

МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Авторы-составители: **Рихтер Татьяна Васильевна**

Рабочая программа дисциплины
БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ
Код УМК 102338

Утверждено
Протокол №1
от «25» февраля 2025 г.

Пермь, 2025

1. Наименование дисциплины

Безопасность компьютерных сетей

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в Блок « ПРОФ » образовательной программы по направлениям подготовки (специальностям):

Направление подготовки: **09.02.06** Сетевое и системное администрирование
направленность Эксплуатация объектов сетевой инфраструктуры

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Безопасность компьютерных сетей** у обучающегося должны быть сформированы следующие компетенции:

09.02.06 Сетевое и системное администрирование (направленность : Эксплуатация объектов сетевой инфраструктуры)

ОК.1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

ОК.2 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

ОК.3 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях

ОК.4 Эффективно взаимодействовать и работать в коллективе и команде

ОК.5 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

ОК.6 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

ОК.7 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

ОК.8 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности

ОК.9 Пользоваться профессиональной документацией на государственном и иностранном языках

ПК.1.1 Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации

ПК.1.2 Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем

ПК.1.3 Устранять неисправности в работе инфокоммуникационных систем

ПК.1.4 Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности

ПК.1.5 Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем

ПК.1.6 Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта

ПК.1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем

4. Объем и содержание дисциплины

Направление подготовки	09.02.06 Сетевое и системное администрирование (направленность: Эксплуатация объектов сетевой инфраструктуры) на базе среднего общего
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	5
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	84
Проведение лекционных занятий	42
Проведение практических занятий, семинаров	14
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	24
Формы текущего контроля	Входное тестирование (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (2)
Формы промежуточной аттестации	Дифференцированный зачет (5 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Актуальность информационной безопасности, понятия и определения. Угрозы информации. Вредоносные программы.

Особенностями современных информационных технологий, ущерб от современных компьютерных преступлений, классификация компьютерных преступлений, способы совершения компьютерных преступлений, причины уязвимости сети Интернет, виды угроз информационной безопасности РФ, удаленные атаки на интрасети, условия существования вредоносных программ, классические компьютерные вирусы, хакерские утилиты и прочие вредоносные программы.

Защита от компьютерных вирусов. Методы и средства защиты компьютерной информации. Криптографические методы информационной безопасности

Признаки заражения компьютера, источники компьютерных вирусов, антивирусные программы, методы обеспечения информационной безопасности РФ, задача средств ограничения доступа, биометрические технологии. методы и средства защиты информации от случайных воздействий, методы защиты информации от аварийных ситуаций, классификация методов криптографического закрытия информации, симметричные крипtosистемы, характеристики существующих шифров, крипtosистемы с открытым ключом (асимметричные).

Защита программ и данных. Особенности защиты в операционных системах. Особенности защиты информации в компьютерных сетях. Особенности защиты информации в СУБД.

Техническая защита от несанкционированного копирования, базовые методы нейтрализации систем защиты от несанкционированного копирования, идентификация жестких дисков, идентификация гибких дисков, классификация угроз безопасности операционной системы, классификация способов несанкционированного доступа и жизненный цикл атак, способы противодействия несанкционированному сетевому и межсетевому доступу, защита баз данных в MS ACCESS, доступ к SQL Server по коммутируемым каналам.

Лицензирование и сертификация в области защиты информации

Законодательство в области лицензирования и сертификации, правила функционирования системы лицензирования, критерии безопасности компьютерных систем.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

- конспекты лекций;
- литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);
- текст лекций на электронных носителях;
- ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;
- лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;
- методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 319 с. — (Высшее образование). — ISBN 978-5-534-20354-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. <https://urait.ru/bcode/558000>
2. Рабчевский, А. Н. Компьютерные сети и системы связи. Вводный курс : учебное пособие для среднего профессионального образования / А. Н. Рабчевский. — Москва : Издательство Юрайт, 2024. — 226 с. — (Профессиональное образование). — ISBN 978-5-534-19073-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. <https://urait.ru/bcode/555886>

Дополнительная:

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/452574>
2. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/453065>

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

www.iprbookshop.ru Электронная библиотечная система

elibrary.ru Научная электронная библиотека eLIBRARY.RU

window.edu.ru Информационная система «Единое окно доступа к образовательным ресурсам»

www.antiplagiat.ru Система Антиплагиат

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Безопасность компьютерных сетей** предполагает использование следующего программного обеспечения и информационных справочных систем: Используется офисный пакет приложений Microsoft Office. Студентам предоставлен доступ к сети Интернет и Единой телематической системе (ЕТИС) ФГБОУ ВО ПГНИУ (etis.psu.ru), ЭБС с помощью браузеров Google Chrome или Yandex.Browser, или Internet Explorer (Microsoft EDGE). Специального программного обеспечения не требуется.

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (student.psu.ru).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (<https://bigbluebutton.org/>).

система LMS Moodle (<http://e-learn.psu.ru/>), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтента, а также тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (<https://indigotech.ru/>).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для занятий лекционного типа - Кабинет математических дисциплин, оснащенный: проектор мультимедийный переносной, ноутбук переносной, экран переносной, доска меловая, учебная мебель (столы, стулья), чертежные инструменты, модели фигур (набор каркасных моделей многогранников, демонстрационные модели круглых тел), измерительные инструменты, интерактивная доска.

Для проведения занятий лабораторного типа требуется Лаборатория настройки сетевой инфраструктуры (ООО «Уралайтех»), со специализированным оборудованием и соответствующим программным обеспечением.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – Кабинет математических дисциплин, оснащенный: проектор мультимедийный переносной, ноутбук переносной, экран переносной, доска меловая, учебная мебель (столы, стулья), чертежные инструменты, модели фигур (набор каркасных моделей многогранников, демонстрационные модели круглых тел), измерительные инструменты, интерактивная доска.

Помещение библиотеки СГПИ филиал ПГНИУ для обеспечения самостоятельной работы обучающихся оснащено:

компьютерной техникой, с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ПГНИУ (ЕТИС (student.psu.ru)).

Библиотека оборудована: специализированной мебелью, меловой доской, проектором, экраном, компьютерами, ноутбуками, телевизором.

Все компьютеры, установленные в помещении библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;
Офисный пакет Libreoffice;
Kaspersky Endpoint Security for Business;
Справочно-правовая система «КонсультантПлюс»;
Яндекс.Браузер (свободно распространяемое ПО).

Фонды оценочных средств для аттестации по дисциплине
Безопасность компьютерных сетей

Планируемые результаты обучения по дисциплине для формирования компетенции и критерии их оценивания

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
OK.1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	Знать: методы и средства защиты компьютерной информации, криптографические методы информационной безопасности. Уметь: выбирать способы решения задач профессиональной деятельности применительно к различным контекстам. Владеть: специализированными средствами для борьбы с вирусами.	Неудовлетворительно Не знает: методы и средства защиты компьютерной информации, криптографические методы информационной безопасности. Не умеет: выбирать способы решения задач профессиональной деятельности применительно к различным контекстам. Не владеет специализированными средствами для борьбы с вирусами. Удовлетворительно Знает: методы и средства защиты компьютерной информации, криптографические методы информационной безопасности. В основном умеет: выбирать способы решения задач профессиональной деятельности применительно к различным контекстам. Частично владеет специализированными средствами для борьбы с вирусами. Хорошо Знает: методы и средства защиты компьютерной информации, криптографические методы информационной безопасности. Умеет: выбирать способы решения задач профессиональной деятельности применительно к различным контекстам. В основном владеет специализированными средствами для борьбы с вирусами. Отлично Знает: методы и средства защиты компьютерной информации, криптографические методы информационной безопасности. Умеет: выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Отлично</p> <p>Владеет специализированными средствами для борьбы с вирусами.</p>
OK.2 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	<p>Знать: основные понятия и определения, используемые при изучении информационной безопасности.</p> <p>Уметь: использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.</p> <p>Владеть навыками: установки и настройки антивирусных программ.</p>	<p style="text-align: center;">Неудовлетворительно</p> <p>Не знает: основные понятия и определения, используемые при изучении информационной безопасности. Не умеет: документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации.</p> <p>Не владеет навыками: установки и настройки антивирусных программ.</p> <p style="text-align: center;">Удовлетворительно</p> <p>Знает: основные понятия и определения, используемые при изучении информационной безопасности.</p> <p>В основном умеет: документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации.</p> <p>Частично владеет навыками: установки и настройки антивирусных программ.</p> <p style="text-align: center;">Хорошо</p> <p>Знает: основные понятия и определения, используемые при изучении информационной безопасности.</p> <p>Умеет: документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации.</p> <p>В основном владеет навыками: установки и настройки антивирусных программ.</p> <p style="text-align: center;">Отлично</p> <p>Знает: основные понятия и определения, используемые при изучении информационной безопасности.</p> <p>Умеет: документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации.</p> <p>Владеет навыками: установки и настройки антивирусных программ.</p>
OK.3 Планировать и	Знать: методы и способы решения профессиональных	<p style="text-align: center;">Неудовлетворительно</p> <p>Не знает: методы и способы решения</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	<p>задач в области обеспечения информационной безопасности компьютерных сетей.</p> <p>Уметь: планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях</p> <p>Владеть навыками: решения стандартных и нестандартных профессиональных задач в области обеспечения информационной безопасности компьютерных сетей.</p>	<p>Неудовлетворительно профессиональных задач в области обеспечения информационной безопасности компьютерных сетей.. Не умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. Не владеет навыками решения стандартных и нестандартных профессиональных задач в области обеспечения информационной безопасности компьютерных сетей.</p> <p>Удовлетворительно Знает: методы и способы решения профессиональных задач в области обеспечения информационной безопасности компьютерных сетей. В основном умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения Частично владеет навыками: решения стандартных и нестандартных профессиональных задач в области обеспечения информационной безопасности компьютерных сетей.</p> <p>Хорошо Знает: методы и способы решения профессиональных задач в области обеспечения информационной безопасности компьютерных сетей. Умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. В основном владеет навыками: решения</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Хорошо стандартных и нестандартных профессиональных задач в области обеспечения информационной безопасности компьютерных сетей.</p> <p style="text-align: center;">Отлично Знает: методы и способы решения профессиональных задач в области обеспечения информационной безопасности компьютерных сетей. Умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. Владеет навыками: решения стандартных и нестандартных профессиональных задач в области обеспечения информационной безопасности компьютерных сетей.</p> <p style="text-align: center;">.</p>
ОК.4 Эффективно взаимодействовать и работать в коллективе и команде	Знать: концепцию защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Уметь: эффективно взаимодействовать и работать в коллективе и команде. Владеть знаниями: в области норм и требований российского законодательства, предъявляемых к лицензированию и сертификации.	<p style="text-align: center;">Неудовлетворительно Не знает: концепцию защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Не умеет: эффективно взаимодействовать и работать в коллективе и команде. Не владеет знаниями: в области норм и требований российского законодательства, предъявляемых к лицензированию и сертификации.</p> <p style="text-align: center;">Удовлетворительно Знает: концепцию защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. В основном умеет: эффективно взаимодействовать и работать в коллективе и команде. Частично владеет знаниями: в области норм и требований российского законодательства,</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Удовлетворительно предъявляемых к лицензированию и сертификации.</p> <p>Хорошо Знает: концепцию защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Умеет: эффективно взаимодействовать и работать в коллективе и команде. В основном владеет знаниями: в области норм и требований российского законодательства, предъявляемых к лицензированию и сертификации.</p> <p>Отлично Знает: концепцию защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Умеет: эффективно взаимодействовать и работать в коллективе и команде. Владеет знаниями: в области норм и требований российского законодательства, предъявляемых к лицензированию и сертификации.</p>
ОК.5 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	Знать: особенности современных информационных технологий. Уметь: осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста. Владеть: основными понятиями в области информационной безопасности.	<p>Неудовлетворительно Не знает: особенности современных информационных технологий. Не умеет: осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста Не владеет основными понятиями в области информационной безопасности.</p> <p>Удовлетворительно Знает: особенности современных информационных технологий. В основном умеет: осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Удовлетворительно Частично владеет основными понятиями в области информационной безопасности.</p> <p>Хорошо Знает: особенности современных информационных технологий. Умеет: осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста. В основном владеет основными понятиями в области информационной безопасности.</p> <p>Отлично Знает: особенности современных информационных технологий. Умеет: осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста. Владеет основными понятиями в области информационной безопасности.</p>
ОК.6 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты анткоррупционного поведения	Знать нормы и требования российского законодательства в области лицензирования и сертификации, классификацию автоматизированных систем, согласно руководящим документам. Уметь: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты анткоррупционного поведения. Владеть навыками: оформления и получения лицензий и сертификатов в области информационной	<p>Неудовлетворительно Не знает: нормы и требования российского законодательства в области лицензирования и сертификации, классификацию автоматизированных систем, согласно руководящим документам.</p> <p>Не умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты анткоррупционного поведения. Не владеет навыками оформления и получения лицензий и сертификатов в области информационной безопасности.</p> <p>Удовлетворительно Знает: нормы и требования российского законодательства в области лицензирования и сертификации, классификацию</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
	безопасности.	<p>Удовлетворительно автоматизированных систем, согласно руководящим документам.</p> <p>В основном умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. Частично владеет навыками: оформления и получения лицензий и сертификатов в области информационной безопасности.</p> <p>Хорошо Знает: нормы и требования российского законодательства в области лицензирования и сертификации, классификацию автоматизированных систем, согласно руководящим документам. Умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. В основном владеет навыками: оформления и получения лицензий и сертификатов в области информационной безопасности.</p> <p>Отлично Знает: нормы и требования российского законодательства в области лицензирования и сертификации, классификацию автоматизированных систем, согласно руководящим документам. Умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. Владеет навыками: оформления и</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Отлично</p> <p>получения лицензий и сертификатов в области информационной безопасности.</p>
OK.7 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	<p>Знать: классификацию пользователей и злоумышленников в сети Интернет, причины уязвимости сети Интернет; основные понятия и определения, используемые при изучении информационной безопасности.</p> <p>Уметь: содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.</p> <p>Владеть навыками: установки и настройки антивирусных программ.</p>	<p style="text-align: center;">Неудовлетворительно</p> <p>Не знает: классификацию пользователей и злоумышленников в сети Интернет, причины уязвимости сети Интернет; основные понятия и определения, используемые при изучении информационной безопасности.</p> <p>Не умеет: содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.</p> <p>Не владеет навыками: установки и настройки антивирусных программ.</p> <p style="text-align: center;">Удовлетворительно</p> <p>Знает: классификацию пользователей и злоумышленников в сети Интернет, причины уязвимости сети Интернет; основные понятия и определения, используемые при изучении информационной безопасности.</p> <p>В основном умеет: содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.</p> <p>Частично владеет навыками: установки и настройки антивирусных программ.</p> <p style="text-align: center;">Хорошо</p> <p>Знает: классификацию пользователей и злоумышленников в сети Интернет, причины уязвимости сети Интернет; основные понятия и определения, используемые при изучении информационной безопасности.</p> <p>Умеет: содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.</p> <p>В основном владеет навыками: установки и</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Хорошо настройки антивирусных программ.</p> <p style="text-align: center;">Отлично Знает: классификацию пользователей и злоумышленников в сети Интернет, причины уязвимости сети Интернет; основные понятия и определения, используемые при изучении информационной безопасности. Умеет: содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях. Владеет навыками: установки и настройки антивирусных программ.</p>
ОК.8 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Знать: классификацию «компьютерных вирусов», и какую угрозу они представляют для безопасности информации. Уметь: использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. Владеть навыками: применения полученных профессиональных знаний.	<p style="text-align: center;">Неудовлетворительно Не знает: классификацию «компьютерных вирусов», и какую угрозу они представляют для безопасности информации Не умеет: использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. Не владеет навыками: применения полученных профессиональных знаний.</p> <p style="text-align: center;">Удовлетворительно Знает: классификацию «компьютерных вирусов», и какую угрозу они представляют для безопасности информации В основном умеет: использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности Частично владеет навыками: применения полученных профессиональных знаний.</p> <p style="text-align: center;">Хорошо Знает: классификацию «компьютерных вирусов», и какую угрозу они представляют для безопасности информации. Умеет: использовать средства физической</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Хорошо культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. В основном владеет навыками: применения полученных профессиональных знаний.</p> <p>Отлично Знает: классификацию «компьютерных вирусов», и какую угрозу они представляют для безопасности информации . Умеет: использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. Владеет навыками: применения полученных профессиональных знаний.</p>
OK.9 Пользоваться профессиональной документацией на государственном и иностранном языках	Знать: состав мероприятий по защите персональных данных. Уметь: пользоваться профессиональной документацией на государственном и иностранном языках. Владеть навыками: работы с информацией, используя возможности новых информационных технологий	<p>Неудовлетворительно Не знает: состав мероприятий по защите персональных данных. Не умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. Не владеет навыками работы с информацией, используя возможности новых информационных технологий.</p> <p>Удовлетворительно Знает: состав мероприятий по защите персональных данных. В основном умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения Частично владеет навыками: работы с информацией, используя возможности</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Удовлетворительно новых информационных технологий.</p> <p style="text-align: center;">Хорошо Знает: состав мероприятий по защите персональных данных.</p> <p style="text-align: center;">Умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. В основном владеет навыками: работы с информацией, используя возможности новых информационных технологий.</p> <p style="text-align: center;">Отлично Знает: состав мероприятий по защите персональных данных.</p> <p style="text-align: center;">Умеет: проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. Владеет навыками: работы с информацией, используя возможности новых информационных технологий.</p>
ПК.1.1 Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации	Знать: виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них, основные процедуры административного управления. Уметь: документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации. Владеть навыками: ведения отчетной и технической документации.	<p style="text-align: center;">Неудовлетворительно Не знает: виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них, основные процедуры административного управления. Не умеет: документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации. Не владеет навыками: ведения отчетной и технической документации.</p> <p style="text-align: center;">Удовлетворительно Знает: виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них, основные</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Удовлетворительно процедуры административного управления. В основном умеет: документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации. Частично владеет навыками: ведения отчетной и технической документации.</p> <p>Хорошо Знает: виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них, основные процедуры административного управления. Умеет: документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации. В основном владеет навыками: ведения отчетной и технической документации.</p> <p>Отлично Знает: виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них, основные процедуры административного управления. Умеет: документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации. Владеет навыками: ведения отчетной и технической документации.</p>
ПК.1.2 Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем	Знать: правила защиты от «компьютерных вирусов», определение аутентификации и разрешения. Уметь: поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем. Владеть навыками: ограничивать/разграничивать доступ к ресурсам Интернет, восстановления пораженных «компьютерными вирусами» объектов.	<p>Неудовлетворительно Не знает: правила защиты от «компьютерных вирусов», определение аутентификации и разрешения. Не умеет: устранять неисправности в работе инфокоммуникационных систем. Не владеет навыками: ограничивать/разграничивать доступ к ресурсам Интернет, восстановления пораженных «компьютерными вирусами» объектов.</p> <p>Удовлетворительно Знает: правила защиты от «компьютерных вирусов», определение аутентификации и разрешения. В основном умеет: устранять неисправности</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Удовлетворительно в работе инфокоммуникационных систем. Частично владеет навыками: ограничивать/разграничивать доступ к ресурсам Интернет, восстановления пораженных «компьютерными вирусами» объектов.</p> <p>Хорошо Знает: правила защиты от «компьютерных вирусов», определение аутентификации и разрешения. Умеет: устранять неисправности в работе инфокоммуникационных систем. В основном владеет навыками: ограничивать/разграничивать доступ к ресурсам Интернет, восстановления пораженных «компьютерными вирусами» объектов.</p> <p>Отлично Знает: правила защиты от «компьютерных вирусов», определение аутентификации и разрешения. Умеет: устранять неисправности в работе инфокоммуникационных систем. Владеет навыками: ограничивать/разграничивать доступ к ресурсам Интернет, восстановления пораженных «компьютерными вирусами» объектов.</p>
ПК.1.3 Устранять неисправности в работе инфокоммуникационных систем	Знать: виды нападений на политику безопасности, основные методы обеспечения безопасности. Уметь: устранять неисправности в работе инфокоммуникационных систем. Владеть навыками: применения программных средств для защиты программ и данных.	<p>Неудовлетворительно Не знает: виды нападений на политику безопасности, основные методы обеспечения безопасности. Не умеет: устранять неисправности в работе инфокоммуникационных систем. Не владеет навыками: применения программных средств для защиты программ и данных.</p> <p>Удовлетворительно Знает: виды нападений на политику безопасности, основные методы обеспечения безопасности. В основном умеет: устранять неисправности в работе инфокоммуникационных систем. Частично владеет навыками: применения программных средств для защиты программ</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Удовлетворительно и данных.</p> <p>Хорошо Знает: виды нападений на политику безопасности, основные методы обеспечения безопасности. Умеет: устранять неисправности в работе инфокоммуникационных систем. В основном владеет навыками: применения программных средств для защиты программ и данных.</p> <p>Отлично Знает: виды нападений на политику безопасности, основные методы обеспечения безопасности. Умеет: устранять неисправности в работе инфокоммуникационных систем. Владеет навыками: применения программных средств для защиты программ и данных.</p>
ПК.1.4 Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности	<p>Знать: классификацию «компьютерных вирусов», методы и средства защиты компьютерной информации.</p> <p>Уметь: проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.</p> <p>Владеть навыками: правильного выбора и использования антивирусной программы.</p>	<p>Неудовлетворительно Не знает: классификацию «компьютерных вирусов», методы и средства защиты компьютерной информации. Не умеет: устранять неисправности в работе инфокоммуникационных систем. Не владеет навыками: правильного выбора и использования антивирусной программы.</p> <p>Удовлетворительно Знает: классификацию «компьютерных вирусов», методы и средства защиты компьютерной информации. В основном умеет: устранять неисправности в работе инфокоммуникационных систем. Частично владеет навыками: правильного выбора и использования антивирусной программы.</p> <p>Хорошо Знает: классификацию «компьютерных вирусов», методы и средства защиты компьютерной информации. Умеет: устранять неисправности в работе инфокоммуникационных систем. В основном владеет навыками: правильного</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Хорошо выбора и использования антивирусной программы.</p> <p style="text-align: center;">Отлично Знает: классификацию «компьютерных вирусов», методы и средства защиты компьютерной информации. Умеет: устранять неисправности в работе инфокоммуникационных систем. Владеет навыками: правильного выбора и использования антивирусной программы.</p>
ПК.1.5 Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем	Знать: особенности защиты информации в компьютерных сетях. Уметь: осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем. Владеть навыками: настройки защищенного сетевого соединения, применения сканеров безопасности операционных систем.	<p style="text-align: center;">Неудовлетворительно Не знает: особенности защиты информации в компьютерных сетях. Не умеет: осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем. Не владеет навыками настройки защищенного сетевого соединения, применения сканеров безопасности операционных систем.</p> <p style="text-align: center;">Удовлетворительно Знает: особенности защиты информации в компьютерных сетях. В основном умеет: Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем. Частично владеет навыками: настройки защищенного сетевого соединения, применения сканеров безопасности операционных систем.</p> <p style="text-align: center;">Хорошо Знает: особенности защиты информации в компьютерных сетях. Умеет: осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем. В основном владеет навыками: настройки защищенного сетевого соединения, применения сканеров безопасности операционных систем.</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Отлично</p> <p>Знает: особенности защиты информации в компьютерных сетях. Умеет: осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем. Владеет навыками: настройки защищенного сетевого соединения, применения сканеров безопасности операционных систем.</p>
ПК.1.6 Одно из вариантов: 1. Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта 2. Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведения диагностики	<p>Знать: особенности защиты в операционных системах. Уметь: осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта. Владеть навыками: установки парольной защиты баз данных, администрирования базы данных.</p>	<p style="text-align: center;">Неудовлетворительно</p> <p>Не знает: особенности защиты в операционных системах. Не умеет: Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта. Не владеет навыками: установки парольной защиты баз данных, администрирования базы данных.</p> <p style="text-align: center;">Удовлетворительно</p> <p>Знает: особенности защиты в операционных системах. В основном умеет: осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта. Частично владеет навыками: установки парольной защиты баз данных, администрирования базы данных.</p> <p style="text-align: center;">Хорошо</p> <p>Знает: особенности защиты в операционных системах. Умеет: осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта. В основном владеет навыками: установки парольной защиты баз данных, администрирования базы данных.</p> <p style="text-align: center;">Отлично</p> <p>Знает: особенности защиты в операционных системах. Умеет: осуществлять инвентаризацию</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Отлично</p> <p>технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта. Владеет навыками: установки парольной защиты баз данных, администрирования базы данных.</p>
ПК.1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	<p>Знать: алгоритмы работы «компьютерных вирусов» и пути их внедрения в систему. Уметь: осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем. Владеть навыками: настройки программ, применения программных средств для защиты программ и данных.</p>	<p style="text-align: center;">Неудовлетворительно</p> <p>Не знает: алгоритмы работы «компьютерных вирусов» и пути их внедрения в систему. Не умеет: осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем Не владеет навыками: настройки программ, применения программных средств для защиты программ и данных.</p> <p style="text-align: center;">Удовлетворительно</p> <p>Знает: алгоритмы работы «компьютерных вирусов» и пути их внедрения в систему. В основном умеет: осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем. Частично владеет навыками: настройки программ, применения программных средств для защиты программ и данных.</p> <p style="text-align: center;">Хорошо</p> <p>Знает: алгоритмы работы «компьютерных вирусов» и пути их внедрения в систему. Умеет: осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем В основном владеет навыками: настройки программ, применения программных средств для защиты программ и данных.</p> <p style="text-align: center;">Отлично</p> <p>Знает: алгоритмы работы «компьютерных вирусов» и пути их внедрения в систему. Умеет: осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Отлично</p> <p>серверного оборудования инфокоммуникационных систем.</p> <p>Владеет навыками: настройки программ, применения программных средств для защиты программ и данных.</p>

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Дифференцированный зачет

Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.

Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100

«хорошо» - от 61 до 80

«удовлетворительно» - от 43 до 60

«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль OK.2 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности OK.5 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста OK.7 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях OK.8 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Актуальность информационной безопасности, понятия и определения. Угрозы информации. Вредоносные программы. Входное тестирование	Проведение входного тестирования Знать: особенности современных информационных технологий. Уметь: классифицировать компьютерные преступления. Владеть: информацией о национальных интересах РФ в информационной сфере и их обеспечение

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ОК.1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам</p> <p>ОК.2 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности</p> <p>ОК.5 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста</p> <p>ОК.7 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях</p> <p>ОК.8 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности</p> <p>ПК.1.2 Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем</p> <p>ПК.1.4 Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности</p> <p>ПК.1.7</p>	<p>Защита от компьютерных вирусов. Методы и средства защиты компьютерной информации. Криптографические методы информационной безопасности</p> <p>Письменное контрольное мероприятие</p>	<p>Знать: источники компьютерных вирусов, основные правила защиты, классификацию симметричных криптосистем. Уметь: устанавливать и настраивать антивирусные программы. Владеть: общими методами обеспечения информационной безопасности РФ.</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем		

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ОК.1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам</p> <p>ОК.2 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности</p> <p>ОК.5 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста</p> <p>ОК.7 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях</p> <p>ОК.8 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности</p> <p>ПК.1.1 Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации</p> <p>ПК.1.2 Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем</p> <p>ПК.1.3 Устранять неисправности в работе инфокоммуникационных</p>	<p>Защита программ и данных. Особенности защиты в операционных системах. Особенности защиты информации в компьютерных сетях. Особенности защиты информации в СУБД.</p> <p>Письменное контрольное мероприятие</p>	<p>Знать: алгоритм защиты документов в MS WORD, алгоритм защиты документов в MS EXCEL, современные средства защиты USB носителей, способы противодействия несанкционированному сетевому и межсетевому доступу. Уметь: аутентифицировать пользователя локальной сети, проводить идентификацию жестких и гибких дисков, осуществлять выбор модели безопасности MS SQL Server.</p> <p>Владеть: навыками защиты баз данных в MS ACCESS.</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>систем</p> <p>ПК.1.4 Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности</p> <p>ПК.1.5 Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем</p> <p>ПК.1.6 Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта</p> <p>ПК.1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем</p>		

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
OK.1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	Лицензирование и сертификация в области защиты информации Итоговое контрольное мероприятие	Знать: законодательство в области лицензирования и сертификации, критерии безопасности компьютерных систем Уметь: противодействовать возможным угрозами информационной безопасности. Владеть: навыками установки и настройки и эксплуатации антивирусных программ, информацией по лицензированию в области защиты информации.
OK.2 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности		
OK.3 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях		
OK.4 Эффективно взаимодействовать и работать в коллективе и команде		
OK.5 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста		
OK.6 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения		
OK.7 Содействовать сохранению окружающей среды.		

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях</p> <p>ОК.8</p> <p>Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности</p> <p>ОК.9</p> <p>Пользоваться профессиональной документацией на государственном и иностранном языках</p> <p>ПК.1.1</p> <p>Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации</p> <p>ПК.1.2</p> <p>Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем</p> <p>ПК.1.3</p> <p>Устранять неисправности в работе инфокоммуникационных систем</p> <p>ПК.1.4</p> <p>Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности</p> <p>ПК.1.5</p> <p>Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем</p> <p>ПК.1.6</p> <p>Осуществлять инвентаризацию технических средств сетевой</p>		

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
инфраструктуры, контроль оборудования после проведенного ремонта ПК.1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем		

Спецификация мероприятий текущего контроля

Актуальность информационной безопасности, понятия и определения.Угрозы информации.Вредоносные программы.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**

Проходной балл: **0**

Показатели оценивания	Баллы
Владеет информацией о национальных интересах РФ в информационной сфере и их обеспечение	4
Знает особенности современных информационных технологий.	3
Умеет классифицировать компьютерные преступления.	3

Защита от компьютерных вирусов.Методы и средства защиты компьютерной информации.Криптографические методы информационной безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

Показатели оценивания	Баллы
Знает источники компьютерных вирусов, основные правила защиты, классификацию симметричных крипtosистем.	10
Владеет общими методами обеспечения информационной безопасности РФ.	10
Умеет устанавливать и настраивать антивирусные программы.	10

Защита программ и данных.Особенности защиты в операционных системах.Особенности защиты информации в компьютерных сетях.Особенности защиты информации в СУБД.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знает алгоритм защиты документов в MS WORD, алгоритм защиты документов в MS EXCEL, современные средства защиты USB носителей, способы противодействия несанкционированному сетевому и межсетевому доступу.	10
Владеет навыками защиты баз данных в MS ACCESS.	10
Умеет аутентифицировать пользователя локальной сети, проводить идентификацию жестких и гибких дисков, осуществлять выбор модели безопасности MS SQL Server.	10

Лицензирование и сертификация в области защиты информации

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **17**

Показатели оценивания	Баллы
Умеет противодействовать возможным угрозам информационной безопасности.	15
Владеет навыками установки и настройки и эксплуатации антивирусных программ, информацией по лицензированию в области защиты информации.	15
Знает законодательство в области лицензирования и сертификации, критерии безопасности компьютерных систем	10