производственной практике

Целью оценки по производственной практике является установление степени освоения профессиональных и общих компетенций.

Дифференцированный зачет по производственной практике выставляется на основании данных аттестационного листа (характеристики профессиональной деятельности обучающегося на практике) с указанием: видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика.

Форма аттестационного листа

(характеристика профессиональной деятельности обучающегося во время производственной практики)

Аттестационный лист
по производственной практике ПМ 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем

1. _____
(Ф.И.О. студента)

2. _____АПОУ УР «ТРИТ им.А.В.Воскресенского»_____
(наименование учебного заведения)

_____11.02.15 Инфокоммуникационные сети и системы связи _____
(специальность)

3. Место проведения практики _____
(наименование организации юридический адрес)

_____

4. Сроки проведения практики с _____ по _____
_____

5. Количество часов _____108_____

6. Виды и объем работ, выполненных обучающимся во время производственной практики

№ п/п	Виды работ	Коды проверяемых результатов (ПК, ПО, У)	Объем работ (часы)	Качество выполненных работ (баллы)	
				Макси-мальное количество баллов	Результат

5. Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика_____
_____

«____»_____2025 г. Руководитель практики _____/_____

МП Ответственное лицо организации _____/_____

Критерии оценивания

Оценка по 5-балльной шкале	«5»	«4»	«3»	«2»
Оценка по 100-балльной шкале	91-100	81-90	71-80	Менее 70
Вербальная оценка	отлично	хорошо	удовлетвори тельно	Неудовлетворител ьно

Дифференцированный зачет по учебной практике считается сданным, если обучающийся набирает 71-100 баллов.

4 Промежуточная аттестация по модулю: контрольно-оценочные материалы для экзамена по модулю ПМ.03

Типовое профессионально-ориентированное задание для проведения экзамена

На объекте имеется Wi-fi точка доступа, подключиться к которой можно используя следующие параметры:

Имя сети: DE-2024

Ключ: de24-key

Для организации подключения отдельной группы пользователей к беспроводной сети необходимо установить WDS соединение (мост), используя вторую точку доступа.

При организации соединения необходимо использовать следующие обозначения:

SSID – Student#

Ключ - #key

Тип защиты сети - WPA2-PSK.

Служба DHCP должна быть

отключена. IP-адрес: 172.16.0.10#

Маска подсети: 255.255.0.0

Убедитесь в наличии подключения к сети Интернет.

Помимо роутера на объекте должен быть установлен IP камера видеонаблюдения.

Для настройки IP камеры:

Имя IP-камеры DVR#

IP-адрес: 172.16.0.11#

Маска подсети: 255.255.0.0

Шлюз: 172.16.0.1

Параметры видеопотока: Разрешение: 1024x768

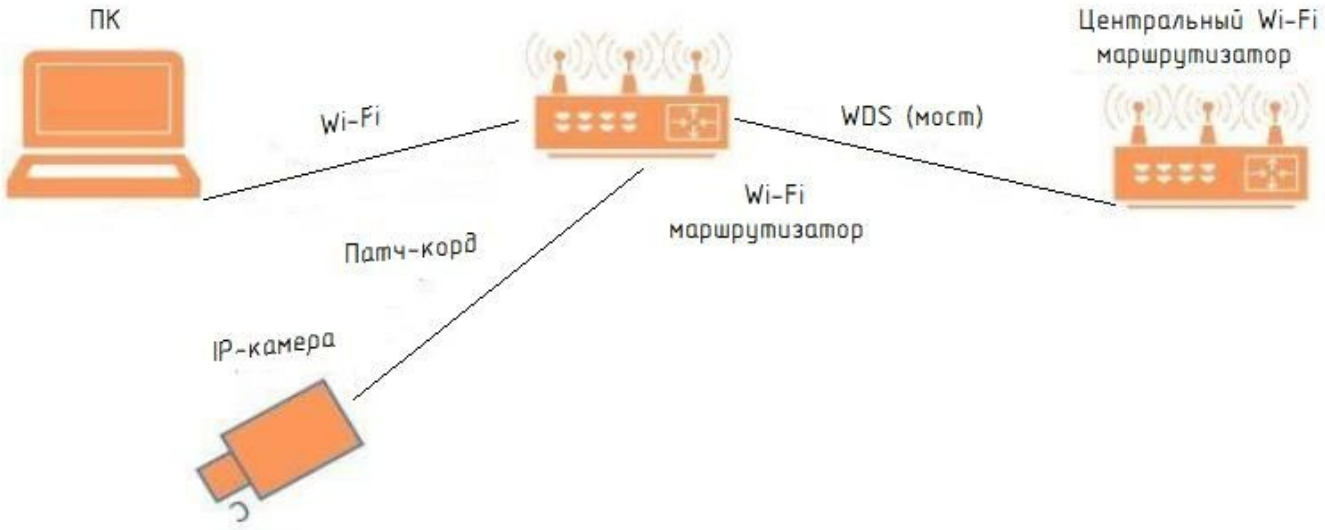
ПК должен быть подключен к созданной беспроводной сети.

Для подключения IP камеры необходимо изготовить патч-корд длиной 1 метр.

Трансляция видеопотока должна осуществляться на экране ПК, при помощи любого свободного программного обеспечения или WEB ресурса.

1. (# - номер рабочего места).

Схема организации подключения



Критерии оценки

Оценка «5» «отлично» - обучающийся самостоятельно и правильно решает учебно- профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия, ссылаясь на нормативно-правовую базу; обучающийся демонстрирует полные и глубокие знания программного материала, показывает высокий уровень теоретических знаний и практических умений.

Оценка «4» «хорошо» - обучающийся самостоятельно и в основном правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия; обучающийся показывает глубокие знания программного материала, грамотно его излагает, умело формулирует выводы; в тоже время при ответе допускает несущественные погрешности.

Оценка «3» «удовлетворительно» - обучающийся в основном решает учебно-профессиональные задачи (задания), допускает несущественные ошибки, слабо аргументирует свое решение, используя в основном понятия; обучающийся показывает достаточные, но не глубокие знания программного материала; при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами; для получения правильного ответа требуется уточняющие вопросы.

Оценка «2» «неудовлетворительно» - обучающийся не решил учебно-профессиональную задачу (задание); дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками.